universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Geldwäsche und virtuelle Währungen"

verfasst von / submitted by

Marina Kindel, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2018/Vienna, 2018

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 914
Studienrichtung lt. Studienblatt: degree programme as it appears on the student record sheet:	Masterstudium Internationale Betriebswirtschaft
Betreut von / Supervisor:	o. Univ.-Prof. Dr. Dr. Arthur WEILINGER

Vorwort

Die Masterthesis zum Thema „Geldwäsche und virtuelle Währungen“ ist im Rahmen des Abschlusses meines Masterstudiums Internationale Betriebswirtschaftslehre an der Universität Wien entstanden.

Im Rahmen des Vorwortes möchte ich mich ganz herzlich bei meinem Betreuer Univ.-Prof. Dr. Dr. Arthur Weilinger für die Unterstützung, während der Erstellung meiner Arbeit, bedanken.

Ein ganz besonderer Dank gilt meiner Familie, ohne die ich mein Studium nicht realisieren hätte können und die mich während meines gesamten Studiums stets unterstützt haben.

Des Weiteren möchte ich mich für die Kooperationsbereitschaft von Max Tertinegg, Di, Geschäftsführer von Coinfinty; Mag. Matthias Reder, Leiter der Compliance und AML Abteilung von Coinfinty; Ing. Johannes Grill, Präsident von Bitcoin Austria; Mag. Lukas Leys MSc, Blockchain Consultant, Dr. Oliver Völkel, LL.M., Partner von Rechtsanwaltskanzlei Stadler Völkel ; Dr. Arthur Stadler, Partner der Rechtsanwaltskanzlei Stadler Völkel; Andreas Pfeil LL.M., Kanzlei Stadler Völkel; Mag.Weratschnig Thomas, Prävention von Geldwäscherei und Terrorismusfinanzierung der Finanzmarktaufsicht; MMag. Christopher Miess, BSc, Bakk.phil, BSc, MSc, CEO von ICONIC Capital sowie Mitglied des Fintech Advisory Board; Florian Wimmer, CEO Blockpit und Mag. Patrick Schreiner, MSc, Abteilung II/BK/7 Bundeskriminalamt; bedanken, die mir bei diesem hoch interessanten und vor allem ganz aktuellen Thema mit ihrem Know-How wichtigen Input für die Arbeit gegeben haben.

Abstract

Dezentral verwaltete Geldsysteme wurden entwickelt um zentral verwaltete zu ersetzen. Ein Pseudonym hat 2008 die erste virtuelle Währung erschaffen und somit einen bahnbrechenden Schritt in Richtung Substitution bestehender Geldsysteme bewirkt.
Obwohl es virtuelle Währungen bereits seit 10 Jahren gibt, befassen sich die gesetzgebenden Instanzen in Österreich erst seit wenigen Jahren mit diesen.
Auf Grund der technologisch komplexen Struktur virtueller Währungen gestaltet sich die Schaffung rechtlicher Rahmenbedingungen für solche Systeme als sehr schwierig. Mit neuen technologischen Innovationen gehen nicht immer nur positive, sondern auch negative Begleiterscheinungen einher. Einer dieser negativen Begleiterscheinungen stellt den Missbrauch virtueller Währungen für Zwecke von Geldwäsche und Terrorismusfinanzierung dar. Die Europäische Union hat aktuell Maßnahmen getroffen um diesen Entwicklungen entgegen zu wirken. Am 20. Mai 2018 wurde die 5. Geldwäscherichtlinie im Amtsblatt der Europäischen Union veröffentlicht die es bis zum 10. Jänner 2020 in das nationale Recht der einzelnen Mitgliedsstaaten umzusetzen gilt. Aktuell wurden diesbezüglich noch keine Bestimmungen getroffen. Die Zuständigkeit der Ressorts ist ungeklärt. Die Frage ist, ob es aus rechtlicher Sicht gelingen wird mit den technischen Entwicklungen Schritt halten zu können. Fast täglich entstehen neue virtuelle Währungen, Geschäftsmodelle sowie auf Blockchain-basierende technische Anwendungen, die gewisse Risiken in sich bergen. Eine schnelle Anpassungsfähigkeit von Seiten der Behörden ist unabdingbar, denn die Technologie ist nicht mehr aufzuhalten.

Abstract

Decentralized managed money systems have been developed to replace centrally managed ones. A pseudonym created the first virtual currency in 2008, thus taking a pioneering step towards the substitution of existing monetary systems.

Although there have been virtual currencies for 10 years, the legislative bodies in Austria have only been dealing with them for a short time.

Due to the technologically complex structure of virtual currencies, the creation of legal framework conditions for such systems is very difficult. New technological innovations are not always accompanied by positive but also negative side effects. One of these negative side effects is the misuse of virtual currencies for the purpose of money laundering and terrorist financing. The European Union has taken measures to counter these developments. On 20 May 2018, the 5th Money Laundering Directive was published in the Official Journal of the European Union, which is to be transposed into the national law of the individual member states by 20 January 2020. Currently no provisions have been made in this regard. The responsibility for the individual departments is unclear. However, the question is whether, from a legal perspective, it will be possible to keep pace with technological developments. Almost every day, new virtual currencies, business models and blockchain-based technical applications are created, which entail certain risks. A quick adaptability on the part of the authorities is essential, because the technology is unstoppable.

Inhaltsverzeichnis

Glossar

ABGB	Allgemein Bürgerliches Gesetzbuch
Abs	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
A-FIU	Austrian Financial Intelligence Unit
AGBG	Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen
AI	Artificial Intelligence
AML	Anti-Money-Laundering
AMLD	Anti-Money Laundering Directive
Art	Artikel
ASI	Austrian Standards Intenrtaional
ATM	Automated teller machine
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BATMs	Bitcoin-Automaten
BC	Blockchain
BK	Bundeskriminalamt
BKA-G	Bundeskriminalamt-Gesetz
BMDW	Bundesministerium für Digitalisierung und Wirtschaftsstandort
BMF	Bundesministerium für Finanzen
BMWFW	Bundesministerium für Wissenschaft, Forschung und Wirtschaft
BörseG	Börsengesetz
BTC	Bitcoin
BWG	Bankwesengesetz
Bzw.	Beziehungsweise
CEO	Chief Executive Office
CFT	Combating the Financing of Terrorism
CO	Compliance Officer
CR	Cryptocurrencies
CRR	Capital Requirements Regulation
C2C	Criminal to Criminal
DASH	Dash
DLT	Distributed Ledger Technologie
EG	Europäische Gemeinschaft
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
ESMA	European Securities and Markets Authority
EU	Europäische Union
EU-FIUS	EU Financial Intelligence Unit
EUR	Euro
EUV	Vertrag über die Europäischen Union
FATF	Financial Action Task Force
FIUs	Financial Intelligence Unit
FMA	Finanzmarktaufsicht
FM-GwG	Finanzmarkt Geldwäschegesetz

GewO	Gewerbeordnung
GwR	Geldwäscherichtlinie
G7	Gruppe der Sieben
ICO	Initial Coin Offering
ID	Identity document
II/BK/KWK	Kompetenzzentrum Wirtschaftskriminalität
insb	Insbesondere
iSd	Im Sinne des
iS	Im Sinne
ITO	Initial Token Offering
i.V.m.	In Verbindung mit
KAGB	Kapitalanlagegesetzbuch
KMG	Kapitalmarktgesetz
KYC	Know-Your-Customer
KWG	Kreditwesengesetz
Lit	Litera
MAR	Marktmissbrauchsverordnung
MICK	My Identity Check
MiFID II	Markets in Financial Instruments Directive II
OECD	Organization for Economic Cooperation and Development
OTC	Over the Counter
PaßG	Passgesetz
PEP	Politically exposed person
PoW	Proof-of-Work
P2P	Peer-to-peer
RingCT	Ring Confidential Transactions
RL	Richtlinie
SCC	Standard Compliance Code
SDS	Smart and Digital Service
SEPA	Single Euro Payments Area
SHA	Secure Hash Algorithm
SHA256	Secure Hash Algorithm 256
StGB	Strafgesetzbuch
STO	Security Token Offering
TOR	The Onion Router
UNODC	United Nations Office on Drugs and Crime Prevention
US	United States
VAG	Versicherungsaufsichtsgesetz
VO	Verordnung
VW	Virtuelle Währungen
WAG	Wertpapieraufsichtsgesetz
WiEReG	Wirtschaftliche Eigentümer Registergesetz
WKO	Wirtschaftskammer Österreich
XMR	Monero
ZaDiG	Zahlungsdienstgesetz
ZAG	Zahlungsdienstaufsichtsgesetz
ZEC	Zcash

1. Einleitung

Der exorbitante technologische Wandel in den vergangenen Jahrzehnten hat auf alle Bereiche der Gesellschaft und Wirtschaft massive Auswirkungen. Mit vielen positiven Effekten gehen jedoch auch negative einher, welche zwangsweise zur Anpassung der Gesetzgebung führen. Dies ist vor allem im Finanzsektor bemerkbar der in den vergangenen Jahren durch neue technologische Systeme einen sehr starken Wandel unterlegen ist. In diesem Zusammenhang ist ein besonderes Augenmerk auf virtuelle Währungen zu legen. Die Anfänge von virtuellen Währungen sind in die Cypherpunks-Szene der 80iger Jahre zurückzuführen, dessen Grundgedanke der Schutz der Privatsphäre des Users durch Verschlüsselungssysteme gegenüber Dritten, insbesondere Firmen und staatlichen Institutionen, war.[1]

Die erste und bekannteste virtuelle Währung ist die Kryptowährung „Bitcoin", dessen Idee auf der Basis von der 1998 erfundenen Währung „b-money" sowie auf dem Konzept von „bit gold" basiert. Der Bitcoin wurde erstmals 2008 in dem Whitepaper „Bitcoin: A Peer-to-Peer Electronic Cash System" von Satoshi Nakamoto, einem Pseudonym, vorgestellt. Im Jahr 2009 wurde das Bitcoin-Netzwerk in Betrieb genommen. Im Laufe der Jahre gewann dieses, durch Eigenschaften wie Anonymität und Schnelligkeit, zunehmend an Bedeutung.[2]

In den letzten Jahren haben sich hunderte neue virtuelle Währungen gebildet, die immer mehr Akzeptanz durch die breite Bevölkerung erfahren und eine ernstzunehmende Alternative bestehender Finanzsysteme darstellen. Bedingt durch die im Jahr 2008 entstanden Finanzkrise und den damit einhergehenden Verlust des Vertrauens in die Zentralbanken haben virtuellen Währungen Eingang in die Gesellschaft und Finanzwirtschaft erlangt. Virtuellen Währungen, allen voran Bitcoin, entstand aus dem Grundgedanken das exorbitant bestehende zentrierte Geldsystem der Notenbanken zu durchbrechen.[3] Der Terminus Kryptowährung entstand durch die Übersetzung der englischen Bezeichnung „Cryptocurrency", welche auf die kryptografische Verschlüsselung zurückzuführen ist. Bei Kryptowährungen erfolgt weder eine Aufsicht noch eine Kontrolle durch die Regierung oder zentrale Organe. Zudem liegt auch keine Deckung durch werthaltige Gegenstände vor. Die meisten virtuellen Währungen basieren auf Quellcodes, die öffentlich zugänglich und veränderbar sind. Man spricht von sogenannten Open Source Programmen. Die Erzeugung und Übertragung solcher Währungen erfolgt digital und dezentral in einem Computernetzwerk und werden durch eine Software, die

[1] *Meisser,* Kryptowährungen: Geschichte, Fuktionsweise, Potenzial https://www.mme.ch/fileadmin/files/documents/160520_luzius_meissner_-_bitcoin___crypto_currency_funktionsweise____entstehung_.pdf (2ff), (abgerufen am 14.07.2018).

[2] *Eberwein/ Steiner,* Bitcoins, (2014) 13.

[3] *Jilch,* Die Wurzeln von Bitcoin (Teil 2): Von der Donaumonarchie bis zur Blockchain, https://www.derbrutkasten.com/die-wurzeln-von-bitcoin-teil-2-von-der-donaumonarchie-bis-zur-blockchain, (abgerufen am 16.07.2018).

sich auf jeden Computer der Teilnehmer befindet, verwaltet. Anerkannte Zahlungsmittel werden im Gegensatz dazu von Zentralbanken erzeugt und über Banken den Wirtschaftskreislauf zugeführt.[4]

Entscheidungsträger in sämtlichen Bereichen der Politik und Wirtschaft müssen auf den Wandel und den damit eingehenden Veränderungen in den Sektoren reagieren. Eine wichtige Rolle nimmt die gesetzgebende Instanz ein, die aktuell rechtliche Rahmenbedingungen für virtuelle Währungen zu schaffen versucht.

1.1. Problemstellung und Forschungsfrage

Auf Grund der Eigenschaften und Komplexität der Technologie virtueller Währungen, gestaltet sich die Schaffung rechtlichen Rahmenbedingungen als sehr schwierig. Zudem muss, die stetige Weiterentwicklung und das immense Innovationspotenzial der Technologie berücksichtigt werden.

Am 30. Mai 2018 wurde die 5. Geldwäscherichtlinie[5] im Amtsblatt der Europäischen Union veröffentlicht die erstmals eine Definition virtueller Währungen beinhaltet. Ferner wurde der Geltungsbereich auf *„...Dienstleister, die virtuelle Währungen in Fiatgeld und umgekehrt tauschen*[6] und *„Anbieter elektronischer Geldbörsen ...*“[7] – sogenannte Wallet Provider – erweitert.[8]

Da es sich um eine Richtlinie und keine Verordnung, die unmittelbar und verbindlich Anwendung findet, handelt, müssen dessen Bestimmungen erst in das nationale Recht umgewandelt werden.[9] Ziel dieser Arbeit ist die Analyse der möglichen Umsetzung der Bestimmungen der 5. Geldwäscherichtlinie in Bezug auf virtuelle Währungen. Es soll geklärt werden wie der gesetzliche Status quo ist, welche unionsrechtlichen Vorgaben bestehen und welche Auswirkungen es auf die durch die 5. Geldwäscherichtlinie bestimmten Verpflichtenden haben wird. Ferner soll in diesem Zusammenhang ein Augenmerk auf den Terminus „Smart Regulation“ gelegt werden. Zudem muss geklärt werden in welchem Zusammenhang virtuelle Währungen und Geldwäsche stehen. Die in diesem Zusammenhang aufkommenden Begriffe müssen aus technischer Sicht ausreichend geklärt werden. Überdies muss geklärt werden ob die rechtlich geschaffenen Rahmenbedingungen mit den technischen

[4] *Kerscher*, Handbuch der digitalen Währungen, (2014) 16ff.
[5] RL 2018/843/EU des europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl L 2018/156, 43.
[6] RL 2018/843 ABl L 2018/156, 43.
[7] RL 2018/843 ABl L 2018/156, 43.
[8] RL 2018/843 ABl L 2018/156, 43.
[9] *Euopa.eu,* Verordnungen, Richtlinien und sonstige Rechtsakte https://europa.eu/european-union/eu-law/legal-acts_de (Stand 24.05.2018).

Eigenschaften virtuelle Währungen kompatibel sind.

1.2. Aufbau der Arbeit

Der erste Teil der Arbeit legt den Status Quo der Geldwäschebestimmungen auf europäischer und nationaler Ebene dar. Die Begriffe Geldwäsche und Terrorismusfinanzierung werden im Sinne der 4. Richtlinie voneinander abgegrenzt. Anschließend werden die Veränderung der 4. Geldwäscherichtlinie (4. GwR) zur 5. Geldwäscherichtlinie (5. GwR) analysiert. Es werden die Ziele und Anforderungen der Richtlinie für virtuelle Tauschbörsen und Wallet-Provider dargelegt. Die Termini „Wallet Provider", „Kryptobörsen" und „virtuelle Währungen" werden definiert. Darüber hinaus erfolgt eine Analyse der Definition von virtuellen Währungen, welche in der 5. Geldwäscherichtlinie vorzufinden ist. Es werden die Begriffe Know-Your-Customer (KYC), Anti-Money Laundering (AML) und Combating the Financing of Terrorism (CFT) erklärt, welche für die weiteren Analysen der Arbeit von Bedeutung sind. Es wird der Hintergrund der 5. Geldwäscherichtlinie bzw. das Aufkommen der Begriffe Distributed-Ledger-Technologie, Blockchain-Technologie und virtuelle Währungen in der Europäischen Union dargelegt. Die Einschätzung der EU-Organe, u.a. des Europäisches Parlaments, der Europäischen Kommission und vom Rat der Europäischen Union zu virtuellen Währungen soll dargelegt werden. Durch den ersten Teil der Arbeit soll der Status Quo, die unionsrechtlichen Vorgaben und die Veränderung für die „neuen Verpflichteten" gemäß der 5. GwR dargelegt werden. Zudem soll der Leser ein Verständnis für die Materie erlangen bevor im zweiten Teil der Arbeit eine Analyse der Möglichkeit der Unterstellung in bestehende Gesetze, speziell der Gewerbeordnung, für jene Dienstleister, die virtuelle Währungen in ein anerkanntes Zahlungsmittel und umgekehrt tauschen, erfolgt. Die Analyse erfolgt an Hand des österreichischen Unternehmens Coinfinity. Zudem wird kurz auf die mögliche Anwendbarkeit des Finanzmarkt-Geldwäschegesetzes eingegangen.

Der letzte Abschnitt der Arbeit umfasst die Analyse in welchem Zusammenhang virtuelle Währungen und Geldwäsche stehen. Es werden unterschiedliche Verschlüsselungstechnologien dargelegt, die aufzeigen, dass sich nicht jede virtuelle Währung im gleichen Maße für Geldwäscheaktivitäten eignet. Es werden die wichtigsten technischen Komponenten an Hand von Beispielen verschiedener virtueller Währungen erklärt. Des Weiteren erfolgt ein Einblick in ein weiteres neuartiges Finanzierungsmodell durch Initial Coin Offerings / Initial Token Offerings, basierend auf „Smart Contracts" und „Blockchain-Technologie". Es folgt eine Analyse darüber, welches potenzielle Risiko für Geldwäsche und Terrorismusfinanzierung hierbei besteht.

2. Status Quo

2.1. 4. Geldwäscherichtlinie auf Europäische Ebene

Die Richtlinie (EU) 2015/849 (4. Geldwäscherichtlinie) wurde am 5. Juni 2015 im Amtsblatt der Europäischen Union verlautbart und musste bis zum 26. Juni 2017 durch die Mitgliedstaaten umgesetzt werden. EU-Richtlinien sind im Gegensatz zu EU-Verordnungen nicht direkt anwendbar, sondern müssen erst in das nationale Recht des jeweiligen Mitgliedstaates umgesetzt werden. Des Weiteren gab es Ergänzungen zu den Richtlinien (EU) 2016/1675, (EU) 2018/105 und (EU) 2018/212 sowie durch die Verordnung (EG) Nr. 1889/2005.[10]

2.2. 4. Geldwäscherichtlinie auf nationaler Ebene

Aktuell sind die nationalen Umsetzungsbestimmungen der 4. Geldwäscherichtlinie (GwR) anwendbar. Die 4. GwR wurde in Österreich unter anderem durch das Finanzmarkt-Geldwäschegesetz (FM-GwG), Wirtschaftliche Eigentümer Registergesetz (WiEReG) und die Gewerbeordnung (GewO) umgesetzt. Zudem gibt es weitere Bestimmungen im Glückspielgesetz sowie in der Rechtsanwalts- und Notariatsordnung.[11] Das FM-GwG ist nur auf Kredit- und Finanzinstitute anzuwenden. Davon ausgenommen sind gemäß § 1 FM-GwG *„… die in anderen Mitgliedstaaten gelegenen Zweigstellen bzw. Zweigniederlassungen von Kredit- und Finanzinstituten mit Sitz im Inland.*“ § 2 Z 1 FM-GwG bestimmt den Begriff Kreditinstitut: *„Kreditinstitut: ein Kreditinstitut gemäß § 1 Abs. 1 BWG und ein CRR-Kreditinstitut gemäß § 9 BWG, das Tätigkeiten im Inland über eine Zweigstelle erbringt.“* Ein Finanzinstitut ist gemäß *§ 2 Z 2 FM-GwG ein:*

a) „Finanzinstitut gemäß § 1 Abs. 2 Z 1 bis 6 BWG;
b) ein Versicherungsunternehmen gemäß § 1 Abs. 1 Z 1 VAG 2016 und ein kleines Versicherungsunternehmen gemäß § 1 Abs. 1 Z 2 VAG 2016 jeweils im Rahmen des Betriebes der Lebensversicherung (Zweige 19 bis 22 gemäß Anlage A zum VAG 2016);
c) eine Wertpapierfirma gemäß § 3 Abs. 1 WAG 2018 und ein Wertpapierdienstleistungsunternehmen gemäß § 4 Abs. 1 WAG 2018;
d) einen AIFM gemäß § 1 Abs. 5 und § 4 Abs. 1 AIFMG und einen Nicht-EU-AIFM gemäß § 39 Abs. 3 AIFMG;

[10] *Bundesministerium Finanzen,* Geldwäscherei und Terrorismusfinanzierung, https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/geldwaesche.html, https://www.bmf.gv.at/finanzmarkt/register-wirtschaftlicher-eigentuemer/Uebersicht/Rechtliche-grundlagen.html (abgefragt am 6. Oktober 2018).
[11] *Bundesministerium Finanzen,* Geldwäscherei und Terrorismusfinanzierung, https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/geldwaesche.html, (abgefragt am 6. Oktober 2018).

e) ein E-Geldinstitut gemäß § 3 Abs. 2 E-Geldgesetz 2010;

f) ein Zahlungsinstitut gemäß § 10 ZaDiG 2018;

g) die Post hinsichtlich ihres Geldverkehrs;

h) Finanzinstitute gemäß Art. 3 Z 2 lit. a bis d der Richtlinie (EU) 2015/849 mit Sitz in einem anderen Mitgliedstaat mit dem über im Inland gelegene Zweigstellen bzw. Zweigniederlassungen ausgeübten Geschäftsbetrieb sowie im Inland gelegene Zweigstellen bzw. Zweigniederlassungen von solchen Finanzinstituten, die in Drittländern zugelassen sind."

Da Händler von virtuellen Währungen nicht unter die Begriffe der Finanz- und Kreditinstitute im Sinne des FM-GwG subsumierbar sind, ist das FM-GwG nicht anwendbar. Jedoch könnten die Händler von virtuellen Währungen von den geldwäscherechtlichen Bestimmungen der GewO umfasst sein. Die GewO gilt für alle (außer jene in §§ 2 bis 4 ausgenommen) gewerbsmäßig ausgeübten und nicht gesetzlich verbotenen Tätigkeiten (§ 1 (1) GewO). Somit sind Händler von Kryptowährungen davon umfasst. Die geldwäscherechtlichen Bestimmungen sind in § 365m ff GewO geregelt. Die Sorgfaltspflichten, also die Verpflichtungen zum Tätigwerden werden jedoch erst ab den Schwellenwerten von Euro 10.000/15.000 gemäß § 365m.1 Abs 2 Z 1 GewO / § 365o. Abs 2 Z 2 GewO oder bei Verdachtsmomenten schlagend.
Erst durch den Bitcoin Hype in den Jahren 2016/2017 und der damit verbundenen hohen Marktkapitalisierung wurde diesbezüglich ein geldwäscherechtlicher Regulierungsbedarf ausgelöst.[12]

2.3. Begriffsabgrenzung Geldwäsche und Terrorismusfinanzierung im Sinne der 4. Geldwäscherichtlinie

Das Ziel der Richtlinie (EU) 2015/849 *„... ist die Verhinderung der Nutzung des Finanzsystems der Union zum Zwecke der Geldwäsche und Terrorismusfinanzierung"*[13] Zudem muss auf der Begriff Geldwäsche, welcher im Art 1 Abs 3 der RL (EU) 2015/849 definiert wird, näher eingegangen werden. Grundsätzlich bedingt Geldwäsche Vorsatz. Gemäß § 7 Abs 1 Strafgesetzbuch (StGB) ist nur vorsätzliches Verhalten strafbar, es sei denn, dass gesetzlich verankert ist, dass Fahrlässigkeit ausreicht. In diesem Zusammenhang ist der Eventualvorsatz, der in § 5 Abs 1 StGB geregelt ist, zu berücksichtigen: *„Vorsätzlich handelt,*

[12] *Andreas Pfeil LL.M.* Interview geführt von Marina Kindel (4. Oktober 2018).
[13] Richtlinie 2015/849/EU des europäischen Parlamentes und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl L 2015/141, 73.

wer einen Sachverhalt verwirklichen will, der einem gesetzlichen Tatbild entspricht; dazu genügt es, daß der Täter diese Verwirklichung ernstlich für möglich hält und sich mit ihr abfindet." (§ 5 Abs 1 StGB). Vorsatz muss immer zum Zeitpunkt der Tathandlung und nicht zu einem späteren oder früheren Tatzeitpunkt gegeben sein. Vorsatz kann auf der einen Seite im Bewusstsein und auf der anderen Seite im Mitbewusstsein bestehen. Sämtliche objektiven Tatbestände müssen vorliegen.[14]

Fahrlässig handelt gemäß § 6 Abs 1 StGB, *„...wer die Sorgfalt außer acht läßt, zu der er nach den Umständen verpflichtet und nach seinen geistigen und körperlichen Verhältnissen befähigt ist und die ihm zuzumuten ist, und deshalb nicht erkennt, daß er einen Sachverhalt verwirklichen könne, der einem gesetzlichen Tatbild entspricht."* Paragraph 6 Abs 1 StGB hält somit die subjektiven Tatbestände fest. Gemäß § 4 Abs 2 StGB handelt jemand auch fahrlässig, wenn *„... er es für möglich hält, daß er einen solchen Sachverhalt verwirkliche, ihn aber nicht herbeiführen will."* Es liegt eine bewusste Fahrlässigkeit vor. Oftmals gestaltet sich die Abgrenzung zwischen Vorsatz und Fahrlässigkeit als sehr schwierig. Grundsätzlich ist anzumerken, je gefährlicher eine Situation ist, desto weniger ist von Fahrlässigkeit als von Vorsatz auszugehen. Der Ausschluss des Vorsatzes ist nicht gegeben, nur weil die Hoffnung besteht, dass der Erfolgseintritt ausbleiben wird. Grundsätzlich genügt bei einer strafbare Handlung Eventualvorsatz. Dennoch gibt es Tatbestände die Absicht oder Wissentlichkeit erfordern[15]: *„Der Täter handelt absichtlich, wenn es ihm darauf ankommt, den Umstand oder Erfolg zu verwirklichen, für den das Gesetz absichtliches Handeln voraussetzt* " (§ 5 Abs 2 StGB) *„ Der Täter handelt wissentlich, wenn er den Umstand oder Erfolg, für den das Gesetz Wissentlichkeit voraussetzt, nicht bloß für möglich hält, sondern sein Vorliegen oder Eintreten für gewiß hält"*(§ 5 Abs 3 StGB).[16]

Im Sinne der RL (EU) 2015/849 Art 1 Abs 3 lit a sind darunter folgende Handlungen zu verstehen*: „der Umtausch oder Transfer von Vermögensgegenständen in Kenntnis der Tatsache, dass diese Gegenstände aus einer kriminellen Tätigkeit stammen, zum Zwecke der Verheimlichung oder Verschleierung des illegalen Ursprungs der Vermögensgegenstände oder der Unterstützung oder der Unterstützung von Personen, die an einer solchen Tätigkeit beteiligt sind, damit diese den Rechtsfolgen ihrer Tat entgehen;..."*[17] Virtuelle Währungen sind als Vermögensgegenstand gemäß Art 3 Z. 3 RL 2015/849 der wie folgt lautet *„...Vermögenswerte aller Art, ob körperlich oder nichtkörperlich, beweglich oder unbeweglich, materiell oder immateriell, und Rechtstitel oder Urkunden in jeder –*

[14] *Maleczky,* Strafrecht Allgemeiner Teil[8],12ff.
[15] *Maleczky,* Strafrecht Allgemeiner Teil[8],12ff.
[16] *Maleczky,* Strafrecht Allgemeiner Teil[8],12ff.
[17] RL 2015/849 ABl L 2015/141, 73.

einschließlich elektronischer oder digitaler – Form, die das Eigentumsrecht oder Rechte an solchen Vermögenswerten belegen;" [18] zu deklarieren, womit diese in den Geltungsbereich des Art 1 der RL 2015/849 fallen.

Des Weiteren zählen gemäß Art 1 Abs 3 lit b RL 2015/849 die *„...Verheimlichung oder Verschleierung der wahren Natur, Herkunft, Lage, Verfügung oder Bewegung von Vermögensgegenständen oder von Rechten oder Eigentum an Vermögensgegenständen in Kenntnis der Tatsache, dass diese Eggenstände aus kriminellen Tätigkeiten oder aus einer Teilnahme an einer solcher stammen;"*[19] als Geldwäscheaktivitäten.

Gemäß Art 1 Abs 3 lit c RL 2015/849 ist unter Geldwäsche *„der Erwerb, der Besitz oder die Verwendung von Vermögensgegenständen, wenn dem Betreffenden bei der Übernahme dieser Vermögensgegenstände bekannt war, dass sie aus einer kriminellen Tätigkeit oder aus der Teilnahme an einer solchen Tätigkeit stammen*"[20] Auch nur die Beteiligung, Anstiftung oder Beratung zu den in Art 1 Abs 3 lit a-c RL 2015/849 gennannten Handlungen wird gemäß Art 1 Abs 3 lit d als Tatbestand der Geldwäsche verstanden. Der Tatbestand Geldwäsche ist auch dann gegeben, wenn die zugrundeliegende Straftat in einem anderen Mitgliedsstaat oder in einem Drittland begangen worden ist. Die Mitgliedstaaten müssen für die Untersagung von Terrorismusfinanzierung und Geldwäsche Sorge tragen.[21]

Unter Terrorismusfinanzierung im Sinne der RL (EU) 2015/849 Art 1 Abs 5 wird folgendes verstanden*: „ ... die Bereitstellung oder Sammlung finanzieller Mittel, gleichviel auf welche Weise, unmittelbar oder mittelbar, mit dem Vorsatz oder in Kenntnis dessen, dass sie ganz oder teilweise dazu verwendet werden, eine der Straftaten im Sinne der Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI des Rates zu begehen."*[22]

2.4. Geldwäscherichtlinie – Unionsrechtliche Ziele/Vorgaben

Der Vertrag über die Europäischen Union (EUV, ex EGV) regelt in § 5 die Subsidiarität der Europäischen Union: *„Nach dem Subsidiaritätsprinzip wird die Union in den Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, nur tätig, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen von den Mitgliedstaaten weder auf zentraler noch auf regionaler oder lokaler Ebene ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs oder ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind ...."* (§ 5 Abs 3 Vertrag über die europäische Union, Amtsblatt der Europäischen Union, C

[18] RL 2015/849 ABl L 2015/141, 73.
[19] RL 2015/849 ABl L 2015/141, 73.
[20] RL 2015/849 ABl L 2015/141, 73.
[21] RL 2015/849 ABl L 2015/141, 73.
[22] RL 2015/849 ABl L 2015/141, 73.

326/13 vom 26.10.2012). Die Begründung der Anwendbarkeit des Art 5 EUV in Zusammenhang mit Geldwäsche und Terrorismus beruht auf der Auffassung, dass Entscheidungen, die ausschließlich auf nationaler Ebene getroffen werden, zu massiven Beeinträchtigung und Schädigung des Binnenmarktes sowie der Reputation des Finanzsektors führen. Das organisierte Verbrechen weist einen grenzüberschreitenden Charakter auf, sodass fehlende unionsweite, zusammenhängende, konsequente und aufeinander abgestimmte Bestimmungen verheerende Folgen haben können. Zudem könnten Kriminelle, auf Grund fehlender einheitlicher Rahmenbedingungen, Nutzen daraus ziehen und dadurch andere Mitgliedsstaaten massiv in Mitleidenschaft ziehen.[23]

Ziel der vorgeschlagenen Änderungen der 4. GwR sind die Steigerung der Transparenz von Wirtschaftsteilnehmern und Transaktionen sowie der Schutz der Funktionsfähigkeit des Binnenmarktes, unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit sowie der Grundrechte und ökonomischen Freiheiten:[24] *„Die zuständigen Behörden sollen dadurch in der Lage sein, die Verwendung virtueller Währungen zu überwachen.“*[25]

In Bezugnahme auf virtuelle Währungen wird ausdrücklich erwähnt, dass der Grundsatz der Verhältnismäßigkeit in Bezug auf „Gatekeeper“ eingehalten werden muss. Unter „Gatekeeper“ sind Dienstleister, die den Zugang zu Kryptowährungen kontrollieren zu verstehen. Wallet-Provider sowie Kryptobörsen fallen unter diese Bezeichnung und werden im Sinne des Vorschlages[26] als Verpflichtete definiert. Der Grundgedanke dieser Bestimmung ist die Ermöglichung der Überprüfung bzw. Aufdeckung verdächtiger Transaktionen virtueller Währungen sowie die Identifikation der Personen die diese durchführen. Ferner wird die Fragmentierung pekuniärer Informationen durch die Bestimmung berücksichtigt. Die Informationen, die über Konsumenten solcher Dienste erhoben werden, müssen exorbitant präzise sein, um die Gefahr der Verwechslung mit anderen Personen ausschließen zu können. Die Erfassung, Verarbeitung und Speicherung der Daten müssen unter Berücksichtigung des Grundrechtes auf Schutz der Privatsphäre sowie personenbezogener Daten gemäß Art 7 und 8 der Charta, in denen u.a. geregelt wird, dass Daten nur für festgelegte Zwecke oder auf rechtlicher Grundlage verarbeitet werden dürfen, erfolgen.[27] Personenbezogene Daten *„... dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage*

[23] Vorschlag für eine Richtlinie DES EUOPÄISCHEN PALAMENTS UND RATES zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG, COM/2016/0450 final - 2016/0208 (COD); Charta der Grundrechte der Europäischen Union, ABl. C 2012/326, 391.
[24] ABl. C 2012/326, 391; COM/2016/0450 final - 2016/0208 (COD).
[25] *Barth/Durstberger*, 5. Geldwäsche-Richtlinie reguliert virtuelle Währungen, GesRZ 2018, 203.
[26] COM/2016/0450 final - 2016/0208 (COD).
[27] ABl. C 2012/326, 391;. COM/2016/0450 final - 2016/0208 (COD).

verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.“[28]

Es gilt die Identität natürlicher Personen sowie von[29] *„…wirtschaftlichen Eigentümer von juristischen Personen (Gesellschaften, Trusts und ähnlichen Rechtsvereinbarungen) …“*[30] zu klären und den damit verbundenen Grad des Risikos der Geldwäsche und Terrorismusfinanzierung zu bestimmen. Diese Informationen sind den Behörden zu übermitteln oder mit privaten Firmen derselben Sparte zu teilen[31]: *„Die der Öffentlichkeit zur Verfügung gestellten Daten sind streng beschränkt und beziehen sich nur auf wirtschaftliche Eigentümer in ihrer Eigenschaft als Wirtschaftsteilnehmer.“*[32] Gemäß des Vorschlages der 5. Geldwäscherichtlinie werden die Mitgliedsstaaten zur Veröffentlichung der Angaben verpflichtet um so zur Förderung der Prävention und Minimierung der Finanzkriminalität beizutragen. Die Identifizierung kann über elektronische Mechanismen erfolgen.

Die verlangten Veränderungen stützen sich einerseits auf die Grundlage von Berichten internationaler Organisationen sowie auf Konsultation der Interessenvertreter virtueller Währungen, die mittels Fragebogen u.a. die Marktstruktur, Nutzung und Regulation dieser dargelegt haben.[33]

Als eine internationale Arbeitsgruppe wurde die Financial Action Task Force (FATF) am G7 Gipfel in Paris 1989 innerhalb der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) als unabhängige Organisation zur Bekämpfung von Geldwäsche etabliert. Die FATF erstellt seit 1990 Empfehlungen, welche in vielen Mitgliedsländern als Grundlage für Gesetze dienen. So waren die Empfehlungen der FATF eine wesentliche Quelle für die innerhalb der Europäischen Union geltenden Geldwäscherichtlinien, insbesondere der 4. Geldwäscherichtlinie.[34]

Die Inhalte des Vorschlages zur Änderung der RL (EU) 2015/849 sollen zur Erreichung der Unionsziele: Gesamtsicherheit, Reduktion von kriminellen Aktivitäten, Einhaltung internationaler Standards und der Schaffung innovativer Finanzdienste, dienen.

Im Vorschlag wird zudem auf die Glaubwürdigkeit von virtuellen Währungen unter Bezugnahme der Anonymität eingegangen. Die Anonymität wird als Hindernis dargestellt, die es zu minimieren gilt, um einerseits das Potenzial der Technologie zu fördern und andererseits virtueller Währungsadressen an juristische/natürliche Personen zuordnen zu

[28] ABl. C 2012/326, 391.
[29] COM/2016/0450 final - 2016/0208 (COD).
[30] COM/2016/0450 final - 2016/0208 (COD).
[31] COM/2016/0450 final - 2016/0208 (COD).
[32] COM/2016/0450 final - 2016/0208 (COD).
[33] COM/2016/0450 final - 2016/0208 (COD).
[34] *Die Österreichischen Rechtsanwälte,* Verhinderung von Geldwäscherei und Terrorismusfinanzierung, https://www.ooerak.at/fileadmin/OOERAK/Downloads/Geldw%C3%A4sche_Leitfaden_April2017.pdf, (abgerufen am 3. September 2018).

können. Aus diesem Grund wurden Wallet-Provider und Umtauschplattformen als Verpflichtete iSd 5. GwR bestimmt. Durch die Bestimmung ist es jedoch möglich, die Anonymität nur zu einem gewissen Grad zu minimieren, da Transaktionen auch ohne derartige Plattformen durchgeführt werden können.[35] Im Kapitel 3.2.3. wird auf die unterschiedlichen Möglichkeiten virtuelle Währungen zu erwerben eingegangen. Zudem soll es den Usern möglich sein, freiwillige Selbsterklärungen abgeben zu können.[36]

[35] COM/2016/0450 final - 2016/0208 (COD).
[36] COM/2016/0450 final - 2016/0208 (COD).

3. Novellierung 4. Geldwäscherichtlinie

3.1. Definition von virtuellen Währungen und Wallet Providern

Artikel 2 der RL Richtlinie (EU) 2015/849 regelt wer im Sinne der RL als Verpflichtete gelten. Zum 5.6.2015 galten Kredit- und Finanzinstitute, juristische und natürliche Personen die eine berufliche Tätigkeit ausüben sowie Immobilienmakler, Glücksspielanbieter und Dienstleister für Trusts/Gesellschaften als Verpflichtete.[37] Zudem Personen *„... die mit Gütern handeln, soweit sie Zahlungen in Höhe von 10 000 EUR oder mehr in bar tätigen oder entgegen nehmen, unabhängig davon, ob Transaktionen in einem einzigen Vorgang oder in mehreren Vorgängen, zwischen denen eine Verbindung zu bestehen scheint, getätigt wird."*[38] Anbieter virtueller Geldbörsen sowie Umtauschplattformen stellen weder Kreditinstitute *„... ein Unternehmen, dessen Tätigkeit darin besteht, Einlagen oder andere rückzahlbare Gelder des Publikums entgegenzunehmen und Kredite für eigene Rechnung zu gewähren"*[39] noch Finanzinstitute gemäß Art 3 Nummer 2 lit a bis f der RL (EU) 2015/849 oder sonstige Verpflichtete nach Art 2 Nummer 3 der RL (EU) 2015/849 dar.[40] Aus diesem Grund erfolgte die Änderung des Art 2 durch die RL (EU) 2018/843 indem folgende Buchstaben an Nummer 3 angehängt werden: *„...g) Dienstleister, die virtuelle Währungen in Fiatgeld und umgekehrt tauschen; h) Anbieter von elektronischen Geldbörsen..."*[41] Zudem wurden folgende Nummern an Art 3 angefügt:

- *„ 18. „virtuelle Währungen" eine digitale Darstellung eines Wertes, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzliche festgelegte Währung angebunden ist und die nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischen Wege übertragen, gespeichert und gehandelt werden kann;*[42]
- *19. „Anbieter von elektronischen Geldbörsen" einen Anbieter, der Dienste zur Sicherung privater kryptografischer Schlüssel in Namen seiner Kunden anbietet, um virtuelle Währungen zu halten, zu speichern und zu übertragen."*[43]

[37] RL 2015/849 ABl L 2015/141, 73.
[38] RL 2015/849 ABl L 2015/141, 73.
[39] VO (EU) 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012, ABl. L 2013/176,1.
[40] RL 2015/849 (EU) ABl L 2015/141,73.
[41] RL 2018/843 ABl L 2018/156, 43.
[42] RL 2018/843 ABl L 2018/156, 43.
[43] RL 2018/843 ABl L 2018/156, 43.

Es gibt keine nationale Norm oder nationale Legaldefinition von Wallet Providern. Rechtlich unterliegen Wallet Provider keiner Konzessionspflicht und Ihre Tätigkeit ist auch keinem reglementierten Gewerbe zuzuordnen, weshalb es als freies Gewerbe ausgeübt werden kann.[44] „Ferner ist völlig unklar, was mit „Walletprovider" gemeint sein soll. Aus technischer Sicht würde das nur Sinn machen, wenn damit „bankähnliche Aufbewahrservice-Anbieter" gemeint sind. Die technische Verfügungsgewaltliegt in diesem Fall beim Dienstleister, der demnach seine Kunden identifizieren müsste so Ing. Johannes Grill, Präsident von Bitcoin Austria.[45]

3.2. Abgrenzung Tauschmittel/Zahlungsmittel

In der 5. GwR wird festgehalten, dass Kryptowährungen kein elektronisches Geld im Sinne des Art 2 Nummer 2 der RL 2009/110/EG[46], dessen Bestimmungen im § 1 Abs 1 E – Geldgesetz 2010 umgesetzt wurden: *„E-Geld bezeichnet jeden elektronisch – darunter auch magnetisch – gespeicherten monetären Wert in Form einer Forderung gegenüber dem E-Geld-Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge im Sinne von § 4 Z 5 des Zahlungsdienstegesetzes 2018 – ZaDiG 2018, BGBl. I Nr. 17/2018 durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten angenommen wird" sind. „Elektronisches Geld ist zuvorderst ein monetärer Wert. Ein monetärer Wert ist jede Art von Zahlungsmittel. Der Begriff des monetären Werts erfasst neben gesetzlichen Zahlungsmitteln jede Art von Tauschmittel, das allgemein oder auch nur in einem bestimmten soziokulturellen Umfeld oder auch nur von den Parteien einer multilateralen Rahmenvereinbarung als Bezahlung für bestimmte Waren oder Dienstleistungen akzeptiert wird*.[47] Somit wäre der Tatbestand des monetären Wertes erfüllt. Es ist jedoch festzuhalten, dass der monetäre Wert eine Forderung gegenüber einem Emittenten darstellen muss. Virtuelle Wahrungen könnten somit einen monetären Wert verkörpern, da jedoch keine Forderung gegenüber einen Emittenten besteht, stellen Kryptowährungen kein elektronisches Geld dar.[48] Tauschverträge sind im österreichischen Recht in § 1045 ABGB verankert, durch den festgelegt wird, dass jede Sache als Tauschmittel dienlich ist: *„Der Tausch ist ein Vertrag, wodurch eine Sache gegen eine andere Sache überlassen wird. Die wirkliche Uebergabe ist nicht zur Errichtung; sondern nur zur Erfüllung des Tauschvertrages, und zur Erwerbung des Eigenthumes nothwendig*.(§ 1045 ABGB). Der zivilrechtliche Sachenbegriff ist in § 285 ff ABGB geregelt. Grundsätzlich ist eine Sache im rechtlichen Sinn: *„Alles, was von der Person*

[44] *Andreas* Pfeil *LL.M.* Interview geführt von Marina Kindel (4.10.2018).
[45] *Ing. Johannes Grill,* Präsident Bitcoin Austria, Interview geführt von Marina Kindel (3.08.2018).
[46] Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG, ABl L 2009/267, 7.
[47] *Bundesanstalt für Finanzen,* Merkblatt - Hinweise zum Zahlungsdiensteaufsichtsgesetz (ZAG), https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html;jsessionid=188D4736DCEA8F5307F430288FF8A302.1_cid298?nn=9450978#doc7846622bodyText30 (abgerufen am 20.08.2018).
[48] *Bundesanstalt für Finanzen*, Merkblatt - Hinweise zum Zahlungsdiensteaufsichtsgesetz (ZAG), (abgerufen am 20.8.2018).

unterschieden ist, und zum Gebrauche der Menschen dient, wird im rechtlichen Sinne eine Sache genannt" (§285 ABGB). Zum Tausch geeignet sind jene in § 285 ABGB und 285a ABGB genannten Sachen. In Folge dessen können unkörperliche Sachen sowie systemeigene Zahlungsmittel unter § 1045 ABGB subsumiert werden.[49] *„Die Erfüllung des Tauschvertrages erfordert die sogenannte wirkliche Übergabe der zu vertauschenden Sachen. Insoweit sind alle gesetzlich vorgesehenen Besitztraditionen (§§ 431 ff für unbewegliche Sachen, §§ 426 ff für bewegliche Sachen) denkbar. Der Tausch stellt dabei nur den Titel des Eigentumserwerb dar."*[50] Zum Zeitpunkt des Abschlusses des Tauschvertrages ist das Vorliegen des Eigentums von einer der Vertragsparteien nicht zwingend.[51] Kryptowährungen können unter den bürgerlich-rechtlichen Sachbegriff subsumiert werden.[52] Wie bereits erwähnt sind Kryptowährungen *„ ... unkörperliche und bewegliche Sachen, die verbrauchbar und vertretbar sind. Virtuelle Währungen können Gegenstand rechtsgeschäftlicher Vereinbarungen sein wie etwa Kauf-, Tausch-, Schenkungs-oder Darlehensvertrag.*[53] Um als Sache im Sinne des Gesetzes zu gelten, müssen zwei Kriterien erfüllt sein: Erstens die Unterscheidung zum Menschen, da der Mensch keine Sache ist und zweitens die Eignung zum Gebrauch, welche Beherrschbarkeit bedingt.[54] Kryptowährungen unterschieden sich einerseits vom Menschen und andererseits weisen diese, verglichen mit anderen unkörperlichen Sachen, eine extrem hohe Beherrschbarkeit auf. Um Einheiten virtueller Währungen an Dritte zu übertragen muss Kenntnis über den „private key" vorherrschen[55]:*„ Obwohl es sich um unkörperliche Sachen handelt, legt dieser Umstand eine analoge Anwendung sachenrechtlicher Bestimmungen inbs zum Besitz- und Eigentumserwerb nahe."*[56] Ab dem Zeitpunkt bei dem eine Einheit einer virtuellen Währung hergestellt wurde, handelt es ich somit um Sachen iSd § 285 AGBG. Aktuell wurde der technische Prozess, der bei der Erzeugung eines Coins entsteht, höchstgerichtlich noch nicht entschieden wie dieser rechtlich einzuordnen ist.[57]

Von Seiten der FMA wird die Einstufung von Kryptowährungen, allem voran von Bitcoin, als E-Geld im Sinne des E-Geldgesetzes 2010 mit folgender Begründung verneint: *„Bei*

[49] *Schwimann/Neumayr* in Schurr, ABGB[4] (2017) § 1045 (Stand 27.09.2018, lexisnexis.at).
[50] *Schwimann/Neumayr* in Schurr, ABGB[4] (2017) § 1045.
[51] *Schwimann/Neumayr* in Schurr, ABGB[4] (2017) § 1045.
[52] *Völkel,* Privatrechtliche Einordnung der Erzeugung virtueller Währungen, ecolex 2017, 639.
[53] *Völkel,* ecolex 2017, 639.
[54] *Schwimann/Neumayr* in Schurr, ABGB[4] (2017) § 285 (Stand 27.09.2018, lexisnexis.at).
[55] *Völkel,* ecolex 2017, 639.
[56] *Völkel,* ecolex 2017, 639.
[57] *Völkel,* ecolex 2017, 639.

virtuellen Währungen besteht keine Forderung gegenüber einem Emittenten, da es keinen Emittenten als solchen gibt.“[58]

Die Entwickler des Bitcoin-Systems, welche unbekannt sind, haben ein System entwickelt, welches sich eigenständig verwaltet und betreibt. Ein Emittent im herkömmlichen Sinn ist somit nicht vorzufinden. Auch die Ansicht, dass jeder Miner als Emittent betrachtet werden kann, da[59] *„… er sich selbst durch das Finden des richtigen Hashwerts Bitcoins gutschreibt und diese dann in der Folge weiterverkauft“*[60], ist zu entkräften. Der Bitcoin als solcher entsteht nicht selbst beim Miner, sondern wird durch einen Vorgang gutgeschrieben. Zudem ist der exakte Zeitpunkt des Findens des richtigen Hashwertes nicht beeinflussbar. Die Chance kann lediglich durch Steigerung der Rechenleistung erhöht werden. Somit entsteht ein Bitcoin nicht zufällig oder durch bloßen Willensakt. Aus den angeführten Gründen ist ein Miner somit nicht als Emittent zu klassifizieren.[61]

Zudem *„… stellen Bitcoins derzeit* ***kein gesetzliches Zahlungsmittel*** *dar, weshalb die Einstufung als E-Geld nicht gegeben ist. Auch handelt es sich aus diesem Grund um* ***keine Form der Zahlungsdienstleistung****, welche insbesondere auf den Zahlungscharakter iS eines gesetzlichen Zahlungsmittels abstellt.“*[62] Gemäß § 1 Eurogesetz in Verbindung mit der EU – Verordnung (EG) Nr. 974/98 sind seit 1. Jänner 2002 in Österreich

1. *„… auf Euro lautende Banknoten, die von der Oesterreichischen Nationalbank, der Europäischen Zentralbank (EZB) oder anderen nationalen Zentralbanken der an der dritten Stufe der Wirtschafts- und Währungsunion (WWU) ohne Ausnahmeregelung teilnehmenden Mitgliedstaaten ausgegeben wurden,*
2. *auf Euro oder Cent lautende Münzen, die gemäß den Bestimmungen des Artikels 106 Abs. 2 EG-Vertrag und Artikel 11 der Verordnung (EG) Nr. 974/98 über die Einführung des Euro, ABl. Nr. L 139 vom 11. Mai 1998, von der Münze Österreich Aktiengesellschaft oder anderen an der dritten Stufe der WWU ohne Ausnahmeregelung teilnehmenden Mitgliedstaaten ausgegeben wurden,*
3. *auf Euro oder Cent lautende Sammlermünzen, die von der Münze Österreich Aktiengesellschaft gemäß § 12 des Scheidemünzengesetzes, BGBl. Nr. 597/1988, in der Fassung BGBl. I Nr. 72/2000 ausgegeben wurden, sowie*
4. *vorbehaltlich der Bestimmung des § 2 die auf Schilling lautenden Banknoten und die auf Schilling oder Groschen lautenden Scheidemünzen.“* (§ 1 Eurogesetz Artikel 1 Z 1 bis 4) gesetzliche Zahlungsmittel.

[58] *WKO,* Die Kryptowährung Exkurse: Bitcoins und Mining https://www.wko.at/branchen/information-consulting/finanzdienstleister/artikel-kryptowaehrung.pdf (Stand 07.02.2018).;*Piska,* ecolex 2017 632.
[59] *Eberwein/ Steiner,* Bitcoins, (2014) 41.
[60] *Eberwein/ Steiner,* Bitcoins, (2014) 41.
[61] *Eberwein/ Steiner,* Bitcoins, (2014) 41.
[62] *WKO,* Die Kryptowährung Exkurse: Bitcoins und Mining, (Stand 07.02.2018).

Neben der Tatsache, dass virtuelle Währungen kein gesetzlich anerkannten Zahlungsmittel im Sinne der Rechtsordnung sind, sind diese unmittelbare Wertträger, die keine Forderungsrechte begründen.[63] Der Wert von Bitcoins setzt sich aus Angebot und Nachfrage zusammen. Dieser wird jedoch nicht elektronisch abgespeichert, sondern nur die Transaktionen, durch die Teilnehmer einen gewissen Betrag erhalten. Es gibt unterschiedliche Ansichten, ob dies als Speicherung des Wertes betrachtet werden kann. Doch nur die Speicherung begründet noch keine Forderung gegenüber einem Ausgeber. Zudem beruht der[64] *„ ... innere Wert lediglich auf dem Tauschwert, den die beteiligten Verkehrskreise dem Objekt zumessen, nicht aber auch auf einer potenziellen Forderung gegen Dritte, die das betreffende Objekt dem Inhaber jederzeit und unbedingt gegen Geld abnehmen würden.“*[65]

Durch die Verwendung des Terminus „Tauschmittel“ in der Definition der RL wurde eindeutig von gesetzlich anerkannten Zahlungsmitteln Abstand genommen und der eingebürgerte Begriff „Kryptowährung“ stellt somit bloß eine sprachgebräuchliche Bezeichnung dar. Durch die Festlegung VW als Tauschmittel werden die Eigenschaften als Wirtschaftsgut und digitales Produkt hervorgehoben. Die Erzeugung virtueller Einheiten erfolgt auf elektronischem Wege unter Einsatz von Rechenleistung. Obwohl der Produktionsprozess nur digital erfolgt ist dieser trotzdem zuordenbar. Die Verfügungsmacht liegt auf Seiten des Erzeugers, welche auf Märkten handelbar ist und weitergegeben werden kann. [66] *„Diese Strukturanalyse zeigt, dass Kryptowährungen die Qualität eines Wirtschaftsguts haben. Letztlich handelt es sich um von Privatrechtssubjekten hergestellte, physisch nicht berührbare digitale Produkte.“*[67] Kryptowährungen sind somit vom Geld verschieden und als Zahlungsmittel mit dem etwas gekauft werden kann verschieden. Virtuelle Währungen sind als Tauschmittel zu qualifizieren. Um Eigentum an einer Sache zu erhalten, kann entweder eine Sache mit Geld gekauft oder gegen eine andere Sache getauscht werden. Bei Kryptowährungen handelt es sich folglich[68] *„... um unkörperliche Sachen, die gegen andere Waren oder gesetzliche Zahlungsmittel getauscht werden können.“*[69] Mit der ausdrücklichen Verankerung von virtuellen Währungen *„...als Objekte privater Tauschgeschäfte wird dieses digitale Produkt auch mitten in den Anwendungsbereich der wirtschaftlichen Grundrechte ... Recht auf Unverletzlichkeit des Eigentums und des Rechts*

[63] *WKO,* Die Kryptowährung Exkurse: Bitcoins und Mining (Stand 07.02.2018).; *Piska,* ecolex 2017 632.
[64] *Eberwein/ Steiner,* Bitcoins, (2014) 41.
[65] *Eberwein/ Steiner,* Bitcoins, (2014) 42.
[66] *Piska/Völkel*, Kryptowährungen reloaded- auf den Weg aus dem Bermuda-Dreieck[1] ecolex 2017, 733.; *Piska,* Kryptowährungen und ihr Rechtscharakter - eine Suche im Bermuda- Dreieck ecolex 2017 632.
[67] *Piska,* ecolex 2017 632.
[68] *Piska/Völkel*, ecolex 2017, 733.
[69] *Piska/Völkel,* ecolex 2017, 733.

auf Erwerbsfreiheit …platziert.“ [70] Auf Grund dessen besteht für Regulierungsmaßnahmen eine Beschränkung.[71] Es handelt sich um ein *„… Währungssystem ohne zentrales Lenkungs- Steuerungs- sowie Aufsichtsorgan.“*[72] Dadurch, dass virtuelle Währungen keiner Aufsicht bzw. Ordnungssystem unterliegen bleiben sie den Kräften des Marktes überlassen. Zudem weisen sie eine geringere Stabilität, als Währungssysteme die einer Aufsicht unterliegen, auf: [73] *„Die Wertermittlung-und Gewinnung dieser Onlinewährung erfolgt somit ausschließlich anhand eines digitalen peer-to-peer Netzwerkes, an welchem sich beliebig viele Computer beteiligen können.* [74] Durch diese Eigenschaft ist es schier unmöglich einheitliche rechtliche Rahmenbedingungen für das Währungssystem zu schaffen.[75]

Ferner werden darunter weder Geldbeträge gemäß RL (EU) 2015/2366 Art 4 Nummer 25: *„ „Geldbetrag“ Banknoten und Münzen, Giralgeld oder E-Geld im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/110/EG “*[76] noch nach Art 3 Buchstabe k und l der RL 2015/2366 verstanden. Auch sind virtuelle Währungen weder mit Spielwährungen noch mit lokalen Währungen zu verwechseln.[77]

Folgender Abschnitt bezieht sich vor allem auf die virtuelle Währung Bitcoin. Bitcoin und Co können funktionell sowie herkunftsbezogen betrachtet werden. Im folgenden Abschnitt wird die funktionelle Betrachtung erörtert. Sinngemäß wird unter Bitcoin eine „digitale Münze“ verstanden, in dessen Zusammenhang sich die Termini „virtuelle Währungen“ bzw. „Kryptowährungen“ gebildet haben. Der Zweck der Währungen wird wie folgt beschrieben:[78] *„ Ihr Wert, der sich in jeder beliebigen offiziellen Währung, also in Geld, ausdrücken lässt, unterliegt Marktmechanismen und sie sind für den Erwerb von Gütern oder die Inanspruchnahme von Dienstleistungen einsetzbar …“* [79] Voraussetzung dafür ist die Akzeptanz von virtuellen Währungen der Vertragspartner.[80] Es ist festzuhalten, dass kein Annahmezwang, wie dies bei gesetzlichen Zahlungsmitteln der Fall ist, herrscht. Die Akzeptanz von virtuellen Währungen als Zahlungsmittel erfolgt auf freiwilliger Basis.[81]

In dem Personenkreis, die Kryptowährungen anerkennen, erfüllen diese somit[82] *„… eine ähnliche wirtschaftliche Funktion wie offiziell anerkannte Zahlungsmittel, also insb das von*

---

[70] *Piska/Völkel,* ecolex 2017, 733.
[71] *Piska/Völkel*, Kryptowährungen und AML – smart regulation in Sicht, ecolex 2018 671.
[72] *Eberwein/ Steiner,* Bitcoins, (2014) 30.
[73] *Eberwein/ Steiner,* Bitcoins, (2014) 30.
[74] *Eberwein/ Steiner,* Bitcoins, (2014) 30.
[75] *Eberwein/ Steiner,* Bitcoins, (2014) 30.
[76] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABl. L 2015/337, 35.
[77] RL 2018/843 ABl L 2018/156, 43.
[78] *Piska,* ecolex 2017 632.
[79] *Piska,* ecolex 2017 632.
[80] *Piska,* ecolex 2017 632.
[81] *Eberwein/ Steiner,* Bitcoins, (2014) 31.
[82] *Piska,* ecolex 2017 632.

Zentralbanken emittierte Geld"[83] Aus Sicht der Wirtschaft und Nutzer stellen virtuelle Währungen, vor allem Bitcoin, eine Währung dar. Nur unter Beachtung der reinen Funktion könnte dies bejaht werden. Aus rechtlicher Sicht sind Währungen jedoch[84] *„... staatlich zentriert, dh, sie basieren, da sie von der jeweiligen Zentralbank emittiert werden, auf hoheitlicher Grundlage und unterliegen obrigkeitlichen, währungspolitischen Steuerungsmechanismen ..."*[85] Es bestehen hoheitliche Normen, welche eingesetzt und Währungen somit zu gesetzlich anerkannten Zahlungsmittel erklären. Virtuelle Währungen wurden gezielt als staatferne Konstrukte entwickelt und können nicht durch staatliche Organe beeinflusst werden. Obwohl Bitcoin Eigenschaften eines staatlich anerkannten Zahlungsmittels aufweist, stellen diese, auf Grund des Fehlens der hoheitlichen Grundlage, nicht einmal im Ansatz eine Währung im volkswirtschaftlichen bzw. rechtdogmatischen Sinn dar. Somit ist die Bezeichnung virtuelle Währungen als solche, aus rechtlicher Sicht, irreführend.[86] Die herkunftsbezogene Betrachtung deklariert Virtuelle Währungen als privates Wirtschaftsgut. Diese werden durch einen digitalen Prozess erzeugt, sind eindeutig identifizierbar, zuordenbar und befinden sich in der Verfügungsmacht der Hersteller. Aus diesen Gründen ist eine Einordnung in das bestehende Kapital- und Finanzmarktrecht nicht möglich. Es ist ein dezentrales System ohne Emittenten[87]: *„ Deshalb wird in der Regel auch die Subsumation von Kryptowährungen unter Begriffe wie Geld [13)] , e-Geld [14)], Finanz-bzw. Zahlungsinstrument [15)] usw in konkreten Untersuchungen aufgrund geltender Rechtsnormen im Prinzip verneint [16)] ."*[88] Mit der in der RL 2018/847 bestimmten Definition Virtueller Währungen wurde somit die herkunftsbezogene Betrachtung der funktionelle Betrachtung, Bitcoin als Zahlungsmittel, vorgezogen. Auf Grund der Verwendung des Begriffes „Tauschmittel" wurden VW klar von staatlich anerkannten Zahlungsmitteln abgegrenzt. Zudem sind VW handelbar wodurch wird die Einstufung VW als digitale, private Wirtschaftsgüter bestärkt wird.[89]

Von Seiten der FMA wird Bitcoin als eine alternative Währung betrachtet, die in Wahrheit eine Ware ist, so Klaus Grubelnik.[90]

[83] *Piska,* ecolex 2017 632.
[84] *Piska,* ecolex 2017 632.
[85] *Piska,* ecolex 2017 632.
[86] *Piska,* ecolex 2017 632.
[87] *Piska,* ecolex 2017 632.
[88] *Piska,* ecolex 2017 632.
[89] *Piska/Völkel,* ecolex 2018 671.
[90] *Piska,* ecolex 2017 632.

3.2.1. Preisstabilität im Europäischen Raum

Bitcoins können, wenn diese in großen Bereichen der Ökonomie als alternative Bezahlmöglichkeit angeboten werden, eine Beeinflussung der Stabilität des Preises im Euro - Raum hervorrufen. Folgende drei Faktoren könnten dazu führen: Erstens die Entstehung eines eigenen Währungssystems, bei dem Maßnahmen der Europäischen Zentralbank nicht greifen. Zweitens bei Substituierung gesetzlich anerkannter Zahlungsmittel und drittens bei Entstehung eines Schattenwährungssystems. Obwohl es einige Verlinkungsversuche der Gemeinschaft von virtuellen Währungen zur realen Wirtschaft gab, unter anderem durch Bitbills, ist jedoch nicht davon auszugehen, dass Bitcoins oder andere Kryptowährungen den Euro oder andere Währungen substituieren werden. Zudem ist die Finanzstabilität nicht gegeben, da sich der Kurs lediglich aus Angebot und Nachfrage bzw. sich aus dem Vertrauen der Nutzer zusammensetzt und keine Auskunft über die ökonomische Stärke der Währung erteilt.[91] Bitbills waren eine Idee um Bitcoins mobil in physischen Plastikkarten verwendbar zu machen. Sie waren die erste physische Form von Bitcoins. Es gab sie jedoch nur kurze Zeit von 2011-2012 und zu damaligen Preisen: 1 BTC, 5 BTC, 10 BTC und 20 BTC. Die Idee war, dass auf den Karten der Private Key für die Bitcoins gespeichert war und sie damit wie Gutscheine oder Bargeld eingetauscht werden konnten. Falls jemand die Bitcoins runter transferiert, verliert die Karte den Wert. Es war so konstruiert, dass man sehen konnte ob Bitcoins auf der Karte waren. Der Private Key war hinter einem Plastik-Sticker (Hologram), den man zerstören musste um den Key lesen zu können und die Coins transferieren zu können, versteckt.[92]

3.2.2. Voraussetzungen für sicheres Zahlungssystem

Damit Bitcoin und sonstige virtuelle Währungen ein sicheres Zahlungsmittel darstellen müssten diverse Voraussetzungen vorliegen. Sichere Zahlungssysteme müssen auf einer rechtlich stabilen Basis gegründet werden. Sämtliche Regeln der Generierung von Bitcoins müssten einheitlich, fair und nachvollziehbar sein. Zudem müsste das System vor Hackerangriffen geschützt sein und bei solchen Angriffen über klar definierte Regelwerke verfügen. Der Umrechnungskurs muss tagesaktuell und transparent sein. Ferner muss die Teilnahme an diesem System transparent sein. Das Bitcoin-System müsste sicher und stabil sein und einfache Bezahlmöglichkeiten schaffen. Effektivität, Wirksamkeit und

[91] *Eberwein/ Steiner,* Bitcoins, (2014) 31ff.
[92] *Feigelson,* United States, Patent Application Publication, https://patentimages.storage.googleapis.com/a0/71/ef/a5115ad8a70b d0/US20130166455A1.pdf, (abgerufen am 5. Oktober 2018).

Nachvollziehbarkeit der rechtlichen Rahmenbedingungen müssten gegeben sein. Auf Grund des Vorliegens eines Peer-to-Peer Systems bei virtuellen Währungen ist die Erfüllung der angeführten Punkte als fraglich zu betrachten.[93]

3.2.3. Arten des Erwerbes von virtuellen Währungen

Aktuell gibt es drei Möglichkeiten virtuelle Währungen zu erwerben und diese in ein anerkanntes Zahlungsmittel umtauschen zu lassen.

Die erste und wohl am weitesten verbreitete Möglichkeit sind Online-Börsen, bei denen je nach Standort der Firma gewisse Know-Your-Customer Richtlinien (KYC) angewendet werden. In den meisten Börsen, vor allem bei seriösen Börsen die eine gute Reputation anstreben werden eindeutige Identifizierungsverfahren gegenüber Nutzern angewendet. Wenn die Identifizierung erfolgt ist, sind die Konsumenten somit berechtigt Transaktionen über die Online-Plattform durchzuführen.[94] Wie Firmen aktuell Know-Your-Customer Verfahren umsetzen wird im Kapitel 8 an Hand der Coinfinity GmbH, einer der renommiertesten virtuellen Börsen für Kryptowährungen in Österreich, dargelegt.

Die zweite Möglichkeit stellt den Kauf über Automaten (ATMs) dar, bei denen virtuelle Währungen in Fiatgeld getauscht werden können. Es wird lediglich ein Wallet benötigt, welche aus einer Adresse und einen Schlüssel besteht. Es ist keine Verifizierung nötig, jedoch ist die Höhe der Beträge beschränkt, welche eine freiwillige und keine rechtlich verankerte Beschränkung darstellt.[95]

Die dritte Möglichkeit besteht über den direkten Handel mit anderen Personen sogenannten Krypto-Broker. Diese Möglichkeit wird als „Over-the-counter-Trades“ bezeichnet. Bei diesen Geschäften ist das Limit der Geldmenge höher als bei Automaten, jedoch ist dies mit erhöhter Vorsicht zu genießen. Indizien dafür, dass Schwarzgeld im Spiel ist, ist, wenn keine Know-Your-Customer Verfahren angewendet werden oder der Händler nicht gemeldet ist. Von diesen Geschäften ist Abstand zu halten.

Zukünftig soll es noch eine vierte Möglichkeit geben, sogenannte dezentrale Börsen. Aktuell werden zentralisierte Börsen in einem gewissen Umfang reguliert. Dies soll mit dezentralen Börsen nicht mehr möglich sein. Weder Firmen noch Personen stehen hinter solchen Börsen, wodurch es der Regierung nicht möglich ist an Transaktions- bzw. Kundeninformationen zu

[93] *Eberwein/ Steiner,* Bitcoins, (2014) 35.
[94] *Florian Wimmer,* CEO, Co-Founder, Interview geführt von Marina Kindel (22.07.2018).
[95] *Florian Wimmer,* CEO, Co-Founder, Interview geführt von Marina Kindel (22.07.2018).

gelangen. Aktuell ist die Umsetzbarkeit solcher Börsen aus technischer Sicht noch nicht möglich, dennoch wird aktiv an einer Umsetzung gearbeitet.[96]

Aktuell gibt es rund 14 000 Marktplätze, bei denen der Handel mit virtuellen Währungen möglich ist.[97] *„Der Handel findet dabei analog zu klassischen Devisenmärkten in Form des Tausches einer Einheit einer Währung gegen eine bestimmte Menge einer anderen Währung" statt."*[98] Das Marktvolumen betrug per Anfang 2018 rund USD 800 Milliarden.[99] Des Weiteren existieren ca. 1000 virtuelle Währungen (Stand 1 Q. 2018), von denen jedoch nur wenige von großer Bedeutung sind. Dennoch kommen stetig weitere dazu, da die Schaffung solcher verhältnismäßig einfach ist.[100]

3.3. Verstärkte Sorgfaltspflichten gegenüber Drittländern

Beim Vorschlag zur Änderung der RL (EU) 2015/849 wird der Umgang mit Drittländern beschrieben. Es wird von den Mitgliedsstaaten, auf nationaler Ebene verlangt, den Verpflichteten verstärkte Sorgfaltspflichten gegenüber Drittländern mit hohem Risiko vorzuschreiben. Dennoch wird ein harmonisierender Ansatz verlangt, da es andernfalls zu Schwachstellen im System kommen kann, die von Kriminellen ausgenutzt werden könnten. Zudem sollten weitere risikomindernde Maßnahmen, unter Berücksichtigung internationaler Standards, von den einzelnen Mitgliedsstaaten erlassen werden.[101]

In der 5. GwR wird festgehalten, dass Transaktionen mit Drittländern, die ein erhöhtes Risiko aufweisen zu beschränken sind, es sei denn, dass zusätzlich Maßnahmen zur Risikominderung ergriffen werden. Ein unionsweites Gesamtkonzept soll entstehen, um zu prüfen ob die national entwickelten Systeme wirksam sind und mit den unionsrechtlichen Bestimmungen übereinstimmen.[102]

3.4. Pflicht zur Eintragung von Kryptobörsen und Wallet Providern

Der Art 47 Abs 1 der 4. GwR erhält folgende Fassung: *„(1) Die Mitgliedstaaten sehen vor, dass Dienstleistungsanbieter, bei denen virtuelle in Fiatgeld und umgekehrt getauscht werden können, und Anbieter von elektronischen Geldbörsen eingetragen werden müssen und dass Wechselstuben, Scheckeinlösestellen und Dienstleister für Trusts und Gesellschaften*

[96] *Florian Wimmer,* CEO, Co-Founder, Interview geführt von Marina Kindel (22.07.2018).
[97] *Brauneis/Mestel,* Finanzwesen- allgemein verständlich: Kryptowährungen, ÖBA (2018), 711.
[98] *Brauneis/Mestel,* Finanzwesen- allgemein verständlich: Kryptowährungen, ÖBA (2018), 711.
[99] *Brauneis/Mestel,* Finanzwesen- allgemein verständlich: Kryptowährungen, ÖBA (2018), 711.
[100] *Freitag,* Die Blockchain- Technologie Nur ein Hype oder doch mehr?, Linde 2018, 59.
[101] COM/2016/0450 final -2016/0208 (COD).
[102] RL 2018/843 ABl L 2018/156, 43.

zugelassen oder eingetragen und Anbieter von Glücksspieldiensten reguliert sein müssen.“[103] Hiermit ist gemeint, dass sich zukünftig die Gatekeeper registrieren lassen müssen.[104]

Eine genauere Ausführung wie die Eintragung zu erfolgen hat wird aus der Richtlinie nicht ersichtlich, wodurch die Mitgliedstaaten einen gewissen Gestaltungsfreiraum haben werden: [105] „*Erst eine innerstaatliche Umsetzung wird zeigen, welche Zulassung oder Eintragung notwendig sein wird, um dieser Vorgabe zu entsprechen.“*[106]

Ziel der Erfassung der „neuen“ Verpflichteten gemäß der 5. RL ist es, die Schnittstelle zwischen der bisher bekannten Geldwirtschaft und der neu geschaffenen Kryptowirtschaft zu regulieren. Fraglich ist jedoch, ob Dienstleister, die virtuelle Währungen in andere virtuelle Währungen tauschen ebenfalls von der Richtlinie erfasst sein werden. Dies ist vor allem für die Frage der Finanzierung von Initial Coins Offerings von Bedeutung, welche in Kapitel 12. erörtert werden.[107]

Die 5. Geldwäsche-Richtlinie verschärft die geltenden EU-Rechtsvorschriften hinsichtlich der Transparenz von Vermögenswerten, Verstärkung der Kontrollen von risikobehafteten Drittländern, Verbesserung der Zusammenarbeit zwischen nationalen Behörden und der Bekämpfung von Risiken im Zusammenhang mit Prepaid-Karten und virtuellen Währungen. Die Hintergründe der Verschärfungen sind die angespannte Sicherheitslage durch die Bedrohung durch Terrorismus und die Rolle von Geldwäsche und Terrorismusfinanzierung in Europa.[108] Zur Bekämpfung und Einschränkung von Geldwäsche wurden spezifische AML-Maßnahmen entwickelt, welche die verschiedenen Phasen des Geldwäscheprozesses betreffen. Diese setzen sich aus Rahmenwerken und konkreten Prozessen zusammen, welche wiederum auf Fakten rund um die Kunden und das Verhalten der Kunden abzielen.[109]

[103] RL 2018/843 ABl L 2018/156, 43.
[104] *Piska/Völkel*, ecolex 2018 671.
[105] *Schock*, Virtuelle Währungen- Ein Blick über die Grenzen, ecolex 2017, 636.
[106] *Schock*, Virtuelle Währungen- Ein Blick über die Grenzen, ecolex 2017, 636.
[107] *Piska/Völkel*, ecolex 2018 671.
[108] *Europäischer Rat/ Rat der Europäischen Union*, Bekämpfung der Geldwäsche und der Terrorismusfinanzierung, http://www.consilium.europa.eu/de/policies/fight-against-terrorism/fight-against-terrorist-financing/, (abgerufen am 03.09.2018).
[109] *Bundesministerium für Finanzen*, Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt (Finanzmarkt-Geldwäschegesetz – FM-GwG), https://www.bmf.gv.at/rechtsnews/FM-GwG_TXT_161109.pdf?67rvn7 (3ff), (abgerufen am 03.09.2018).

4. Begriffsabgrenzung Know-Your-Customer (KYC), Anti-Money Laundering (AML) und Combating the Financing of Terrorism (CFT)

4.1. Know-Your-Customer (KYC)

Know-Your-Customer (KYC), bezeichnet den Prozess einer Legitimationsprüfung und der Identifizierung von Kunden.[110] Dabei steht die Erhebung und Verifizierung von Daten über natürliche und juristische Personen im Vordergrund. KYC wird durchgeführt um den Kunden und seine finanziellen Verbindungen zu verstehen, bevor und während man Geschäfte mit diesen tätigt. Es beinhaltet eine Reihe von Prozessen und Prozeduren, durch welche insbesondere Banken, Finanzinstitute und FinTechs die Durchführung von illegalen Aktivitäten (Geldwäsche, Terrorismusfinanzierung, Wirtschaftskriminalität, etc.) vermeiden sollen.[111] KYC beinhaltet die Elemente von Unternehmenspolitik, Kundenidentifizierung, Überwachung von Transaktionen und Risikomanagement.[112]

KYC Regeln variieren international und sind abhängig von der jeweiligen Jurisdiktion.[113] In der Europäischen Union sind durch Geldwäscherichtlinien Mindeststandards für die Mitgliedsstaaten vorgegeben. Diese KYC-Mindeststandards wurden in Österreich im Jahr 2007 durch die Umsetzung der 3. Geldwäscherichtlinie über die Novellierung des Bankwesengesetzes, Börsegesetzes, des Versicherungsaufsichtsgesetzes und des Wertpapieraufsichtsgesetzes eingeführt.[114] Die Know-Your-Customer Überprüfung ist ein Teil der Vorkehrungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung.[115]

4.2. Anti-Money Laundering (AML) und Combating the Financing of Terrorism (CFT)

Im Zuge von vielen Tätigkeiten innerhalb des Finanzsektors besteht das grundsätzliche Risiko mit kriminellen Aktivitäten der Geldwäsche und Terrorismusfinanzierung in Kontakt zu kommen. Geldwäsche bezeichnet den Prozess des Einschleusens von Finanzmitteln illegalen Ursprungs in den Finanzkreislauf mit dem Ziel der Verschleierung der Herkunft der Geld- oder Vermögenswerte.[116] Die Bekämpfung von Terrorismusfinanzierung umfasst die

[110] *LexisNexis,* KYC: Versteckte Risiken, https://www.lexisnexis.de/begriffserklaerungen/compliance/kyc-know-your-customer (abgerufen am 13.10.2018).
[111] *Bankenverband,* Know Your Customer: Privatkundenverifizierungen im EU- Binnenmarkt, https://bankenverband.de/media/files/Positionspapier_KYC.pdf, (3ff), (abgerufen am 3 September 2018).
[112] *Gemalto*, Know-Your-Customer-Verfahren und Anti-Geldwäsche-Richtlinie, https://www.gemalto.com/deutschland/financial/dienstleistungen-fur-banken/identitatsverifizierung/know-your-customer, (abgerufen am 3. September 2018).
[113] *LexisNexis,* KYC: Versteckte Risiken, (abgerufen am 13. Oktober 2018).
[114] *Unternehmensservice Portal,* Geldwäsche, https://www.usp.gv.at/Portal.Node/usp/public?gentics.rs=PDF &gentics.pb=notvisibleposition&contentId=10007.50238, (3), (abgerufen am 3. September 2018).
[115] *Bankenverband,* Know Your Customer: Privatkundenverifizierungen im EU- Binnenmarkt, (3), (abgerufen am 3 September 2018).
[116] *Unternehmensservice Portal,* Geldwäsche, https://www.usp.gv.at/Portal.Node/usp/public?gentics.rs=PDF&gentics. pb=notvisibleposition&contentId=10007.50238, (2), (abgerufen am 3. September 2018).

Untersuchung, Analyse, Abschreckung und Verhinderung von Aktivitäten. [117] Terrorismusfinanzierung inkludiert jene Gruppierungen, welche beabsichtigen durch den Einsatz von Gewalt politische, religiöse oder ideologische Ziele zu erreichen.[118] Geldwäsche geschieht branchenübergreifend und über verschiedene Prozesse. Das Risiko der Geldwäsche geht für Unternehmen einher mit signifikanten rechtlichen, finanziellen, operationellen Risiken sowie Reputationsrisiken. [119] Der Geldwäscheprozess kann in 5 Phasen des Geldwäsche-Prozesses unterteilt werden:

1. Illegaler Erwerb der Mittel;
2. Vorwäsche: Verschleierung der Herkunft der Mittel, in der Regel durch Unternehmen mit hoher Verwendung von Bargeld;
3. Placement: Einführung der Mittel in den legalen Finanzkreislauf;
4. Layering: Verschleierung der Herkunft der Gelder, z.B. durch In- und Auslandstransaktionen;
5. Integration: Verwendung der Mittel in legalen Geschäften.[120]

Geldwäsche ist ein Prozess, welcher die Verschleierung von Mitteln aus illegaler Herkunft involviert, wogegen Terrorismusfinanzierung sowohl aus legalen als auch illegalen Quellen stammen kann. Darüber hinaus besteht im Falle von Terrorismusfinanzierung die Absicht die Mittelverwendung zu verschleiern. Bei Geldwäsche und Terrorismusfinanzierung kommen ähnliche oder identische Methoden zum Einsatz und beide Aktivitäten verwenden potentiell dieselbe Infrastruktur zum Transfer von finanziellen Mitteln. Daher sind die Strategien zur Bekämpfung von Geldwäsche (AML) und Terrorismusfinanzierung (CFT) ähnlicher Natur.[121]

Geldwäscherei ist in § 165 StGB verankert:

(1) Wer Vermögensbestandteile, die aus einer mit mehr als einjährigen Freiheitsstrafe bedrohten Handlung oder einem Vergehen nach den §§ 223, 229, 289, 293, 295 oder nach den §§ 27 oder 30 Suchtmittelgesetz herrühren, verbirgt oder ihre Herkunft verschleiert, insbesondere, indem er im Rechtsverkehr über den

[117] *Financial Action Task Force on Money Laundering (FATF),* F-Leitfaden zum risikoorientierten Ansatz zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Deutsche Übersetzung), https://www.bafin.de/SharedDocs/Downloads/DE/Leitfaden/lf_fatf_leitfaden_risikoorientierter_ansatz.html, (2ff), (abgerufen am 3. September 2018).
[118] *Sieber / Vogel*, Terrorismusfinanzierung – Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht, https://www.mpicc.de/files/pdf3/Band_S_150_Online-Version.pdf (70), (abgerufen am 13. Oktober 2018).
[119] *Deloitte*, Geldwäscheprävention bei Güterhändlern Ergebnis einer qualitativen Studie, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/finance/Forensic-Studie-Geldwaeschepraevention_safe.pdf, (abgerufen am 3. September).
[120] *Deloitte*, Geldwäscheprävention bei Güterhändlern Ergebnis einer qualitativen Studie, (abgerufen am 3. September).
[121] *IWF*, Anti-Money Laundering/Combating the Financing of Terrorism - Topics https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm#moneylaundering (abgerufen am 13. Oktober 2018).

Ursprung oder die wahre Beschaffenheit dieser Vermögensbestandteile, das Eigentum oder sonstige Rechte an ihnen, die Verfügungsbefugnis über sie, ihre Übertragung oder darüber, wo sie sich befinden, falsche Angaben macht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(2) Ebenso ist zu bestrafen, wer wissentlich Vermögensbestandteile an sich bringt, verwahrt, anlegt, verwaltet, umwandelt, verwertet oder einem Dritten überträgt, die aus einer in Abs. 1 genannten mit Strafe bedrohten Handlung eines anderen stammen.

(3) Ebenso ist zu bestrafen, wer wissentlich der Verfügungsmacht einer kriminellen Organisation (§ 278a) oder einer terroristischen Vereinigung (§ 278b) unterliegende Vermögensbestandteile in deren Auftrag oder Interesse an sich bringt, verwahrt, anlegt, verwaltet, umwandelt, verwertet oder einem Dritten überträgt.

(4) Wer die Tat in Bezug auf einen 50 000 Euro übersteigenden Wert oder als Mitglied einer kriminellen Vereinigung begeht, die sich zur fortgesetzten Geldwäscherei verbunden hat, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

(5) Ein Vermögensbestandteil rührt aus einer strafbaren Handlung her, wenn ihn der Täter der strafbaren Handlung durch die Tat erlangt oder für ihre Begehung empfangen hat oder wenn sich in ihm der Wert des ursprünglich erlangten oder empfangenen Vermögenswertes verkörpert.

Der *„... Vorgang der Einschleusung der Geldmengen in den legalen Finanzkreislauf unter Verschleierung der wahren Herkunft wird Geldwäscherei genannt."*[122] Gemäß der Wiener Konvention[123] und des Übereinkommen des Europarates[124] verpflichteten sich einige Staaten, darunter auch Österreich, zur Bekämpfung der Geldwäsche.[125] Es wird vor allem auf das Einhalten der Sorgfaltspflichten der Banken aufmerksam gemacht. Zudem auf die Notwendigkeit der Nachforschung bei auffälligen Geldflüssen.[126] *„**Objekt** der Geldwäscherei nach Abs 1 bis 3 sind **Vermögensbestandteile jeder Art**, neben beweglichen und unbeweglichen körperlichen Sachen (einschließlich Geld), insb auch Forderungen (z.B. Bankguthaben) und andere Rechte von Vemögenswert.*[127] *Die **Tathandlung** der eigentlichen Geldwäscherei nach **Abs 1** besteht im **Verbergen** oder in der **Verschleierung der Herkunft** der Vermögensbestandteile ..."*[128] Der bedingte Vorsatz, normiert in § 5 Abs 1 StGB, kann für dir Verwirklichung des Tatbestandes der Geldwäscherei nach § 165 Abs 1 StGB bereits ausreichend sein.[129] Der Tatbestand des § 165 Abs 2 StGB hingegen setzt Wissentlichkeit voraus: *„**Abs 2** stellt das Ansichbringen, Verwahren, Anlegen, Verwalten, Umwandeln,*

[122] *Fabrizy* StGB[9] (2006) § 165 Rz 1
[123] ÜBEREINKOMMEN DER VEREINTEN NATIONEN GEGEN DEN UNERLAUBTEN VERKEHR MIT SUCHTGIFTEN UND PSYCHOTROPEN STOFFEN; BGBl. III Nr. 154/1997
[124] ÜBEREINKOMMEN ÜBER GELDWÄSCHE SOWIE ERMITTLUNG, BESCHLAGNAHME UND EINZIEHUNG VON ERTRÄGEN AUS STRAFTATENStF: BGBl. III Nr. 153/1997
[125] *Fabrizy,* StGB[9] (2006), § 165 Rz 1
[126] *FAbrizy*, StGB[9] (2006), § 165 Rz 6
[127] *Fabrizy*, StGB[9] (2006), § 165 Rz 2
[128] *Fabrizy*, StGB[9] (2006), § 165 Rz 2a
[129] *Fabrizy*, StGB[9] (2006), § 165 Rz 4

Verwerten und einem Dritten Übertragen eines Vermögensbestandteils aus einer Vortat (s Rz2) – ***ohne Verschleierung seiner Herkunft*** *– unter Strafe.“*[130]

[130] *Fabrizy*, StGB[9] (2006), § 165 Rz 3

5. Tainted Coins und Geldwäsche

In diesem Zusammenhang sind „tained coins“ (verdorbene Münzen) zu erwähnen. Diese Coins können auf Grund der gegebenen Transparenz in Verbindung mit kriminellen Tätigkeiten gebracht werden und sind somit gebrandmarkt. Nun werden diese mit „untained coins“ vermischt damit die „tained coins“ nunmehr zu einem geringeren Grad verdorben sind. Ziel ist die Häufigkeit der Durchmischung und die Intransparenz der Zahlungsabläufe zu steigern um den Taintedness-Grad gegen Null streben zu lassen. Nun stellt sich die Frage weshalb dieser Vorgang betrieben wird. Ein ausschlaggebendes Kriterium ist die Verschleierung der Mittelherkunft. Darüber hinaus kann es ein, dass Tauschbörsen einen zu starken „getainted Coin“ ablehnen. Bei der virtuellen Währung Bitcoin sind die meisten Coins zu einem ganz minimalen Anteil „getainted“.[131]

Im Falle der Nutzung von tainted coins, welche aufgrund ihrer Verwendung im virtuellen Schwarzmarkt Silk Road getainted wurden, lässt es sich nicht bestimmen, ob diese dort zu illegalen Zwecken verwendet wurden. Die Silk Road war ein illegaler Online-Marktplatz in dem Bitcoin als Zahlungsmittel zur Anwendung kam. Die Plattform bot jedoch sowohl illegale als auch legale Produkte und Dienstleistungen an, weshalb keine Aussage darüber getroffen werden kann ob illegale oder legale Transaktionen vorlagen bzw. vorliegen.[132]

In diesem Zusammenhang kann das Vorliegen eines Vorsatzes auf die Verwirklichung der Geldwäscherei in den meisten Fällen (§ 7 Abs 1 StGB) ausgeschlossen werden. Ferner ist das Vorliegen eines Eventualvorsatzes zu prüfen. Grundsätzlich bedingt Eventualvorsatz die Annahme, dass ein Sachverhalt auch wirklich eintreten kann und die Person sich damit abfindet.[133] Wie im oberen Absatz beschrieben ist es nicht möglich zu bestimmen ob ein „tainted coin“ aus einer kriminellen Aktivität herrührt, es lässt sich nur bestimmen, ob der Coin vom virtuellen Schwarzmarkt stammt oder nicht, was jedoch damit gekauft wurde kann nicht bestimmt werden.[134] Es können zahlreiche legale Produkte und Dienstleistungen auf der Silk Road gekauft werden. Die Annahme, dass ein Coin, nur weil er von der Silk Road stammt, aus illegalen Handlungen herrührt, kann nicht bestätigt werden, so Florian Wimmer, Gründer von Blockpit, welcher folgende Auffassung teilt: „Da Kryptowährungen wie z.B. der Bitcoin nicht eindeutig identifizierbar sind, so wie wir das von Geldscheinen kennen (Registrierungsnummer), ist es unmöglich zu bestimmen, ob ein Bitcoin aus dem

[131] *Hosp,* Kryptowährungen, (2018) 153.
[132] *DOLLIVER/ERICSON/LOVE,* A GEOGRAPHIC ANALYSIS OF DRUG TRAFFICKING PATTERNS ON THE TOR NETWORK, *https://onlinelibrary.wiley.com/doi/epdf/10.1111/gere.12241,* (49), (abgefragt am 3. Oktober 2018).
[133] *Maleczky,* Strafrecht Allgemeiner Teil[8] 12ff
[134] *DOLLIVER/ERICSON/LOVE,* A GEOGRAPHIC ANALYSIS OF DRUG TRAFFICKING PATTERNS ON THE TOR NETWORK, *https://onlinelibrary.wiley.com/doi/epdf/10.1111/gere.12241,* (49), (abgefragt am 3. Oktober 2018).

Schwarzmarkt oder aus Geldwäschegeschäften stammt. Da sich Transaktionen über die Blockchain öffentlich zurückverfolgen lassen, ist es zu einem gewissen Grad möglich, die Herkunft zu ermitteln, jedoch ist ein Bitcoin bis auf acht Kommastellen teilbar. Hier stellt sich die Frage, ab wann ein Bitcoin als Schwarzgeld einzustufen ist, wenn er zu 51% aus dubiosen Quellen stammt? Zu 100%? Zu 1%? Selbst wenn es hier eine Richtlinie geben würde, sprechen wir nur von Bitcoin."[135] Darüber hinaus gibt es zahlreiche andere virtuelle Währungen, dessen oberstes Ziel die vollkomme Privatsphäre, durch Verschleierung von Absender / Empfänger und der Assetmenge im Transaktionsprotokoll ist.[136] An dieser Stelle ist zu erwähnen, dass Geldwäsche auch dann vorliegt, wenn nur ein Bruchteil des Bitcoins „Schwarzgeld" ist. Es hängt immer vom subjektiven Tatbestand ab. Bei entsprechendem Vorsatz ist es irrelevant ob 1%, 51% oder 100% aus illegalen Quellen stammen.[137]

Als letzte Möglichkeit muss das mögliche Vorliegen von Fahrlässigkeit in Bezug auf tainted coins gemäß § 6 Abs 2 StGB geprüft werden. Hier stellt sich die Frage ob ein Laie bzw. Nutzer über das entsprechende Know-How verfügt um bestimmen zu können, ob ein tainted coin aus dem „Schwarzmarkt" stammt oder nicht. Bei Unternehmen, die über entsprechendes Know-How und Tools verfügen, könnte bei Annahme von tainted coins mitunter der Tatbestand Fahrlässigkeit vorliegen.[138] Im Kapitel 11.4 werden drei der am meisten verwendeten anonymen Kryptowährungen im Detail beschrieben.

[135] *Florian Wimmer,* CEO, Co-Founder, Interview geführt von Marina Kindel (22. Juli 2018).
[136] *Florian Wimmer,* CEO, Co-Founder, Interview geführt von Marina Kindel (22. Juli 2018).
[137] *Andreas* Pfeil *LL.M.* Interview geführt von Marina Kindel (4. Oktober 2018).
[138] *Maleczky,* Strafrecht Allgemeiner Teil[8] 12ff.

6. Hintergrund 5. Geldwäscherichtlinie

6.1. Begriffsabgrenzung

Es sollten die Begriffe DLT, Blockchain-Technologie und virtuelle Währungen voneinander abgegrenzt werden: „*DLT ist also ein digitales System zur Erfassung von Transaktionen der Assets. Dazu werden die Daten einer Transaktion im Detail erfasst und an mehreren Orten gleichzeitig gespeichert. Im Gegensatz zu traditionellen Datenbanken verfügen verteilte Ledger über keine zentrale Datenspeicher- oder Verwaltungsfunktionalität"*[139] Die Aufgabe eines Knotens ist die Verifizierung und Verarbeitung von Transaktionen wodurch diese aufgezeichnet wird um eine Einigkeit der Wahrhaftigkeit zu erlangen.[140]
Die Blockchain ist nur ein Teilbereich der DLT bei der[141] *„... Transaktionen oder auch andere Daten in Blöcken zusammengefasst und an eine Kette von bereits verifizierten Blöcken angehängt wird*."[142] Es stellt somit *„... eine vollständige und unveränderliche Transaktions-Historie zu allen Transaktionen einer dezentralen Community, der jeder, der ein Teil davon ist, zustimmt."*[143] Eine virtuelle Währung ist somit eine Applikation der Blockchain - Technologie, die dezentral und digital ist und durch kryptografische Verfahren gesichert wird. Kryptographie, bestehend aus Ziffern und Buchstaben, spielt eine unabdingbare Rolle bei virtuellen Währungen. Ein[144] *„... Private Key signiert (eine kryptographische Funktion, bei der der Private Key mit einer anderen Zeichenfolge kombiniert wird, wodurch eine völlig neue, einzigartige Zeichenfolge entsteht) eine andere Folge aus neuen Zahlen und Buchstaben, ..."*[145] Die Text-ID ist das Ergebnis dieser „Unterzeichnung" und stellt eine vollkommen neue und unverwechselbare Zeichenfolge dar. Diese wird durch die Miner mit der Public-Address abgeglichen und verifiziert. Nun wird von den Minern versucht[146] *„... einen Block zu finden, indem sie den Hash, Zeichenfolge, des alten Blocks mit allen inkludierten Tx-IDs des aktuellen Blocks und der Nonce zu hashen und dabei eine Merkle – Root mit einer bestimmten Anzahl an Nullen zu finden."*[147] Jeder Hash entspricht einer neuen Zeichenfolge wodurch ein Block[148] *„... also nichts anderes als diese Zeichenfolge, in die unzählig viele andere Zeichenfolgen integriert sind"*[149] *ist.*

[139] *Negin,* Distributed Ledger Technologie (DLT) ist mehr als Blockchain, https://blockchainwelt.de/dlt-distributed-ledger-technologie-ist-mehr-als-blockchain/ (Stand 16.2.2018).
[140] *Negin,* Distributed Ledger Technologie (DLT) ist mehr als Blockchain, (Stand 16.2.2018).
[141] *Negin,* Distributed Ledger Technologie (DLT) ist mehr als Blockchain, (Stand 16.2.2018).
[142] *Negin,* Distributed Ledger Technologie (DLT) ist mehr als Blockchain, (Stand 16.2.2018).
[143] *Hosp,* Kryptowährungen. (2018) 45.
[144] *Hosp,* Kryptowährungen, (2018) 84.
[145] *Hosp,* Kryptowährungen, (2018) 84.
[146] *Hosp,* Kryptowährungen, (2018) 84.
[147] *Hosp,* Kryptowährungen, (2018) 84.
[148] *Hosp,* Kryptowährungen, (2018) 84.
[149] *Hosp,* Kryptowährungen, (2018) 84.

Im Kapitel 11 wird auf die unterschiedlichen Verschlüsselungstechniken virtueller Währungen eingegangen und dargelegt in welchen Maß sich diese für Geldwäscheaktivitäten eignen.

6.2. Vorschlag zur 5. Geldwäscherichtlinie

Obwohl die erste Kryptowährung, Bitcoin, bereits 2008 entwickelt wurde, kommt der Terminus in der 4. Geldwäscherichtlinie (GwR)[150] nicht vor. Erst im Vorschlag zur 5. Geldwäsche-Richtlinie[151] der am 05.07.2016 veröffentlicht wurde wird auf den Begriff virtuelle Währung im Zusammenhang mit Geldwäsche näher eingegangen. Es wird darauf aufmerksam gemacht, dass es auf Grund technologischer Fortschritte neue Möglichkeiten gibt das Finanzsystem zu Zwecken der Terrorismusfinanzierung und der Geldwäsche auszunutzen. Diese Lücken gilt es, durch geeignete Kontroll- und Analyseinstrumente, zu schließen. Weder die Grundrechte der Bürger, noch die Funktionalität der Zahlungs- und Finanzmärkte sollen beeinträchtigt werden. Die Änderungen der 4. Geldwäscherichtlinie erfolgen auf Grundlage der Art 114 und 50 des Vertrages über die Arbeitsweise der europäischen Union (AEUV). Zudem wird ausdrücklich erwähnt, dass bestehende Vorschriften und Systeme sinnvoll ergänzt und verbessert werden sollen um eine Erhöhung der Transparenz in Bezug auf Mittelherkunft und Wirtschaftsteilnehmer zu erreichen.[152]
Es ist festzuhalten, dass trotz der Geldwäscherichtlinie virtuelle Tauschbörsen sowie Wallet Provider weiterhin auf Unionsebene unreguliert bleiben und somit keine regulierten Finanzdienstleistungen darstellen. Dies hat u.a. zur Folge, dass es keinen spezifischen Rechtsschutz für Nutzer gibt. Es besteht somit kein Schutz vor Veruntreuung, Cyberattacken, Insolvenz der Anbieter oder bei Vernichtung von Vermögenswerten.[153]

6.3. Erwägungsgründe

Die Entschließung des EU-Parlaments zu Kryptowährungen basiert unter Bezugnahme zahlreicher Ergebnisse von Berichten und Stellungnahmen u.a. von der FATF, ESMA, Europäischen Bankenaufsichtsbehörde, Kommission, Europol, OECD und Europäischen Zentralbank. Seit der Entwicklung von Bitcoin, der einen Marktanteil von 90% der virtuellen

[150] Richtlinie 2015/849 (EU) des europäischen Parlamentes und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl L 2015/141, 73.
[151] COM/2016/0450 final - 2016/0208 (COD).
[152] COM/2016/0450 final - 2016/0208 (COD).
[153] *ESMA,EBA,EIOP,* Warnmeldung, Ahttps://eiopa.europa.eu/Publications/Other%20 Documents/Joint%20ESAs%20Warning%20on%20Virtual%20Currencies_DE.pdf (abgerufen am 24.07.2018).

Währungen aufweist und einen Marktwert von 5 Milliarden Euro hat, wurden bereits weitere 600 Kryptowährungen geschaffen. Virtuelle Währungen basieren auf der DLT und die Investitionssumme in diesem Bereich beträgt rund 1 Milliarde EUR (Stand 2016). Zudem werden Transaktionen exorbitant schnell verarbeitet und weisen eine hohe Transformationskapazität auf. Obwohl keine allgemein gültige Begriffsbestimmung vorliegt, werden Kryptowährungen als digitales Bargeld bezeichnet und von natürlichen/ juristischen Personen als Zahlungsmittel akzeptiert. Es wird festgehalten, dass virtuelle Währungen weder von einer Zentralbank noch von einer öffentlichen Stelle ausgegeben werden, aber als Darstellung eines digitalen Wertes Seitens der Europäischen Bankaufsichtsbehörde deklariert werden. Das Europäische Parlament weist auf vorhanden Chancen und Gefahren der DLT hin und erkennt zudem das Innovationspotenzial der DLT über den Zahlungsbereich hinaus an und spricht sich für eine intelligente Regulierung und Förderung der Technologie aus.[154]

6.4. Sicherheitsagenda

In der Sicherheitsagenda [155] wird auf die Wichtigkeit der Rückverfolgbarkeit von Finanzgeschäften aufmerksam gemacht, um terroristischer Netze leichter aufdecken zu können. Es sollen neue Rahmenbedingungen geschaffen werden, um eine Steigerung der Transparenz des Geldtransfers zu erreichen und den Möglichkeiten des Missbrauches entgegen zu wirken. Es wird explizit erwähnt, dass der Finanzierung von terroristischen Akten mit Hilfe von virtuellen Währungen entgegengesteuert werden muss.
Auch auf die Gefahren der Internetkriminalität wie z.B. „Cloud-Computing“ und „Internet of Things“ wird eingegangen, was jedoch für den Inhalt dieser Arbeit von keiner Relevanz ist. Die geltenden Rechtsvorschriften müssen auf Grund technischer Veränderungen schnell ergänzt werden können und ein grenzüberschreitender Zugriff auf Informationen muss ermöglicht werden.[156]

6.5. Aktionsplan

Bezugnehmend auf die Sicherheitsagenda verdeutlicht zudem der Aktionsplan [157] die Notwendigkeit der Rückverfolgung von Finanzströmen. Es wird von einer erhöhten Gefahr der Verschleierung der Mittelherkunft in Bezug auf Umtausch-Plattformen ausgegangen, bei

[154] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[155] Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen Die europäische Sicherheitsagenda, COM (2015) 185 final am 28.4.2015.
[156] COM (2015) 185 final am 28.4.2015.
[157] Mitteilung der Kommission an das europäische Parlament und den Rat Ein Aktionsplan für ein intensiveres Vorgehen gegen Terrorismusfinanzierung COM (2016) 50 final am 2.2.2016.

denen aktuell keine Berichtspflichten und Identifikationspflichten, wie es bei normalen Bankensystemen verlangt wird, bestehen.

Eines der Ziele des Plans ist es Terroristen bzw. terroristische Netzwerke[158] *„…von ihren Finanzquellen abzuschneiden, ihnen die heimliche Nutzung der Mittel zu erschweren, und die aus dem Finanzierungsprozess gewonnenen Informationen bestmöglich zu nutzen …“*[159] Neue technologische Trends fördern die Verschleierung der Mittelherkunft und erschweren die Terrorismusbekämpfung. Durch die Möglichkeit einer pseudoanonymen Nutzung entstehen Schlupflöcher, die es durch einheitliche EU-Rahmenbedingungen zu beseitigen gilt. Es wird erwähnt, dass die EU-Kommission Drittländer mit strategischen Mängeln benennen wird, gegenüber denen besondere Sorgfaltspflichten herrschen werden. Bevor die 5. Geldwäscherichtlinie veröffentlicht wurde, kam bereits eine Definition von Umtausch-Plattformen und Kontenanbietern im Aktionsplan vor[160] : *„Umtausch – Plattformen für virtuelle Währungen können als elektronische Umtauschbüros betrachtet werden, in denen virtuelle in richtige Währungen und zurück getauscht werden. Kontoanbieter sind Einrichtungen, die auf eine virtuelle Währung lautende Konten für ihre Kunden führen, und die ähnlich wie Banken funktionieren, die Sichtkonten in reale Währungen führen. Sie speichern Beträge in virtuellen Währungen und führen Überweisungen auf andere virtuelle Währungen lautende Konten aus.“*[161] Diese Definitionen kann als Leitgedanke für die Begriffsbestimmungen der 5. Geldwäscherichtlinie, welche im Kapitel 3.1. näher erörtert werden, verstanden werden.

6.6. Bericht virtuelle Währungen

Der Bericht des Ausschusses für Wirtschaft und Währung[162] vom 3. Mai 2016 hebt sowohl positive als auch negative Aspekte und notwendige Leitfäden im Zusammenhang mit virtuellen Währungen hervor. Distributed-Ledger-Technology sowie die Blockchain-Technologie wird als immenses Potenzial für den Wirtschafts- und Finanzsektor beschrieben. Zudem wird auf die positiven Eigenschaften, wie niedrigere Transaktionskosten und den Schutz der Privatsphäre hingewiesen. Es sollen Systeme entstehen, die einerseits die Privatsphäre der Nutzer schützen und andererseits eine 100 % Anonymität der Nutzer entgegensteuern. Der Vorschlag der Kommission Plattformen, die Kryptowährungen in ein staatlich anerkanntes Zahlungsmittel und umgekehrt tauschen, in die 5. Geldwäscherichtlinie

[158] COM (2016) 50 final am 2.2.2016.
[159] COM (2016) 50 final am 2.2.2016.
[160] COM (2016) 50 final am 2.2.2016.
[161] COM (2016) 50 final am 2.2.2016.
[162] Bericht über virtuelle Währungen BlgEP A8-0168/2016.

aufzunehmen wird begrüßt, da zumindest die damit verbundene Anonymität beendet werden kann.[163] Ferner wird auch von Seiten des Europäischen Parlaments dieser Vorschlag begrüßt. Das Europäischen Parlaments[164] *„… begrüßt die von der Kommission vorgeschlagene Einbeziehung von Plattformen zum Tausch von virtuellen Währungen in die Richtlinie zur Bekämpfung der Geldwäsche (AMLD), damit der mit solchen Plattformen verbundenen Anonymität ein Ende bereitet werden kann"* (Erwägungsgrund 20).[165] Überdies wird in dem Bericht auf das Fehlen traditioneller Formen der Aufsicht, des Nutzerschutzes sowie rechtlicher Bestimmungen aufmerksam gemacht. Dennoch wird verdeutlicht, dass die rechtlichen Rahmenbedingungen unbedingt im Einklang mit der Innovation stehen müssen und bei Systemrelevanz eine verhältnismäßige Anpassung auf EU-Ebene erfolgen soll, da eine zu starke Regulation der Innovation schaden kann.[166] In diesem Zusammenhang sind auf die Termini „Smart Regulation" und „Sandboxes" aufmerksam zu machen, welche im Kapitel 7 und 10 näher erörtert werden.

Zudem wird auf das Risiko von eingeschränkter Rückverfolgbarkeit von Transaktionen hingewiesen wobei erwähnt wird, dass die Rückverfolgung von Bargeld-Transaktionen schwieriger sei als jene von virtuellen Währungen.[167]

Die Annahme, dass virtuelle Währungen Großteils nur für illegale Aktivitäten verwendet werden und sich diese besser für Geldwäsche eignen als andere Finanzprodukte sei falsch, so Florian Wimmer, Gründer von Blockpit: „Im Gegensatz zu Bargeld weisen Kryptowährungen einen digitalen Fingerprint auf, welcher (wenn auch durch hohen Ressourcenaufwand) zu einem gewissen Grad nachverfolgt werden kann."

Einerseits wird explizit auf die Gefahr von kriminellen Handlungen wie Schwarzmarkt-Transaktionen im Zusammenhang mit Kryptowährungen hingewiesen, andererseits auf das Potenzial der Distributed-Ledger-Technologie (DLT) Geldwäsche, Betrug und Korruption verringern zu können.

Die Kommission, die Mitgliedsstaaten und Vertreter der Branche sollen Informations- und Aufklärungsarbeit gegenüber Nutzern betreiben um die Transparenz des Systems zu steigern. Es soll eine Arbeitsgruppe, Task Force, bestehend aus Experten geründet werden, die von der Kommission geleitet werden soll.

Der Ausschuss für Binnenmarkt und Verbraucherschutz hat zu diesem Bericht Stellung genommen und betont, dass einerseits die Risiken in Zusammenhang mit virtuellen

[163] Bericht über virtuelle Währungen BlgEP A8-0168/2016.
[164] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[165] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[166] Bericht über virtuelle Währungen BlgEP A8-0168/2016.
[167] Bericht über virtuelle Währungen BlgEP A8-0168/2016.

Währungen wie Cyberkriminalität, Terrorismus und Geldwäsche nicht unterschätzt werden dürfen, andererseits die Innovation nicht gebremst werden darf. Es wird darauf hingewiesen, dass virtuelle Währungen ein Risiko für die Integrität und Stabilität des bestehenden Finanzsystems darstellen.[168]

Abschließend weißt der Ausschuss darauf hin[169], *„… dass es kaum Anzeichen dafür gibt, dass virtuelle Währungen in großem Umfang als Zahlungsmittel für kriminelle Tätigkeiten genutzt wurden, und dass Bargeld in der Regel viel schwieriger zurückzuverfolgen ist ….“*[170] Dieser Standpunkt wird auch im EU-Bericht vom 26.6.2017 verdeutlicht.

6.7. Bericht der Kommission an das europäische Parlament vom 26.06.2017

Im EU-Bericht[171] vom 26.6.2017 wird verdeutlicht, dass Transaktionen mit Bargeld weiterhin die beste Möglichkeit für Geldwäscheaktivitäten darstellen, da die Anonymität uneingeschränkt gegeben ist. Zudem gibt es Faktoren die Geldwäsche mit Hilfe von Kryptowährungen erschweren. Üblicherweise ist die Höhe einzelner Transaktionen geringer als bei Bargeldtransaktionen und in einem gewissen Umfang überwachbar.[172] Auf die Transparenz von Transaktionen wird im Kapitel 11. eingegangen.

6.8. Fin Tech Aktionsplan

Zum Verständnis sollte der Begriff Fin Tech näher erklärt werden: *„…“FinTech bezeichnet technologiegestützte Innovationen bei Finanzdienstleistungen, die neue Geschäftsmodelle, Anwendungen, Prozesse oder Produkte hervorbringen und die Finanzmärkte und -institute sowie Art und Weise, wie Finanzdienstleistungen erbracht werden, erheblich beeinflussen könnten.“*[173] Unter diesen Begriff „Fin Tech“ fällt die Distributed-Ledger Technologie sowie die auf diesem Konzept aufbauende Blockchain-Technologie.[174] Im Aktionsplan wird von einem hohen bis sehr hohen Risiko im Zusammenhang mit virtuellen Währungen und Geldwäsche ausgegangen. Die europäische Kommission hat zudem die Ausschreibung einer Warnung für Nutzer veranlasst. Dennoch wird in dieser Mitteilung, Fin Tech Aktionsplan,

[168] Bericht über virtuelle Währungen BlgEP A8-0168/2016.
[169] Bericht über virtuelle Währungen BlgEP A8-0168/2016.
[170] Bericht über virtuelle Währungen BlgEP A8-0168/2016.
[171] Bericht der Kommission an das europäische Parlament und den Rat über die Bewertung der mit grenzüberschreitenden Tätigkeiten im Zusammenhang stehenden Risiken der Geldwäsche und Terrorismusfinanzierung für den Binnenmarkt. COM (2017) 340 final vom 26.6.2017.
[172] COM (2017) 340 final vom 26.6.2017.
[173] Mitteilung der Kommission an das europäische Parlament, den Rat, die europäische Zentralbank, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen Fin Tech- Aktionsplan: Für einen wettbewerbsfähigeren und innovativeren EU-Finanzsektor , COM (2018) 109 final am 8.3.2018.
[174] *Negin,* Distributed Ledger Technologie (DLT) ist mehr als Blockchain, (Stand 16.2.2018).

auch das Potenzial der Technologie hervorgehoben, welches dazu beitragen kann, dass Europa zukünftig zu den führenden Akteuren der Finanzbranche zählt. Durch Zusammenarbeit der Kommission und Normierungseinrichtungen werden bis zum Ende des Jahres Vorschläge für Fin Tech Normen vorgebracht. Aktuell bestehen in 13 EU-Mitgliedstaaten „FinTech-Moderatoren", die dazu dienen Firmen bei der Zulassung zu unterstützten. Initiativen zur Innovationsförderung von Seiten der Kommission werden eingeleitet, da auch die Marktattraktivität in anderen Teilen der Welt berücksichtigt werden muss.[175] *„Das Fehlen klarer und harmonisierter Verfahren zur Online-Identifizierung von Verbrauchern und Unternehmen unter uneingeschränkter Beachtung der Geldwäsche- und Datenschutzvorschriften wurde auch als Herausforderung für FinTech-Lösungen bezeichnet"*[176]

Bis Ende 2019 wird geprüft, ob die geforderten Regulierungen für Finanzinnovationen Hemmnisse darstellen. Es wird gefordert, dass Unternehmen, Innovatoren und Behörden zusammenarbeiten, um die Technologieinnovationen zu fördern. Im Fin Tech Aktionsplan wird vor allem auf die positiven Eigenschaften der DLT und BC-Technologie per se nicht jedoch auf die von virtuellen Währungen hingewiesen.[177]

[175] COM (2018) 109 final am 8.3.2018, ABl C 109.
[176] COM (2018) 109 final am 8.3.2018, ABl C 109.
[177] COM (2018) 109 final am 8.3.2018, ABl C 109.

7. Smart Regulation

7.1. Smart Regulation – de lege ferenda

In Anlehnung an den minimalistischen Ansatz von Regulierungen wird von dem Terminus „Smart Regulation" gesprochen. Die Motivation der Gefahrenvermeidung im öffentlichen Interesse bedingt oftmals massive Grundrechtseingriffe. Jede Technologie kann nicht nur für den angedachten Zweck, sondern auch missbräuchlich verwenden werden. Eine vollständige Ausschaltung dieser Problematik kann durch ein Regelwerk nicht gegeben werden. Die Menschheit selbst stellt die Gefahrenquelle dar, bei dem jedes Individuum selbst entscheidet ob es rechtskonform handelt oder nicht. Das Existieren von Gefahren muss in jedem Regelwerk berücksichtigt werden und eine verhältnismäßige Regulierung als Gegenstand haben. Die Feststellung der Tatsache, dass Technologien per se Gefahren in sich bergen kann jedoch keine Grundlage für Verbote oder massive Regulierungen bilden.[178] „ *Der Schutz öffentlicher Interessen ist stets mit geeigneten sowie mit verhältnismäßigen, angemessenen, also möglichst* ***eingriffsfernen Mitteln*** *zu bewerkstelligen, die im Zweifel den gelindesten denkbaren Maßnahmenkatalog darstellen."*[179] Sämtliche regulatorische Maßnahmen auf nationaler sowie auf EU-Ebene sind einer Prüfung der Verhältnismäßigkeit zu unterziehen.[180] Auch in der Mittteilung des Europäischen Parlaments[181] wird eine intelligente Regulierung mit *„... einen verhältnismäßigen regulatorischen Ansatz auf EU-Ebene, damit Innovationen nicht im Keim erstickt werden und in dieser frühen Phase keine unnötigen Kosten entstehen ..."*[182] verlangt (Erwägungsgrund 9). Oftmals werden die Probleme die durch zu starke Regulation verursacht werden von Seiten der Regierung in den Hintergrund gedrängt, da der Bevölkerung das Gefühl von Sicherheit vermittelt werden soll. Zu starke regulatorische Maßnahmen können innovationsfeindlich sein, zur Unübersichtlichkeit des Rechtssystems beitragen und schlussendlich zur Beschränkung der Freiheitssphäre der Bevölkerung und der Wirtschaftseilnehmer führen. Die bereits bestehenden Gesetze, sowohl auf nationaler als auch auf europäischer Ebene müssen eingehend überprüft werden. Vor allem bei virtuellen Währungen sind diese zu prüfen um die Technologie durch Überregulation nicht zu gefährden. Eine Überregulation in diesem Bereich ist deutlich zu verneinen. Es gilt bestehende Gesetze des Wirtschafts- und Privatrechts eingehend zu untersuchen und stets

[178] *Piska / Völkel,* Blockchain und Kryptorecht Regulierungs- Chancen de lege lata und de lege ferenda, ZTR 2017 97.
[179] *Piska / Völkel,* ZTR 2017 97.
[180] *Piska / Völkel,* ZTR 2017 97.
[181] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[182] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.

einen minimalistischen Ansatz zu wählen. Bestehendes Rechtsmaterial soll nutzbar gemacht werden.[183]

Aktuell liegt der Fokus auf der Entwicklung eines geeigneten Rahmenwerkes für die Bekämpfung von Geldwäscheaktivitäten durch Verwendung virtueller Währungen. Obwohl die ersten Schritte - aus privat und öffentlich-rechtlicher Sicht getan sind - sind diese dennoch durch Unsicherheit, fehlende Forschungsergebnisse und fehlendes technisches Know-How geprägt.[184]

7.2. Smart Regulation – Gewerbeordnung

Am 23. Mai 2018 erfolgte eine parlamentarische Anfrage[185] an das Bundesministerium für Wissenschaft, Forschung und Wirtschaft (BMWFW). Der Inhalt der Anfrage war u.a. ob der Handel mit Bitcoin dem Gewerberecht zu unterstellen ist. Das BMWFW teilte mit: *„Ein Handelsgeschäft, das der Gewerbeordnung 1994 unterliegt, setzt eine Handelsware als Geschäftsgegenstand voraus, die einen Gebrauchsnutzen zum Gegenstand hat. Das bedeutet, dass die primär anderen Zwecken als dem Eintausch gegen eine andere Ware dient, womit der Nutzen im Gegenstand selbst liegt und nicht in dessen Eintausch.“*[186] Zahlungsmittel dessen primärer Zweck der Austausch gegen eine Ware ist stellen somit keine Handelsware dar: [187] *„Bitcoins besitzen offensichtlich den spezifisch für eine Währung bzw. ein Zahlungsmittel charakteristischen Austauschzweck, hingegen fehlt ihnen jeder eigene Gebrauchsnutzen im oben beschriebenen Sinn.“* [188] Aus diesem Grund kann kein Handelsgeschäft im Sinne des Gewerberechts vorliegen. Auch wenn kein Handelsgewerbe gemäß der Gewerbeordnung vorliegt, ist dennoch die Anwendbarkeit des Gesetzes nicht zu verneinen.[189] Der Geltungsbereich der Gewerbeordnung wird in § 1. GewO geregelt: *„ Dieses Bundesgesetz gilt, soweit nicht die §§ 2 bis 4 anderes bestimmen, für alle gewerbsmäßig ausgeübten und nicht gesetzlich verbotenen Tätigkeiten.“* (§ 1 Abs GewO). Da virtuelle Währungen nicht unter die allgemeinen Ausnahmentatbestände fallen und überdies keine sondergesetzlichen Ausnahmen für die gewerbliche Tätigkeit VW bestehen ist die Anwendbarkeit der Gewerbeordnung gegeben. Auch wenn Geschäftsmodelle mitunter der Konzessionierung unterliegen, begründet dies nicht einen allgemeinen Ausnahmetatbestand.

[183] *Piska / Völkel,* ZTR 2017 97.
[184] *Piska / Völkel,* ZTR 2017 97.
[185] *Alm,* Anfrage 1578 vom 23.05.2018 (XXV. GP), https://www.parlament.gv.at/PAKT/VHG/XXV/J/J_01578/fname_351518.pdf, (abgerufen am 20. August 2018).; *Bundesministerium für Wissenschaft, Forschung und Wirtschaft, 1446/AB vom 22.07.2014 zu 1578/J (XXV.GP),*
[186] *Bundesministerium für Wissenschaft, Forschung und Wirtschaft,* 1446/AB vom 21.07.2014 zu 1578/J (XXV.GP), (Stand 22.7.2014).
[187] *Bundesministerium für Wissenschaft, Forschung und Wirtschaft,* 1446/AB vom 21.07.2014 zu 1578/J (XXV.GP), (Stand 22.7.2014).
[188] *Bundesministerium für Wissenschaft, Forschung und Wirtschaft,* 1446/AB vom 21.07.2014 zu 1578/J (XXV.GP), (Stand 22.7.2014).
[189] *Piska / Völkel,* ZTR 2017 97.

Zudem sind die Ausnahmentatbestände[190] *„ ... für den Betrieb von Bankgeschäften, Dienstleistungen nach dem WAG 2007, Zahlungsinstituten oder E-Geld-Instituten vorbehaltenen Geschäfte (§ 2 Abs 2 Z 14 GewO) nicht allgemein einschlägig ...“*[191]

Ferner muss die Möglichkeit der Subsumierung des Handels mit Kryptowährungen in das freie Gewerbe betrachtet werden. Die Gewerbeordnung differenziert zwischen dem reglementierten, bei dem ein Befähigungsnachweis erforderlich ist, und dem freien Gewerbe. Im Gegensatz zum reglementierten Gewerbe ist beim freien Gewerbe kein Befähigungsnachweis für die Ausübung der Tätigkeit erforderlich.[192]

Das BMFWF hat eine Bundeseinheitliche Liste der freien Gewerbe ausgegeben. In dieser Liste wird festgehalten, dass das[193] *„ ... Handelsgewerbe mit Ausnahme der reglementierten Handelsgewerbe ...auch den Verkauf elektronischer Medien ohne Datenträger ...“*[194] umfasst. Diese Qualifizierung trifft auf Kryptowährungen zu. Zudem werden Kryptowährungen, wie bereits in Kapitel 3. erwähnt, von Seiten der FMA als Waren bzw. von Seiten des Bundesministeriums für Finanzen als Wirtschaftsgüter klassifiziert.[195]

Ein freies Gewerbe wird gemäß der Gewerbeordnung wie folgt bestimmt: *„Freie Gewerbe sind Tätigkeiten im Sinne des § 1 Abs. 1, die nicht als reglementierte Gewerbe (§ 94) oder Teilgewerbe (§ 31) ausdrücklich angeführt sind. Unbeschadet allfälliger Ausübungsvorschriften ist für freie Gewerbe kein Befähigungsnachweis zu erbringen*“ (§ 5(2) GewO**.**

Es ist festzuhalten, dass der Handel oder sonstige gewerbliche Tätigkeiten die in Verbindung mit Kryptowährungen stehen nicht unter den in § 94 GewO aufgezählten reglementierten Gewerben vorzufinden sind und es sich somit um ein freies Gewerbe handelt. Somit würde für Unternehmen die mit virtuellen Währungen handeln die KYC/AML Bestimmungen der §§ 365m. bis 365z. GewO Anwendung finden. Voraussetzung dafür ist jedoch, dass Handelsgewerbetreibende *„... Zahlungen von mindestens 10 000 Euro in bar tätigen oder entgegennehmen, unabhängig davon, ob die Transaktion in einem einzigen Vorgang oder in mehreren Vorgängen, zwischen denen eine Verbindung besteht oder zu bestehen scheint, getätigt wird; ...“* (§ 365m1. (2) Z 1 GewO).

---

[190] *Piska / Völkel,* ZTR 2017 97.
[191] *Piska / Völkel,* ZTR 2017 97.
[192] *Andreas Pfeil LL.M.* Interview geführt von Marina Kindel (4. Oktober 2018).
[193] *Bundesministerium für Wissenschaft, Forschung und Wirtschaft,* Bundeseinheitliche Liste der freien Gewerbe, https://www.bmdw.gv.at/Unternehmen/Gewerbe/Documents/Bundeseinheitliche_Liste_der_freien_Gewerbe.pd, (Stand: 20. Oktober 2017).
[194] *Bundesministerium für Wissenschaft, Forschung und Wirtschaft,* Bundeseinheitliche Liste der freien Gewerbe, (abgerufen am 22. August 2018).
[195] *Piska / Völkel,* ZTR 2017 97.

Dem Gesetz ist nicht zu entnehmen was unter „bar“ zu verstehen ist. Es werden die in der Bankenbranche üblichen Anschauen herangezogen.[196] Zudem liegt auch eine Barzahlung vor, wenn nur ein Teilbetrag in Barzahlung erfolgt und der Rest durch bankmäßige Überweisung erfolgt. Überweisungen im herkömmlichen Sinn, vom Bankkonto des Käufers an den Verkäufer, stellen keine Barzahlungen dar.[197]

Die in § 365m GewO bis § 365 z GewO Pflichten bestehen auch dann, wenn eine Verbindung zwischen mehrere Transaktionen besteht oder eine solche vermutet wird. Es besteht eine Zusammenrechnungspflicht. Die Pflicht besteht also schon dann, wenn lediglich eine Vermutung einer Verbindung zwischen mehreren Geschäften besteht, wenn diese z.B. zum selben Kunden zurechenbar sind.[198]

Unter gewerbsmäßig wird gemäß § 1 der GewO folgendes verstanden: *„Eine Tätigkeit wird gewerbsmäßig ausgeübt, wenn sie selbständig, regelmäßig und in der Absicht betrieben wird, einen Ertrag oder sonstigen wirtschaftlichen Vorteil zu erzielen, gleichgültig für welche Zwecke dieser bestimmt ist; hiebei macht es keinen Unterschied, ob der durch die Tätigkeit beabsichtigte Ertrag oder sonstige wirtschaftliche Vorteil im Zusammenhang mit einer in den Anwendungsbereich dieses Bundesgesetzes fallenden Tätigkeit oder im Zusammenhang mit einer nicht diesem Bundesgesetz unterliegenden Tätigkeit erzielt werden soll.“* Die freien und reglementierten Handelsgewerbe werden in § 154 GewO geregelt.[199] Zudem erfolgt die Abgrenzung des Begriffes Handels: *„Handel iSd GewO ist die auf den Warenaustausch zwischen einzelnen Wirtschaftsmitgliedern gerichtete Tätigkeit, wobei bereits dem Erwerb der Ware der Zweck der Weiterveräußerung zu Grunde liegen muss.“*[200]

Die Gewerbeordnung nimmt eine Einteilung der Gewerbearten in reglementierte und freie Gewerbe vor. Für die Ausübung eines reglementierten Gewerbes ist die Erbringung eines Befähigungsnachweises obligatorisch. Bei einem Handelsgewerbe handelt es sich hingehen um ein freies Gewerbe, welches bei Vorliegen der allgemeinen gewerberechtlichen Voraussetzung und nach Anmeldung des Gewerbes, es dem Gewerbetreibenden erlaubt ohne Befähigungsnachweis den Handel mit Waren zu tätigen. Als Handel im Sinne der Gewerbeordnung ist eine auf den Warenaustausch gerichtete Tätigkeit zu verstehen. Kryptowährungen welche keine Rechte verkörpern, sind somit als Handelsware zu qualifizieren. Durch die sachenrechtliche Einordnung von Kryptowährungen ist der Handel mit Kryptowährungen unter das freie Handelsgewerbe zu subsumieren und folglich finden die

[196] *Grabler/Stolzechner/Wendl* GewO² (2018), § 365m. (Stand 27.9.2018, lexisnexis.at).
[197] *Grabler/Stolzechner/Wendl* GewO² (2018), § 365m.
[198] *Grabler/Stolzechner/Wendl* GewO² (2018), § 365m.
[199] *Stolzlechner/Seider/Vogelsang* GewO² (2018), § 154 (Stand 27.9.2018, lexisnexis.at).
[200] *Stolzlechner/Seider/Vogelsang* GewO² (2018), § 154.

geldwäscherechtlichen Bestimmungen der Gewerbeordnung auf Handelsgewerbetreibende Anwendung.[201]

Einen weiteren wichtigen Punkt stellen die Standes und Ausübungsregeln dar: *„Weiters kann der Bundesminister für Wissenschaft, Forschung und Wirtschaft nach Anhörung der zuständigen Gliederung der Bundeskammer der gewerblichen Wirtschaft durch Verordnung Regeln über die Verhaltensweisen, die bei der Ausübung eines bestimmten Gewerbes einzuhalten sind, und über die für die Gewerbeausübung erforderliche Betriebsausstattung festlegen (Standesregeln)*" bestimmen (§ 69 Abs 2 GewO). Um den Schutz des Vermögens oder der Privatsphäre zu garantieren sind Ausübungsregeln erforderlich. Kunden sollen ausreichen informiert sein, um Irreführung zu vermeiden. Aktuell herrscht von Seiten der Nutzer vorwiegend Unwissenheit in Bezug auf virtuelle Währungen. Viele Nutzer sind schlecht informiert, können die Gefahren wie z.B. den möglichen Totalverlust vom eingesetzten Kapital nicht abschätzen. Zudem wird oft fälschlicherweise gedacht, dass völlige Anonymität vorherrscht, obwohl z.B. bei Bitcoin sämtliche Transaktionen einsehbar sind. Auf der einen Seite kann auf Grund der genannten Gründe ein Regelwerk zum Schutz von Vermögensschäden erlassen werden und auf der anderen Seite ein Regelwerk zum Schutz der Privatsphäre. Die Ausübungs- sowie die Standesregeln können Basis für eine Smart Regulation sein und ein regulatorisches Rahmenwerk mit Augenmaß darstellen.[202]

Von einer Unterstellung in das Finanzmarkt-Geldwäschegesetz bzw. kapital- und finanzmarktrechtlichen Instrumenten wird ausdrücklich Abstand genommen. Eine Unterstellung in dieses Gesetz passt nicht zu den Eigenschaften und der Herkunft von virtuellen Währungen. Ferner würde dies die Innovation der Technologie nicht fördern und Österreich als Wirtschaftsstandort nicht stärken.[203]

[201] *Andreas Pfeil LL.M.* Interview geführt von Marina Kindel (4. Oktober 2018).
[202] *Piska / Völkel,* ZTR 2017 97.
[203] *Piska/Völkel,* ecolex 2018 671.

8. Analyse der Anwendbarkeit der Gewerbeordnung anhand des Unternehmens Coinfinity

Wie im Kapitel 7. bereits dargestellt ist aktuell eine eindeutige Rechtslage bezogen auf Dienstleister, die Kryptowährungen in ein anerkanntes Zahlungsmittel tauschen und umgekehrt, gegeben. Es gibt aktuell unterschiedliche Auffassungen, ob für solche Dienstleister die KYC/AML Bestimmungen des § 365m. bis 365z. GewO, auf Grund des Vorliegens eines freien Gewerbes, Anwendung finden oder nicht.

Die nachfolgende Analyse geht von der Annahme aus, dass aktuell keine Unterstellung der Gewerbeordnung vorliegt.

Viele Firmen der Branche wenden seit Jahren freiwillig KYC/AML Maßnahmen im Unternehmen an um Geldwäsche und Terrorismusfinanzierung vorzubeugen.

Die Analyse soll verdeutlichen wie der Status quo in der Branche ist, welche gesetzlichen Vorlagen für bereits entwickelte Maßnahmen herangezogen wurden bzw. herangezogen werden könnten und mit welchen Maßnahmen zukünftig Unternehmen konfrontiert sein werden. Es soll verdeutlicht werden, dass mit bereits existierenden Gesetzen umfassende Maßnahmen zur Prävention gegen Geldwäsche getroffen werden können und die Auffassung der Smart Regulation dadurch bestärkt wird. In diesem Teil der Arbeit wird vor allem die Möglichkeit betrachtet, dass Dienstleister die Kryptowährungen in Fiatgeld und umgekehrt tauschen zukünftig den Bestimmungen der Gewerbeordnung unterliegen.

Es erfolgt eine Analyse der unternehmensinternen Compliance und Geldwäschemaßnahmen von Coinfinity – einer der renommiertesten österreichischen Händler. Coinfinity ist ein Unternehmen zu dessen obersten Zielen die Einhaltung bestehender rechtlicher Rahmenbedingungen sowie die Adaption für zukünftig sich ändernde rechtliche Bestimmungen zählen, so das Unternehmen.[204] Auch wenn die Bestimmungen der 5. GwR erst in das nationale Recht umgesetzt werden müssen wendet Coinfinity bereits jetzt sehr umfangreiche und strenge Compliance- und Geldwäschemaßnahmen an. Es soll dargelegt werden auf welche rechtliche Grundlage sich das Unternehmen stützt.

Auf Grund des hohen Sicherheitsstandards, so das Unternehmen, könnten die Maßnahmen, die vom Unternehmen entwickelt wurden als Leitfaden für Dienstleister, die Kryptowährungen in Fiatgeld und umgekehrt tauschen, angesehen werden. Mit Hilfe der vorliegenden Unternehmensdaten soll die Möglichkeit der Unterstellung in die Gewerbeordnung geprüft bzw. dargelegt werden. Die gesetzgebende Instanz sollte unbedingt

[204] *Coinfinity,* https://coinfinity.com, (abgerufen am 26. August 2018).

mit Unternehmen der Branche zusammenarbeiten um die Bestimmungen der 5. GwR in einem vernünftigen und praxisbezogenen Rahmen in das nationale Recht umzusetzen.
Zudem wird *„... betont, wie wichtig Verbraucherbewusstsein, Transparenz und Vertrauen für die Nutzung virtueller Währungen sind.“* [205] Das Europäische Parlament: *“...fordert die Kommission auf, in Zusammenarbeit mit den Mitgliedstaaten und der Branche für virtuelle Währungen Leitlinien auszuarbeiten, mit denen gewährleistet wird, dass bestehende und künftige Nutzer virtueller Währungen korrekt, eindeutig und umfassend informiert werden, sodass sie eine sachkundige Entscheidung treffen können, wodurch die Transparenz von virtuellen Währungen in Bezug darauf, wie sie organisiert und betrieben werden ... verbessert wird ...“* [206] (Erwägungsgrund 23).

8.1. Coinfinity

Coinfinity ist ein österreichischer Broker, bei dem u.a. die virtuelle Währung Bitcoin in ein anerkanntes Zahlungsmittel und umgekehrt getauscht werden kann. Coinfinity war der erste Bitcoin-Automaten Aufsteller Österreichs und etablierte das erste österreichische "Walk-In Office" rund um Bitcoin.[207] Geschäftsgegenstand ist der Handel mit Bitcoin und anderen Kryptowährungen sowie der Betrieb von “Bitcoin-Automaten“ für den An- und Verkauf von Kryptowährungen. Zudem ist es möglich durch “Bitcoinbons“, welche in über 4000 Verkaufsstellen erhältlich sind, Kryptowährungen zu erwerben. Coinfinity versteht sich zudem als Kompetenzzentrum für Bitcoin und Blockchain-Technologie. Die Firma entwickelt Produkte und Lösungen rund um Bitcoin und bietet Firmen und Entscheidungsträgern von Politik und öffentlichen Institutionen Beratungsdienste an. Ferner werden auch Beratungsdienste für Händler, welche Bitcoin als Zahlungsmittel akzeptieren möchten, angeboten. Im Fokus der nachstehenden Analyse steht jedoch nur der Handel mit Kryptowährungen. Auf die anderen Geschäftsfelder des Unternehmens wird nicht eingegangen.[208]
Coinfinity ist sich über die möglichen Risiken von Geldwäsche und Terrorismusfinanzierung bewusst. Neben zahlreichen Präventionsmaßnahmen werden zusätzliche Schutzmaßnahmen, wie z.B. ein Compliance- und Geldwäscheteam, getroffen um sicherzustellen, dass eine Übereinstimmung auch mit künftig geltenden Gesetzen, Verordnungen und regulatorischen Vorschriften sowie nationalen und internationalen Standards und innerbetrieblichen

[205] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[206] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[207] *Coinfinity,* (abgerufen am 26. August 2018).
[208] *Coinfinity,* (abgerufen am 26. August 2018).

Regelwerken vorliegt, so das Unternehmen. Das Unternehmen weist höchste Standards bei der Prävention von Geldwäsche und Terrorismusfinanzierung sowie bei der Sicherheit von Kundendaten auf, so das Unternehmen.

8.1.1. Compliance

Compliance bedeutet das Handeln in Übereinstimmung mit geltenden Gesetzen, regulatorischen Vorschriften und über- bzw. innerbetrieblichen Regelwerken in allen Geschäftsbereichen. Das Fehlen eines einheitlichen Standard Compliance Code (SCC) auf österreichischer bzw. EU-Ebene für Kryptowährungen bedingt eine angelehnte Vorgehensweise an bestehende SCC der Kreditwirtschaft sowie SCC der Versicherungswirtschaft.[209] Der SCC der Versicherungswirtschaft basiert auf den Grundlagen der EU-Marktmissbrauchsverordnung (MAR) und des Börsengesetz 2018 (BörseG).[210] Für österreichische Kreditinstitute wurde unter Beachtung des § 48b Börsengesetz und § 16 Wertpapieraufsichtsgesetz (WAG) ein SCC entwickelt, der als Grundlage für die Geschäftstätigkeit, vor allem in den Bereichen Anlageberatung, Vermögensverwaltung, Fondsmanagement und Wertpapierhandel, anzusehen ist. Die Richtlinien sind als Mindeststandard anzusehen, die durch die Unternehmen jedoch auch strenger ausgestaltet sein können. Der SCC regelt unter anderem die Vorgabe der Compliance-Organisation als solche und die Tätigkeitsbereiche des Compliance-Beauftragten.[211] Hier besteht eindeutig Nachholbedarf für den Sektor von virtuellen Währungen. Eine Anpassung bestehender Standard Compliance Codes oder ein eigens entwickelter SCC wird zukünftig unabdingbar sein. Ziel ist es durch ein geeignetes Compliance-Organisationskonzept eine Basis von Fairness, Solidarität und Vertrauen getragenes Verhältnis der Informationssymmetrie zwischen den Kunden, dem Unternehmen und den Mitarbeitern zu erreichen und interne sowie externe Regelungen einzuhalten. Die Entwicklung von Organisationsvorschriften und Richtlinien dient u.a. zur Einhaltung der Regeln der Organe und Mitarbeiter des Unternehmens. Im Vordergrund des Konzeptes steht die Prävention.[212]

[209] *Coinfinity*, AML Abteilung.
[210] *Versicherungsverband Österreich,* Standard Compliance Code der österreichischen Versicherungswirtschaft,https://home.kpmg.com/content/dam/kpmg/at/pdf/Newsletter/insurance/download_VAG/4-c-vvo-standard-compliance-code-21092017%20.pdf, (1), (Stand 21.9.2017).
[211] *O.V.* Standard Compliance Code der österreichischen Kreditwirtschaft, http://www.rlb-tirol.at/eBusiness/services/resources/media/136344902797510738-NA-241427574725518235-1-1-NA.pdf, (abgerufen am 26. August 2018).
[212] *Coinfinity*, AML Abteilung.

8.1.2. Geldwäsche

Es ist festzuhalten, dass Broker mit direkter Anweisung/Überweisung an eine Wallet – wie auch Coinfinity einer ist – nicht in den Anwendungsbereich der 4. Geldwäsche-RL fallen. Wie bereits erwähnt gibt es strittige Ansichten ob das Unternehmen aktuell der Gewerbeordnung unterstellt ist oder nicht. Es stellt keine Finanztransaktion, sondern einen Verkauf eines Wirtschaftsgutes dar. Das bedeutet, dass seitens Kryptobörsen und Wallet Provider die in den unterschiedlichen Gesetzen angeführten Vorschriften bezüglich Geldwäsche und Terrorismusfinanzierung derzeit nicht als bindend zu betrachten sind, da eine Umsetzung der 5. Geldwäscherichtlinie in das nationale Recht bis dato nicht erfolgt ist.[213] Dennoch unterwirft sich die Firma den Geldwäschebestimmungen für Gewerbetreibende des Paragraphen § 365 lit m bis z der Gewerbeordnung. Somit wurden bereits präventive Maßnahmen gegen Geldwäsche vor Bekanntgabe der neuen Verpflichteten durch die 5. Geldwäscherichtlinie getroffen.

Zu den Aufgabenbereichen des Compliance und Geldwäschebeauftragten zählen unteranderem die Entscheidungsbefugnis ob ein Verdachtsfall vorliegt, dessen Meldung bei den Behörden sowie die Dokumentation des Sachverhaltes. Kommunikation und Korrespondenz mit dem Bundeskriminalamt und sonstigen Behörden. Des Weiteren die Festlegung der Betragsgrenzen je Risikoklasse, Durchführung und Aktualisierung von Risikoanalysen sowie sämtliche Entscheidungen in Bezug auf Kundenbeziehungen. Der Compliance Officer entscheidet im Zweifelsfall ob eine Kundenbeziehung aufgenommen, aufgelöst oder eine Kundensperre verhängt wird, eine Transaktion abgelehnt wird oder unter welchen Auflagen die Kundenbeziehung weitergeführt werden soll. Auch hier besteht eine Dokumentationspflicht. Obwohl Coinfinity bei Verdacht auf Geldwäsche oder Terrorismusfinanzierung eine Meldung beim Bundeskriminalamt durchführt, hat die Behörde jedoch keine Verfügungsmacht über die Geschäftsbeziehungen des Unternehmens.[214] Es gilt: *„Der Geldwäschemeldestelle steht keine Entscheidungsbefugnis über Begründung/Verlauf oder Kündigung von Geschäftsbeziehungen zu. Vielmehr handelt es sich hier um geschäftspolitische Entscheidungen der einzelnen Institutionen. Es obliegt dem jeweiligen Verpflichteten, nach Durchführung der erforderlichen Risikoanalyse eine diesbezügliche Entscheidung zu treffen und die Geschäftsbeziehung allenfalls zu beenden.“*[215]

Es ist festzuhalten, dass aktuell Coinfinity keiner meldepflichtigen Berufsgruppe angehört.

[213] *Coinfinity,* AML Abteilung.
[214] *Coinfinity,* AML Abteilung.
[215] *Bundeskriminalamt,* Informationsblatt, http://www.bundeskriminalamt.at/308/files/Geldwaeschemeldung_Info.pdf, (abgerufen am 12. August 2018).

Erst nach Umsetzung der RL (EU) 2018/843 werden diese im Sinne des Gesetzes als Verpflichtete bzw. meldepflichtige Berufsgruppe gelten. *„Die Geldwäschemeldestelle (§ 4 Abs. 2 BKA-G) nimmt Meldungen von meldepflichtigen Berufsgruppen über verdächtige Transaktionen nach dem Finanzmarkt-Geldwäschegesetz, dem Bilanzbuchhaltungsgesetz, dem Börsegesetz (1989), der Gewerbeordnung (1994), dem Glückspielgesetz, dem Körperschaftssteuergesetz (1988), der Notariats- und der Rechtsanwaltsordnung, dem Wirtschaftstreuhandberufsgesetz und dem Zollrechts-Durchführungsgesetz entgegen.“*[216] Da aktuell Dienstleister, die Kryptowährungen in ein anerkanntes Zahlungsmittel und umgekehrt tauschen keiner der oben genannten Gesetze unterliegen, unter Bedacht, dass es strittige Aussagen gibt, sind diese nicht zu einer Verdachtsmeldung verpflichtet. Sämtliche Meldungen erfolgen auf freiwilliger Basis.

Überdies ist der CO für die Erstellung von periodischen und anlassbezogenen Berichten zuständig. Ferner werden sämtliche Mitarbeiter zwecks Erkennung von Verdachtsmomenten im Zusammenhang mit Geldwäscherei geschult. Coinfinity ist der Auffassung, dass Geldwäscheprävention nur durch aktive Mitwirkung aller Mitarbeiter funktioniert. Diese müssen, gemäß den festgelegten unternehmensinternen Richtlinien umgehend Verdachtsmeldungen an den Geldwäschebeauftragten melden und stets nach dem Know-Your-Customer Prinzip arbeiten, das als Basis zur Verhinderung von Geldwäsche dient. Zudem wurde ein Verhaltenskodex für Mitarbeiter erarbeitet. Die Mitarbeiter sind zudem vertraglich an die unternehmensinternen Anti-Money-Laundering Vorkehrungen gebunden, so das Unternehmen.

8.1.3. Aufbewahrung der Unterlagen

Die Unterlagen, die der Dokumentation und der Information für die Erfüllung der Sorgfaltspflichten gegenüber einem Kunden dienen, werden bis mindestens 7 Jahre nach Beendigung der Geschäftsbeziehung mit diesem aufbewahrt. Sämtliche Unterlagen von Transaktionen, Belegen, Aufzeichnungen sowie Vermerken werden bis mindestens 7 Jahre nach Beendigung der Geschäftsbeziehung aufbewahrt, so das Unternehmen.[217]

Gemäß § 365y. Abs 1 Z 1 und 2 GewO müssen diese nur 5 Jahre nach Beendigung der Geschäftsbeziehung oder nach einer gelegentlichen Transaktion aufbewahrt werden. Hier spricht sich Coinfinity eindeutig für einen längeren Aufbewahrungszeitraum aus. Diese spezielle Vorgehensweise dient ausschließlich dem Sinn und Zweck zur Vermeidung von

[216] *Bundeskriminalamt,* Meldestellen, http://www.bundeskriminalamt.at/602/start.aspx, (abgerufen am 12. August. 2018).
[217] *Coinfinity,* AML Abteilung.

Geldwäsche und Terrorismusfinanzierung und ist dem speziellen Umfeld von Geschäften mit Kryptowährungen geschuldet. Zudem müssen sichere Kommunikationskanäle bestehen, um einen richtigen Umgang mit vertraulichen Dokumenten gewährleisten zu können (§ 365y. Abs 3 GewO).

8.2. Erwerb von virtuellen Währungen

Wie bereits im Kapitel 3.2.3. erklärt gibt es unterschiedliche Möglichkeiten Kryptowährungen zu erwerben. Je nach Art des Erwerbes gibt es aktuell unterschiedliche Beschränkungen und Identifikationsverfahren, die im folgenden Abschnitt genauer betrachtet werden. Zu diesem Zweck werden die Geschäftsfelder des Unternehmens, insbesondere die Bereiche Onlinehandel, Bitcoin-Automaten (BATMs) und Bitcoinbons betrachtet.[218]

8.2.1. Bitcoin – Automaten

Wie bereits erwähnt war die Coinfinity GmbH der erste Bitcoin-Automaten Austeller Österreichs. Kunden können aktuell bei Bitcoin-Automaten im Austausch gegen Bargeld Bitcoins sowie einige weitere virtuelle Währungen erhalten, die direkt auf das Kundenwallet geliefert werden. Da die Gefahr für Geldwäsche besonders groß ist, wurden spezielle Sicherheitsvorkehrungen getroffen. Bis zu einem Betrag von 250 EUR können Kunden anonym Bitcoin kaufen. Ab 250 EUR ist eine Verifizierung über den Automaten notwendig.[219] Die Identifikation der Nutzer findet wie folgt statt. Der Kunde muss seine Telefonnummer in das Gerät eingeben um einen Pin zu erhalten, mit welchem er die Kamera des Gerätes für die Verifizierung aktivieren kann. Jeder Automat ist mit einer hochauflösenden Kamera ausgestattet mit welcher in weiteren Schritten Front- und Rückseite eines amtlichen Lichtbildausweises, sowie ein Foto des Ausweis-Inhabers gemeinsam mit dem Ausweis zu machen sind. Diese werden in Echtzeit an die Mitarbeiter der Kurant GmbH gesendet, welche darüber entscheiden ob ein Kunde verifiziert wird. Bei Rückfragen wird der Kunde direkt telefonisch verständigt. Diese Maßnahmen dienen zur Minimierung des Risikos von Geldwäscheaktivitäten. An dieser Stelle ist jedoch anzumerken, dass es österreichweit hunderte Automaten gibt, bei denen Personen mit kriminellen Absichten virtuelle Währungen gegen Bargeld erwerben können und unter einem Betrag von 250 Euro nicht verifiziert werden. Durch die Begrenzung des Betrages soll Geldwäsche im schnellen und großen Stil verhindert werden, so Coinfinity. Das Unternehmen hält fest, dass der Höchstbetrag eine

[218] *Coinfinity,* (abgerufen am 27.8.2018).
[219] *Coinfinity,* AML Abteilung.

freiwillige Beschränkung darstellt und es für den Höchstbetrag aktuell keine rechtliche Grundlage gibt.[220]

Zudem ist anzumerken, dass Auffälligkeiten wie z.B. zahlreiche Transaktionen an ein und dieselbe Public Address unter den Schwellenwert von 250 Euro von Seiten des Unternehmens sehr wohl wahrgenommen werden können und eine Meldung bzw. Zusammenarbeit mit den Behörden stattfindet.[221]

Neben den sogenannten „ One-Way Automaten“ , bei denen Bitcoins gegen Fiatgeld gekauft und direkt an die Wallets überwiesen werden können, gibt es auch “ Two-Way Automaten“, bei dem Nutzer Bitcoins verkaufen können[222]: *„ In diesem Fall können via QR-Code Bitcoins von der Wallet des Kunden an den Betreiber der Bitcoin- Automaten verkauft werden. Im Gegenzug erhält der Kunde Bargeld ausbezahlt.“*[223]

Grundsätzlich ist der reine Ankauf und Verkauf von virtuellen Währungen über Automaten nicht konzessionspflichtig. Je nach Ausgestaltung des Geschäftsmodelles kann dieses jedoch eine Konzessionspflicht auslösen:[224] *„So kann die Entleerung des Bitcoin Automaten und anschließende Überweisung der darin befindlichen Gelder an einen Dritten, eine Konzession nach dem ZaDiG, etwa für das Finanztransfergeschäft (§ 1 Abs. 2 Z 5 ZaDiG) auslösen“*[225]

8.2.2. Bitcoinbon

Beim Bitcoinbon handelt es sich um einen Gutscheincode in Euro. Solche Bons können in unterschiedlich hohen Beträgen erworben werden. Der maximale Betrag ist 250 Euro. Bei Übersteigerung der Beträge ist die Identifizierung des Erwerbes durch Vorlage bzw. Kopie eines Ausweises notwendig. Das Produkt ist an mehreren tausend Standorten erhältlich.[226]

8.2.3. Onlinehandel

Vorab ist festzuhalten, dass grundsätzlich nur Kunden mit Hauptwohnsitz in Österreich den Onlinedienst des Unternehmens in Anspruch nehmen dürfen. Auf Grund der unterschiedlichen rechtlichen Behandlung bzw. Einordnung von virtuellen Währungen und dem Handel mit solchen innerhalb der EU werden nur selten Nutzer mit Hauptwohnsitz in einem anderen EU-Staat durch das Unternehmen berechtigt: „Wir sind ein österreichisches

[220] *Coinfinity,* AML Abteilung.
[221] *Coinfinity,* AML Abteilung.
[222] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, https://www.fma.gv.at/querschnittsthemen/fintech/fintech-navigator/ (29. September 2018).
[223] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, (29. September 2018).
[224] *FMA*, FinTech-Navigator durch das Aufsichtsrecht, (29. September 2018).
[225] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, (29. September 2018).
[226] *Coinfinity,* (abgerufen am 27.8.2018).

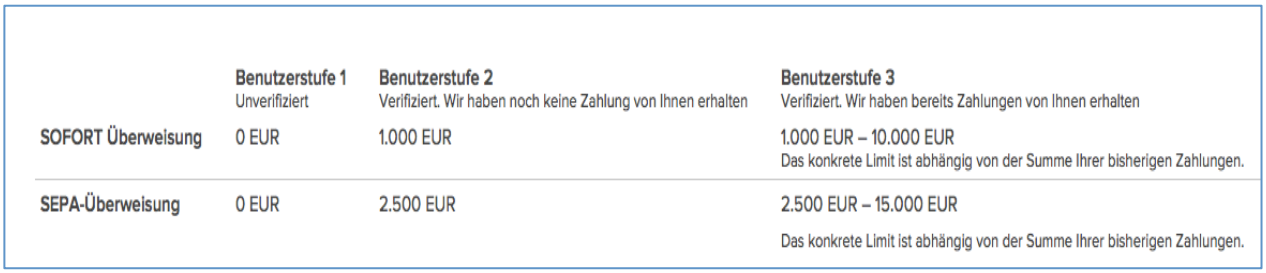
Unternehmen mit Sitz in Graz und Wissen um die rechtlichen Rahmenbedingungen in unserem Land. Gerade Bitcoin bzw. generell Kryptowährungen werden innerhalb der EU bzw. in Drittländern sehr stark rechtlich unterschiedlich gehandhabt. Somit könnten uns Risikoarten unserer Kunden hinsichtlich Haftung etc. treffen, wenn wir nicht rechtzeitig unsere Ordersoftware diesen Gegebenheiten anpassen. Diesen Onlinestandard können wir nur Kunden mit Wohnsitz Österreich bieten, alles andere unterliegt bei einer Einzelorder einer händischen Einzelprüfung“ so Mag. Matthias Reder, Leiter der Compliance und AML Abteilung von Coinfinty.[227]

Staaten bei denen erhöhtes Risiko der Terrorismusfinanzierung, Geldwäsche und Korruption bestehen werden dadurch von vornherein ausgeschlossen. Nur in seltenen Fällen und unter eingehender Prüfung werden Personen von Drittländern verifiziert. In solchen Fällen erfolgt eine persönliche Kontrolle durch den Compliance-Officer. Zudem werden nur Zahlungen aus dem Europäischen Zahlungsraum (SEPA) akzeptiert.[228]

Derzeit gibt es zwei verschiedene Zahlungsmöglichkeiten mit unterschiedlichen Limits, auf Grund unterschiedlich hoher unternehmerischer Risiken. Wie in der folgenden Grafik ersichtlich wird erfolgt eine Unterteilung der Kunden in drei unterschiedliche Benutzerstufen mit unterschiedlichen Limits. In der Benutzerstufe eins wird ersichtlich, dass Personen die nicht ausreichend verifiziert wurden nicht berechtigt sind Überweisungen zu tätigen. In die Benutzerstufe zwei fallen jene Personen, die bereits verifiziert wurden aber noch keine Zahlungen getätigt haben. Hier gibt es je nach Art der Bezahlung unterschiedliche Transaktionslimits. Personen die bereits Zahlungen getätigt haben dürfen je nach Zahlungsmethode und bisherigen Transaktionssummen für Beträge zwischen 1 000 Euro und 15 000 Euro virtuelle Währungen kaufen. Wenn Kunden höhere Limits benötigen, müssen sich diese an den Compliance-Officer wenden. Nach eingehender Prüfung entscheidet dieser ob die Limits erhöht werden dürfen. Die genannten Limits bestehen jeweils für einen Zeitraum von 72 Stunden. Aktuell können Kunden Zahlungen über SEPA oder SOFORT-Überweisung (Klarna) tätigen.[229]

[227] *Mag. Matthias Reder,* Leiter der Compliance und AML Abteilung von Coinfinty, Interview geführt von Marina Kindel (3. August 2018).
[228] *Coinfinity,* AML Abteilung.
[229] *Coinfinity,* AML Abteilung.

Abbildung 1: Benutzerstufen



	Benutzerstufe 1 Unverifiziert	Benutzerstufe 2 Verifiziert. Wir haben noch keine Zahlung von Ihnen erhalten	Benutzerstufe 3 Verifiziert. Wir haben bereits Zahlungen von Ihnen erhalten
SOFORT Überweisung	0 EUR	1.000 EUR	1.000 EUR – 10.000 EUR Das konkrete Limit ist abhängig von der Summe Ihrer bisherigen Zahlungen.
SEPA-Überweisung	0 EUR	2.500 EUR	2.500 EUR – 15.000 EUR Das konkrete Limit ist abhängig von der Summe Ihrer bisherigen Zahlungen.

Quelle: Coinfinity

Um über das Unternehmen Bitcoins zu kaufen oder verkaufen zu können ist eine Verifizierung mit amtlichen Lichtbildausweis und Adressnachweis verpflichtend. Es gibt drei unterschiedliche Wege um eine Verifizierung durchzuführen:[230]

1. Die erste Möglichkeit stellt die Verifizierung mittels Videoidentverfahren, durch die Österreichische Staatsdruckerei, dar. Hier wird die Prüfung durch Mitarbeiter der Österreichischen Staatsdruckerei durchgeführt, welche über entsprechend geschulte Fähigkeiten verfügen. Dieser Service ist zertifiziert und ist auch für Banken möglich. Coinfinity erhält zu jeder Verifizierung Bilder der Ausweise sowie das Audioprotokoll der Verifizierung.
2. Als zweites ist die Verifizierung per Mail möglich: Hier werden die Dokumente direkt an Coinfinity gesendet und von entsprechend geschulten Mitarbeitern geprüft. Bei Bedarf oder Unklarheit werden weitere Dokumente oder ein weiteres Bild mit höherer Auflösung angefordert.
3. Die letzte Möglichkeit stellt die Verifizierung vor Ort dar. Kunden können sich direkt im Büro von Coinfinity mit einem Lichtbildausweis und einem Adressnachweis verifizieren. Ein geschulten Mitarbeiter überprüft die Daten und speichert diese in der Kundendatenbank.[231]

8.2.4. Identifizierungsverfahren

Seit 1. Jänner 2017 ist, es auf Grund neuer Regelungen des FM-GwG i.V.m. der Online-Identifikationsverordnung der FMA, für Firmen möglich mittels Video-Anruf Ausweiskontrollen durchzuführen. Das Identifikationsverfahren wird mit dem Service "My Identity Check" (MICK) der österreichischen Staatsbibliothek durchgeführt. Das "MICK" ist

[230] *Coinfinity,* AML Abteilung.
[231] *Coinfinity,* AML Abteilung.

ein hochsicheres Video-Identitätsverfahren, dessen erhobene Daten im Hochsicherheitsraum der Staatsdruckerei gesichert werden. Diese sind rund um die Uhr verfügbar. Auf Grund der hohen Sicherheitsaspekte, da u.a. Personendaten mit der Datenbank der Republik Österreich verglichen werden, können in Minuten rechtskräftige Verträge abgeschlossen werden. Neben dem Sicherheitsaspekt entstehen für die beteiligten Parteien erhebliche Kosten- sowie Zeitersparnisse, da medienfreie Vertragsabschlüsse innerhalb von nur wenigen Minuten abgeschlossen werden können.[232] *„Bei der Video-Prüfung wird die Echtheit des vorgezeigten Ausweises geprüft. Der Kunde muss seinen gültigen Personalausweis oder seinen Reisepass vor die Webcam halten und u.a. kippen, damit die Sicherheitsmerkmale geprüft werden können. Es werden Fotos angefertigt und die Ausweisnummer erfasst.“*[233]

Es wird nur eine Internetverbindung sowie ein internetfähiges Gerät und eine (integrierte) Kamera benötigt. Der Identifikationsprozess setzt sich aus vier Schritten zusammen. Zuerst beantragt der Kunde online die Registrierung bzw. die Erkennung, dann erfolgt ein Videoanruf zur Feststellung der Identität, die Prüfung der Dokumente durch Experten und die abschließende Rücksendung der Ergebnisse in Echtzeit.[234]

Gemäß der RL 2018/843 Art 13 Abs 1 wird folgendes bezüglich der Identifikationsverfahren bestimmt: *„Feststellung der Identität des Kunden und Überprüfung der Kundenidentität auf der Grundlage von Doku- menten, Daten oder Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen, ein- schließlich soweit verfügbar elektronischer Mittel für die Identitätsfeststellung, einschlägiger Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates (*) oder mittels anderer von den zuständigen nationalen Behörden regulierter, anerkannter, gebilligter oder akzeptierter sicherer Ver- fahren zur Identifizierung aus der Ferne oder auf elektronischem Weg eingeholt wurden.“*[235]

8.3. Sorgfaltspflichten gemäß der Gewerbeordnung

8.3.1. Allgemeine Sorgfaltspflichten gemäß der Gewerbeordnung

Gemäß § 365o. GewO kommen in folgenden Fällen die in der Gewerbeordnung festgelegten Sorgfaltspflichten zum Tragen:

[232] *Youniqx Identity AG*, MICK My Identity Check, https://www.myidcheck.at/#x-section-5 (abgerufen am 10. August 2018).
[233] *Youniqx Identity AG*, MICK My Identity Check, (abgerufen am 10.8.2018).
[234] *Youniqx Identity AG*, MICK My Identity Check, (abgerufen am 10.8.2018).
[235] RL 2018/843 ABL L 2018/156, 43.

- Die Sorgfaltspflichten kommen bei Begründung einer Geschäftsbeziehung zur Anwendung
- Bei Anzweiflung der Echtheit von Daten
- „ *... bei Ausführung gelegentlicher Transaktionen in Höhe von 15 000 Euro oder mehr... im Falle von Handelsgewerbetreibenden einschließlich Versteigerern bei Abwicklung gelegentlicher Transaktionen in bar in Höhe von 10 000 Euro oder mehr und zwar unabhängig davon, ob die Transaktion in einem einzigen Vorgang oder in mehreren Vorgängen, zwischen denen eine Verbindung zu bestehen scheint, getätigt wird ..“* § 365o. Abs 1 und 2 GewO.
- Ferner wenn Verdacht besteht, dass beim Kunden der Tatbestand des § 278b StGB, § 278d StGB oder der des § 165 StGB – unter Einbeziehung der Eigengeldwäscherei – vorliegt (§365o. Z 4 GewO).

Eine vertragliche Vereinbarung, dessen Gegenstand der Austausch von Leistungen über einen längeren Zeitraum ist, ist als Geschäftsbeziehung anzusehen.[236] Unter dem Begriff „Transaktionen“ sind: *„ ... wohl Geschäfte zu verstehen, die grundsätzlich* ***kein Dauerelement*** *in Bezug auf den Kontakt des Gewerbetreibenden mit den Kunden haben.“*[237] Wie bereits erwähnt, besteht eine Zusammenrechnungspflicht, welche naturgemäß dort endet[238] *„ ... wo praktische Grenzen bestehen. Allgemeines Kriterium ist, dass bei gehöriger Aufmerksamkeit ein Zusammenhang hergestellt werden kann oder ein solcher bekannt ist.“* [239] Die allgemeinen Sorgfaltspflichten finden Anwendung, ungeachtet möglicher Ausnahmeregelungen, Befreiungen oder Grenzwerten, wenn ein Verdacht auf Geldwäsche oder Terrorismusfinanzierung vorliegt. Bei vorliegendem Verdacht ist die Meldestelle umgehend davon zu informieren. Dies ist auch der Fall, wenn z.B. der Schwellenwerte nach lit b unterschritten ist oder ein geringes Risiko vorliegt.[240]

8.3.2. Umfang der Sorgfaltspflichten gegenüber Kunden gemäß der Gewerbeordnung

§ 365p. GewO regelt den Umfang der Sorgfaltspflichten gegenüber Kunden. Die Eruierung und Überprüfung der Identitäten der Kunden erfolgt gemäß § 365p. Abs 1 Z 1 lit a GewO bei natürlichen Personen durch einen amtlichen Lichtbildausweis und bei juristischen Personen gemäß § 365p. Abs 1 Z 1 lit b GewO durch beweiskräftige Urkunden, die am Sitz der juristischen Personen gemäß den dort herrschenden Bestimmungen verfügbar sind.

[236] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365o. (Stand 27.9.2018, lexisnexis.at).
[237] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365o.
[238] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365o.
[239] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365o.
[240] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365o.

Ein „Amtlicher Lichtbildausweis ist ein von der zuständigen Behörde ausgestellter Ausweis mit Lichtbild und Unterschrift"[241] Die Pflicht, mit Hilfe eines amtlichen Lichtbildausweises, Kundenidentitäten festzustellen bzw. diese zu überprüfen[242] *„ ... ist gesetzlicher Ausdruck des iZm der Bekämpfung der Geldwäsche und Terrorismusfinanzierung wesentlichen Prinzips* ***„Know your customer".***[243] Es ist zwischen Feststellung und Überprüfung wie folgt zu differenzieren: Bei der Identitätsfeststellung werden Angaben zu Identität erhoben und bei der Überprüfung werden die erhobenen Daten mit einem amtlichen Lichtbildausweis abgeglichen bzw. kontrolliert. Der gesetzliche Vor- und Zuname, das Geburtsdatum sowie die Wohnadresse dienen zur Identitätsfeststellung:[244] *„ Als amtlicher Lichtbildausweis in diesem Sinn gelten von einer staatlichen Behörde ausgestellte Dokumente, die mit einem nicht austauschbaren erkennbaren Kopfbild der betreffenden Person versehen sind, und den Namen, das Geburtsdatum und die Unterschrift der Person sowie die ausstellende Behörde enthalten"* (§ 40 Abs 1 Z 5 BWG). Somit werden Reisepässe gemäß § 3 PaßG, Passersätze gemäß § 18PaßG sowie Personalausweise als solche deklariert. Coinfinity akzeptiert zur Identifikation natürlichen Personen folgende von staatlichen Behörden ausgestellte Dokumente: Reisepass, Personalausweis, welcher zum Grenzüberschritt berechtigt ist, sowie den Führerschein.[245] Zudem sind gemäß § 365p. Abs 1 Z 2 GewO die Identitäten wirtschaftlicher Eigentümer, durch geeignete Verfahren zur Überprüfung, festzustellen: *„... im Fall von juristischen Personen, Trusts, Gesellschaften, Stiftungen und ähnlichen Rechtsvereinbarungen schließt dies ein, dass angemessene Maßnahmen ergriffen werden, um die Eigentums- und Kontrollstruktur des Kunden zu verstehen ..."* (§ 365p. Abs 1 Z 2 GewO). Paragraph 365n. Z 3 lit a bis c der GewO definiert wirtschaftliche Eigentümer im rechtlichen Sinn. Die gesetzliche Grundlage für den risikobasierten Ansatz bzw. für angemessene Maßnahmen zur Überprüfung ist in Art 8 Abs 1 sind in der RL 2015/849 vorzufinden, welche in § 365p. Abs 1 Z 2 GewO umgesetzt wurden. In der Richtlinie 2015/849 wird auch festgehalten, dass der Prüfungsumfang nach Höhe des Risikos zu erfolgen hat. Somit hat der Gewerbetreibende einen gewissen Ermessungsspielraum. Die Identitätsfeststellung einer natürlichen Person durch einen amtlichen Lichtbildausweis wurde in 365p. GewO nicht explizit erwähnt. Geeignete Methoden zur Identitätsfeststellung können auch Auskünfte Dritter, öffentlich zugängliche Register und Befragungen sein.[246]

Um darüber Kenntnis zu erlangen bedient sich Coinfinity verschiedener Maßnahmen wie z.B.

---

[241] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365p. (Stand 27.9.2018, lexisnexis.at).
[242] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365p.
[243] *Grabler/Stolzlechner/Wendl*, GewO[3] (2011), § 365p.
[244] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365p.
[245] *Coinfinity*, AML Abteilung.
[246] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365p.

der Vorlage diverser Unterlagen wie Notariatsakte. Erst wenn mit größter Sorgfalt Auskünfte erteilt werden, um zu wissen, wer der wirtschaftliche Eigentümer ist (im Fall von juristischen Personen muss die Eigentums- und Kontrollstruktur des Kunden verstanden werden), wird eine Transaktion durchgeführt bzw. eine Geschäftsbeziehung aufgenommen/fortgesetzt.[247]

Der Umfang der Identitätsfeststellung wird durch mehrere Faktoren: *„…nach den vom Gewerbetreibenden zu bewertenden Risiken, insbesondere nach dem Zweck der Geschäftsbeziehung, der Höhe der von einem Kunden eingezahlten Vermögenswerte oder dem Umfang der Transaktion sowie Regelmäßigkeit oder Dauer der Geschäftsbeziehung*" (§ 365p. Abs 2 GewO) bestimmt. Die Geschäftsbeziehung muss gemäß § 365p. Abs 1 Z 4 GewO dauerhaft überwacht und kontrolliert werden: *„Mit kontinuierlicher Überwachung der Geschäftsbeziehung ist eine aufmerksame Verfolgung betreffend die Plausibilität der Transaktionen gemeint. Nicht gemeint ist die Überwachung des Kunden; dies stünde kaufmännischen Prinzipien entgegen."*[248] Die Höhe der Transaktionen muss mit dem Risikoprofil des Kunden übereinstimmen. Die Informationen über die Nutzer müssen auf aktuellen Stand gehalten werden (§ 365p. Abs 1 Z 4 GewO). Nicht nur bei Neukunden, sondern auch bei bestehenden Kunden sind die Sorgfaltspflichten gemäß des risikobasierenden Ansatzes anzuwenden (§ 365p. Abs 6 GewO).

Für den Fall, dass ein Kunde, bei dem diese Sorgfaltspflichten zu tragen kommen, sich nicht kooperativ verhält und eingeforderte Belege nicht oder nur unvollständig liefert bzw. aufgrund der Unterlagen der begründete Verdacht entsteht, dass die Person Geldwäsche- oder Terrorismusfinanzierung betreibt, so unterlässt Coinfinity jegliche Transaktion bzw. begründet kein Geschäftsverhältnis oder führt dieses nicht fort.[249] Hier bezieht sich das Unternehmen auf die in § 365p. Abs 7 GewO festgelegten Bestimmungen. Erhärtet sich bei einer Person der Verdacht, dass *„… eine versuchte, bevorstehende, laufende oder bereits erfolgte Transaktion im Zusammenhang mit Vermögensbestandteilen, die aus einer in § 165 StGB aufgezählten strafbaren Handlung herrühren (unter Einbeziehung von Vermögensbestandteilen, die aus einer strafbaren Handlung des Täters selbst herrühren)..."* (365t. Abs 1 Z1 GewO) oder Vermögensbestandteile aus einer in § 165 StGB verankerten Handlung, unter Berücksichtigung von Eigengeldwäsche, herrühren (365t. Abs 1 Z 2 GewO) oder diese in Zusammenhang mit § 278a bis d StGB stehen (365t. Abs 1 Z 3 GewO) so ist die Geldwäschemeldestelle gemäß § 365t. GewO unverzüglich darüber in Kenntnis zu setzen.

Gemäß § 365u Abs 2 GewO gilt dies nicht, wenn die Gefahr besteht, dass die Verzögerung

[247] *Coinfinity*, AML Abteilung.
[248] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365p.
[249] *Coinfinity,* AML Abteilung.

der Transaktion die Ermittlung des Sachverhalts erschwert oder verhindert.
Die Übermittlung der Verdachtsmeldung hat in einem geläufigen elektronischen Format, unter Verwendung der durch die Geldwäschemeldestelle festgelegten sicheren Kommunikationskanal, zu erfolgen. Wenn ein Verfahren eingeleitet wird, muss der Compliance-Beauftrage oder ein informierter Mitarbeiter des Unternehmens für Fragen oder Zeugenaussagen zur Verfügung stehen.[250]
Zudem holt Coinfinity Informationen über den Zweck und die angestrebte Art der Geschäftsbeziehung immer vor Begründung einer Geschäftsbeziehung ein.
Gemäß der Gewerbeordnung hat die Identitätsfeststellung *„… vor der Begründung einer Geschäftsbeziehung oder der Abwicklung einer Transaktion zu erfolgen …*“ (§ 365q. Abs 1 GewO). Nur bei möglicher Beeinträchtigung des Geschäftsablaufes sowie einem verminderten Risiko der Geldwäsche oder Terrorismusfinanzierung darf gemäß § 365q. Abs 2 GewO die Identitätsfeststellung erst während des Zustandekommens einer Geschäftsbeziehung erfolgen.

8.3.3. Vereinfachte Sorgfaltspflichten gemäß § 365r. Gewerbeordnung

Vereinfachte Sorgfaltspflichten gegenüber Kunden sind anzuwenden, wenn gemäß 365n.1 GewO i.V.m. 365r. Abs 4 und Abs (5) GewO eine Risikobewertung durchgeführt wurde und durch diese Analyse festgestellt wurde, dass bei der Geschäftsbeziehung im Sinne des § 365n. Z 7 GewO sowie bei der Transaktion ein geringes Risiko vorliegt. Anlage 7 der Gewerbeordnung listet Faktoren auf, die ein potenziell geringeres Risiko begründen. Die in Anlage 7 der Gewerbeordnung aufgezählten Faktoren unterteilen sich in drei Bereiche:

1. *„… Risikofaktoren bezüglich Kunden …*
2. *… Risikofaktoren bezüglich Produkte, Dienstleistungen, Transaktionen oder Vertriebskanäle“ …*
3. *… Risikofaktoren in geographischer Hinsicht … „(*Anlage 7 Gewerbeordnung).

Es handelt sich gemäß der Gewerbeordnung um eine demonstrative Aufzählung, die auf ein mögliches geringeres Risiko hinweist. Punkt eins umfasst u.a. Personen dessen Wohnsitz, geografisch betrachtet, ein geringes Risiko aufweist oder die Kunden ein öffentliches Unternehmen sind. Produkte bei denen ein geringeres Risiko, durch zusätzliche Beschränkungen in Bezug auf Geldwäsche, vorherrscht werden u.a. unter Punkt 2 aufgelistet.

[250] *Bundeskriminalamt,* Informationsblatt, (abgerufen am 12. August 2018).

Mitgliedsstatten oder Drittländer mit einem geringen nachweisbaren Risiko für Geldwäsche und anderen illegalen Aktivitäten werden u.a. unter Punkt drei aufgelistet. (Anlage 7 Gewerbeordnung). Unter vereinfachten Pflichten ist folgendes zu verstehen: *„Gemeint ist damit, dass Gewerbetreibende von „einzelnen" der in § 365p Abs 1 und 2 und § 365q Abs 1 festgelegten Maßnahmen Abstand nehmen können ..."* [251] Dies bedeutet, dass die Durchführung gewisser Maßnahmen, bei Vorliegen eines geringeren Risikos sowie bei Kunden gemäß 1 - 4 des § 365 r Abs 1 GewO, nicht erforderlich ist.[252] *„„ Nicht erforderlich" sind solche Maßnahamen dann, wenn der für eine entsprechende Kontrollmaßnahme erforderliche Aufwand und die Geringfügigkeit des Risikos in keinem vernünftigen Verhältnis zueinander stehen."*[253] Dies bedeutet somit wenn der Aufwand/ Kosten der Kontrolle im erheblichen Maße größer ist als das mögliche Risiko der Geldwäsche und Terrorismusfinanzierung können die Maßnahmen unterlassen werden. Diese Bestimmungen ergeben sich aus der FATF Empfehlung 5.9.[254] Es wird festgehalten, dass in diesen Fällen die Sorgfaltspflichten zur Gänze entfallen kann. Die Feststellung der Kundenidentität (§ 365p Abs 1 Z 2 und 4, § 365q Abs 1 GewO) hat jedoch ausnahmslos in jedem Fall stattzufinden. Die Plicht zur Informationseinholung, um auffällige Tatbestände überhaupt erst feststellen zu können (Abs 1 letzter Satz), jedoch nicht.[255]

Coinfinity ist sich der Tatsache bewusst, dass in ihrem Geschäftsfeld besondere Risikofaktoren bestehen. Diese ergeben sich aus der Anonymität des Kunden sowie der Kontaktlosigkeit bei Geschäften bis zu einem Gegenwert von EUR 250, -- wie auch aus der gewissen Anonymität, welche Bitcoins und Kryptowährungen insgesamt bieten. Zudem ist Coinfinity in Österreich Vorreiterin auf ihrem Geschäftsfeld, wodurch sich – gepaart mit dem relativ jungen und innovativen Phänomen Bitcoin – ebenfalls gewisse Risiken ergeben.[256]

8.3.4. Verstärkte Sorgfaltspflichten gemäß § 365s Gewerbeordnung

Bei den verstärkten Sorgfaltspflichten gemäß § 365s. GewO sind neben den in Paragraph § 365p. GewO festgelegten Sorgfaltspflichten zudem zusätzliche Maßnahmen von den Gewerbetreibenden zu ergreifen. Gemäß § 365s. Abs 1 Z 1 GewO hat der Gewerbetreibende *„... über angemessene Risikomanagementsysteme einschließlich risikobasierter Verfahren zu*

[251] *Grabler/Stolzlechner/Wendl*, GewO[3] (2011), § 365r. (Stand 27.9.2018, lexisnexis.at).
[252] *Grabler/Stolzlechner/Wendl*, GewO[3] (2011), § 365r.
[253] *Grabler/Stolzlechner/Wendl,* GewO[3] (2011), § 365r.
[254] *FATF,* INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION The FATF Recommendations,http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, (abgerufen am 3. Oktober 2018).
[255] *Grabler/Stolzlechner/Wendl*, GewO[3] (2011), § 365r.
[256] *Coinfinity,* AML Abteilung.

verfügen, um feststellen zu können, ob es sich bei dem Kunden oder dem wirtschaftlichen Eigentümer des Kunden um eine politisch exponierte Person handelt.“ Möchten Gewerbetreibende mit politisch exponierten Personen Geschäfte eingehen muss vorab die Zustimmung der Führungsebene eingeholt werden. Ansonsten wäre nach den Bestimmungen der Gewerbeordnung eine Geschäftsaufnahme bzw. Fortführung nicht gesetzeskonform (§ 365s. Abs 1 Z 2 GewO). Bevor Coinfinity eine Geschäftsbeziehung zu einer politischen exponierten Person aufnimmt oder fortführt, haben die Beschäftigten die Zustimmung der Führungsebene einzuholen. Diese werden dementsprechend geschult und durch Weisung verpflichtet, so Coinfinity.[257]

Coinfinity wendet erhöhte Sorgfaltspflichten bei Personen aus Drittländern mit hohem Risiko sowie bei politisch exponierten Personen an, so das Unternehmen.[258] Grundsätzlich bedeutet dies, dass „Kundenordners“ dieser Personengruppe einer verstärkten Überwachung unterzogen werden (§ 365s. Abs 1 Z 4 GewO). Bei der Klassifizierung politisch exponierter Personen orientiert sich Coinfinity an der in §365n Z 4 Gew0 normierten Definition solcher. Zudem stellt Coinfinity klar, dass das Gesetz, hinsichtlich dem Kreis politisch exponierter Personen, bloß eine demonstrative Aufzählung bietet, wodurch impliziert wird, dass betroffene Beschäftigte oder Geschäftspartner mit Vorsicht zu entscheiden haben, ob eine Person als "politisch exponierte Person" nach der Gewerbeordnung zu behandeln ist. Im Sinne des Gesetzes ist gemäß § 365n. Z 4 GewO eine politisch exponierte Person *„... eine natürliche Person, die wichtige öffentliche Ämter ausübt oder ausgeübt hat; ...*“

Zu dieser Gruppe zählen unter anderem folgende Personengruppen:

- *„Staatschefs, Regierungschefs, Minister, stellvertretende Minister und Staatssekretäre; ...*
- *... Parlamentsabgeordnete oder Mitglieder vergleichbarer Gesetzgebungsorgane; ...*
- *... Mitglieder der Führungsgremien politischer Parteien ... Gerichtshöfen, Verfassungsgerichtshöfen ... Rechnungshöfen oder Leitungsorgane von Zentralbanken ...“* (§ 365n. Z 4 GewO).

Des Weiteren sind abgesehen vom Funktionsträger selbst, ausgenommen mittleren und niederen Ranges (§ 365n. Z 4 GewO), dessen Familienmitglieder (§ 365n. Z 5 GewO) und nahestehende Personen (§ 365n. Z 6 GewO) im Sinne der Gewerbeordnung als politisch exponierte Personen zu deklarieren. Funktionsträger mittleren und niederen Ranges sind explizit ausgenommen. Wenn festgestellt wird, dass es sich bei einem Kunden um eine

[257] *Coinfinity,* AML Abteilung..
[258] *Coinfinity,* AML Abteilung..

politisch exponierte Person handelt, wird auf Grundlage des § 365s. Abs 1 Z 3 GewO die Herkunft des Vermögens und des eingesetzten Mittels überprüft. Diese Überprüfung erfolgt durch Vorlage von Dokumenten, Daten oder Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen (Kontoauszügen, Dienstverträgen, etc.). Per Gesetz ist geregelt, dass ab dem Zeitpunkt der Beendigung eines Amtes einer politisch exponierten Person 12 Monate verstärkte Sorgfaltspflichten anzuwenden sind (§ 365s. Abs 3 GewO). Coinfinity wendet jedoch bei ehemals politisch exponierten Personen immer erhöhte Sorgfaltspflichten an und wendet somit strengere Regeln, als in der Gewerbeverordnung verankert, an. [259] Bei Nichteinhaltung der KYC/AML Maßnahmen drohen verwaltungsrechtliche Konsequenzen gemäß § 366b. Abs 2 GewO.

Der Gewerbetreibende hat bei der Risikobewertung nach § 365n1. GewO i.V.m. § 365s. Abs 4 und Abs 5 GewO die Anlage 8 der Gewerbeordnung zu berücksichtigen. In Anlage 8 der Gewerbeordnung sind jene Faktoren aufgezählt die ein potenziell erhöhendes Risiko darstellen können. Hier erfolgt genau wie in der Anlage 7 der Gewerbeordnung vorzufinden eine Unterteilung in diese drei Bereiche. Zu den Faktoren mit erhöhten Risiko zählen unter anderem: *„… neue Produkte und neue Geschäftsmodelle einschließlich neuer Vertriebsmechanismen sowie Nutzung neuer oder in der Entwicklung begriffener Technologien für neue oder bereits bestehende Produkte …*“ (Anlage 8 Gewerbeordnung).Würden Kryptobörsen als Verpflichtete gemäß der Gewerbeordnung gelten, so würde das Ergebnis der Risikobewertung erhöhte Sorgfaltspflichten bedingen. Coinfinity ergreift folgende risikobasierende Maßnahmen zur Aktualisierung der Risikofaktoren:

- 1 x p.a Check auf Gesamtumsatz pro Kunde
- 1 x p.a. Check Legitimationsdaten auf Dokumentenablauf
- 1 x p.a. Check PEP Liste auf Aktualität
- 1 x p.a Abgleich aktueller Wohnsitz und Staatsbürgerschaft mit Staatenliste aus geografischen Gebieten mit hohen Risiko[260]

Die Finanzmarktaufischt hat am 13.3.2018 das Rundschreiben „Risikoanalyse zur Prävention von Geldwäscherei und Terrorismusfinanzierung“ herausgegeben, das als Orientierungshilfe zur Umsetzung eines risikoorientierten Ansatzes der Verpflichteten nach dem Finanzmarkt-Geldwäschegesetz dient. Es dient u.a. als Leitfaden zur Risikoanalyse auf Unternehmenseben

[259] *Coinfinity,* AML Abteilung.
[260] *Coinfinity,* AML Abteilung.

und Einzelkundeneben. Es stellt keine Verordnung sondern lediglich die Auffassung der Finanzmarktaufsicht dar.[261] Da aktuell noch in keinem Gesetz Regelungen für die „neuen" Verpflichtete im Sinne der 5. Geldwäscherichtlinie getroffen wurden, könnten Dienstleistern die virtuelle Währungen in anerkannte Zahlungsmittel und umgekehrt tauschen in Anlehnung an dieses Schreiben eine Risikoanalyse erstellen um zumindest für die zukünftigen Regelungen vorbereitet zu sein.

Grundsätzlich gibt es Risikoerhebungsbögen für jedes betroffene Gewerbe der Gewerbeordnung, die nach Verlangen der Behörden auszuhändigen sind. Hier wäre aktuell der Risikoerhebungsbogen für Händler anwendbar, der sich in 6 Bereiche (Geografisches Risiko, Vertriebskanalrisiko, Produktrisiko, Kundenrisiko, Transaktionsrisiko und sonstiges Risiko) mit insgesamt 23 Unterpunkten unterteilet. Er kann digital ausgefüllt werden und das Risiko automatisch berechnet werden. Inhaltlich betrachtet ist dieser sehr dürftig und bei Unterstellung der Verpflichteten in das Gewerberecht müsste ein auf das Gewerbe mit virtuellen Währungen angepasster Risikofragebogen ausgearbeitet werden.[262]

8.3.5. Umsetzung des Geldwäschekonzepts

Im Mittelpunkt des Unternehmens steht neben der Akquirierung neuer Kunden der Schutz des Geschäftszweiges sowie des gesamten Unternehmens vor kriminellen Machenschaften, so das Unternehmen. Das Unternehmen weist fünf Kernbereiche auf, welche die Zielausrichtung des Unternehmens unterstützen und die Ausnützung des Unternehmens für Geldwäsche oder Terrorismusfinanzierung verhindern sollen:

1. Know-Your-Customer Check
2. Überprüfung der Mittelherkunft
3. Dokumentation & Aufbewahrung
4. Einschulung der Mitarbeiter
5. Meldepflicht[263]

Einer der wichtigsten Punkte ist der Know-Your-Customer Check, welcher vor jeder Geschäftsabwicklung durchgeführt wird. Das Unternehmen begründet nur dann eine Geschäftsbeziehung mit einer natürlichen oder juristischen Person, wenn die Identität der

[261] *Finanzmarktaufsicht,* Rundschrieben Risikoanalyse zur Prävention von Geldwäscherei und Terrorismusfinanzierung, https://www.fma.gv.at/download.php?d=3297,(abgerufen am 26. August 2018).
[262] *Wirtschaftskammer Österreich,* Geldwäschebekämpfung und Wirtschaftliche Eigentümer-Register, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/geldwaeschebekaempfung-wirtschaftliche-eigentuemer-register.html, (zugriff am 20. August 2018).
[263] *Coinfinity,* AML Abteilung.

wirtschaftlich berechtigten Person ausnahmslos geklärt ist. Geschulte Mitarbeiter sind für die Feststellung und Überprüfung der Kundenidentitäten zuständig und speichern sämtlich eingeholte Informationen.
Neben der Feststellung der Kundenidentität stellt die Überprüfung der Mittelherkunft den zweitwichtigsten Faktor dar. Grundsätzlich ist ein Mittelherkunftsnachweis ein Dokument, das unmittelbar belegt, wie und zu welchem Zeitpunkt ein Geldbetrag in die Vermögenssphäre einer Person eingegangen ist. Für die Überprüfung ist das Compliance-Team der Firma zuständig. Die Überprüfung erfolgt durch Vorlage von Dokumenten, Daten oder Informationen, die von unabhängigen und glaubwürdigen Quellen stammten. Dazu zählen Geschäftsberichte, Bilanzen, Gehaltsnachweise, Verträge sowie Auszahlungsbestätigungen von Banken. Bei Vermögenszuwachs durch Erbschaften muss Mittels (gerichtlichen) Einantwortungsbeschluss der Nachweis erbracht werden. Grundsätzlich sind nur Schenkungen über 50.000 Euro bei dem Finanzamt zu melden. Dennoch ist es nicht unüblich, dass bei größeren Beträgen unter 50.000 Euro von den Kunden das Vorlegen eines Schenkungsvertrages verlangt wird. Dies kann damit zusammenhängen, dass die Höhe der Transaktionen der Kunden auffällig bzw. unüblich für dessen Risikoprofil ist und die Mittelherkunft durch illegale Aktivitäten ausgeschlossen werden sollen.
Keine Herkunftsnachweise stellen Erklärungen Dritter, welche angeben, dass der Kunde vermögend sei, dar. Ferner das Vorlegen eines Safevertrages falls der Kunde angegeben hat, dass er das Geld im Safe gelagert hatte. Eine eidesstattliche Erklärung oder das Vorlegen eines Anlegerprofils einer Bank wird nicht als Herkunftsnachweis akzeptiert.
Es ist festzuhalten, dass je höher das Risiko / die Auffälligkeiten sind, desto weiter muss „zurück“ in die Vergangenheit geprüft werden. Ist die Vorlage von Nachweisen nicht möglich, ist mit dem Geldwäschebeauftragten Kontakt aufzunehmen und der Geschäftsfall schriftlich zu plausibilisieren.[264]

In folgenden Fällen prüft das Compliance Team des Unternehmens die Herkunft der Mittel:

- Sofern sich im Rahmen einer Kundenidentifikation herausstellt, dass ein Kunde eine politisch exponierte Person ist oder war, ein Familienmitglied einer politisch exponierten Person oder einer politisch exponierten Person bekanntermaßen nahestehende Person ist,
- wenn die Transaktion in bar den Gegenwert von EUR 10.000,-- übersteigt bzw. unbar

[264] *Coinfinity,* AML Abteilung.

den Gegenwert von EUR 15.000,-- übersteigt.[265]

Ein weiterer wichtiger Punkt ist die Plausibilität der Mittelherkunft. Das alleinige Vorlegen von Dokumenten reicht nicht aus. Zuerst werden geeignete Informationen und Dokumente vom Kunden eingeholt. Anschließend erfolgt eine Überprüfung der Stelle, die das Dokument ausgestellt hat. Es wird geprüft ob die Stelle glaubwürdig ist und ob das amtliche Dokument mit anderen bekannten, von der amtlichen Stelle ausgestellten Dokumenten, übereinstimmt. Zudem muss die Möglichkeit der Dokumentationsmanipulation berücksichtigt werden.
Abschließend wird die Auskunft der Kunden mit dem Nachweis der Mittelherkunft abgeglichen. Es wird überprüft ob die Aussagen stimmig und nachvollziehbar sind und ob die Beträge nachvollziehbar aus der angegebenen Quelle stammen. Zudem wird überprüft ob die Beträge auch zeitlich mit den Angaben aus dem Mittelherkunftsnachweis übereinstimmen.[266]
Sämtliche Daten die erhoben werden, werden in Anlehnung an § 365y. GewO aufbewahrt und auf verschlüsselten Servern gespeichert. Paragraph § 365y. GewO legt den Umfang der Aufzeichnung und Aufbewahrung von den erhobenen Daten fest. Informationen und Dokumente der Nutzer, die zur Einhaltung der Sorgfaltspflichten dienen, müssen 5 Jahre aufbewahrt werden und nach Ablauf der Frist gelöscht werden. Zudem müssen sichere Kommunikationskanäle im Unternehmen bestehen. Sämtliche Bestimmungen dienen zur Aufdeckung möglicher Geldwäscheaktivitäten (§ 365y. GewO).

Wie bereits erwähnt ist Coinfinity der Auffassung, dass Geldwäscheprävention nur durch aktive Mitwirkung aller Mitarbeiter funktioniert. Das Compliance Team des Unternehmens nimmt jährlich an besonderen Fortbildungsprogrammen, die der Erkennung von Geldwäsche- und Terrorismusfinanzierung und dem richtigen Verhalten in solchen Fällen dienen, teil (§ 365z. Abs 7 GewO). Zudem werden sämtliche Mitarbeiter des Unternehmens besonders geschult, da diese im Zweifelsfall jederzeit dazu in der Lage sein müssen Verdächtigkeiten zu erkennen und zu melden.[267]

8.4. Verdachtsmeldung nach § 365t. Gewerbeordnung

In § 365t. GewO wird die allgemeine Meldepflicht der Gewerbetreibenden geregelt. Es ist mit der Geldwäschemeldestelle zusammen zu arbeiten und bei Verdacht der Erfüllung der Paragraphen § 165 StGB oder § 278 StGB umgehend eine Verdachtsmeldung an das Bundeskriminalamt (§ 365t. GewO) zu erfolgen.

[265] *Coinfinity,* AML Abteilung.
[266] *Coinfinity,* AML Abteilung.
[267] *Coinfinity,* AML Abteilung.

Die Leitung, Koordination und Steuerung von überregionalen und internationalen Maßnahmen zur Bekämpfung von Kriminalität zählt zu den Aufgabenbereichen des Bundeskriminalamtes. Zudem können Personen, die verdächtigte Aktivitäten melden und Informationen haben diese anonym und unkompliziert dem Bundeskriminalamt übergeben.[268]
Gemäß § 4 Abs 2 des Bundeskriminalamt-Gesetz hat das Bundeskriminalamt unteranderem folgende Aufgabe zu erfüllen: *„ ... durch die Geldwäschemeldestelle die Entgegennahme und Analyse von Meldungen über verdächtige Transaktionen und sonstigen Informationen, die im Hinblick auf Geldwäscherei, damit zusammenhängende Vortaten oder Terrorismusfinanzierung relevant sind, sowie die Weiterleitung des Analyseergebnisses und zusätzlicher relevanter Informationen an inländische Behörden oder Stellen, soweit dies zur Bekämpfung von Geldwäscherei, damit zusammenhängender Vortaten oder Terrorismusfinanzierung erforderlich ist“* (§ 4 Abs 2 Z 1 des Bundeskriminalamt-Gesetz). Das dreiseitige Formular, welches vom BK zur Verfügung gestellt wird ist mit Hilfe einer sicheren Kommunikationsleitung zu übermitteln. Es müssen sämtliche Informationen die einen Grund zur Annahme der Geldwäsche begründen vorgelegt werden:[269]*„Bei Erhärtung des strafrechtlichen Verdachts im Zuge der Analyse kommt es zur Einleitung eines strafprozessualen Verfahrens. In der Regel erfolgt in diesem Kontext eine Vernehmung des Gemeldeten, die Berichterstattung an die zuständige Staatsanwaltschaft und das damit einhergehende Recht auf Akteneinsicht durch den Beschuldigten.[270]* Obwohl aktuell keine Pflicht zur Meldung durch Coinfinity besteht, erfolgt dennoch bei begründeten Verdacht eine Meldung von Seiten des Unternehmens.[271]
Zusammenfassend ist festzuhalten, dass anhand der Analyse der Anti-Money-Laundering Maßnahmen bzw. der Know-Your-Customer Maßnahmen des Unternehmens Coinfinity aufgezeigt wurde, dass aktuell genügend Bestimmungen vorhanden sind um ausreichende Maßnahmen zur Prävention von Geldwäsche und Terrorismusfinanzierung treffen zu können.
Abschließend ist festzuhalten, dass die Bestimmungen der Gewerbeordnung zur Anwendung kommen könnten und zukünftig eine explizite Unterstellung in die Gewerbeordnung der „neuen“ Verpflichteten durchaus denkbar und umsetzbar wäre. Durch Erlass einer Verordnung des Bundesministers für Wirtschaft, Forschung und Wirtschaft (BMWFW) könnten Dienstleister, die Kryptowährungen in ein anerkanntes Zahlungsmittel und umgekehrt tauschen sowie Wallet Provider zukünftig von der Gewerbeordnung erfasst werden. Der BMWFW ist gemäß § 365m1. Abs 1 Z 2 GewO berechtigt: *„... in*

[268] *Bundeskriminalamt*, Meldestellen, (abgerufen am 12. August 2018).
[269] *Bundeskriminalamt*, Informationsblatt, (abgerufen am 12. August 2018).
[270] *Bundeskriminalamt,* Informationsblatt, (abgerufen am 12. August 2018).
[271] *Coinfinity,* AML Abteilung.

Übereinstimmung mit dem risikobasierten Ansatz den Geltungsbereich der Bestimmungen dieses Abschnittes ganz oder teilweise auf Berufe oder Unternehmenskategorien dieses Bundesgesetzes auszudehnen, die zwar keine Gewerbetreibenden gemäß Abs. 2 sind, jedoch diesem Bundesgesetz unterliegende Tätigkeiten ausüben, bei denen es besonders wahrscheinlich ist, dass diese für Zwecke der Geldwäsche oder der Terrorismusfinanzierung genutzt werden; der Bundesminister für Wissenschaft, Forschung und Wirtschaft hat eine solche Ausdehnung der Europäischen Kommission mitzuteilen...“

8.4.1. Geldwäschemeldestelle

Die Aufsichtsbehörde kontrolliert ob die Sorgfaltspflichten ordnungsgemäß angewendet bzw. eingehalten wurden. Bei Nichteinhaltung der KYC/AML Maßnahmen drohen verwaltungsrechtliche Konsequenzen gemäß § 366b. Abs 2 GewO. Im Finanzsektor obliegt der Finanzmarktaufsicht die Überprüfung der Einhaltung der Sorgfaltspflichten der Verpflichteten. Die Bezirkshauptmannschaft überprüft die Einhaltung der Sorgfaltspflichten von Personen, die der Gewerbeordnung unterstellt sind. Sonstige Sorgfalts- und Meldepflichtige Personen werden durch die jeweiligen Kammern überprüft. Werden die Sorgfalts- und Meldepflichten von den Verpflichteten nicht eingehalten, so[272] *„ ... kommen die in den erwähnten Normen enthaltenen Strafbestimmungen zur Anwendung, die je nach Materie und Schwere des Verstoßes mit Geld- und Freiheitsstrafen sanktioniert werden. Die Überprüfung der Einhaltung dieser Bestimmungen und die Sanktionierung der Verstöße erfolgt durch die jeweils zuständigen Aufsichtsbehörden.“*[273]

Die Aufgaben der Geldwäschemeldestelle umfassen neben der eigenständigen Geldwäscheermittlung auch die Koordinierung der Ermittlungen, welche über die nationalen Grenzen hinausgehen. Zudem ist diese für den internationalen Schriftverkehr zuständig. Der Fachbereich Austrian Financial Intelligence Unit (A-FIU) nimmt die Funktion der Geldwäschemeldestellen ein, dessen Hauptaufgabe die Annahme und Analyse von verdächtigen Transaktionen ist. Die Ergebnisse der Analyse sowie weitere Informationen werden an inländische Behörden weitergeleitet. Des Weiteren arbeitet die Geldwäschemeldestelle mit zahlreichen anderen Behörden / Organisation zusammen. Es wird intensiv mit dem Europarat, dessen Expertenausschuss für Anti-Money-Laundering und Terrorismusfinanzierung und der Europäischen Union zusammengearbeitet. Die A-FIU ist Mitglied der Egmont Group, welche ein Zusammenschluss von 155 Finacial Intelligence

[272] *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, http://www.bundeskriminalamt.at/308/files/Geldwaesche_17_web.pdf (10), (abgerufen am 20. August 2018).
[273] *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, (10), (abgerufen am 20. August 2018).

Groups darstellt und die durch Verwendung einer sicheren Plattform gegenseitig Informationen über Geldwäsche und Terrorismusfinanzierung austauschen.[274] Es bestehen Kooperationen u.a. mit der Financial Action Task Force in Money Laundering (FATF), EU-FIUS und dem United Nations Office on Drugs and Crime Prevention (UNODC). Die FTAF ist eine Vereinigung von Ministern der angehörigen Mitgliedstaaten, dessen Ziel es ist internationale Standards zu setzen um die Integrität und den Schutz des internationalen Finanzsystems zu sichern. Es sollen einheitliche Rahmenbedingungen zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung entstehen welche jedoch auf die unterschiedlichen rechtlichen Rahmenbedingungen und Finanzsysteme der einzelnen Länder angepasst werden müssen. Es bereits erwähnt gibt 40 Empfehlungen die dazu dienen das Finanzsystem vor Missbrauch von Geldwäsche, Terrorismusfinanzierung und Proliferation zu schützen. Die Festlegung der zuständigen Behörden, Anwendung von Präventivmaßnahmen, Risikoeinschätzung, nationale Koordination, Verfolgung bei Vergehen, Transparenz und Bereitstellung von Informationen bilden die Kernelemente der Empfehlungen.[275]

8.4.2. Analyseverfahren

Nachdem eine Verdachtsmeldung bei der Geldwäschemeldestelle eingelangt ist, wird ein Analyseverfahren, welches in Abbildung 3 dargestellt ist, eingeleitet welches der Effektivität der Strafverfolgung dient:[276] *„In Anwendung der gesetzlich vorgesehenen Filterfunktion wird bereits im Vorfeld eines allfälligen strafprozessualen Ermittlungsverfahrens die eingegangene Information auf ihre wirtschaftliche Plausibilität und ihre mögliche strafrechtliche Relevanz geprüft.“*[277] Aus diesem Grund ist die Geldwäschemeldestelle zur Erhebung, Verarbeitung und Weiterleitung sämtlicher damit entstehenden Daten ermächtigt. Bestätigt sich durch das Analyseverfahren der anfängliche Verdacht, so wird ein Ermittlungsverfahren nach der Strafprozessordnung eingeleitet. Eine Abtretung der Zuständigkeit kann nach örtlichen oder sachlichen Zuständigkeitskriterien erfolgen.[278]

Die folgenden Abbildungen (Abbildung 2 & Abbildung 3) dienen zum Verständnis des gesamten Prozesses beginnend bei der Anwendung der Sorgfaltspflichten bis hin zur Meldung, Analyse und statischen Erfassung. Dennoch ist anzumerken, dass auf Grund

[274] *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, (13f), (abgerufen am 20. August 2018).
; *Egmont Group*, About, https://egmontgroup.org/content/about, (abgerufen am 20.August 2018).
[275] *FATF,* INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION, http://www.fatfgafi.org/media/fatf/ documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (abgerufen am 20. August 2018). *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, (13ff), (abgerufen am 20. August 2018).
[276] *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, (11ff), (abgerufen am 20. August 2018).
[277] *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, (13ff), (abgerufen am 20. August 2018).
[278] *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, 813ff), (abgerufen am 20. August 2018).

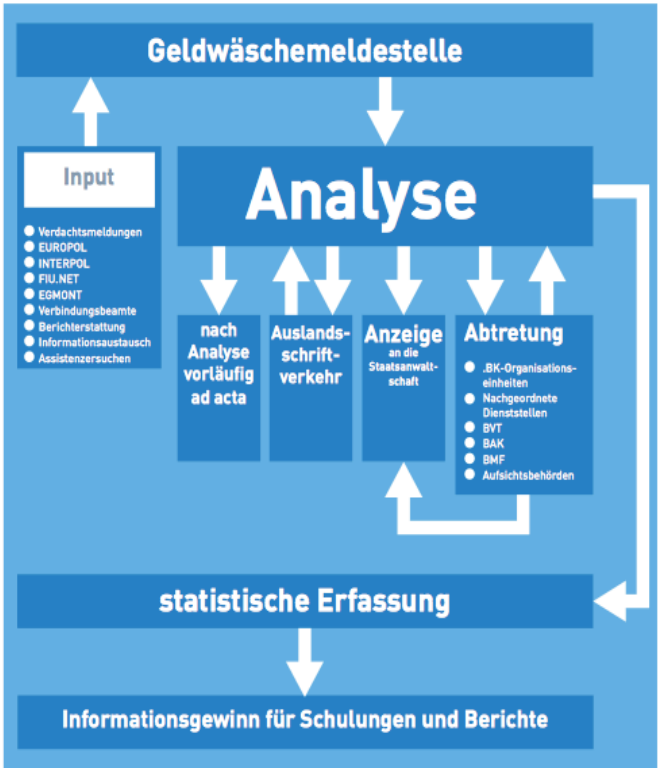
fehlender einheitlicher Regelungen keine einheitlichen Strukturen und somit kein einheitliches Vorgehen vorzufinden sind und jede Verdachtsmeldung mit einem Bezug zu Kryptowährungen individuell gehandhabt wird, so Mag Patrick Schreiner, MSc vom Bundeskriminalamt II/BK/KWK (Kompetenzzentrum Wirtschaftskriminalität). Die meisten Verdachtsmeldungen erfolgen von Seiten der Banken, welche oftmals unschlüssig und wenig aussagekräftig sind. Zudem werden meistens lediglich Screenshots von Exchanges bzw. unzureichende Informationen übermittelt, wodurch sich die Nachvollziehbarkeit der Mittelherkunft als äußerst schwierig erweist. Neben den regulativen Schwächen bestehen zudem Wissensdefizite Seitens der Mitarbeiter der Banken als auch der entgegennehmenden Behörde. Als Resultat hat die Strafverfolgungsbehörde Probleme bzgl. einer adäquaten Dokumentation sowie bei allfällig folgenden Ermittlungen. Aus diesem Grund gibt es aktuell keine seriös erhobenen Daten, was die Anzahl von derartigen Verdachtsmeldungen betrifft.
Aktuell wird daran gearbeitet eine neue Software zu implementieren, welche zukünftig auch ein Dokumentationsschema für virtuelle Währungen beinhalten soll. Um die Materie besser zu verstehen sowie auch am Puls der Zeit zu bleiben, arbeitet das BK mit Forschungseinrichtungen sowie den Key Play ern der Industrie zusammen, um mitunter das notwendige Know-How zu erlangen. Das BK nimmt dabei auch an nationalen und internationalen Projekten teil. Zudem erfolgt eine Sensibilisierung durch Bewusstseinsbildung bzw. werden Schulungen für Mitarbeiter im Bereich um virtuelle Währungen und Geldwäsche und Terrorismusfinanzierung angeboten.[279]

[279] *Mag Patrick Schreiner, MSc,* Bundeskriminalamt II/BK/KWK (Kompetenzzentrum Wirtschaftskriminalität) Interview geführt von Marina Kindel (28.September 2018).

Abbildung 2: Sorgfaltspflichten

Quelle: Bundeskriminalamt

Abbildung 3: Analyseverfahren



Quelle: Bundeskriminalamt

Im Lagebericht "Geldwäscherei 2017" des Bundeskriminalamtes werden virtuelle Währungen als neuere Entwicklungen der Geldwäsche deklariert. Ferner wird vermerkt, dass die Gründe die Novellierung der 4. Geldwäscherichtlinie in Bezug auf virtuelle Währungen mit dem erhöhten Risiko der Terrorismusfinanzierung einhergeht. Zudem sollte die Identifikation von Eigentümer von Kryptowährungen durch nationale Financial Intelligence Units (FIUs) ermöglicht werden. Überdies finden Überlegungen zu einer zentralen Datenbank, bei der sämtliche Identitäten der Eigentümer virtueller Währungen gespeichert werden, statt. Die Europäische Kommission soll diesbezüglich einen Bericht verfassen.[280]

Das Bundeskriminalamt steht der 5 GwR positiv gegenüber. Durch die Richtlinie erfolgt eine zusätzliche Informationsgewinnung für ein mögliches Ermittlungsverfahren innerhalb der EU-Mitgliedsstaaten. Dennoch ist darauf aufmerksam zu machen, dass die RL gravierende Mängel aufweist. Die Richtlinie umfasst weder Dienstleister, die virtuelle Währungen in andere virtuelle Währungen tauschen, noch Initial Coins Offerings, was äußerst bedenklich ist. Zudem stellt die RL keine global einheitliche Regelung dar, sondern lediglich eine Regelung auf EU- Ebene. Dadurch können Personen auf „Exchanger" in Ländern, außerhalb des EU- Raumes, die nicht von der Richtlinie erfasst sind „zurückgreifen". Potentielle

[280] *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, (23), (abgerufen am 20. August 2018).

Straftäter werden sich somit „Exchanger“ bedienen, welcher von dieser RL nicht umfasst sind. Durch die Umsetzung der RL wird man Straftaten mit einem Bezug zu Kryptowährungs zwar verringern, aber nicht verhindern können. Man macht es den Straftätern schlichtweg unangenehmer.[281]

[281] *Mag Patrick Schreiner, MSc,* Bundeskriminalamt II/BK/KWK (Kompetenzzentrum Wirtschaftskriminalität) Interview geführt von Marina Kindel (28.September 2018).

9. Konzessionspflicht von Geschäftsmodellen mit Virtuellen Währungen

Bei neuen Geschäftsmodellen von virtuellen Währungen ist zu prüfen ob eine Konzessionierung durch die Finanzmarktaufischt zu erfolgen hat.

Die Klärung der Konzessionspflicht ist jedoch oftmals ein sehr schwieriges Unterfangen, da grundsätzlich solche Geschäfte keine Konzessionsplicht bedingen, aber Änderungen im Detail zu verschiedenen Resultaten führen können[282]: *„Die Österreichische FMA kommt zum Ergebnis, dass der Kauf und Verkauf von Bitcoins kein konzessionspflichtiges Bankgeschäft gem. § 1 Abs. 1 BWG darstellt. Dennoch kann es sein, dass ein anderes Geschäftsmodell im Zusammenhang mit virtuellen Währungen einer Konzession unterliegt"*[283] Die deutsche Bundesanstalt für Finanzdienstleistungsaufsicht ordnet Bitcoins aufsichtsrechtlich[284] *„ ... als Finanzinstrumente in der Form von Rechnungseinheiten gemäß § 1 Absatz 11 Satz 1 Kreditwesengesetz (KWG).."*[285] ein. Solche Einheiten, sind mit Devisen vergleichbar, lauten jedoch nicht auf gesetzlich anerkannte Zahlungsmittel[286]: *„Hierunter fallen Werteinheiten, die die Funktion von privaten Zahlungsmitteln bei Ringtauschgeschäften haben, sowie jede andere Ersatzwährung, die aufgrund privatrechtlicher Vereinbarungen als Zahlungsmittel in multilateralen Verrechnungskreisen eingesetzt wird. Auf einen zentralen Emittenten kommt es hierbei nicht an."*[287] Obwohl die deutsche Regierung die virtuelle Währung Bitcoin explizit anerkannt hat, ist diese dennoch nicht als gesetzlich anerkanntes Zahlungsmittel oder als E-Geld zu klassifizieren.[288] Es gilt die Frage nach der Konzessionspflicht vor Aufnahme des Geschäftsbetriebes zu klären, da ansonsten neben Untersagung auch Verwaltungs- und gerichtliche Strafen drohen. Da aktuell jedoch oftmals Unklarheit vorherrscht werden Innovationen und in weiterer Folge der Wirtschaftsstandort Österreich als solcher gehemmt. Grundsätzlich soll der faire Wettbewerb zwischen bestehenden und neuen Unternehmen im Finanzsektor gewährleistet werden. Das Verfahren zur Erlangung der Konzession kann langwierig sein und mit hohen Investitionen verbunden sein. Um dieser Problematik entgegen

[282] *Bundesministerium für Digitalisierung und Wirtschaftsstandort*, 386/AB vom 30.4.2018 zu 383/J (XXXVI.GP) https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_00386/imfname_691962.pdf (Stand 30.4.2018).; *Piska / Völkel,* ZTR 2017 97.

[283] *Wirtschaftskammer Österreich,* Die Kryptowährung, https://www.wko.at/branchen/information-consulting/finanzdienstleister/artikel-kryptowaehrung.pdf, (abgerufen am 20. August 2018).

[284] *Bundesanstalt für Finanzdienstleistungsaufsicht,* Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, (abgerufen am 20. August 2018).

[285] *Bundesanstalt für Finanzdienstleistungsaufsicht,* Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, (abgerufen am 20. August 2018).

[286] *Bundesanstalt für Finanzdienstleistungsaufsicht,* Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, (abgerufen am 20. August 2018).

[287] *Bundesanstalt für Finanzdienstleistungsaufsicht,* Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, (abgerufen am 20. August 2018).

[288] *Wirtschaftskammer Österreich,* Die Kryptowährung, (abgerufen am 20. August 2018).

zu steuern sollten zusätzliche Mechanismen zu Erteilung der Konzession gesetzlich verankert werden. Zukünftig sind regulatorische Sandboxes für Unternehmen geplant.[289]

[289] *Bundesministerium für Digitalisierung und Wirtschaftsstandort*, 386/AB vom 30.4.2018 zu 383/J (XXXVI.GP), (Stand 30.4.2018).

10. Sandboxes

Am 1. März 2018 erfolgte eine parlamentarische Anfrage[290] zu virtuellen Währungen und rechtlichen Rahmenbedingungen sowie Blockchain-Anwendungen für den Wirtschaftsstandort Österreich an das Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW).

Inhalt der Anfrage war unter anderem welche Maßnahmen das Ministerium für Blockchain - Unternehmen zukünftig treffen wird, um für diese den Wirtschaftsstandort Österreich aus Unternehmenssicht attraktiver zu gestalten.[291] Die Beantwortung dieser Frage hatte den Terminus „Sandboxes" zum Inhalt. Firmen soll es ermöglicht werden innovative Technologien, für die es noch keine klar formulierten rechtlichen Regelungen gibt, in einem beschränkten Umfeld mit Aufsicht testen lassen zu können, ohne dass den Unternehmen rechtliche Konsequenzen drohen. Voraussetzung ist die vollständige Einsicht von sämtlichen Behörden. Es ist festzuhalten, dass grundsätzlich keine Ausnahmen des EU-Rechts von Seiten der Aufsichtsbehörden genehmigt werden dürfen. Es gilt stets die europarechtlichen sowie die verfassungsrechtlichen Vorgaben zu berücksichtigen.[292]

Um zukünftig über die Förderung von Finanzprodukte und somit über die Steigerung der Attraktivität des Wirtschaftsstandortes Österreich zu entscheiden wurde Anfang April 2018 der „FinTech-Beirat" ins Leben gerufen. Die Finanzmarktaufsicht sowie die Nationalbank und Vertreter des Finanzsektors sind Mitglieder. Hier steht der Wirtschaftsstandort als solcher und nicht die Klärung rechtlicher Rahmenbedingungen im Fokus. Damit Unternehmen an Behörden herantreten können und Fragen zu rechtliche Rahmenbedingungen wie Compliance oder Geldwäsche stellen können wurde die Kontaktstelle „FinTech" in der Finanzmarktaufsicht eingerichtet.[293] Die Finanzmarktaufsicht konnte aktuell keine Auskunft darüber erteilen, in welche Richtung die Umsetzung der 5. Geldwäscherichtlinie in das nationale Recht tendiert, da beim aktuellen Stand der Arbeit diesbezüglich keine Informationen vorlagen. Zudem erkennt die Finanzmarktaufsicht Lücken, die nicht durch die 5 Geldwäscherichtlinie geschlossen werden können, an.[294] Neben den FinTech-Beirat entstand 2017 die „Blockchain Roadmap for Austria", wodurch unter anderem ein Neun

[290] *Gamon,* Anfrage 383/J vom 01.03.2018 (XXVI.GP), https://www.parlament.gv.at/PAKT/VHG/XXVI/J/J_00383/imfname_683622.pdf (Stand 01.03.2018).
[291] *Gamon,* Anfrage 383/J vom 01.03.2018 (XXVI.GP), (Stand 01.03.2018).
[292] *Bundesministerium für Digitalisierung und Wirtschaftsstandort*, 386/AB vom 30.4.2018 zu 383/J (XXXVI.GP) (Stand 30.4.2018); *Piska / Völkel,* ZTR 2017 97.
[293] *Bundesministerium für Finanzen,* 382/AB vom 30.4.2018 zu 382/J (XXVI.GP), https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_00382/imfname_691926.pdf, (Stand 30.4.2018).
[294] *Mag.Weratschnig Thomas,* Prävention von Geldwäscherei und Terrorismusfinanzierung der Finanzmarktaufsicht, Interview geführt von Marina Kindel (22. August 2018).

Punkte Plan für Österreich entwickelt wurde. Dieser beinhaltet unteranderem die Bereiche Forschung, Förderung, Information und Reports.[295]

Es wurde das Forschungsinstitut für Kryptoökonomie an der Wirtschaftsuniversität Wien sowie das Förderungsprogramm Smart and Digital Services (SDS) der österreichischen Förderungsgesellschaft ins Leben gerufen, bei denen unterschiedliche Blockchain-basierende Projekte gefördert werden. Zudem wird die Anwendbarkeit Blockchain-basierender Dienste im E-Government geprüft:[296] *„Darüber hinaus ist das BMDW in der ASI (Austrian Standards International) - Arbeits- gruppe 001.88 "Blockchain und distributed ledger technologies" vertreten. Eines der Ziele ist dabei, ein bundesweit einheitliches Vorgehen und die Kompatibilität der tech- nischen Lösungen sicherzustellen."*[297]

Da jedoch zum aktuellen Zeitpunkt nicht abschätzbare Risiken und Chancen bei virtuellen Währungen bestehen, wurde im Februar 2018 von der Europäischen Kommission das EU „Blockchain Observatory" gegründet, welches sich auf europäischer Ebenen mit der Thematik auseinandersetzt. Das Bundesministerium für Finanzen hält fest[298] : „*Generell ist die Frage der Förderung spezifischer Finanzprodukte oder Technologien eine rechtspolitische und keine Angelegenheit des Vollzuges. Aus Sicht des Vollzuges geht es primär darum, klare Rahmenbedingungen und Rechtssicherheit zu schaffen."*[299]

Besonders interessant ist, dass einige rechtliche Fragen der Anfrage 382/J[300] nicht beantwortet bzw. umgangen wurden. Vor allem die Fragen in Bezug auf die rechtliche Einordnung von Utility Token und Equity Token bzw. die rechtliche Unterscheidung von Coins und Token wurden nicht beantwortet. Zudem muss aus technischer Sicht zwischen pseudoanonymen und anonymen Kryptowährungen unterschieden werden. In der Frage 21 der Anfrage 382/J wurde darauf hingewiesen und nach der damit möglichen einhergehenden rechtlichen Unterscheidung bzw. Einordnung dieser gefragt. Auch hier gab es weder eine Antwort noch einen Verweis auf andere zuständige Behörde.

Des Weiteren wurde in Punkt 14 der Anfrage 382/J nach regulatorischer Klarheit in Bezug auf virtuelle Währungen, ICOs, Coins und Tokens gefragt, da aktuell widersprüchliche Einstufungsversuche von Seiten der zuständigen Ministerien, Rechtsprechung und Lehre vorzufinden sind. Ferner sind Divergenzen auf sämtlichen Ebenen, ob auf europäischer, internationaler oder österreichischer Ebene, vorzufinden. Dies wurde in der Anfrage angemerkt und zudem wurden die bisherigen Schritte erfragt, um bestehende Widersprüche

[295] *Blockchain Austria,* Unser 9 Punkte Plan, https://www.blockchain-austria.gv.at/unser-9-punkte-plan/ (abgerufen am 20. August 2018).
[296] *Bundesministerium für Digitalisierung und Wirtschaftsstandort,* 386/AB vom 30.4.2018 zu 383/J (XXXVI.GP), (Stand 30.4.2018).;
[297] *Bundesministerium für Digitalisierung und Wirtschaftsstandort,* 386/AB vom 30.4.2018 zu 383/J (XXXVI.GP) (Stand 30.4.2018).
[298] *Bundesministerium für Finanzen,* 382/AB vom 30.4.2018 zu 382/J (XXVI.GP), (Stand 30.4.2018).
[299] *Bundesministerium für Finanzen,* 382/AB vom 30.4.2018 zu 382/J (XXVI.GP), (Stand 30.4.2018).
[300] *Claudia Gamon,* Anfrage 382/J vom 01.03.2018 (XXVI.GP),
https://www.parlament.gv.at/PAKT/VHG/XXVI/J/J_00383/imfname_683622.pdf, (Stand 1.3.2018).

zu beseitigen. Hier wurde von Seiten des BMF vermerkt, dass aktuell regulatorische Unklarheit besteht, da die Zuständigkeit der Ressorts erst geklärt werden muss. Zudem wird festgehalten, dass virtuelle Währungen keine Finanzinstrumente, E-Geld, kein Zahlungsmittel oder ein Zahlungsinstrument gemäß der vorherrschenden Gesetze darstellen, sondern als sonstige unkörperliche Wirtschaftsgüter zu deklarieren sind.[301]

Neben der Finanzmarktaufischt konnte auch das Bundesministerium für Digitalisierung und Wirtschaft sowie das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz keine Auskunft darüber erteilen, in welche rechtliche Richtung die Umsetzung der 5. Geldwäscherichtlinie in das nationale Recht tendiert.

Es ist sich die Frage zu stellen, ob die zuständigen Behörden bzw. die gesetzgebende Instanz über genügend technisches Know-How in Bezug auf virtuelle Währungen verfügt um für diese realistische rechtliche Rahmenbedingungen schaffen zu können. Wie es den Anschein erweckt, bedarf es einer genaueren Auseinandersetzung mit den technischen Details virtueller Währungen um zukünftig ausreichend Klarheit über die rechtliche Einordnung solcher schaffen zu können. Zudem muss zügig geklärt werden welches Ressort zuständig ist.

[301] *Gamon,* Anfrage 382/J vom 01.03.2018 (XXVI.GP), (Stand 1.3.2018), *Bundesministerium für Finanzen,* 382/AB vom 30.4.2018 zu 382/J (XXVI.GP), (Stand 30.4.2018).

11. Technischer Aspekt

Um rechtliche Regelungen treffen zu können, ist das technische Verständnis von virtuellen Währungen bzw. von der dahinterstehenden Technologie unabdingbar. Folgender Abschnitt soll die wichtigsten technischen Komponenten darlegen. Es soll verdeutlicht werden, dass nicht jede virtuelle Währung im gleichen Umfang für Geldwäschezwecke geeignet ist. Zudem soll das in der Politik, Gesellschaft und Wirtschaft bestehende Vorurteil, dass sich vor allem die virtuelle Währung Bitcoin besonders gut für Geldwäscheaktivitäten eignet entkräftet werden. Es muss eine Unterscheidung zwischen anonymen und pseudoanonymen Währungen getroffen werden, die durch verschiedene Anonymisierungsmethoden einen unterschiedlich hohen Grad an Anonymität der Zahlungen vorweisen und sich dadurch in unterschiedlichen Maß für Geldwäscheaktivitäten eignen.

11.1. Verwendung von Bitcoin im Darknet

Kryptowährungen genießen einen zweifelhaften Ruf als unreguliertes und anonymes Zahlungsmittel. Der selbst bis heute anonyme Erfinder von Bitcoin und Blockchain, eine Person oder eine Gruppe von Personen hinter dem Pseudonym Satoshi Nakamoto, legte großen Wert auf die Privatsphäre der Nutzer von Kryptowährungen.[302] Unter Privatsphäre ist die Möglichkeit des Versteckens von Informationen über eine Person oder Gruppe zu verstehen. Die Privatsphäre bezogen auf Geld setzt sich aus folgenden zwei Faktoren zusammen: Anonymität und Transparenz. Das Maximum an Privatsphäre wird ermöglicht, wenn die Anonymität am größten und die Transparenz am niedrigsten ist. Die Anonymität bei virtuellen Währungen bezieht sich auf die Kryptowährungs-Adresse und die Transparenz auf die Nachvollziehbarkeit von Transaktionen bzw. der Einsehbarkeit der Transaktionshistorie.[303] Als erste Kryptowährung basierend auf Blockchain-Technologie wurde Bitcoin in den frühen Phasen seiner Entwicklung oft als Zahlungsmittel für Transaktionen im Internet verwendet. Eine erste breitere Anwendung fand Bitcoin im sogenannten „Deep Web“ bzw. „Darknet“, in welchen es als anonymes Zahlungsmittel für Transaktionen auf dem virtuellen Schwarzmarkt Silk Road verwendet wurde. Die Silk Road war ein Hidden Service im TOR-Netzwerk (The Onion Router) welcher eine Reihe von illegalen Drogen, Dienstleistungen und anderen Produkten zum Kauf und Verkauf anbot. Zudem spielte Bitcoin eine nachweislich wesentliche Rolle als Mittel zur Geldwäsche

[302] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, (6), (abgerufen am 26. August 2018).
[303] *Hosp,* Kryptowährungen, (2018) 128f.

innerhalb des Tor-Netzwerks. [304] Die Möglichkeit mit Bitcoin illegale Aktivitäten durchzuführen begründet sich jedoch nicht in den technischen Eigenschaften der Kryptowährung alleine, sondern primär in jenen des TOR-Netzwerks.[305] Die Financial Action Task Force in Money Laundering (FATF) hebt hervor, dass der kombinierte Einsatz von Anonymisierungsverfahren des TOR-Netzwerks, sowie die technischen Eigenschaften von Bitcoin notwendig waren um den Nutzern der Silk Road weitestgehende Anonymität zu ermöglichen.[306] Die wesentlichen potentiellen Risiken der Geldwäsche in Bezug auf Bitcoin basieren auf der erhöhten Anonymität und der Abwesenheit zentraler Verwaltungsstellen im Vergleich zu anderen Zahlungsmethoden. Bitcoin Nutzer müssen keine Identifikationen oder Verifikationen vornehmen um am Bitcoin-Zahlungsnetzwerk teilnehmen zu können. Der vermutete Umsatz auf der Silk Road betrug laut FATF ca. 1,2 Milliarden US Dollar (ca. 9.5 Millionen Bitcoins zu damaligen Preisniveaus). Darüber hinaus besagen Schätzungen, dass hunderte Millionen an US Dollars in Form von Bitcoins auf der Silk Road gewaschen wurden.[307]

11.2. Darknet – Nationale Risikoanalyse 2015

Um Zugang zum Dark Net, Anonymisierungstool, zu erhalten muss der Nutzer eine Software, TOR, herunterladen. Diese wurde extra dafür entwickelt und ist für jeden Nutzer frei zugänglich:[308] *„ Dieses Anonymisierungstool erwirkt, dass u.a. auf Peer-to-Peer-Basis (P2P) lose Verbindungen einzelner Computer untereinander aufgebaut werden und Headerdaten der anfragenden Computer nach Zwischenschaltung von mindestens drei weiteren Rechnern (nodes) zur Gänze ausgetauscht und somit anonymisiert werden. "*[309] TOR ist ein dezentrales Netzwerk welches die Verbindungsdaten der Nutzer anonymisiert und keine Analyse des Datenverkehrs zulässt. Bitcoin selbst ermöglicht jedoch keine anonymen Transaktionen, die Identität des Nutzers ist lediglich hinter einem kryptographischen Pseudonym versteckt.[310] Die Transparenz der meisten Blockchains, allem voran die von Bitcoin, ist zu 100 % gegeben.

[304] *Read / Gräslund,* EU-Regulierung von Bitcoin und anderen virtuellen Währungen: erste Schritte, https://link.springer.com/article/10.1007/s10273-018-2323-6 (507ff.), (abgerufen am 01. Oktober 2018).
[305] *Leistert,* BITCOIN UND BLOCKCHAIN, https://www.uni-muenster.de/Ejournals/index.php/pop/article/viewFile/1732/1667, (80), (abgerufen am 26. August 2018).
[306] *Financial Action Task Force in Money Laundering,* Virtual Currencies – Key Definitions and Potential AML/CFT Risks, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (11), (Zugriff: am 30. September 2018).
[307] *Financial Action Task Force in Money Laundering,* Virtual Currencies – Key Definitions and Potential AML/CFT Risks, (Zugriff: am 30. September 2018).
[308] *Bundesministerium für Finanzen,* Nationale Risikoanalyse Österreich 2015, https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/Nationale_Risikoanalyse_Oesterreich_PUBLIC.pdf (11), (Stand 2015).
[309] *Bundesministerium für Finanzen,* Nationale Risikoanalyse Österreich 2015, (11), (Stand 2015).
[310] *Möser /Böhme / Breuker*, An inquiry into money laundering tools in the Bitcoin ecosystem. https://ieeexplore.ieee.org/document/6805780, (1), (abgerufen am 28. August 2018).

Die Transaktionen sind komplett einsehbar und zurück verfolgbar.[311] Staatliches Bargeld ist demnach für Geldwäsche und andere kriminelle Aktivitäten deutlich besser geeignet, so Johannes, Präsident von Bitcoin Austria.

Das Darknet stellt somit eine Kommunikationsplattform, bei der jeder User absolut anonym bleibt, dar. Die Daten werden zwischen den Teilnehmern, durch Verwendung von diversen Verschlüsselungstools, verschlüsselt ausgetauscht. Dadurch wird die Abwicklung von illegalen Geschäften erleichtert. Die Geldwäschemeldestelle stuft die Risiken, die sich auf Grund der Verwendung virtueller Währungen im Darknet ergeben als hoch ein.[312] „ Kryptowährungen haben in Bezug auf KYC/AML keinen guten Ruf, was aus den Anfängen von Bitcoin herrührt, wo es als Zahlungsmittel im Darknet verwendet wurde. Es gibt empirisch keine Daten die belegen würden, dass Geldwäsche und Terrorismusfinanzierung überproportional stark bei Kryptowährungen stattfinden würde. Eine Arbeitsgruppe des US Kongresses kam im September zum Schluss, dass virtuelle Währungen bei der Finanzierung terroristischer Aktivitäten kaum eine Rolle spielen, wichtigstes Zahlungsmittel für Terrororganisationen ist Bargeld“ so Dr. Oliver Völkel. Obwohl Virtuelle Währungen seit 2008 existieren wurden diese zur damaligen Zeit Seitens der Strafverfolgungsbehörden nicht als relevant betrachtet. Erst in den letzten Jahren wurden Virtuelle Währungen und die damit einhergehende Möglichkeit der Geldwäsche und Terrorismusfinanzierung als realistisches Problem anerkannt. Seitdem wird aktiv an Gegenmaßnahmen gearbeitet.[313] Mag. Patrick Schreiner, MSc, Abteilung II/BK/7/KWK, ist folgender Auffassung: „Die Annahme, dass sich Bargeld für Geldwäscheaktivitäten besser eignet als Virtuelle Währungen kann als solche nicht pauschal bestätigt werden. Es müssen stets die unterschiedlichen Geldwäschemöglichkeiten der zwei Systeme berücksichtigt werden. Auch die kriminelle Energie, welche Straftäter zum Zwecke der Geldwäsche gewillt sind einzubringen, unterscheiden die Systeme immanent. Zudem sind je nach System und Ausgestaltung unterschiedliche Intermediäre involviert, wodurch sich Geldwäscheaktivitäten unterschiedlich ausgestalten. Krypotowährungen können sich sehr wohl für Geldwäscheaktivitäten, u.a. durch Verwendung von Verschleierungsdiensten, eignen.

Der Kauf von Suchtmitteln erfolgt fast ausschließlich durch Kryptowährungen, allem voran mit Bitcoins und Litecoins. Das Problem wird wie folgt dargestellt: Kryptowährungen können nicht durch Finanzmechanismen kontrolliert oder überwacht werden. Man spricht von einem

[311] *Hosp,* Kryptowährungen, (2018) 130.
[312] *Bundesministerium für Finanzen,* Nationale Risikoanalyse Österreich 2015, (Stand 2015).
[313] *Mag Patrick Schreiner, MSc,* Bundeskriminalamt II/BK/KWK (Kompetenzzentrum Wirtschaftskriminalität) Interview geführt von Marina Kindel (28.September 2018).

sogenannten „Grauen Finanzmarkt“. Diese werden in elektronischen Geldbörsen virtuell abgespeichert und sind vor externen Zugriffen geschützt. Diese Probleme versucht man auf EU-Ebene durch Regulierungsversuche entgegen zu steuern. Da es jedoch ein grenzüberschreitendes bzw. ein weltweites Problem darstellt, sind geographisch begrenzte Regulierungen keine Lösung.[314] Bitcoin-Transaktionen sind für alle Zeiten für jeden einsehbar und in der Blockchain gespeichert. Selbst wenn heute bei manchen Behörden noch Know-How oder benutzerfreundliche Analysetools fehlen, so kann man durchaus davon ausgehen, dass zu einem späteren Zeitpunkt Identitäten und Geldflüsse im Zusammenhang mit Bitcoin-Transaktionen aufgedeckt werden können.[315]

Seit der Entwicklung von Bitcoin sind eine große Anzahl weiterer Kryptowährungen konzipiert worden, welche sich in spezifische Aspekte dieser Technologie unterscheiden. Darunter findet sich jene Gruppe der sogenannten „Privacy Coins“, welche verschiedene Methoden der Anonymisierung von Kryptowährungs-Transaktionen und den Identitäten der Nutzer verwenden.[316] Es erfolgt eine Differenzierung zwischen pseudonymen und anonymen Kryptowährungen. Ist nun die Anonymität und die Transparenz nahezu grenzenlos wird von Pseudo-Anonymität gesprochen. Darunter ist folgendes zu verstehen[317]: *„Pseudo-anonym bedeutet, dass ein Computer aufgrund der hohen Transparenz (dessen, was passiert) und trotzt zunächst scheinbar hoher Anonymität Transaktionen rückrechnen, die fehlenden Informationen zu einer Identität zusammensetzen und somit die Anonymität reduzieren könnte.“*[318] Somit kann herausgefunden werden welche Person hinter welchem User steht ohne die Identität zu kennen.[319] Auf der einen Seite gibt es Mustererkennungsverfahren und die Möglichkeit durch aufwendige Analysen Identitäten festzustellen, andererseits gibt es die Möglichkeiten etwa durch „Einzahlung über ATMs, Prepaid-Karten oder geheime OTC-Deals, gefolgt von einem Handel über z.B. Shapeshift, ausländischen oder dezentralen Börsen komplett anonym zu bleiben.[320] Shapeshift ist ein Anbieter, bei dem nur Wallet Adressen benötigt werden um virtuelle Währungen gegen andere virtuelle Währungen tauschen zu können. Virtuelle Währungen gegen Fiatgeld zu tauschen und umgekehrt ist nicht möglich. Shapeshift stellt dennoch eine Alternative zu bestehenden Tauschbörsen dar. Solche Anbieter sind nicht von der Geldwäscherichtlinie erfasst und unterliegen keinerlei rechtlichen

[314] *Bundesministerium für Finanzen,* Nationale Risikoanalyse Österreich 2015, (13), (Stand 2015).
[315] *Ing. Johannes Grill,* Präsident Bitcoin Austria, Interview geführt von Marina Kindel (3. August 2018).
[316] *Prinz,* Vollständige Liste der Anonymen Kryptowährungen, https://www.bitfantastic.com/kryptowaehrung/vollstaendige-liste-der-anonymen-kryptowaehrungen/2018/ (Zugriff 28. August 2018).
[317] *Hosp,* Kryptowährungen, (2018) 130 f.
[318] *Hosp,* Kryptowährungen, (2018) 130 f.
[319] *Hosp,* Kryptowährungen, (2018) 130.
[320] *Florian Wimmer,* CEO, Co-Founder, Interview geführt von Marina Kindel (22. Juli 2018).

Bedingungen. Es erfolgt keine Identifikation, die Kunden müssen keinerlei Daten bekanntgeben wodurch die Anonymität somit zur Gänze gegeben ist.[321]
Aktuell wendet das Bundeskriminalamt kommerzielle und selbstentwickelte Analysetools an. Für Mustererkennungsverfahren ist in Österreich keine eindeutige Rechtslage vorzufinden, da dies möglicherweise auch einer Rasterfahndung gleichkommt. Bedingt durch diesen Umstand und einem exorbitant hohen Ressourcenaufwand kommen aktuell keine Mustererkennungsverfahren in Österreich zur Anwendung.[322]
Zudem gibt es zahlreiche virtuelle Währungen wie z.B. Monero, Zcash oder Verge, die durch Verschleierungstechniken im Transaktionsprotokoll, die Privatsphäre der User maximieren und von diesen gerne verwendet werden um ihre Transaktionsflüsse zu verschleiern.[323]

11.3. Pseudonyme Kryptowährungen

11.3.1. Bitcoin

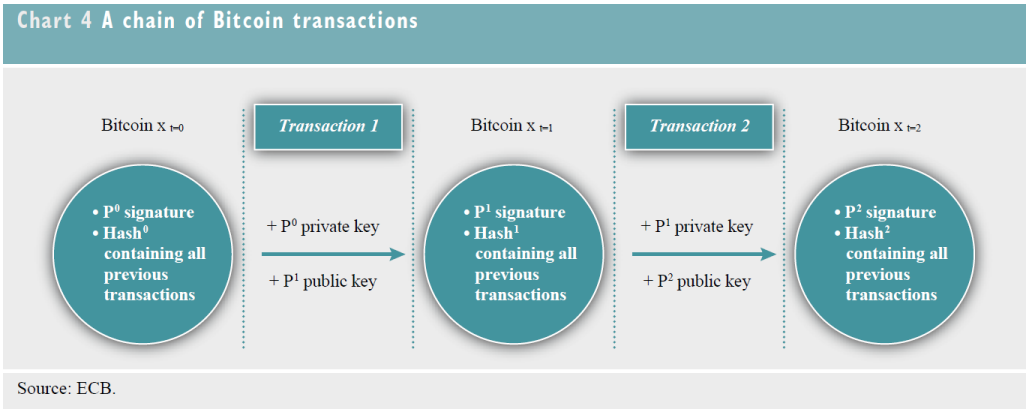
Bitcoin ist die bekannteste und am weitesten verbreitete pseudonyme Kryptowährung. Sie basiert auf einem dezentralen Buchungssystem, welches sämtliche Transaktionen und Vermögenswerte spezifischen kryptographischen „Adressen" zuweist und diese transparent und öffentlich zugänglich macht. Die dezentral verwaltete öffentliche Datenbank in der alle Transaktionen verzeichnet sind, wird als Blockchain bezeichnet. Eigentumsverhältnisse und Transaktionen basieren auf Public-Key-Verschlüsselungsverfahren.
Bitcoin basiert auf dem Secure Hash Algorithm 2 (spezifisch: SHA-256).[324] Ein Hashwert das Ergebnis einer mathematischen Streuwertfunktion, welche eine beliebig große Menge an Information (Input) in eine Zielmenge mit fixer Länge (Output) transformiert. Generierte Hashwerte sind hierbei einzigartig und können wie eine Art Fingerabdruck für Daten gesehen werden. Kleinste Veränderungen an dem Input verändern den resultierenden Output signifikant.[325] Somit kann nachvollzogen werden, ob Veränderungen am Input vorgenommen wurden. Die Informationen, welche über einen so generierten Hashwert verarbeitet werden, können mathematisch nicht errechnet werden. Die Kenntnis über einen Hashwert erlaubt keine Möglichkeit die darin verarbeiteten Informationen herauszufinden. In der Bitcoin Blockchain werden diese Hashwerte verwendet um Transaktionen zu gruppieren und in

[321] *Wimmer*, Mit Shapeshift.io unkompliziert Kryptowährungen tauschen, https://www.crypto-magazin.com/shapeshift-io/ (abgerufen am 10 August 2018).
[322] *Mag Patrick Schreiner, MSc,* Bundeskriminalamt II/BK/KWK (Kompetenzzentrum Wirtschaftskriminalität) Interview geführt von Marina Kindel (28.September 2018).
[323] *Hosp,* Kryptowährungen, (2018) 152ff
[324] *Antonopoulos*, Mastering Bitcoin, https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf, (192), (abgerufen am 01. September 2018).
[325] *Antonopoulos*, Mastering Bitcoin, (71), (abgerufen am 01. September 2018).

Datenblöcken zu speichern, sowie um Transaktionen durchzuführen und miteinander zu verknüpfen.[326]

Ein weiterer technischer Aspekt von Bitcoin ist Asymmetrische Kryptographie in Form von Public-Key-Kryptographie. Hierbei werden über ein Verschlüsselungsverfahren zwei verknüpfte „Schlüssel" erstellt. Jenes Schlüsselpaar bezeichnet man als öffentlichen und privaten Schlüssel, welche mathematisch eindeutig miteinander verknüpft sind. In dem Transaktionssystem von Bitcoin werden öffentliche Schlüssel als Zuordnungen von Bitcoin-Vermögen verwendet. Private Schlüssel erlauben den Zugriff und die Durchführung von Transaktionen in Kombination mit dem korrespondierenden öffentlichen Schlüssel. Ähnlich wie bei den Input- und Output-Werten von Hashwerten herrscht eine einseitige Beziehung: Das Wissen über den privaten Schlüssel erlaubt die Berechnung des korrespondierenden öffentlichen Schlüssels, jedoch ist es nicht möglich anhand des öffentlichen Schlüssels den korrespondierenden privaten Schlüssel zu erfahren.[327] Verschlüsselte Daten können nur mit dem privaten Schlüssel entschlüsselt werden.[328]

Abbildung 4: Funktionsweise von Bitcoin Transaktionen



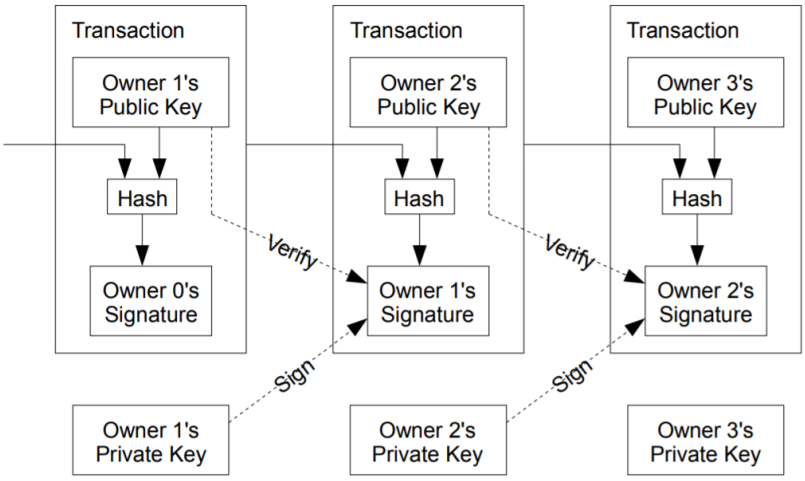
Quelle: Europäische Zentralbank

Eine Bitcoin Transaktion involviert sowohl Hashwerte, als auch asymmetrische Kryptographie. Um eine Transaktion durchzuführen, teilt der Empfänger dem Sender seinen öffentlichen Schlüssel mit, welche als Zieladresse fungiert. Der Sender signiert seine Transaktion mit dem Hashwert aller vorherigen Transaktionen und dem öffentlichen Schlüssel des Empfängers. Der private Schlüssel des korrespondierenden öffentlichen

[326] *Antonopoulos*, Mastering Bitcoin, (27), (abgerufen am 01. September 2018).
[327] *Kammler / Pohlmann*, Bitcoin: Geldverkehr ohne Banken Kryptografie wird Währung, https://norbert-pohlmann.com/app/uploads/2015/08/308-Kryptografie-wird-W%C3%A4hrung-Bitcoin-Geldverkehr-ohne-Banken-Prof-Norbert-Pohlmann.pdf (60f), (abgerufen am 31. August 2018).
[328] *Antonopoulos*, Mastering Bitcoin, (63ff), (abgerufen am 01. September 2018).

Schlüssels wird zur Erstellung einer digitalen Signatur verwendet, welche die Transaktion bestätigt. Private Schlüssel müssen daher vom jeweiligen Nutzer stets geheim gehalten werden, während öffentliche Schlüssel als Mittel zur Identifikation von Sender und Empfänger fungieren. Daher ist Bitcoin nicht als anonyme Kryptowährung zu klassifizieren, sondern entspricht der Definition einer pseudonymen Kryptowährung.[329]

Abbildung 5: Verkettung von Bitcoin Transaktionen



Quelle: Satoshi Nakamoto

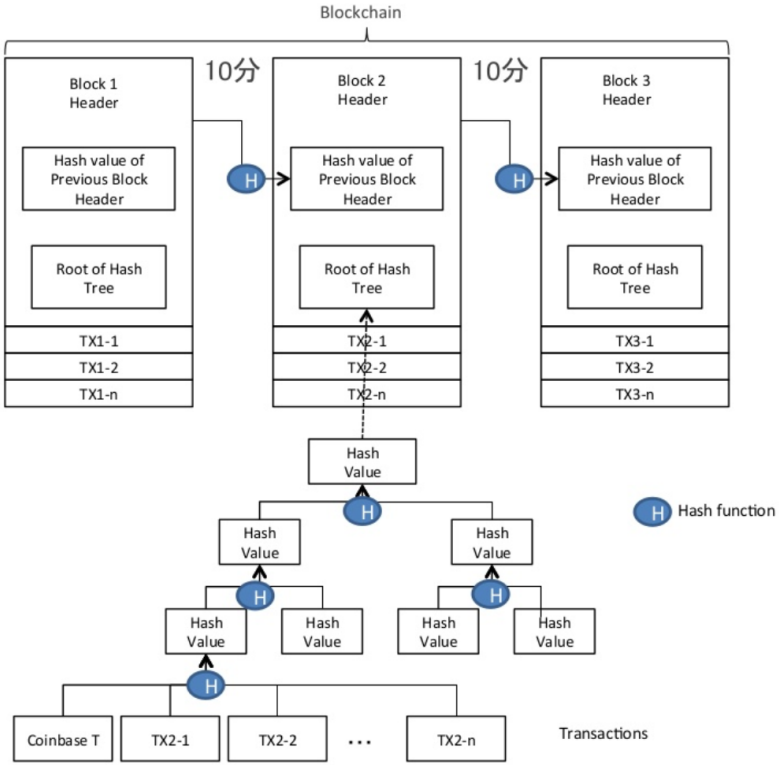
Durch die Inklusion von allen vorhergegangenen Transaktionen in eine neue Bitcoin Transaktion wird eine nachvollziehbare Kette von Transaktionen gebildet, welche in der Blockchain öffentlich zugänglich verwahrt wird.[330] Die Identität des Nutzers wird lediglich durch ein kryptographisches Pseudonym (öffentliche Bitcoin Adresse) geschützt. Um Transaktionen durchzuführen, müssen Sender und Empfänger sich zwangsweise über öffentliche Schlüssel identifizieren und können darüber hinaus die jeweilige Transaktionshistorie der verwendeten öffentlichen Adressen und vorher verwendeten öffentlichen Adresse einsehen.[331] Nutzer können eine sehr große Anzahl an öffentlichen Adressen generieren um keinen bzw. einen erschwerten Einblick auf ihre Vermögensverhältnisse und Transaktionshistorie zu geben. Ist ein Nutzer über eine öffentliche Adresse und damit sein kryptographisches Pseudonym identifiziert, lassen sich jedoch alle vorangegangenen Transaktionen der verwendeten Bitcoins und korrespondierenden Adressen nachvollziehen. Es lässt sich jedoch nicht bestimmen, ob die

[329] *Hosp,* Kryptowährungen, (2018) 52ff.
[330] *Europäische Zentralbank***,** Virtual Currency Schemes, www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, (23), (abgerufen am 31. August 2018).
[331] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, (2), (abgerufen am 26. August 2018).

öffentlichen Adressen zu denen die verwendeten Bitcoins vorher zugewiesen waren ebenfalls zum selben Nutzer gehören.[332]

Transaktionen von Nutzern im Bitcoin-Netzwerk werden dezentral geprüft, bestätigt und verwaltet. Hierbei arbeitet ein dezentral organisiertes Peer-to-Peer Netzwerk an der Validierung und Verbreitung der Transaktionsinformationen an das gesamte Netzwerk, welche diese in der Blockchain-Datenbank verwalten. Dies wird durch einen sogenannten Konsens-Algorithmus durchgeführt.[333] Die wesentlichen pseudonymen Kyptowährungen wie Bitcoin, Litecoin, Ethereum, etc. verwenden hier einen Proof-of-Work Algorithmus.[334] Der Prozess der Transaktionsdaten in Datenblöcken zusammenfasst und validiert wird als „Mining" bezeichnet.

Abbildung 6: Bitcoin Blockchain



Quelle: Soichiro Takagi

Mining bezeichnet einen iterativen Prozess in dem alle Mining Nodes des Netzwerks daran arbeiten ein mathematisches Problem zu lösen, welches als Ergebnis einen Block aus Daten erzeugt und an die Blockchain angefügt wird. Hierbei werden alle dem Miner bekannten Transaktionen über Hashoperationen zu Datenstruktur zusammengefügt und ein einziger

[332] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, (6), (abgerufen am 2. September 2018).
[333] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, (181 ff), (abgerufen am 26. August 2018).
[334] *Tar*, Proof-of-Work, Erklärt, https://de.cointelegraph.com/explained/proof-of-work-explained, (abgerufen am 02. September 2018).

Hashwert („Root of Hash Tree“) an der Spitze aus allen Transaktionen gebildet.[335] Dies erzeugt eine Datenstruktur die als „Merkle Tree“ bezeichnet wird.[336] Jede Veränderung an einem der Hashwerte innerhalb des Merkle Trees würde die Root of Hash Tree bzw. Merkle Root signifikant verändern. Im Mining Prozess des Proof-of-Work Algorithmus werden zur Generierung von Blöcken die Merkle Root aller Transaktionen sowie ein Hashwert des vorherigen Blocks zusammen gehasht. [337] Zusätzlich wird eine Zahlen- und Buchstabenkombination (Nonce) von den Minern verwendet, mit dem Ziel einen Hashwert aus diesen Inputs (und einigen weiteren Inputs) zu generieren, welcher eine bestimmte Anzahl Nullen am Beginn aufweist.[338] Miner suchen hierbei nach jener Kombination aus Inputs und einer Nonce die diesem Kriterium gerecht wird. Im Falle der Bitcoin-Blockchain wird auf diese Weise ca. alle 10 Minuten ein sogenannter Block generiert, welcher alle in dieser Zeit durchgeführten Transaktionen beinhaltet und mit den zuvor in der Blockchain verzeichneten Transaktionen verknüpft.[339] Der erste Miner, welcher einen validen Block findet, propagiert diesen an das gesamte Peer-to-Peer Netzwerk zur Überprüfung. Für den eingesetzten Ressourcenaufwand erhält der erfolgreiche Miner neu geschürfte Bitcoins sowie die enthaltenen Transaktionsgebühren der Transaktionen in seinem Block. Über den Konsens-Algorithmus und den Proof-of-Work (PoW) Mining Prozess wird erzielt, dass sich das gesamte Netzwerk transparent auf einen korrekten Block und damit auf eine gemeinsame Wahrheit einigt, ohne dass es hierzu einer zentralen Stelle zur Datenvalidierung benötigt.[340]

Im Falle von pseudonymen Kryptowährungen wie Bitcoin werden alle Transaktionen von einzelnen Bitcoins mit den jeweiligen vorherigen Transaktionen untrennbar verknüpft und transparent in der Blockchain gespeichert. Es gibt keine Bitcoin Transaktionen, welche nicht einsehbar sind.[341] Somit ergibt sich ein Transaktionssystem in welchem der Ursprung und Transaktionsverlauf von allen Bitcoins Krytowährungseinheiten vollständig nachvollziehen lässt. [342]

[335] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, (4), (abgerufen am 26. August 2018).
[336] *Schiller*, Merkle Tree – Eine Basis der Blockchain, https://blockchainwelt.de/merkle-tree-basis-von-blockchain-und-hash-trees/ (abgerufen am 01. September 2018).
[337] *Antonopoulos*, Mastering Bitcoin, https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf, (170ff), (abgerufen am 01. September 2018).
[338] *Antonopoulos*, Mastering Bitcoin, (198), (abgerufen am 01. September 2018).
[339] *Antonopoulos*, Mastering Bitcoin, (177ff), (abgerufen am 01. September 2018).
[340] *Antonopoulos*, Mastering Bitcoin, (181ff), (abgerufen am 01. September 2018).
[341] *Antonopoulos*, Mastering Bitcoin, (111ff), (abgerufen am 01. September 2018).
[342] *Ing. Johannes Grill,* Präsident Bitcoin Austria, Interview geführt von Marina Kindel (3. August 2018).

11.3.2. Anonymisierung von Pseudonymen Kryptowährungen am Beispiel Bitcoin

Pseudonyme Kryptowährungen zeichnen sich dadurch aus, dass ab dem Zeitpunkt in dem ein Bitcoin-Vermögen mit einem Eigentümer in Verbindung gebracht werden kann, durch die Verkettung aller vorherigen Transaktionen mit der aktuellsten Transaktion, auch Rückschlüsse über die Transaktionshistorie möglich sind. Zudem ist auch die Beobachtung der zukünftigen Transaktionen des Nutzers möglich.[343]

Es existieren mehrere Methoden zur Anonymisierung von pseudonymen Kryptowährungen. Als erste Methode wird die Verwendung von neuen Bitcoin Adressen für jede Transaktion angewendet. Bitcoin Adressen sind sehr leicht zu generieren und es gibt eine enorm große Anzahl an verfügbaren, generierbaren Adressen. Hierdurch kann ein Nutzer sich über eine Transaktion identifizierbar machen, jedoch nur einen Teil seiner Bitcoin Transaktionen und Vermögenswerte nachvollziehbar machen. Je mehr Adressen ein Nutzer verwaltet, desto schwieriger wird die Zuordenbarkeit an seine Identität.[344]

Eine weitere Methode ist die Verwendung von „Tumblern" oder „Mixern", welche die Bitcoins von mehreren Nutzern zusammenmixen und so zur Obfuskation beitragen sollen. Diese werden insbesondere für die Reinwaschung von identifizierbaren oder „tainted" Bitcoins verwendet. Ziel ist es hierbei die „tainted" Bitcoins mit „sauberen" Bitcoins zu vermengen und so den nachvollziehbaren Transaktionsverlauf von Kryptowährungen zu unterbrechen. Diese Methode kann sowohl zur Erhöhung der Privatsphäre als auch als Mittel zur Geldwäsche genutzt werden.[345] Es gibt eine Reihe von Anbietern dieser Dienstleistungen im Internet. Tumbler und Mixer sind jedoch keineswegs vollständig sichere Methoden um die Identifizierung von Nutzern pseudonymer Kryptowährungen zu eliminieren und weisen oft selbst hohe Sicherheitsrisiken auf.[346] Die Eignung von diesen Dienstleistungen für Geldwäsche im Falle signifikanter Geldbeträge zu betreiben ist somit zumindest fraglich.

Eine weitere Möglichkeit zur Anonymisierung involviert keine Transaktionen durchzuführen, sondern den direkten Austausch von privaten Schlüsseln, welche den Zugang zu Adressen mit bestimmten Geldbeträgen ermöglichen. Diese beinhalten das Risiko, dass Käufer und Verkäufer den privaten Schlüssel bei Übergabe kennen bzw. dass Käufer die Echtheit des

[343] *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, (6), (abgerufen am 26. August 2018).
[344] *Androulaki / Karame / Roeschlin / Scherer / Capkun*, Evaluating User Privacy in Bitcoin, https://eprint.iacr.org/2012/596.pdf (4ff) (abgerufen am 13. Oktober 2018).
[345] *Chohan*, The Cryptocurrency Tumblers: Risks, Legality and Oversight, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361 (1f), (abgerufen am 03. September 2018).
[346] *de Balthasar / Hernandez-Castro,* An Analysis of Bitcoin Laundry Services, https://kar.kent.ac.uk/63502/193/An%20Analysis%20of%20Bitcoin%20Mixers.pdf, (311), (abgerufen am 3. September 2018).

privaten Schlüssels verifizieren müssen. Eine solche Transaktion würde jedoch nie in der Bitcoin Blockchain nachweisbar sein.[347]

11.3.3. Trends krimineller Machenschaften durch virtuelle Währungen

Neben "Criminal-2-Criminal-Payments" (C2C), worunter man die Verwendung von virtuellen Währungen um illegale Güter oder Dienstleistungen im Darknet zu erwerben versteht, sind weitere neue Entwicklungen in diesem Bereich zu beobachten. Finanzagenten bezahlen Personen, die Wallets eröffnen und anschließend die Zugangsdaten retournieren um somit über sämtliche Transaktionen der Vermögenswerte zu verfügen. Zudem wird durch Inanspruchnahme von Mixern- oder Tumblerdiensten, unter Voraussetzung des Vorliegens einer kriminellen Vortat, versucht die Herkunft der Mittel zu verschleiern, wodurch die Strafverfolgung erschwert wird.
Wenn Bitcoins auf eine in der Realwirtschaft frei verfügbaren Prepaid-Karte geladen werden, spricht man von „Bitcoins-to-Plastic". Firmen die solche Dienste anbieten sind oftmals in Offshore-Destinationen angesiedelt. Auch bei dieser Vorgehensweise gestaltet sich eine Zuordnung der Vermögenswerte als äußerst schwierig.[348]

11.4. Anonyme Kryptowährungen

Aufgrund der schwach ausgeprägten Anonymität verbunden mit früher entwickelten Kryptowährungen wie Bitcoin, Litecoin, Ethereum,[349] etc. entstand das Interesse der Entwicklung von alternativen Kryptowährungen, welche tatsächliche Anonymität von Zahlungen ermöglichen. So entstanden in den Jahren nach dem Aufkommen von Bitcoin mehrere alternative Kryptowährungen, welche technisch auf den Schutz der Privatsphäre der Nutzer ausgerichtet sind. Diese unterscheiden sich signifikant von der Mehrheit der existierenden Kryptowährungen, hinsichtlich der verwendeten kryptographischen Verfahren, Transparenz und Nachvollziehbarkeit von Transaktionen. Diese werden als so genannte „Privacy Coins" bezeichnet.[350]
Es stellt sich die Frage warum Nutzer Kryptowährungen verwenden, bei denen die Transaktionshistorie nicht oder nicht vollständig bekannt ist. Auf der einen Seite eignen sich die erwähnten Verschlüsselungstechniken für illegale Aktivitäten wie den Kauf von Drogen,

[347] *Tokens 24*, So tauschen sie Bitcoin offline aus, https://www.tokens24.com/de/cryptopedia/basics/so-tauschen-sie-bitcoin-offline-aus, (abgerufen am 3. September 2018).
[348] *Bundeskriminalamt,* Lagebericht Geldwäsche 2017, (25), (abgerufen am 20. August 2018).
[349] Ethereum bietet eine optionale Form von Zero-Knowledge Proof Transaktionen.
[350] *Prinz*, Vollständige Liste der Anonymen Kryptowährungen, (Zugriff 05. September 2018).

Waffen, Geldwäsche usw., anderseits möchten viele Personen ihre Privatsphäre schützen. Viele möchten verhindern, dass dessen getätigte Zahlungen wie z.B. Investitionen oder Käufe, bei vollständig gegebener Transparenz, ersichtlich und nachvollziehbar sind. [351]

Auch einige Startup-Unternehmen wie z.B. Blockpit, welches sich mit der korrekten Versteuerung von Gewinnen aus Kryptowährungen, allem voran mit dessen Handel, aber auch mit andere Arten von Einkünften, wie etwa von Mining und der Akzeptanz von Kryptowährungen im alltäglichen Geschäft befasst, verwendet Zero-Knowledge Proof. Es wird die Steuerlast der Nutzer korrekt berechnet, ohne jedoch sensible Daten der Nutzer speichern bzw. zuordnen zu müssen. Dadurch wird die Privatsphäre der Nutzer geschützt.[352]

Da solche Verschlüsselungstechniken jedoch illegale Aktivitäten fördern arbeiten bereits internationale Behörden an Lösungsansätzen: „Allem voran natürlich die automatisierte Nachverfolgung von verdächtigen Transaktionsflüssen, die über die Blockchains eingesehen werden können. Auch wird an Algorithmen (AI) gearbeitet, die von selbst lernen sollen, welche Transaktionswege für Geldwäsche genutzt werden um dann über Wahrscheinlichkeiten Verdachtspersonen zu identifizieren“ so Florian Wimmer, CEO und Co-Founder von Blockpit. Jedoch stellt die Gegensteuerung der Verschlüsselungstechniken, auf Grund der schnellen Weiterentwicklung der Technologie, Ressourcenverschwendung dar. Zudem ist es aus technischer Sicht schier unmöglich den Entwicklungen entgegen zu steuern. Lediglich aus ökonomischer Sicht könnte dies gelingen. Den Händlern/Dienstleistern könnte es verboten werden Kryptowährungen zu akzeptieren. Die Sinnhaftigkeit solcher Verbote ist jedoch anzuzweifeln.[353]

Zudem sollte auch beachtet werden, dass *„ Jede Beschränkung der Struktur, der Erzeugung, des Besitzes, der Weitergabe oder der freien Wertbildung von Bitcoin und Co durch hoheitliche Maßnahmen können einen Eingriff in das Eigentumsgrundrecht oder in das Grundrecht auf Erwerbsfreiheit bedeuten.“* [354] Da virtuelle Währungen *„.. digitale Erzeugnisse privatrechtlicher Wirtschaftssubjekte“* [355] und somit „ *als vermögenswerte Privatrechte anzusehende Produkte“* [356] sind fallen diese in den Schutzbereich des Eigentumsgrundrechtes sowie, auf Grund der bestehenden Gewinnabsicht, unter das Grundrecht auf Erwerbsfreiheit. Zudem unterliegen sie dem Schutz der Warenverkehrsfreiheit. Die Erlassung von Regelungen u.a. zur Verhinderung von Geldwäsche und Terrorismusfinanzierung unterliegen keinen freien Ermessensspielraum der

[351] *Hosp,* Kryptowährungen, (2018) 158.
[352] *Florian Wimmer,* CEO, Co-Founder, Interview geführt von Marina Kindel (22. Juli 2018).
[353] *Florian Wimmer,* CEO, Co-Founder, Interview geführt von Marina Kindel (22. Juli 2018).
[354] *Piska,* ecolex 2017 632.
[355] *Piska,* ecolex 2017 632.
[356] *Piska,* ecolex 2017 632.

Legislative. Sämtliche Regulierungsmaßnahmen auf nationaler und unionsrechtlicher Ebene müssen vorab einer Prüfung der Verhältnismäßigkeit unterzogen werden.[357]

Unter den am meisten verbreiteten anonymen Kryptowährungen finden sich Monero, Dash, und Zcash, auf die im folgenden Abschnitt kurz eingegangen wird. Speziell diese drei Kryptowährungen wenden Anonymisierungsverfahren an um die Nachvollziehbarkeit von Transaktion und somit u.a. die Mittelherkunft zu verschleiern. Einerseits wird dadurch die Privatsphäre der Nutzer erhöht, andererseits das potenzielle Risiko kriminelle Aktivitäten durchzuführen.[358] Durch den nachfolgenden Abschnitt soll ein Überblick über die Funktionsweise der Verschlüsselungstechniken an Hand der virtuellen Währungen Monero, Zcash und Dash ermöglicht und zudem aufgezeigt werden, dass durch die bereits erläuterten technischen Eigenschaften von Bitcoin dieser oft fälschlicherweise als Paradebeispiel für Geldwäsche verwendet wird. Ferner soll damit verdeutlicht werden, dass der technologische Fortschritt unaufhaltsam und sehr komplex ist und die gesetzgebende Instanz mit einer hoch komplexen Innovation konfrontiert ist: „Die Technologie entwickelt sich rasant. Die rechtlichen Regulative können mit der technischen Entwicklung zum jetzigen Zeitpunkt nicht mithalten und werden dies auch zukünftig nicht im gewünschten Ausmaß schaffen. Im Moment ist Bitcoin „die Coin" für Straftaten, doch dringt man weiter in die Materie ein, so wird man feststellen, dass Bitcoin „nur" der Pionier der Kryptowährungen ist, und es aktuell bereits Kryptowährungen gibt, welche die Strafverfolgungsbehörden noch vor viel größere Probleme stellen werden. Man wird wohl das Phänomen Bitcoin verstanden haben, wenn es nicht mehr nötig ist. Vendoren und Käufer im Darknet werden sich anderer Coins bzw. Token bedienen bzw. tun dies auch bereits, welche einen höheren Pseudonymitätsgrad versprechen als Bitcoin es macht bzw. wird die Pseudoanonymität dabei in den Fokus gelegt. Der Mensch ist ein Gewohnheitstier, deshalb verwenden noch viele Straftäter Bitcoins, jedoch wurde die Post-Bitcoin-Ära längst eingeläutet. Innerhalb von Strafverfolgungsbehörden fehlt es oft an nötigen Ressourcen sowie Know-How, um dieser Schnelllebigkeit entsprechend entgegentreten zu können. Aus Gründen wie diesen sind Kooperationen mit Forschungseinrichtungen und privaten Unternehmen unerlässlich.", so Mag. Patrick Schreiner, MSc, Bundeskriminalamt Abteilung II/BK/7.

[357] *Piska,* ecolex 2017 632.
[358] *Hosp,* Kryptowährungen, (2018) 152.

11.4.1. Monero

Monero (XMR) ist eine alternative Kryptowährung basierend auf Bitcoin, welche 2014 entwickelt und spezifisch für höhere Privatsphäre und bessere Skalierbarkeit konzipiert wurde. Sie geht aus der im Jahr 2012 entwickelten Kryptowährung Bytecoin hervor. Der wesentliche Unterschied zu Bitcoin ist die Verwendung des CryptoNote Protokolls[359] anstatt des SHA256 Proof-of-Work Algorithmus der bei Bitcoin zum Einsatz kommt. Darüber hinaus verwendet Monero eine Reihe von Technologien, welche die Informationen zu Nutzern, Transaktionen und Transaktionshöhen anonymisieren. Im Gegensatz zu den stets mit vorherigen Transaktionen verknüpften Transaktionen und daher nachvollziehbaren Transaktionen in der Bitcoin-Blockchain verwendet Monero Ring-Signaturen um die Verknüpfung und Nachvollziehbarkeit von Transaktionen zu verhindern. Statt einer eindeutigen digitalen Signatur der Transaktion, werden bei Ring-Signaturen mehrere Transaktionsinputs und Nutzer verknüpft. Ring-Signaturen sind eine Art von digitaler Signatur, bei der eine Gruppe von möglichen Unterzeichnern zusammengeführt wird. Hierbei wird die echte Transaktionssignatur mit mehreren anderen Signaturen kombiniert. Für Außenstehende wird es somit erschwert zu identifizieren, welche Transaktionen echt sind und welche nur zur Obfuskation eingesetzt werden.[360]

Monero fügt zu der echten Monero Transaktion eine Anzahl an Schein-Transaktionen, genannt „Mixins“ hinzu. Die echten und unechten Transaktionen werden miteinander verknüpft und gleichzeitig mit einer Ring-Signatur bestätigt. Dadurch lässt sich nicht eindeutig bestimmen, welche der bestätigten Transaktionen die echte Transaktion darstellt. Zusätzlich zur Obfuskation der echten Transaktion wird die Höhe der echten und unechten Transaktionen durch ein Verfahren namens Pederson Commitment-Verfahren manipuliert. Hierbei wird eine unbekannte Zufallszahl eingesetzt um die Transaktionssumme für die Öffentlichkeit zu verändern, während die tatsächliche Transaktionshöhe nicht verändert wird.[361] Das Ergebnis sind sogenannte Monero Ring Confidential Transactions (RingCT). Diese sind eine Form eines Zero-Knowledge Proofs, welche für anonyme Transaktionen verwendet werden.[362]

Darüber hinaus kann keine Analyse der Monero Blockchain stattfinden um Transaktionen Identitäten zuzuweisen, da sich stattgefundene Transaktionen nicht mit öffentlichen Schlüsseln von Nutzern in Verbindung bringen lassen. Wenn ein Sender Monero an einen

[359] *van Saberhagen*, CryptoNote v 2.0, https://cryptonote.org/whitepaper.pdf (Zugriff 30. August 2018).
[360] *Alonso*, Zero to Monero: First Edition, https://getmonero.org/library/Zero-to-Monero-1-0-0.pdf (20). (Zugriff 5. September 2018).
[361] *Alonso*, Zero to Monero: First Edition, (20), Zugriff 5. September 2018).
[362] *Alonso*, Zero to Monero: First Edition, (41), (Zugriff 5. September 2018).

Empfänger sendet, werden diese an eine eigens generierte öffentliche Adresse gesendet, welche als Tarnadresse fungiert (Commitment Public Key) und öffentlich sichtbar ist. Diese Adressen sind einmalige Public Keys, welche nach erfolgter Anwendung nicht erneut verwendet werden.[363] Sender und Empfänger erhalten jedoch jeweils einen einzigartigen Secret View Key, welcher erlaubt die tatsächliche Transaktionen, die zur öffentlichen Adresse des Empfängers gesendet werden, einzusehen.[364]

Um Monero Nutzer weiter zu anonymisieren wird an der Verwendung des Invisible Internet Projects (I2P) in der Form des Kovri Projekts gearbeitet. Dieses soll verhindern, dass es Nutzern nachgewiesen werden kann, dass diese Monero verwenden. Monero ist somit eine Kryptowährung die, aufgrund der technischen Eigenschaften und starkem Fokus auf Anonymität, ideale Voraussetzungen für die Zweckentfremdung als Medium für illegale Transaktionen aufweist. Sowohl die Akteure als auch die Transaktionen und Transaktionssummen sind nicht nachweisbar und durch komplexe kryptographische Verfahren geschützt.[365]

11.4.2. Dash

Dash (DASH) ist eine alternative Kryptowährung welche in 2014 entwickelt wurde und eine Erweiterung der Kryptowährung Litecoin darstellt.

Dash anonymisiert Transaktionen indem es die Transaktionen von Nutzern mit denen von anderen Nutzern vermischt und so die Nachvollziehbarkeit von Transaktionshistorien obfuskiert. Der Prozess zur Anonymisierung von Transaktionsdaten wurde in seiner ursprünglichen Konzeption als „Darksend“ bezeichnet. Dieser inkludierte mehrere Möglichkeiten des Verschleierns von Transaktionsdaten.[366]

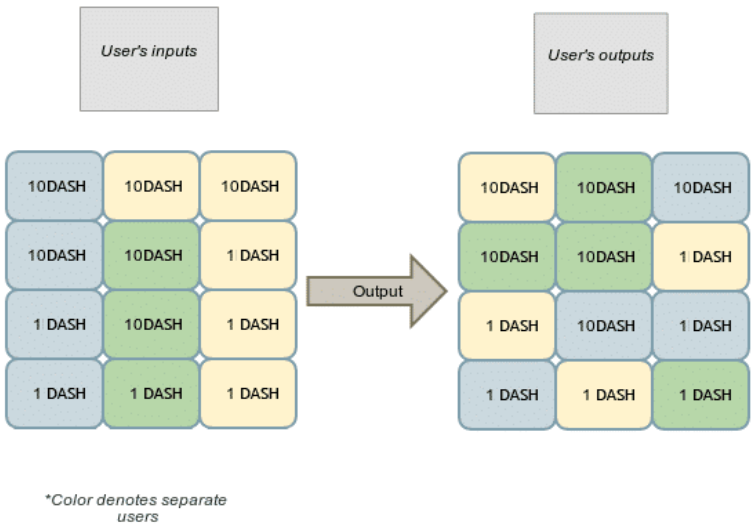
Im Gegensatz zu Bitcoin, in dessen Netzwerk jeder Teilnehmer ein Mining Node im Peer-to-Peer Netzwerk werden kann, setzt Dash auf ein System auf sogenannten „Masternodes“. Die wesentliche Voraussetzung um eine Masternode zu bilden, ist die Hinterlegung einer Sicherheit in Höhe von mindestens 1000 DASH. Masternodes sichern das Dash Netzwerk und bestätigen Transaktionen, dafür werden diese mit Transaktionsgebühren und neu geschürften DASH belohnt. Sie übernehmen zudem eine wichtige Rolle in der Obfuskation von

[363] *Prinz*, Monero ist eine Anonyme Kryptowährung, https://www.bitfantastic.com/kryptowaehrung/monero-ist-eine-anonyme-kryptowaehrung/2018/, (Zugriff 5. September 2018).
[364] *Alonso*, Zero to Monero: First Edition, https://getmonero.org/library/Zero-to-Monero-1-0-0.pdf (34), (Zugriff 5. September 2018).
[365] *Möser /Böhme / Breuker*, An inquiry into money laundering tools in the Bitcoin ecosystem, (1ff), (abgerufen am 28. August 2018).
[366] *o.V.*, What is Dash Cryptocurrency? A Crash Course, https://blockgeeks.com/guides/what-is-dash-cryptocurrency/ (abgerufen am 5. September 2018).

Transaktionsdaten.[367] Der Prozess des passiven Vormischens („passive ahead of time-mixing“) mischt die Transaktionen von mindestens drei Sendern und Empfängern, welche durch die Masternodes zusammengeführt und koordiniert werden.[368]

Die Weiterentwicklung von „Darksend“ und das aktuell verwendete System zur Anonymisierung von Transaktionen wird als „PrivateSend“ bezeichnet. PrivateSend fügt den Transaktionen von Nutzern mehrere identische Inputs von anderen Nutzern hinzu und sendet diese anschließend zu mehreren Outputs. Auf diese Weise wird die eindeutige Verknüpfung zwischen Transaktionen in der Dash Blockchain obfuskiert.[369]

Abbildung 7: DASH Mixen von Kryptowährungen



Quelle: Duffield / Diaz

Dash gibt hierbei zulässige Input- und Output-Größen von 0,01 bis 1000 DASH vor, auf die sich die vom Nutzer gewünschte Transaktionshöhe aufstückelt. Die Stückelungen der Transaktionen mehrerer Nutzer (mindestens drei Nutzer) werden nach dem Zufallsprinzip gemixt und rückgesendet. Hierbei organisieren Masternodes im Netzwerk, dass Nutzer passende Mengen an DASH zusammenführen und mixen können. Jeder Nutzer kann hierbei nur dieselbe Anzahl an Kryptowährungen mixen um keine Identifikation des Ursprungs anhand der Transaktionshöhe zu ermöglichen. Die Wallets der Nutzer wiederholen den Mixprozess mehrmals, um sicherzustellen, dass die Herkunft der Zahlungsmittel vollständig

[367] *Duffield / Diaz*, Dash: A Privacy-Centric Crypto-Currency, https://docs.dash.org/en/latest/introduction/about.html#whitepaper (2f),(Zugriff: 5. September).
[368] *Giese*, Dash – Digitales Cash mit einigen Schmankerln, https://www.btc-echo.de/dash-digitales-cash-mit-einigen-schmankerln-20160410/ (Zugriff 5. September 2018).
[369] *Duffield / Diaz*, Dash: A Privacy-Centric Crypto-Currency, https://docs.dash.org/en/latest/introduction/about.html#whitepaper (Zugriff: 5. September) 6.

anonymisiert wird. Kryptowährungen, welche in diesen Mischprozess involviert sind, verlassen zudem zu keinem Zeitpunkt die Wallet Nutzers, wodurch sichergestellt wird, dass der gesamte Prozess nicht nachvollziehbar bleibt. Als Resultat kann die Nachvollziehbarkeit der Transaktionhistorie von DASH Kryptowährungen verhindert werden. [370]

11.4.3. Zcash

Zcash (ZEC) ist eine auf Bitcoin aufbauende, alternative Kryptowährung welche im Jahr 2016 entwickelt wurde und vergleichbar mit Monero und Dash alternative Technologien inkorporiert um Transaktionen zu anonymisieren. Den Nutzern von Zcash steht die Auswahl zur Verfügung sich zwischen pseudonymen und anonymen Transaktionen auf der Zcash Blockchain zu entscheiden.

Zcash verwendet zk-SNARK (Zero-knowledge Succinct non-interactive Arguments of Knowledge) als eine Form von Zero-Knowledge-Proofs. Hierbei werden zwei verschiedene öffentliche Schlüssel zum Beweis (proving key) und zur Verifizierung (verifying key) generiert. Diese ermöglichen es technisch einen Beweis zu liefern, ohne Inhalte preiszugeben.[371] Dies erlaubt es den Minern des Netzwerks Transaktionen zu bestätigen, ohne dass diese Informationen über die Transaktionen einsehen können. Nutzer von Zcash können jeweils Empfänger, Sender bzw. Transaktionshöhe anonymisieren. Darüber hinaus können Nutzer Informationen über die Höhe ihres Kryptowährungsvermögens auf den besessenen Zcash Adressen schützen.[372] Obwohl es eine transparente, nachvollziehbare Blockchain wie bei Bitcoin gibt, können Nutzer wählen, dass Transaktionen nicht auf der Zcash-Blockchain aufscheinen, indem sie anstatt pseudonymer Adressen (t-addresses) anonyme Adressen (z-addresses) verwenden. Transaktionen zwischen t-addresses und z-addresses sind möglich. Die von Minern neu erzeugten ZEC Kryptowährungstoken werden ausschließlich auf anonymen Adressen gespeichert, bevor sie weiter verwendet werden.[373] Es ergeben sich 9 verschiedene Kombinationen von möglichen Transaktionen, je nachdem welche Aspekte der Transaktion anonymisiert werden (z.B. Sender pseudonym, Empfänger anonym).[374] Im Gegensatz zu den verbreiteteren pseudonymen Kryptowährungen wie Bitcoin und Ethereum, findet sich in der Zcash-Blockchain keine vollständige Verknüpfbarkeit aller Transaktionen. Aufgrund der

[370] *Asolo*, Dash PrivateSend Explained, https://www.mycryptopedia.com/dash-privatesend/, (abgerufen am 6. September 2018).
[371] *Ben-Sasson/Chiesa/Garman/Green/Miers/Tromer/Virza,* Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version), http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf (5), (abgerufen am 30. September 2018).
[372] *Bowe/Hornby/Wilcox,* Zcash Protocol Specification, https://whitepaperdatabase.com/zcash-zec-whitepaper/ (4), (abgerufen am 30. September 2018).
[373] *Kappos/Yousaf/Maller/Meiklejohn*, An Empirical Analysis of Anonymity in Zcash, https://smeiklej.com/files/usenix18.pdf (9), (abgerufen am 01. Oktober 2018).
[374] *Biryukow/Feher,* Deanonymization of Hidden Transactions in Zcash https://cryptolux.org/images/d/d9/Zcash.pdf (2), (abgerufen am 30. September 2018).

Kombination von pseudonymen und anonymen Transaktionen und öffentlichen Schlüsseln bietet Zcash nur eine eingeschränkte Anonymität und eine De-Anonymisierung von Nutzern ist durch verschiedene Methoden möglich.[375]

Bis dato erfolgt, von Seiten der gesetzgebenden Instanz keine Differenzierung von anonymen und pseudoanonymen Kryptowährungen. Aktuell verpflichtet der Gesetzgeber die Gatekeeper von (pseudonymen) Kryptowährungen zur Identifizierung ihrer Kunden. Es wird dennoch davon ausgegangen, dass der Gesetzgeber in Zukunft verstärkte Maßnahmen ergreifen wird, um anonyme Kryptowährungen gänzlich aus dem Wirtschaftskreislauf auszuschließen. Es wird daher immer mehr sogenannte White Coins geben, welche der Gesetzgeber reguliert und dadurch akzeptiert und sogenannte Black Coins geben, welche keinen Anschluss an den Wirtschaftskreislauf haben und ausschließlich im Darknet Verwendung finden werden.[376]

Erwägungsgrund 2[377] weist u.a. auf *„ ... das Risiko von „Schwarzmarkt-Transaktionen", der Geldwäsche, der Terrorismusfinanzierung (1), des Steuerbetrugs, der Steuerhinterziehung und sonstiger strafbarer Handlungen auf der Grundlage von „Pseudonymität" und der „Kombination von Diensten", die einige dieser Dienstleister ermöglichen, sowie die dezentrale Struktur einiger virtueller Währungen, wobei jedoch zu berücksichtigen ist, dass die Rückverfolgbarkeit bei Bargeld-Transaktionen in der Regel immer noch wesentlich schwieriger ist;*[378] hin.

[375] *Kappos/Yousaf/Maller/Meiklejohn*, An Empirical Analysis of Anonymity in Zcash, https://smeiklej.com/files/usenix18.pdf (abgerufen am 30. September 2018).
[376] *Dr. Oliver Völkel, LL.M.,* Partner der Rechtsanwaltskanzlei Stadler Völkel, Interview geführt von Marina Kindel (11. September 2018).
[377] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[378] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.

12. Initial Coin Offerings

Initial Coin Offerings (ICO) sind eine Blockchain-basierte neue Form des Crowdfundings, welche vermehrt in der Finanzierung von Startups im Blockchain-Bereich eingesetzt wird. Die Bezeichnung ICO lehnt sich an die Bezeichnung „Initial Public Offering“ (dt. Börsengang) an. Bei einem ICO wird von einem Unternehmen ein Kryptowährungs-Token emittiert und gegen andere Kryptowährungen oder staatliche Währungen getauscht. Somit können sich Unternehmen ohne Intermediäre wie Börsen, Banken oder Risikokapitalgeber finanzieren. Zudem handelt es sich bei dieser Finanzierungsform um wenig regulierte und teilweise unregulierte Formen der Kapitalaufnahme. ICOs bieten Unternehmen den Zugang zu alternativen Kapitalquellen und eliminieren klassische Intermediäre. Ein wesentlicher Aspekt ist die grenzüberschreitende Natur von ICOs, da ein globaler Pool an potentiellen Investoren an einem ICO teilnehmen kann.[379] Für die Finanzierung über ICOs können sowohl pseudonyme als auch anonyme Kryptowährungen zur Anwendung kommen. Daher kommt es zu verstärkten Risiken in Bezug auf Geldwäsche und die Einhaltung von Know-Your-Customer (KYC) und Anti-Money-Laundering (AML) Anforderungen. Der Vorstand der Österreichischen Finanzmarktaufsicht Klaus Kumpfmüller betont in Hinblick auf die mangelnde Regulation von ICOs die damit einhergehenden Risiken: *„Es entsteht ein völlig unregulierter und unbeaufsichtigter Schattenkapitalmarkt. Es kann zu einer unregulierten Blasenbildung kommen.“*[380] Die Deutsche BaFin spricht im Zuge von ICOs von „*Die systembedingte Anfälligkeit von ICOs für Betrug, Geldwäsche und Terrorismusfinanzierung erhöht das Risiko, dass Anleger das eingesetzte Kapital verlieren, auch aufgrund notwendiger Maßnahmen der Behörden gegen Betreiber oder sonstige Personen und Unternehmen, die in solche illegalen Geschäfte einbezogen sind.“*[381]

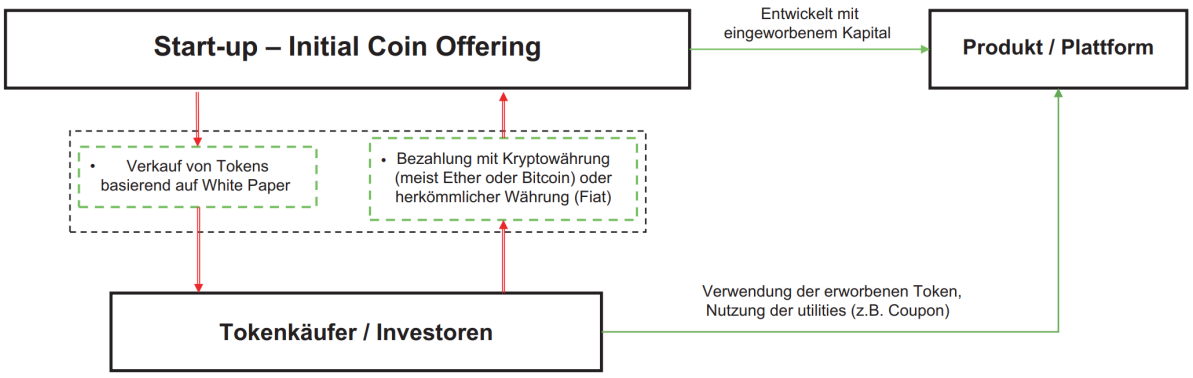
12.1. ICO Transaktionsprozess

Initial Coin Offerings basieren auf der Technologie von Blockchain und Smart Contracts. Über Smart Contract Protokolle werden die Charakteristika von ICOs vordefiniert. Hierbei handelt es sich um programmierte Vereinbarungen, welche transparent einlesbar sind und dezentral auf einer Blockchain ausgeführt werden. Aspekte wie Token-Allokation, Minimum-

[379] *Hönig*, Initial Coin Offering - Studie zu Kryptowährungen und der Blockchain-Technologie, https://www.frankfurt-university.de/fileadmin/standard/Hochschule/Fachbereich_3/Kontakt/Professor_inn_en/Hoenig/20180502_Bitcoin_Studie_fra_uas_Hoenig_V1.0.pdf, (47),(Zugriff 02. September 2018).
[380] *o.V.*,FMA warnt vor "Spekulationsobjekt" Kryptoasset, https://diepresse.com/home/wirtschaft/boerse/5488737/FMA-warnt-vor-Spekulationsobjekt-Kryptoasset (02. September 2018).
[381] *BaFin*, Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs) https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html (02. September 2018).

und Maximum-Finanzierungsbeträge, Wechselkurse, Finanzierungszeitraum oder Folgen bei Nichterreichung des Finanzierungsziels werden transparent im Smart Contract abgebildet.
Im Vorfeld eines ICOs wird das zu finanzierende Projekt beworben und in der Regel eine Roadmap und ein Whitepaper erstellt. Das Whitepaper ist vergleichbar zu einem Prospekt im Rahmen eines IPOs. Es detailliert technische Aspekte und Ziele des Projekts.[382]

Abbildung 8: Ablauf eines ICOs



Quelle: Hahn / Wons

Ein ICO erfolgt über die Zusendung an Kryptowährungen oder staatlichen Währungen an einen Emittenten, der im Gegenzug neu erstellte Tokens in einem vorher definierten Wechselkurs ausgibt.[383] ICOs finden derzeit in zwei Formen statt: Basierend auf Smart Contracts oder durch die Schaffung neuer Blockchains. In ersterer Form werden die Tokens des Emittenten in einem Smart Contract gebildet und über Blockchain-Transaktionen den neuen Eigentümern überwiesen. Im Falle neu generierter Blockchains werden die Token ebenso neu generiert und über sogenannte „Token Sales“ in einem Bieterverfahren verkauft.[384]
Initial Coin Offerings können ein Medium sein, um kriminell erworbene Mittel, basierend auf der pseudonymen bzw. anonymen Funktionsweise von Kryptowährungen, reinzuwaschen und versteckte Terrorismusfinanzierung zu betreiben. Durch den im Finanzierungsprozess stattfindenden Tausch an finanziellen Mitteln gegen neu emittierte Tokens kann die Nachvollziehbarkeit von Finanzströmen unterbrochen werden was förderlich für kriminelle Aktivitäten sein kann.[385] Bei Initial Coin Offerings, aber auch bei institutionellen Presales

[382] *Klumpp*, ICO – Initial Coin Offering, https://www.tech-corporatefinance.de/blog/uncategorized/ico-initial-coin-offering-ablauf-und-beratung/ (abgerufen am 06. September 2018);*Buchleiter/Rabl*, Blockchain und Smart Contracts, ecolex 2017, 4.
[383] *Hahn / Wons*, Initial Coin Offering (ICO) - Unternehmensfinanzierung auf Basis der Blockchain-Technologie, (2018) 2.
[384] *BaFin*, Initial Coin Offerings: Hohe Risiken für Verbraucher, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1711_ICO.html, (06. September 2018).
[385] *BaFin*, Initial Coin Offerings: Hohe Risiken für Verbraucher, (06. September 2018).

besteht die Gefahr der Nichtbekanntheit der Herkunft der finanziellen Mittel. Diese könnten aus unseriösen bis mafiösen Quellen stammen ohne dass man es weiß. Um sicherzugehen, sich hier im rechtlich erlaubten Rahmen zu bewegen, müssen stringente Know Your Customer (KYC) und Anti Money Laundering (AML) Prozesse durchgeführt werden.[386] ICOs haben eine globale Natur und unterliegen in vielen Jurisdiktionen keinen dezidierten ICO-Regulationen. Zusätzlich unterliegen ICO Emittenten derzeit keinen gesetzlichen Transparenzvorschriften.[387] Nun stellt sich die Frage wie sich die globale Natur von ICOs auf Geldwäscherisiken auswirkt. MMag. Christopher Miess, BSc, Bakk.phil, BSc, MSc, Mitglied des Fintech Advisory Board der österreichischen Regierung, teilt folgende Auffassung: „Sie erschwert einfach gesagt die Thematik. Man kann sich dies anhand traditioneller Bankgeschäfte vorstellen. Im einfachsten Fall wird eine Zahlung von einer österreichischen Bank an eine andere durchgeführt. Die Zahlungsmittel im Bankensystem sind bereits sämtlichen KYC und AML Checks unterworfen worden. Nun können diese relativ problemlos verschoben werden. Dies dauert in der Regel wenige Werktage, „no questions asked". Sobald einer der beiden Parteien im Ausland ist, wird es schon komplizierter. Nicht nur dass es länger dauert, auch wird bei größeren Summen gerne nachgefragt, woher das Geld denn jetzt komme. Bei ICO kommt es häufig zum Auftauchen und Investieren großer Summen, die länderübergreifend mittels wenigen Mausklicks verschoben werden. Da auch keine zentralisierte Bankeninstitution dazwischensteht, ist es schwierig einen Ansatzpunkt für KYC und AML Checks zu finden. Der einfachste und häufigste Weg ist heute bei FIAT zu Kryptobörsen anzusetzen. Bei diesen wird Krypogeld in traditionelles Geld gewechselt. Ein bekanntes Beispiel im europäischen Raum wäre Kraken."

Gesetzliche Rahmenbedingungen, welche gezielt auf die Risiken von Betrug, Geldwäsche oder Terrorismusfinanzierung im Bereich von ICOs eingehen müssen geschaffen werden. Hierbei ist ein wesentlicher Bestandteil, dass Unternehmen welche ICOs durchführen verpflichtend verifizieren und nachweisen woher ihre aufgenommenen finanziellen Mittel kommen. Da die meisten ICOs sich über andere Kryptowährungen finanzieren und damit keinen gesetzlichen KYC/AML-Verpflichtungen unterliegen, kann Geldwäsche natürlich ein Thema sein. Spätestens dann, wenn das Unternehmen die eingenommenen Kryptowährungen in Fiat-Währungen umtauschen möchte, muss die Mittelherkunft nachgewiesen werden.[388]

Die Umsetzung von KYC/AML Methoden bei ICOs werden teilweise nicht stringent genug umgesetzt. Speziell bis Mitte 2017 war es so, dass kaum KYC und AML Checks bei der

[386] *MMag. Christopher Miess, BSc, Bakk.phil, BSc, MSc,* CEO von ICONIC Capital sowie Mitglied des Fintech Advisory Board, Interview geführt von Marina Kindel (06. Oktober 2018).
[387] *BaFin*, Initial Coin Offerings: Hohe Risiken für Verbraucher, (06. September 2018).
[388] *Dr. Völkel, LL.M*. Interview geführt von Marina Kindel (11. September 2018).

Entgegennahme von Kryptowährungen im Rahmen eines ICOs vorgenommen wurden. Aktuell gibt es immer wieder Projekte, die in diese Falle tappen. Dennoch wird dies früher oder später zu Problemen führen. Zum Beispiel, wenn das ICO Projekt ihre Kryptowährungen in FIAT umtauschen will und dann bei einer Bank parken will. Die Bank wird diese Mittel nicht annehmen können und wollen, wenn das Start Up dessen Herkunft nicht belegen und beweisen kann.[389]

Mit der 5. Geldwäscherichtlinie wurde der Anwendungsbereich der KYC/AML/CFT-Regulationen auf Plattformen zum Umtausch virtueller Währungen sowie Anbieter von elektronischen Geldbörsen (Wallets) virtueller Währungen ausgedehnt. Es fand jedoch keine explizite Nennung von Initial Coin Offerings, Token Sales oder Security Token Offerings statt. Diesen Umstand könnte der Gesetzgeber leicht ändern, wenn er dazu eine Veranlassung sieht. „ICOs, bei welchen ausschließlich Kryptowährungen akzeptiert werden, unterliegen nicht der Geldwäscherichtlinie. Wenn in Zukunft nach Anwendbarkeit der 5. GwR in einem ICO virtuelle Währungen gegen Fiat-Währungen verkauft werden, dann könnte überlegt werden, ob die Emittentin der virtuellen Währung nicht als Händlerin den Anti-Geldwäschebestimmungen unterliegt“ so Dr. Oliver Völkel, LL.M.

Momentan ist es am Wichtigsten Rechtssicherheit zu schaffen. Viele ICO Projekte fragen sich, ob ihr Geschäftsmodell eher einem Utility Token oder einem Security Token entspricht. Viele haben Angst, dass sich die Klassifizierung nachträglich ändern könnte und dadurch große regulatorische Unsicherheiten und Kosten auf StartUps zukommen. Weiters wird es wichtig sein, länderübergreifende Regulatorien zu definieren. Diese müssen idealerweise EU-weit gelten, sodass es zu keinem ‚regulatory arbitraging‘, also keinem Ausnützen von Start Ups von unterschiedlichen nationalen Gegebenheiten kommt. Für Österreich ist dies auch eine Chance, zu verhindern, dass weiterhin Start Ups in Nachbarländer wie Liechtenstein, Slowenien oder die Schweiz, die allesamt im Blockchain Bereich sehr stark sind, abwandern.[390]

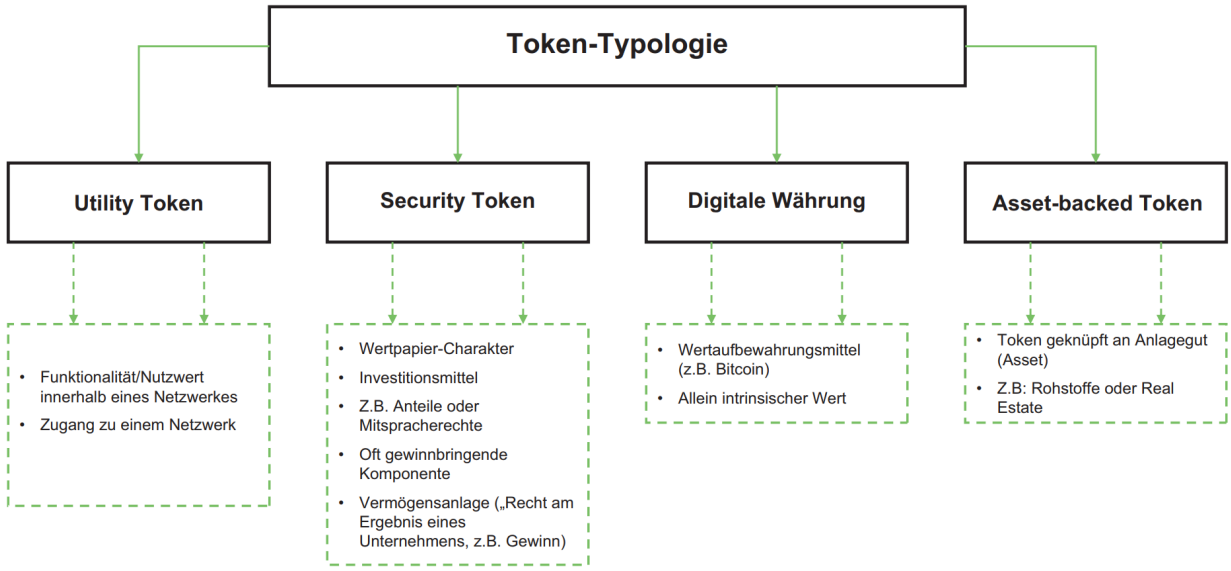
12.2. Einstufung von Token

Seit der Entwicklung von Bitcoin ist eine große Zahl alternativer Kryptowährungen, welche verschiedenste technologische Aspekte inkorporieren, entstanden. Dadurch erfolgt die Notwendigkeit diese anhand ihrer Merkmale in verschiedene Kategorien zu gliedern. Eine

[389] *MMag. Christopher Miess, BSc, Bakk.phil, BSc, MSc,* CEO von ICONIC Capital sowie Mitglied des Fintech Advisory Board, Interview geführt von Marina Kindel (06. Oktober 2018).
[390] *MMag. Christopher Miess, BSc, Bakk.phil, BSc, MSc,* CEO von ICONIC Capital sowie Mitglied des Fintech Advisory Board, Interview geführt von Marina Kindel (06. Oktober 2018).

allgemeingültige Definition von verschiedenen Token-Arten existiert bisher nicht. Viele existierende Token Arten besitzen zudem hybride Formen und können mehreren Klassifizierungen entsprechen. Ein wesentliches Merkmal ist der Unterschied ob eine Kryptowährung ihr eigenes Blockchain-Netzwerk besitzt oder in einer fremden Blockchain inkludiert ist. Darüber hinaus lassen sich Token in 4 Kategorien einteilen.[391] Diese Definitionen stellen jedoch in Abwesenheit spezifischer Regulierungen von Initial Coin Offerings keine rechtliche Einordnung dar. Der Blockchain Bundesverband Deutschland schlägt die Unterteilung in Kryptowährungs-Token, Utility Token und Security Token vor.
Es ist somit festzuhalten, dass der Blockchain Bundesverband Deutschland nicht zwischen den Begriffen Coins und Token differenziert, sondern Coins als Kryptowährungs-Token definiert.[392]

Abbildung 9: Token-Typologie



Quelle: Hahn / Wons

12.2.1. Kryptowährungs-Token

Token welche rein für den Zweck von Transaktionen innerhalb eines Netzwerkes konzipiert sind fallen unter die Definition von Kryptowährungs-Token. Der Blockchain Bundesverband definiert diese als[393] „… *Token, die als Zahlungsmittel innerhalb eines Netzwerkes für*

[391] *Hahn / Wons,* Initial Coin Offering (ICO) - Unternehmensfinanzierung auf Basis der Blockchain-Technologie, (2018) 10f.
[392] *Blockchain Bundesverband*, Regulierung von Token, https://www.bundesblock.de/wp-content/uploads/2018/04/180406-Token-Regulation-Paper-Version-2.0-deutsch_clean_14.00.pdf (10), (abgerufen am 02. September 2018).
[393] *Blockchain Bundesverband*, Regulierung von Token, (21), (abgerufen am 03. September 2018).

Transaktionen zwischen den Nutzern bzw. auch zwischen dem Netzwerkbetreiber und den Nutzern eingesetzt werden.“ [394]

12.2.2. Utility Token

Unter die Definition von Utility Token fallen jene Token, welche den Inhabern einen speziellen funktionalen Nutzen innerhalb eines Netzwerkes ermöglichen. Darunter sind u.a. der Zugang zu einem digitalen Ökosystem, eine derzeitige oder zukünftige Dienstleistung, Stimmrechte oder der Erhalt eines Produkts zu verstehen. Utility Tokens sind die häufigste Form von Tokens und integraler Bestandteil der Plattform auf welcher sie angeboten werden.[395]

12.2.3. Wertpapier Token

Wertpapier Token sind Kryptowährungen welche vergleichbare Rechte wie klassische Eigen- und Fremdkapitalinstrumente gewähren. Der Blockchain Bundesverband Deutschland definiert Wertpapier Token als:[396] *„„Wertpapier- oder Security-Token“: Token, die mit herkömmlichen Wertpapieren nach Art. 4 (1) Nr. 44 Richtlinie 2014/65/EU (“MiFID II”) vergleichbar sind, insbesondere konventionelle Schuldtitel und Eigenkapitalinstrumente“.*[397] Hierbei ist zu beachten, dass die Einordnung in Österreich und Deutschland noch nicht regulatorisch erfasst ist und von Fall zu Fall geprüft werden muss.[398]

12.2.4. Asset-Backed Token

Ein Asset-Backed Token ist eine Form von Kryptowährung welche Rechte, Anspruch oder Eigentum an einem anderen Vermögensgegenstand abbildet (z.B. Gold, Anteil an einer Immobilie).[399]

12.3. Rechtliche Einordnung von ICOs in Österreich

Abhängig von der im Einzelfall zutreffenden Charakterisierung und vertraglichen Ausgestaltung von Tokens fallen diese in verschiedene Anwendungsgebiete von geltenden Rechtsbestimmungen. Die deutsche Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

[394] *Blockchain Bundesverband*, Regulierung von Token, (21), (abgerufen am 03. September 2018).
[395] *Hahn / Wons*, Initial Coin Offering (ICO) - Unternehmensfinanzierung auf Basis der Blockchain-Technologie, (2018) 10.
[396] *Blockchain Bundesverband*, Regulierung von Token, (11), (abgerufen am 03. September 2018).
[397] *Blockchain Bundesverband*, Regulierung von Token, (11), (abgerufen am 03. September 2018).
[398] *Blockchain Bundesverband*, Regulierung von Token, (11), (abgerufen am 03. September 2018).
[399] *Hahn / Wons*, Initial Coin Offering (ICO) - Unternehmensfinanzierung auf Basis der Blockchain-Technologie, (2018) 12.

stellt klar[400]: *„Die BaFin entscheidet im Einzelfall anhand der konkreten vertraglichen Ausgestaltung eines ICOs, ob der Anbieter eine Erlaubnis nach dem Kreditwesengesetz (KWG), dem Kapitalanlagegesetzbuch (KAGB), dem Zahlungsdiensteaufsichtsgesetz (ZAG) oder dem Versicherungsaufsichtsgesetz (VAG) benötigt und ob er Prospektpflichten einzuhalten hat. Tokens stellen in aller Regel Finanzinstrumente (Rechnungseinheiten) im Sinne des Kreditwesengesetzes dar. Deshalb benötigen Unternehmen und Personen, die den Erwerb von Tokens vermitteln, Tokens gewerblich an- oder verkaufen oder Zweitmarktplattformen betreiben, auf denen Tokens gehandelt werden, vorab grundsätzlich eine Erlaubnis der BaFin."* [401]

Eine ähnliche Unterscheidung findet sich im Österreichischen Kapitalmarktgesetz (KMG). Die österreichische Finanzmarktaufsicht stellt klar: *„Für den Fall, dass Coins oder Tokens dem jeweiligen Inhaber Vermögensrechte einräumen, wie beispielsweise Forderungsrechte, Mitgliedschaftsrechte oder dingliche Rechte (wie z.B. Eigentumsrechte, Ansprüche auf Dividenden oder auf Rückzahlung etc.) gegenüber dem ICO Organisator, können sie als Veranlagungen gewertet werden und fallen unter das österreichische Kapitalmarktgesetz.*[402] Zudem besteht eine Prospektpflicht gemäß des KMG, wenn die Bildung einer Risikogemeinschaft zwischen Emittenten und Anleger vorherrscht. Liegt eine wertpapierähnliche Form vor, so hat die Erstellung eines Wertpapierprospektes im Sinne des Kapitalmarktgesetzes zu erfolgen.[403] Gemäß § 2 Abs 1 KMG ist festzuhalten: *„ Ein öffentliches Angebot darf im Inland nur erfolgen, wenn spätestens einen Bankarbeitstag davor ein nach den Bestimmungen dieses Bundesgesetzes erstellter und gebilligter Prospekt veröffentlicht wurde."* (§ 2 Abs 1 KMG) Wird nun ein Wertpapier oder eine Veranlagung ohne ein vorher genehmigtes Prospekt veröffentlicht finden die Straftatbestände gemäß § 15 KMG Anwendung. Aus diesem Grund ist die Klärung der Frage ob ICOs unter das KMG subsumiert werden können von großer Bedeutung. Es ist zu prüfen ob diese als öffentliches Angebot von Wertpapieren oder Veranlagungen zu klassifizieren sind.[404]

Vorab ist festzuhalten, dass in Deutschland Coins als Kryptowährungs-Token klassifiziert werden. In der nachstehenden Betrachtung der kapitalmarktrechtlichen Einordnung von ICOs in Österreich erfolgt jedoch eine Unterscheidung der Begriffe Coins und Token bzw. Initial Coin Offerings und Initial Token Offerings. Coins werden als unmittelbare Wertträger, die durch Mining erzeugt werden definiert. Zudem sind Coins immanent. Das bedeutet, dass sie

[400] *BaFin*, Initial Coin Offerings: Hohe Risiken für Verbraucher, (03. September 2018).
[401] *BaFin*, Initial Coin Offerings: Hohe Risiken für Verbraucher, (03. September 2018).
[402] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, https://www.fma.gv.at/querschnittsthemen/fintech/fintech-navigator/ (abgerufen am 29. September 2018).
[403] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, (abgerufen am 29. September 2018).
[404] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.; *Paulmayer*, Initial Coin Offerings (ICOs) und Initial Token Offerings (ITOs) als prospektpflichtiges Angebot nach KMG?, ZTR 2017 259.

in der Blockchain bereits vorgesehen sind. Tokens hingegen sind nicht immanent. Token sind nicht in der Blockchain vorgesehen[405] *„ ... sondern werden erst später durch die Benutzer der Blockchain ergänzt.“*[406] Token sind daher auf einer, mittels Smart Contracts, bestehenden Blockchain aufsetzende Wertträger“[407] Diese können nicht durch minen erzeugt werden. Obwohl Coins und Token Unterschiede aufweisen, sind sie dennoch beide Wertträger die in der Blockchain übertragen werden können. Somit erfolgt eine Differenzierung zwischen Initional Coin Offerings und Initial Token Offerings.[408]

12.3.1. Coins/ Token als Wertpapiere

Es ist anzumerken, dass keine Legaldefinition von Wertpapieren im Gesetz verankert ist, sondern diese lediglich typologisch erfasst wurde. Der kapitalmarktrechtliche Wertpapierbegriff umfasst gemäß[409] der RL 2004/39/EG[410] Art 4 Abs 1 Z 18 lit a bis c. übertragbare Wertpapiere: *„ ... die Gattungen von Wertpapie- ren, die auf dem Kapitalmarkt gehandelt werden können, mit Ausnahme von Zahlungsinstrumenten, wie*

a) Aktien und andere, Aktien oder Anteilen an Gesellschaften, ...

b) Schuldverschreibungen oder andere verbriefte Schuldtitel, einschließlich Zertifikaten (Hinterlegungsscheinen) für solche Wertpapiere;

c) alle sonstigen Wertpapiere, die zum Kauf oder Verkauf solcher Wertpapiere berechtigen oder zu einer Barzah- lung führen, ...“

Zudem muss jederzeit eine Veräußerung möglich sein. Ferner muss eine Aufnahme in ein Register mit Wertpapiercharakter erfolgen. Auf Grund der Eigenschaften der Blockchain ließ sich diese als ein solches einzustufen. Es ist sich die zentrale Frage zu stellen, ob der jeweilige Token/Coin mit Aktien oder Anleihen im kapitalmarktrechtlichen Sinn zu vergleichen ist und diese somit als Wertpiere im Sinne des KMG zu klassifizieren sind[411]: *„Gewähren Coins oder Token ihren Inhabern Rechte, die für Gewöhnlich mit Aktien oder Schuldverschreibungen verbunden sind, werden sie als Wertpapiere im*

[405] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[406] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[407] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[408] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[409] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[410] Richtlinie2004/39/EGdesEuropä.04.2004 über Märkte für Finanzinstrumente, zur Änderung der Richtlinien 85/611/EWG und 93/6/EWG des Rates und der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates und zur Auf- hebung der Richtlinie 93/22/EWG des Rates, ABl L 2004/45, 1.
[411] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.

kapitalmarktrechtlichen Sinn qualifiziert.“ [412] Sind Token/Coins nicht mit solchen vergleichbar, können diese nicht unter den kapitalmarktrechtlichen Wertpapierbegriff subsumiert werden. Merkmale für das Vorliegen eines Wertpapieres im Sinne des KMG sind u.a. Zinszahlungen, Mitspracherechte, Anteile am Gewinn sowie Rückzahlung der Gelder am Ende einer zuvor definierten Laufzeit.[413]

12.3.2. Coins/ Tokens als Veranlagungen

Neben der Möglichkeit der Einstufung von Token als Wertpapiere ist die mögliche Einstufung als Veranlagung gemäß § 1 Abs 1 Z 3 KMG zu prüfen. Unter Veranlagungen sind *„… Vermögensrechte, über die keine Wertpapiere ausgegeben werden, aus der direkten oder indirekten Investition von Kapital mehrerer Anleger auf deren gemeinsame Rechnung und gemeinsames Risiko oder auf gemeinsame Rechnung und gemeinsames Risiko mit dem Emittenten, sofern die Verwaltung des investierten Kapitals nicht durch die Anleger selbst erfolgt; …“* (§ 1 Abs 1 Z 3 KMG) zu verstehen. Zu Vermögensrechte zählen Forderungsrechte, Mitgliedschaftsrechte oder dingliche Rechte. Der Schlüsselfaktor im Zusammenhang mit der Einordnung von Coins/Tokens als Veranlagung im kapitalmarktrechtlichen Sinn stellt den Vermögenswert dar. Werden dem Inhaber Vermögensrechte gegenüber dem Emittenten eingeräumt, so handelt es sich bei Token um eine Veranlagung gemäß des KMG, räumen Token keine dinglichen Rechte ein, so stellen diese keine Veranlagungen im Sinne des KMG dar. Auch wenn die Einstufung eines Tokens die Anwendbarkeit des Kapitalmarktrechtes begründet, ist dennoch die Frage der wertpapierrechtlichen Einordnung zu klären. Auf Grund des Vorliegens des Typenzwangs im Wertpapierrecht, welches an jenes des Sachenrechtes anknüpft, knüpft der Besitz des Wertpapieres an § 323 ABGB, § 426 ABGB sowie § 367 ABGB an. Von den möglichen Wertpapierarten liegt ein Vergleich mit Inhaberpapieren, auf Grund der leichten Verkehrsfähigkeit, am naheliegendsten. Es ist jedoch festzuhalten, dass bei Inhaberpapieren die Rechte an diesen mit Urkunden verbrieft sind. Einzelverbriefungen sowie Sammelverbriefungen sind möglich. Es ist jedoch anzumerken: [414] *„Eine völlige Entmaterialisierung des Wertpapiers, also ein Verzicht auf eine physische Urkunde ist in Österreich hingegen nicht vorgesehen.“*[415] Daraus resultiert, dass Tokens/Coins auf Grund einer fehlenden physischen Urkunde keine Wertpapiere im klassischen Sinn darstellen

[412] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[413] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[414] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[415] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.

können. Eine mögliche Ausgestaltung könnte die Verknüpfung von Gutglaubensregeln an die Inhaberschaft darstellen. In Anlehnung an das Sachenrecht könnte neben der tatsächlichen Inhaberschaft die Eintragung in ein öffentliches Register erfolgen. Die Blockchain stellt ein öffentlich verfügbares und nicht veränderbares Register dar. Durch diese Eigenschaften könnte den Gedanken des Gutglaubensschutzes Folge geleistet werden.

Somit ist festzuhalten, dass Coins/Tokens je nach Ausgestaltung der eingeräumten Rechte unter die Bestimmungen des KMG fallen können. Werden durch die Emittierung der Token Rechte, welche mit jenen von Anleihen oder Aktien vergleichbar sind, ausgegeben so sind diese als Wertpapiere iSd KMG zu klassifizieren. Räumen hingegen die emittierten Tokens den Inhaber Vermögensrechte ein, so sind diese als Veranlagen iSd KMG zu deklarieren. Liegen jedoch weder Wertpapiere noch Veranlagungen gemäß KMG vor, so werden die ausgegebenen Token kapitalmarktrechtlich nicht erfasst.[416]

„Eine wertpapierrechtliche Qualifikation von Coins oder Token als Wertpapier muss hingegen mangels verbriefter Urkunde ausscheiden. Allerdings könnte überlegt werden, Wertpapiere zu begeben, bei denen die Inhaberschaft eines bestimmten Coins oder Tokens die Vermutung der Inhaberschaft am Wertpapier nahelegt.“[417] Es ist anzumerken, dass bei aktueller österreichischen Rechtslage grundsätzlich ICOs keiner generellen Aufsicht oder Regulierung unterliegen:[418] *„… Aufgrund unterschiedlicher Ausgestaltung von ICOs in technischer, funktionaler und wirtschaftlicher Hinsicht ist eine allgemeingültige aufsichtsrechtliche Einordnung nicht möglich. Derzeit bestehen weder auf internationaler, europäischer noch österreichischer Eben spezifische aufsichtsrechtliche Regelungen zu ICOs.“*[419] Nur unter bestimmten Voraussetzungen stellen diese, wie oben dargestellt, eine konzessionspflichtige Finanzdienstleistung dar oder werden einem anderen Gesetz zum Schutz der Anleger unterstellt. Bei jedem ICO muss eine individuelle rechtliche Prüfung erfolgen. Die Art und Weise wie das Kapital eingenommen und verwendet wird sowie die rechtliche Stellung des Tokeninhabers stellen ausschlaggebenden Kriterien für die rechtliche Einordnung der ICOs dar. Je nach Ausgestaltung können Konzessionstatbestände nach dem Bankwesengesetz (BWG), Wertpapieraufsichtsgesetz 2018 (WAG 2018), Kapitalmarktgesetz (KMG) oder dem Alternativ Investmentfonds Manager-Gesetz (AIFMG) vorliegen.

Sofern ein ICO zu emittierender Token unter die Definition konzessionspflichtiger Tätigkeiten der FMA fällt, unterliegt dieser in jedem Fall der einschlägigen Bestimmungen und Sorgfaltspflichten gegen Geldwäsche und Terrorismusfinanzierung des FM-GwG. Im

[416] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[417] *Völkel*, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.
[418] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, (abgerufen am 29. September 2018).
[419] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, (abgerufen am 29. September 2018).

Falle das die Ausgestaltung des Tokens bzw. die Abwicklung des ICOs keine konzessionspflichtige Tätigkeit nach sich zieht, kann[420] *„ .. die Pflicht zur Einhaltung der Bestimmungen zur Prävention von Geldwäscherei und Terrorismusfinanzierung unter Umständen aufgrund der Gewerbeordnung ... "*[421] oder durch Bestimmungen u.a. in der Rechtsanwalts- und Notariatsordnung oder dem Glücksspielgesetz gegeben sein. Bei Vorliegen einer Konzessionspflicht erfolgt die Aufsicht durch die Finanzmarktaufsicht, bei Nichtvorliegen durch die zuständige Verwaltungsbehörde. [422]

12.3.3. Österreich vs. andere Länder

„Österreich ist gerade dabei eine Regulierung zum Thema zu definieren. Es geht darum, den Kryptowährungs- und Blockchain-Sektor möglichst zu fördern, aber gleichzeitig auch ein Mindestmaß an Anlegerschutz und Rechtssicherheit zu garantieren. Hier ist der Fokus weniger auf dem institutionellen Anleger als mehr auf dem Kleinanleger gelegt. Ähnlich wie im klassischen Wertpapierrecht benötigt dieser mehr Schutz. Einige Länder sind Österreich hier schon voraus", so MMag. Christopher Miess, BSc, Bakk.phil, BSc, MSc, CEO von ICONIC Capital, einer der führenden ICO Beratungs- und Investmentgesellschaft in Asien.
In der Schweiz wird aktuell zwischen drei verschiedenen Token-Arten unterschieden: Zahlungstoken, Nutzungs- und Anlagetoken. Bermuda hat Anfang 2018 ein Gesetz für Initial Coins Offerings erlassen. Erfasst wurden ICOs, dessen Struktur jenen von öffentlichem Crowdfunding ähneln. Diese müssen bewilligt werden und ein „White Paper" erstellen. Malta hat drei Gesetzesentwürfe veröffentlich, dessen Fokus die technologische Beschaffenheit von virtuellen Währungen, Blockchain und DLT darstellt. Neben Exchanges und (Handels) Plattformen steht die Lizenzierung von ICOs im Vordergrund.[423] Liechtenstein hat ein eigenes Blockchaingesetz[424] heraus gegeben. Ferner hat auch die Schweiz eine Jurisdiktion für Initial Coin Offerings etabliert. Eine umfassende aufsichtsrechtliche Beurteilung je nach Art des Token ist erfolgt. Durch die eindeutige Rechtslage sind zahlreiche bedeutende Blockchain-Unternehmen in der Schweiz ansässig geworden.[425]

[420] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, (abgerufen am 29. September 2018).
[421] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, (abgerufen am 29. September 2018).
[422] *FMA,* FinTech-Navigator durch das Aufsichtsrecht, (abgerufen am 29. September 2018).
[423] *Ministerium für Präsidiales und Finanzen,* VERNEHMLASSUNGSBERICHT DER REGIERUNG BETREFFEND DIE SCHAFFUNG EINES GESETZES ÜBER AUF VERTRAUENSWÜRDIGEN TECHNOLOGIEN (VT) BERIHENDE TRANSAKTIONSSYSTEME (BLOCKCHAIN- GESETZ; VT- GESETZ; VTG UND DIE ABÄNDERUNG WEITERER GESETZE), https://www.llv.li/files/srk/vnb-blockchain-gesetz.pdf (30f), (abgerufen am 2. Oktober 2018).
[424] *Ministerium für Präsidiales und Finanzen,* VERNEHMLASSUNGSBERICHT DER REGIERUNG BETREFFEND DIE SCHAFFUNG EINES GESETZES ÜBER AUF VERTRAUENSWÜRDIGEN TECHNOLOGIEN (VT) BERIHENDE TRANSAKTIONSSYSTEME (BLOCKCHAIN- GESETZ; VT- GESETZ; VTG UND DIE ABÄNDERUNG WEITERER GESETZE), (30f), (abgerufen am 2. Oktober 2018).
[425] *Dobrowolski,* Überblick über die unterschiedlichen aufsichtsrechtlichen Rahmenbedingungen für Initial Coin Offerings, Linde 2018, 147.

„In der näheren geographischen Umgebung haben sich, wie oben beschrieben, einige Länder, allem voran die Schweiz, Liechtenstein, aber auch Slowenien sich zu Blockhain Hubs entwickelt. Nicht zuletzt hat die gut durchdachte Regulierung der Länder dazu beigetragen. Liechtenstein z.B. hat kürzlich ein komplett neues Blockchain Gesetz herausgegeben. Seitdem sind einige größere Projekte wie LCX, Aeternity und Neon Exchange in Liechenstein ansässig geworden. Aber auch in anderen europäischen Städten wie Malta, Gibraltar und anderen hat sich einiges hierzu getan. Als Österreich müssen wir deshalb schnell und effizient sein um hier nicht den Anschluss zu verlieren“, so MMag. Christopher Miess, BSc, Bakk.phil, BSc, Mitglied des Fintech Advisory Board in Österreich.

13. Vorschlag Regulierung

Weder eine Überregulierung noch eine fehlende Regulierung sind für Virtuelle Währungen sowie auf Blockchain-basierenden Dienstleistungen und Produkten zu empfehlen. Eine Überregulierung schadet der alternativen Finanzwirtschaft und fehlende Regulierung seriösen Marktteilnehmern, dessen Reputation durch Betrüger massiv in Mitleidenschaft gezogen wird.[426] Der EU-Gesetzgeber hat ein potentielles AML/CFT-Risiko identifiziert und in der 5. GwR adressiert, indem im Kern der Anwendungsbereich der 4. Geldwäscherichtlinie auf Tauschbörsen und E-Wallet Anbieter für virtuelle Währungen erweitert wird. Dies soll mit der Unterwerfung der "Gatekeeper in die Kryptowelt" erreicht werden. Sie unterliegen damit dieselben Standards zur Verhinderung von Geldwäsche und Terrorismusfinanzierung wie andere Finanzmarktteilnehmer. Das Vorhaben wird zu einer weiteren Professionalisierung der Branche führen und wird daher von dieser auch begrüßt. Die Auswirkungen werden begrenzt sein, weil ohnehin viele Unternehmen in der Branche bereits bisher KYC/AML-Verpflichtungen.[427]

Das Finanzministerium spricht sich für klare Regeln im Zusammenhang mit „Bitcoin“ und andere VW aus. Dennoch wird deutlich, dass keine massive Regulation in diesem Sektor geplant ist. Ziel der regulatorischen Maßnahmen stellt der Schutz der Investoren, vor allem als Verbraucher, und der Konsumenten vor dubiosen Geschäften dar. Zudem sollen zukünftig die Identitäten von Eigentümern von Kryptowährungen erfasst werden. Auch beim Kauf von VW oder bei Tauschhandlungen von diesen im Wert von über 10.000 Euro sollen zukünftig Meldungen bei der Geldwäschemeldestelle erfolgen. In Bezug auf Initial Coins Offerings wird erwähnt, dass zukünftig die Prospektpflicht ausgeweitet werden soll und dessen Billigung durch die Aufsicht unabdingbar ist.[428]

Sowohl innerhalb als auch außerhalb der EU werden die auf der DLT basierenden Innovationen analysiert, die je nach Land unterschiedlichen Resultate und Regulierungsmaßnahmen aufweisen. Einige Länder stehen den DLT Innovationen sehr positiv gegenüber, andere Länder/Regierungen jedoch sprechen eindeutige Warnungen aus.[429]

Die Europäische Union *„ ... hebt hervor, dass virtuelle Währungen und DLT das Potenzial besitzen, einen positiven Beitrag zum Wohlergehen der Bürger und zur wirtschaftlichen*

[426] *Presse*, Löger will Bitcoin „mit Maß und Ziel“ regulieren, https://diepresse.com/home/wirtschaft/economist/5377604/Loeger-will-Bitcoin-mit-Mass-und-Ziel-regulieren, (abgerufen am 2. Oktober 2018).
[427] *Dr. Arthur Stadler,* Partner der Rechtsanwaltskanzlei Stadler Völkel, Interview geführt von Marina Kindel (24. Juli 2018).
[428] *Presse*, Löger will Bitcoin „mit Maß und Ziel“ regulieren, (abgerufen am 2. Oktober 2018).
[429] *Ministerium für Präsidiales und Finanzen,* VERNEHMLASSUNGSBERICHT DER REGIERUNG BETREFFEND DIE SCHAFFUNG EINES GESETZES ÜBER AUF VERTRAUENSWÜRDIGEN TECHNOLOGIEN (VT) BERIHENDE TRANSAKTIONSSYSTEME (BLOCKCHAIN- GESETZ; VT- GESETZ ; VTG UND DIE ABÄNDERUNG WEITERER GESETZE), (31ff), (abgerufen am 2. Oktober 2018).

Entwicklung, etwa im Finanzsektor, zu leisten..."[430] (Erwägungsgrund 1). Minimierung der Kosten von grenzüberschreitenden Transaktionen, Erleichterung des Zugangs zu Finanzmitteln sowie Senkung von operativen Kosten werden u.a. als Chancen der DLT genannt. (Erwägungsgrund 1). Dennoch wird auch auf die damit verbunden Risiken wie z.B. hohe Kursschwankungen, rechtliche Unsicherheit und fehlende Dokumentationsmöglichkeit im Zusammenhang von DLT und VW aufmerksam gemacht (Erwägungsgrund 2).[431]

Wie bereits erwähnt steht vor allem der Schutz der User/ Investoren im Vordergrund. Ein Schlüsselfaktor stellt in diesem Zusammenhang der private Key dar. Es muss geklärt werden wie u.a. Eigentumsrecht oder ein Diebstahl von diesem rechtlich einzuordnen ist und wie Transaktionen rückabgewickelt werden könnte. Grundsätzlich sind Transaktionen in der Blockchain unwiderruflich.[432]

Liechtenstein ist der Auffassung das Innovationen nur durch Offenheit der Regierung gefördert werden kann. Zudem muss ein praxisorientierter Ansatz gewählt werden. Es wird mit Unternehmen der Branche zusammengearbeitet. Nur so können das Wachstum des Finanzsektors und der Wohlstand des Landes garantiert werden. Liechtenstein hat liberale Strukturen geschaffen, um den Innovationsprozess zu fördern. Es wurde ein Kanal des staatlichen Innovationsprozesses sowie ein Regierungslabor, bei dem innovative Firmen beim Prozess der Bewilligung begleitet werden, eingerichtet. Es ist stets das Innovationspotenzial der DLT zu berücksichtigen. Aktuell arbeitet Liechtenstein an einem Blockchaingesetz (VT-Gesetz, VTG), welches im europäischen Raum somit einzigartig ist. [433] Der Vernehmlassungsbericht gibt Auskunft über die Eigenschaften der Blockchain-Technologie, Gründe des Regulierungsbedarfs und dessen Zielsetzung. Zudem wurden die Schwerpunkte der Vorlage definiert. Diese umfassen u.a. die Erklärung des Tokenmodells, den aufsichtsrechtlichen Ansatz und die Sorgfaltspflichten. Es werden zahlreiche Gesetze geändert u.a. das Gewerberecht sowie neue Gesetze geschaffen. Bei den Änderungen des Sorgfaltspflichtengesetzes, welches zur Bekämpfung gegen Geldwäscherei und Terrorismusfinanzierung sowie organisierter Kriminalität dient fällt auf, dass der Geltungsbereich umfangreicher als jener in Österreich ist. Es werden sechs sorgfaltspflichtige Gruppe ernannt:

---

[430] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[431] Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.
[432] *Ministerium für Präsidiales und Finanzen,* VERNEHMLASSUNGSBERICHT DER REGIERUNG BETREFFEND DIE SCHAFFUNG EINES GESETZES ÜBER AUF VERTRAUENSWÜRDIGEN TECHNOLOGIEN (VT) BERIHENDE TRANSAKTIONSSYSTEME (BLOCKCHAIN- GESETZ; VT- GESETZ; VTG UND DIE ABÄNDERUNG WEITERER GESETZE), (31f), (abgerufen am 2. Oktober 2018).
[433] *Ministerium für Präsidiales und Finanzen,* VERNEHMLASSUNGSBERICHT DER REGIERUNG BETREFFEND DIE SCHAFFUNG EINES GESETZES ÜBER AUF VERTRAUENSWÜRDIGEN TECHNOLOGIEN (VT) BERIHENDE TRANSAKTIONSSYSTEME (BLOCKCHAIN- GESETZ; VT- GESETZ; VTG UND DIE ABÄNDERUNG WEITERER GESETZE), (37f), (abgerufen am 2. Oktober 2018).

1. Token Emittenten nach dem VTG;
2. VT-Protektoren nach dem VTG;
3. Physische Validatoren nach dem VTG;
4. VT-Verwahrer nach dem VTG;
5. VT-Identitätsdienstleister nach dem VTG;
6. VT-Wechselstubenbetreiber nach VTG; [434]

Auch wenn das Blockchain-Gesetz von Liechtenstein Vorreiter ist, ist dieses jedoch nur als Leitfaden gedacht. Es ist stets, auf europäischer und nationaler Ebene, die Verhältnismäßigkeit der Regularien zu prüfen. Meines Erachtens nach ist sich klar gegen eine Überregulierung von virtuellen Währungen auszusprechen. Eine Überregulation würde sich eindeutig negativ auf die Innovation auswirken. Bereits bestehende Gesetze sollen Anwendung finden. Es ist sich klar für eine Unterstellung der neuen Verpflichteten in die Gewerbeordnung auszusprechen. Dies würde auch die aktuellste Ansicht, dass der Handel mit VW, auf Grund des Vorliegens eines freien Gewerbes, der Gewerbeordnung unterliegt, bestärken. Die Analyse der Anwendbarkeit der Gewerbeordnung in den Kapiteln 7 und 8 hat verdeutlicht, dass mit bestehenden Gesetzen genügend regulatorische Maßnahmen getroffen werden können. Ferner ist von einer möglichen Unterstellung in das Finanzmarktgeldwäschegesetz, auf Grund der strukturellen Eigenschaften virtueller Währungen, deutlich Abstand zu nehmen.

[434] *Ministerium für Präsidiales und Finanzen,* VERNEHMLASSUNGSBERICHT DER REGIERUNG BETREFFEND DIE SCHAFFUNG EINES GESETZES ÜBER AUF VERTRAUENSWÜRDIGEN TECHNOLOGIEN (VT) BERIHENDE TRANSAKTIONSSYSTEME (BLOCKCHAIN- GESETZ; VT- GESETZ; VTG UND DIE ABÄNDERUNG WEITERER GESETZE), (173f), (abgerufen am 2. Oktober 2018).

14. Conclusio

Das Vorurteil, dass sich besonders Bitcoins für Geldwäscheaktivitäten eignen, konnte entkräftet werden. Es ist zwischen anonymen und pseudoanonymen Währungen zu unterschieden, die unterschiedliche technische Eigenschaften aufweisen, wodurch sich diese im unterschiedlichen Maße für Geldwäscheaktivitäten eignen. Es ist wichtig, dass auch von Seiten der gesetzgebenden Instanz die Technologie und dessen Möglichkeiten verstanden werden um geeignete rechtliche Rahmenbedingungen schaffen zu können. Auf Grund der Eigenschaften und Komplexität der Technologie virtueller Währungen, gestaltet sich jedoch die Schaffung rechtlicher Rahmenbedingungen als sehr schwierig. Mit der 5. Geldwäscherichtlinie wurden die ersten Schritte in Richtung Regulation von „Gatekeepern“ in die Wege geleitet, welche jedoch nicht jede Möglichkeit des Erwerbs von Kryptowährungen erfasst und somit lückenhaft ist.

Ferner liegen in vielen Bereichen technische und damit rechtliche Wissensdefizite vor, die durch die Darlegung der parlamentarischen Anfragen bestätigt wurden. Zum Zeitpunkt des Verfassens der Arbeit konnten keine Auskünfte über die rechtliche Einordnung von Tokens bzw. die rechtliche Unterscheidung zwischen Coins und Tokens erteilt werden. Der Aspekt, dass ICOs oder Dienstleister, welche virtuelle Währungen in andere virtuelle Währungen eintauschen nicht in der 5. Gelwäscherichtlinie erwähnt wurden, zeigt wie die gesetzgebende Instanz zeitlich hinterherhinkt. Zudem wurden in keinem einzigen Bericht dezentrale Börsen oder dezentrale Unternehmen erwähnt. Die gesetzgebende Instanz müsste sich bereits jetzt mit solchen Börsen/Unternehmen und möglichen rechtlichen Rahmenbedingungen auseinandersetzen um bei Entstehung dieser eine Chance zuhaben rechtzeitig auf solche mit einem geeigneten rechtlichen Rahmenwerk reagieren zu können.

Es ist festzuhalten, dass es für virtuelle Währungen sowie Initial Coin Offerings einer Grundregulierung bedarf. Auf der einen Seite bedingt eine rechtliche Regulierung die Steigerung der Reputation des Sektors. Zudem werden Nutzer sowie Investoren teilweise abgesichert. Auf der anderen Seite liegt eine technische Innovation vor, die sich exorbitant schnell verändert. Es entstehen täglich abgeänderte und neue Geschäftsmodelle mit neuen technischen Eigenschaften. Die Dauer der Prozesse, bis neue Gesetze umgesetzt werden, sind zulange um mit den Veränderungen mithalten zu können.

Darüber hinaus konnte nicht geklärt werden welche zukünftigen Maßnahmen gesetzt werden, um die gemäß der 5. Gelwäscherichtlinie „neuen Verpflichteten“ zukünftig zu erfassen. Smart Regulation und die damit einhergehende Unterstellung in die Gewerbeordnung bietet eine optimale Lösung.

An dieser Stelle ist anzumerken, dass die auf der Blockchain-Technologie basierenden virtuellen Währungen jahrelang – seitens Wirtschaft, Gesellschaft und Legislative – als Alternative bestehender Finanzsysteme unterschätzt wurden und die Regulation eindeutig hinterherhinkt. Es muss die stetige Weiterentwicklung und das immense Innovationspotenzial der Technologie berücksichtigt werden. Für die gesetzgebende Instanz wird es zukünftig äußerst schwierig sein, auf die sich schnell voranschreitenden technologischen Veränderungen mit geeigneten rechtlichen Rahmenwerken reagieren zu können.

Abbildungsverzeichnis

Literaturübersicht

Alm, Anfrage 1578 vom 23.05.2018 (XXV. GP), https://www.parlament.gv.at/PAKT/VHG/XXV/J/J_01578/fname_351518.pdf, (abgerufen am 28. August 2018).

Asolo, Dash PrivateSend Explained, https://www.mycryptopedia.com/dash-privatesend/, (abgerufen am 31. August 2018).

Alonso, Zero to Monero: First Edition, https://getmonero.org/library/Zero-to-Monero-1-0-0.pdf, (abgerufen am 28. August 2018).

Androulaki / Karame / Roeschlin / Scherer / Capkun, Evaluating User Privacy in Bitcoin, https://eprint.iacr.org/2012/596.pdf, (abgerufen am 13. Oktober 2018).

Antonopoulos, Mastering Bitcoin, https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf, (abgerufen am 01. September 2018).

Ax, Bitcoin promoter Shrem indicted in NY for money laundering. https://www.reuters.com/article/us-usa-crime-bitcoin/bitcoin-promoter-shrem-indicted-in-ny-for-money-laundering-idUSBREA3D1RU20140414, (abgerufen am 31.08.2018).

BaFin, Initial Coin Offerings: Hohe Risiken für Verbraucher, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1711_ICO.html, (abgefragt am 03. September 2018).

BaFin, Verbraucherwarnung: Risiken von Initial Coin Offerings (ICOs) https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html, (abgerufen am 04. September 2018).

Barth/Durstberger, 5. Geldwäsche-Richtlinie reguliert virtuelle Währungen, GesRZ 2018, 203.

Bankenverband, Know Your Customer: Privatkundenverifizierungen im EU- Binnenmarkt, https://bankenverband.de/media/files/Positionspapier_KYC.pdf, (abgerufen am 3 September 2018).

Ben-Sasson/Chiesa/Garman/Green/Miers/Tromer/Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version), http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf (abgerufen am 30. September 2018).

Biryukow/Feher, Deanonymization of Hidden Transactions in Zcash https://cryptolux.org/images/d/d9/Zcash.pdf (abgerufen am 30. September 2018).

Blockchain Austria, Unser 9 Punkte Plan, https://www.blockchain-austria.gv.at/unser-9-punkte-plan/, (abgerufen am 20. August 2018).

Blockchain Bundesverband, Regulierung von Token, https://www.bundesblock.de/wp-content/uploads/2018/04/180406-Token-Regulation-Paper-Version-2.0-deutsch_clean_14.00.pdf, (abgerufen am 02. September 2018).

Bowe/Hornby/Wilcox, Zcash Protocol Specification, https://whitepaperdatabase.com/zcash-zec-whitepaper/ abgerufen am 30. September 2018).

Brauneis/Mestel, Finanzwesen- allgemein verständlich: Kryptowährungen, ÖBA (2018), 711.

Buchleiter/Rabl, Blockchain und Smart Contracts, ecolex 2017, 4.

Bundesanstalt für Finanzdienstleistungsaufsicht, Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html, (abgerufen am 20. August 2018).

Bundesanstalt für Finanzen, Merkblatt - Hinweise zum Zahlungsdiensteaufsichtsgesetz (ZAG),https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html;jsessionid=188D4736DCEA8F5307F430288FF8A302.1_cid298?nn=9450978#doc7846622bodyText30, (abgerufen am 20. August 2018).

Bundeskriminalamt, Informationsblatt, http://www.bundeskriminalamt.at/308/files/Geldwaeschemeldung_Info.pdf, (abgerufen am 12. August 2018).

Bundeskriminalamt, Lagebericht Geldwäsche 2017, http://www.bundeskriminalamt.at/308/files/Geldwaesche_17_web.pdf, (abgerufen am 20. August 2018).

Bundeskriminalamt, Meldestellen, http://www.bundeskriminalamt.at/602/start.aspx, (abgerufen am 12. August. 2018).

Bundesministerium für Digitalisierung und Wirtschaftsstandort, 386/AB vom 30.4.2018 zu 383/J (XXXVI.GP) https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_00386/imfname_691962.pdf, (Stand 30.4.2018).

Bundesministerium für Finanzen, Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt (Finanzmarkt-Geldwäschegesetz – FM-GwG),https://www.bmf.gv.at/rechtsnews/FM-GwG_TXT_161109.pdf?67rvn7, (abgerufen am 3. September 2018).

Bundesministerium für Finanzen, Geldwäscherei und Terrorismusfinanzierung, https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/geldwaesche.html, (abgerufen am 03. September 2018).

Bundesministerium Finanzen, Geldwäscherei und Terrorismusfinanzierung, https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/geldwaesche.html, https://www.bmf.gv.at/finanzmarkt/register-wirtschaftlicher-eigentuemer/Uebersicht/Rechtliche-grundlagen.html, (abgerufen am 6. Oktober 2018).

Bundesministerium Finanzen, Geldwäscherei und Terrorismusfinanzierung, https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/geldwaesche.html, (abgerufen am 6. Oktober 2018).

Bundesministerium für Finanzen, 382/AB vom 30.4.2018 zu 382/J (XXVI.GP), https://www.parlament.gv.at/PAKT/VHG/XXVI/AB/AB_00382/imfname_691926.pdf, (STAND 20.4.2018)

Bundesministerium für Finanzen, Nationale Risikoanalyse Österreich 2015, https://www.bmf.gv.at/finanzmarkt/geldwaesche-terrorismusfinanzierung/Nationale_Risikoanalyse_Oesterreich_PUBLIC.pdf, (Stand 2015)

Bundesministerium für Wissenschaft, Forschung und Wirtschaft, Bundeseinheitliche Liste der freien Gewerbe, https://www.bmdw.gv.at/Unternehmen/Gewerbe/Documents/Bundeseinheitliche _Liste_der_freien_Gewerbe.pdf (Stand 20. Oktober 2017).
Bundesministerium für Wissenschaft, Forschung und Wirtschaft, 1446/AB vom 22.07.2014 zu 1578/J (XXV.GP),https://www.parlament.gv.at/PAKT/VHG/XXV/ AB/AB_01446/imfname_359616.pdf, (abgerufen am 28. August 2018).

Chohan, The Cryptocurrency Tumblers: Risks, Legality and Oversight, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361, (abgerufen am 01. September 2018).

Coinfinity, Geschäftsführer Max Tertinegg, AML Abteilung Matthias Reder

Coinfinity, https://coinfinity.com, (abgerufen am 10. August 2018).

de Balthasar / Hernandez-Castro, An Analysis of Bitcoin Laundry Services, https://kar.kent.ac.uk/63502/193/An%20Analysis%20of%20Bitcoin%20Mixers.pdf, (abgerufen am 3 September 2018).

Deloitte, Geldwäscheprävention bei Güterhändlern Ergebnis einer qualitativen Studie, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/finance/Forensic-Studie-Geldwaeschepraevention_safe.pdf, (abgerufen am 3. September).

der brutkasten, Nikolaus Jilch, Die Wurzeln von Bitcoin (Teil 2): Von der Donaumonarchie bis zur Blockchain, https://www.derbrutkasten.com/die-wurzeln-von-bitcoin-teil-2-von-der-donaumonarchie-bis-zur-blockchain/(abgerufen am 16.07.2018).

Die Österreichischen Rechtsanwälte, Verhinderung von Geldwäscherei und Terrorismusfinanzierung,https://www.ooerak.at/fileadmin/OOERAK/Downloads/Geldw%C3%A4sche_Leitfaden_April2017.pdf, (abgerufen am 3. September 2018).

Dobrowolski, Überblick über die unterschiedlichen aufsichtsrechtlichen Rahmenbedingungen für Initial Coin Offerings, Linde 2018, 147.

DOLLIVER/ERICSON/LOVE, A GEOGRAPHIC ANALYSIS OF DRUG TRAFFICKING PATTERNS ON THE TOR NETWORK, https://onlinelibrary.wiley.com/doi/epdf/10.1111/gere.12241, (abgefragt am 3. Oktober 2018).

Dr. Julian Hosp, Kryptowährungen 1. Auflage. München: FinanzBuch Verlag, 2018.

Duffield / Diaz, Dash: A Privacy-Centric Crypto-Currency, https://bravenewcoin.com/assets/Whitepapers/Dash-WhitepaperV1.pdf (abgerufen am 31. August 2018).

Egmont Group, About, https://egmontgroup.org/content/about, (abgerufen am 20. August 2018).

ESMA,EBA,EIOP, Warnmeldung, Ahttps://eiopa.europa.eu/Publications/Other%20 Documents/Joint%20ESAs%20Warning%20on%20Virtual%20Currencies_DE.pdf, (abgerufen am 24.07.2018).

Eberwein/ Steiner, Bitcoins. Wien: Jan Sramek Verlag KG, 2014.

Europa.eu, Verordnungen, Richtlinien und sonstige Rechtsakte https://europa.eu/european-union/eu-law/legal-acts_de, (Stand 24.05.2018).

Europäischer Rat/ Rat der Europäischen Union, Bekämpfung der Geldwäsche und der Terrorismusfinanzierunghttp://www.consilium.europa.eu/de/policies/fight-against-terrorism/fight-against-terrorist-financing/, (abgerufen am 3. September 2018).

*Europäische Zentralbank***,** Virtual Currency Schemes, www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, (abgerufen am 30. August 2018).

FATF, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION, http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, (abgerufen am 20. August 2018).

Feigelson, United States, Patent Application Publication,https://patentimages.storage.googleapis.com/a0/71/ef/a5115ad8a70bd0/US20130166455A1.pdf, (abgerufen am 5. Oktober 2018).

Financial Action Task Force on Money Laundering (FATF), F-Leitfaden zum risikoorientierten Ansatz zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung (Deutsche Übersetzung),https://www.bafin.de/SharedDocs/Downloads/DE/Leitfaden/lf_fatf_leitfaden_risikoorientierter_ansatz.html, (abgerufen am 3. September 2018).

Financial Action Task Force in Money Laundering, Virtual Currencies – Key Definitions and Potential AML/CFT Risks, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, (abgerufen am 30. September 2018).

Finanzmarktaufsicht, Rundschrieben Risikoanalyse zur Prävention von Geldwäscherei und Terrorismusfinanzierung, https://www.fma.gv.at/download.php?d=3297,(abgerufen am 26. August 2018).

FMA, FinTech-Navigator durch das Aufsichtsrecht, https://www.fma.gv.at/querschnittsthemen/fintech/fintech-navigator/ (abgerufen am 29. September 2018).

Freitag, Die Blockchain- Technologie Nur ein Hype oder doch mehr?, Linde 2018, 59.

Gamon, Anfrage 382/J vom 01.03.2018 (XXVI.GP), https://www.parlament.gv.at/PAKT/VHG/XXVI/J/J_00383/imfname_683622.pdf, (Stand 1.3.2018).

Gamon, Anfrage 383/J vom 01.03.2018 (XXVI.GP), https://www.parlament.gv.at/PAKT/VHG/XXVI/J/J_00383/imfname_683622.pdf (abgerufen am 20. August 2018), (Stand 01.03.2018)

Gemalto, Know-Your-Customer-Verfahren und Anti-Geldwäsche-Richtlinie, https://www.gemalto.com/deutschland/financial/dienstleistungen-fur-banken/identitatsverifizierung/know-your-customer, (abgerufen am 3. September 2018).

Giese, Dash – Digitales Cash mit einigen Schmankerln, https://www.btc-echo.de/dash-digitales-cash-mit-einigen-schmankerln-20160410/ (abgerufen am 31. August 2018).

Hager, Die Tage der unregulierten Bitcoin- Nutzung sind gezählt, Der Standard (2016/44/1).

Hahn / Wons, Initial Coin Offering (ICO) - Unternehmensfinanzierung auf Basis der Blockchain-Technologie. Wiesbaden: Springer Gabler, 2018.

Hönig, Initial Coin Offering - Studie zu Kryptowährungen und der Blockchain-Technologie, https://www.frankfurt-university.de/fileadmin/standard/Hochschule/Fachbereich_3 /Kontakt/Professor_inn_en/Hoenig/20180502_Bitcoin_Studie_fra_uas_Hoenig_V1.0.pdf, (abgerufen am 04. September 2018).

IWF, Anti-Money Laundering/Combating the Financing of Terrorism - Topics https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm#moneylaundering (abgerufen am 13. Oktober 2018).

Kammler / Pohlmann, Bitcoin: Geldverkehr ohne Banken Kryptografie wird Währung, https://norbert-pohlmann.com/app/uploads/2015/08/308-Kryptografie-wird-W%C3%A4hrung-Bitcoin-Geldverkehr-ohne-Banken-Prof-Norbert-Pohlmann.pdf,(abgerufen am 31. August 2018).

Kappos/Yousaf/Maller/Meiklejohn, An Empirical Analysis of Anonymity in Zcash, https://smeiklej.com/files/usenix18.pdf, (abgerufen am 30. September 2018).

Kerscher, Handbuch der digitalen Währungen 1. Auflage. Dingolfing: Kemacon, 2014.

Klumpp, ICO – Initial Coin Offering, https://www.tech-corporatefinance.de/blog/uncategorized/ico-initial-coin-offering-ablauf-und-beratung/, (abgerufen am 06. September 2018).

Leistert, BITCOIN UND BLOCKCHAIN, https://scholar.googleusercontent.com/scholar?q=cache%3AZGJsgdhO_BcJ%3Ascholar.goog

le.com%2F%20tor%20netzwerk&hl=de&as_sdt=0%2C5&as_ylo=2014&as_vis=1, (abgerufen am 26. August 2018).

Maleczky, Strafrecht Allgemeiner Teil, 8. Aufl. : Österreich Lexis Nexis

Meisser, Kryptowährungen: Geschichte, Fuktionsweise, Potenzial https://www.mme.ch/fileadmin/files/documents/160520_luzius_meissner__bitcoin___crypto_currency_funktionsweise____entstehung_.pdf, (abgerufen am 14.07.2018).

Ministerium für Präsidiales und Finanzen, VERNEHMLASSUNGSBERICHT DER REGIERUNG BETREFFEND DIE SCHAFFUNG EINES GESETZES ÜBER AUF VERTRAUENSWÜRDIGEN TECHNOLOGIEN (VT) BERIHENDE TRANSAKTIONSSYSTEME (BLOCKCHAIN- GESETZ; VT- GESETZ ; VTG UND DIE ABÄNDERUNG WEITERER GESETZE), (abgerufen am 2. Oktober 2018).

Möser /Böhme / Breuker, An inquiry into money laundering tools in the Bitcoin ecosystem. https://ieeexplore.ieee.org/document/6805780, (abgerufen am 28. August 2018)

Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, (abgerufen am 21. August 2018).

Negin, Distributed Ledger Technologie (DLT) ist mehr als Blockchain, https://blockchainwelt.de/dlt-distributed-ledger-technologie-ist-mehr-als-blockchain/ (Stand 16.2.2018).

o.V., FMA warnt vor "Spekulationsobjekt" Kryptoasset, https://diepresse.com/home/wirtschaft/boerse/5488737/FMA-warnt-vor-Spekulationsobjekt-Kryptoasset (04. September 2018).

O.V. Standard Compliance Code der österreichischen Kreditwirtschaft, http://www.rlb-tirol.at/eBusiness/services/resources/media/136344902797510738-NA-241427574725518235-1-1-NA.pdf, (abgerufen am 26. August 2018).

o.V., What is Dash Cryptocurrency? A Crash Course, https://blockgeeks.com/guides/what-is-dash-cryptocurrency/ (abgerufen am 31. August 2018).

Paulmayer, Initial Coin Offerings (ICOs) und Initial Token Offerings (ITOs) als prospektpflichtiges Angebot nach KMG?, ZTR 2017.

Piska, Kryptowährungen und ihr Rechtscharakter - eine Suche im Bermuda- Dreieck ecolex 2017.

Piska / Völkel, Blockchain und Kryptorecht Regulierungs- Chancen de lege lata und de lege ferenda, ZTR 2017.

Piska/Völkel, Kryptowährungen reloaded- auf den Weg aus dem Bermuda-Dreieck[1] ecolex 2017.

Piska/Völkel, Kryptowährungen und AML – smart regulation in Sicht, ecolex 2018 671.
Völkel, Privatrechtliche Einordnung der Erzeugung virtueller Währungen, ecolex 2017, 639.

Völkel, Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017 103.;

Presse, Löger will Bitcoin „ mit Maß und Ziel“ regulieren, https://diepresse.com/home/wirtschaft/economist/5377604/Loeger-will-Bitcoin-mit-Mass-und-Ziel-regulieren, (abgerufen am 2. Oktober 2018).

Prinz, Monero ist eine Anonyme Kryptowährung, https://www.bitfantastic.com/kryptowaehrung/monero-ist-eine-anonyme-kryptowaehrung/2018/, (abgerufen am 5. September 2018).

Prinz, Vollständige Liste der Anonymen Kryptowährungen, https://www.bitfantastic.com/kryptowaehrung/vollstaendige-liste-der-anonymen-kryptowaehrungen/2018/,(abgerufen am 05. September 2018)

Youniqx Identity AG, MICK My Identity Check, https://www.myidcheck.at/#x-section-5, (abgerufen am 10. August 2018).

Read/Gräslund, Eu-Regulierung von Bitcoin und anderen virtuellen Währungen: erste Schritte, https://link.springer.com/article/10.1007/s10273-018-2323-6, (abgerufen am 01. Oktober 2018).

Republik Österreich Bundesministerium für Inneres Bundeskriminalamt, Geldwäschemeldestelle Verdachtsmeldung, http://www.bundeskriminalamt.at/308/files/Geldwaesche_Meldeformular_23072018.pdf, (abgerufen am 12. August 2018).

Republik Österreich Bundesministerium für Inneres Bundeskriminalamt, Informationsblatt, http://www.bundeskriminalamt.at/308/files/Geldwaeschemeldung_Info.pdf, (abgerufen am 12. August 2018).

Republik Österreich Bundesministerium für Inneres Bundeskriminalamt, Meldestellen, http://www.bundeskriminalamt.at/602/start.aspx, (abgerufen am 12. August 2018).

Satoshi Nakamoto (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, (abgerufen am 21. August 2018).

Schiller, Merkle Tree – Eine Basis der Blockchain, https://blockchainwelt.de/merkle-tree-basis-von-blockchain-und-hash-trees/ (abgerufen am 01. September 2018).

Schock, Virtuelle Währungen- Ein Blick über die Grenzen, ecolex 2017, 636.

Sieber / Vogel, Terrorismusfinanzierung – Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht, https://www.mpicc.de/files/pdf3/Band_S_150_Online-Version.pdf (70), (abgerufen am 13. Oktober 2018).

Standard Compliance Code der österreichischen Kreditwirtschaft (Stand 14.12.1999), http://www.rlb-tirol.at/eBusiness/services/resources/media/136344902797510738-NA-241427574725518235-1-1-NA.pdf, (abgerufen am 26. August 2018).

Takagi, Blockchain Economics, https://www.slideshare.net/SoichiroTakagi/blockchain-65500089, (abgerufen am 26. August 2018).

Tar, Proof-of-Work, Erklärt, https://de.cointelegraph.com/explained/proof-of-work-explained, (abgerufen am 08. September 2018).

Tokens 24, So tauschen sie Bitcoin offline aus, https://www.tokens24.com/de/cryptopedia/basics/so-tauschen-sie-bitcoin-offline-aus, (abgerufen am 3. September 2018).

Unternehmensservice, Geldwäsche, https://www.usp.gv.at/Portal.Node/usp/public?gentics.rs=PDF&gentics.pb=notvisibleposition&contentId=10007.50238, (abgerufen am 3. September 2018).

van Saberhagen, CryptoNote v 2.0, https://cryptonote.org/whitepaper.pdf (abgerufen am 30. August 2018)

Versicherungsverband Österreich, Standard Compliance Code der österreichischen Versicherungswirtschaft https://home.kpmg.com/content/dam/kpmg/at/pdf/Newsletter/insurance/download_VAG/4-c-vvo-standard-compliance-code-21092017%20.pdf, (Stand 21.9.2017).

Virtuelle Währungen Entschließung des Europäischen Parlaments vom 26. Mai 2016 zu virtuellen Währungen (2016/2007(INI)), 2018/C 076/13.

Weizsäcker, Bericht über virtuelle Währungen (2016/2007(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0168+0+DOC+PDF+V0//DE, (Stand 3.5.2016).

Wirtschaftskammer Österreich Fachverband Finanzdienstleister, Die Kryptowährung Exkurse: Bitcoins und Minings, https://www.wko.at/branchen/information-consulting/finanzdienstleister/artikel-kryptowaehrung.pdf, (abgerufen am 20. August 2018).

Wirtschaftskammer Österreich, Geldwäschebekämpfung und Wirtschaftliche Eigentümer-Register, https://www.wko.at/service/wirtschaftsrecht-gewerberecht/geldwaeschebekaempfung-wirtschaftliche-eigentuemer-register.html, (abgerufen am 20. August 2018).

Wimmer, Mit Shapeshift.io unkompliziert Kryptowährungen tauschen, https://www.crypto-magazin.com/shapeshift-io/, (abgerufen am 10 August 2018).

WKO, Die Kryptowährung Exkurse: Bitcoins und Mining https://www.wko.at/branchen/information-consulting/finanzdienstleister/artikel-kryptowaehrung.pdf, (Stand 07.02.2018).

Wright, The Difference Between AML and KYC, https://www.linkedin.com/pulse/difference-between-aml-kyc-malcolm-wright-finstlm (abgerufen am 3. September 2018).

Interviews

Andreas Pfeil *LL.M.* Interview geführt von Marina Kindel (4. Oktober 2018).

Dr. Arthur Stadler, Partner der Rechtsanwaltskanzlei Stadler Völkel, Interview geführt von Marina Kindel (24. Juli 2018).

Dr. Oliver Völkel, LL.M., Partner der Rechtsanwaltskanzlei Stadler Völkel, Interview geführt von Marina Kindel (11. September 2018).

Florian Wimmer, CEO, Co-Founder, Interview geführt von Marina Kindel (22. Juli 2018).

Ing. Johannes Grill, Präsident Bitcoin Austria, Interview geführt von Marina Kindel (3. August 2018).

Mag. Matthias Reder, Leiter der Compliance und AML Abteilung von Coinfinty, Interview geführt von Marina Kindel (3. August 2018).

Mag Patrick Schreiner, MSc, Bundeskriminalamt II/BK/KWK (Kompetenzzentrum Wirtschaftskriminalität) Interview geführt von Marina Kindel (28.September 2018).

Mag.Weratschnig Thomas, Prävention von Geldwäscherei und Terrorismusfinanzierung der Finanzmarktaufsicht, Interview geführt von Marina Kindel (22. August 2018).

MMag. Christopher Miess, BSc, Bakk.phil, BSc, MSc, CEO von ICONIC Capital sowie Mitglied des Fintech Advisory Board, Interview geführt von Marina Kindel (06. Oktober 2018).