Christian Steiner

Krypto-Assets und das Aufsichtsrecht

Security-, Payment- und Utility-Token und ihre aufsichtsrechtliche Einordnung

finanzverlag

Zitiervorschlag:

Langzitat: *Steiner*, Krypto-Assets und das Aufsichtsrecht (2019) Seite.
Kurzzitat: *Steiner*, Krypto-Assets Seite.

VLB – Verzeichnis Lieferbarer Bücher
Ein Titelsatz für diese Publikation ist bei dem VLB Verzeichnis Lieferbarer Bücher erhältlich.

In vergleichbarer Form auch vorgelegt als:
Master Thesis (MBA) an der WU Executive Academy.

Mag. Elisabeth Löffler-Tüchler
Uraniastraße 4
1010 Wien
loeffler@finanzverlag.at
www.finanzverlag.at

Lektorat, Satz und Umschlaggestaltung: finanzverlag
Herstellung: Druckerei Berger, 3580 Horn

Printed in Austria 2019

ISBN 978-3-9504370-5-8

ABRISS

Krypto-Assets und das Aufsichtsrecht

Security-, Payment und Utility-Token und ihre aufsichtsrechtliche Einordnung

Das vorliegende Fachbuch gibt einen detaillierten Überblick über die rechtliche Einordnung von Krypto-Assets an Hand der drei weitest verbreiteten Archetypen: Security-, Payment- und Utility-Token. Neben einer allgemeinen Darstellung der technischen Abläufe bei Krypto-Assets und einer Übersicht über die unterschiedlichen Meinungen der Aufsichtsbehörden werden die drei Archetypen umfangreich definiert und jeweils auf ihre rechtliche Einordnung untersucht. Ein starker Fokus des Buchs liegt auf dem Security-Token und den Rechtsfolgen bei Einordnung als Wertpapier. Aber auch die Rechtsfolgen von Payment- und Utility-Token sowie andere Formen von Token werden aufgearbeitet. Zudem wird jeweils ein Ausblick auf die weiteren Entwicklungen gewagt und Anhaltspunkte für eine angemessene Regulierung aufgezeigt. Im Ergebnis zeigt sich, dass Security-Token häufig als Wertpapier iSd PVO/WAG zu qualifizieren und daher eine Vielzahl von aufsichtsrechtlichen Vorgaben zu beachten sind. Payment- und Utility-Token sind dagegen idR als unreguliert zu betrachten.

ABSTRACT

Crypto-Asset and regulatory law

Security-, Payment and Utility-Token and their legal qualification

This book gives a detailed overview over the legal qualification of Crypto-Assets and their three common archetypes: Security-, Payment- and Utility-Token. Alongside the main technical characteristics and a summary of the interpretation of different supervisory authorities an in-depth analysis of the three archetypes is presented. The three archetypes are extensively defined and analysed in regard of their legal qualification. A strong focus of this book lies on the Security-Token and the legal consequences of its qualification. Also, the legal consequences for Payment- and Utility-Token and for other forms of Token are shown. Additionally, an outlook of potential future developments in this sector and potential aspects of future regulations are included. In conclusion Security-Token need to be qualified in most of the case as securities in the sense of MIFID II/Prospectus Regulation, which triggers many different financial markets regulations. Payment- and Utility-Token are – as a rule of thumb – not regulated under financial market laws.

AUTOR

Dr. Christian Steiner, BSc MBA

war jahrelang in der österreichischen Finanzmarktaufsicht im Bereich Wertpapierrecht tätig und hat sich schon dort tiefgehend mit Krypto-Assets und ihrer rechtlichen Einordnung beschäftigt. Zudem wurde er als Vertreter der FMA in den Fintech-Beirat beim BMF zu den Themen ICOs/Krypto-Assets entsendet.

Mittlerweile ist Christian Steiner Head of Regulatory bei Bitpanda – einer der europaweit führenden Handelsplattformen für Krypto-Assets sowie Head of Compliance in der PSD II-regulierten Tochter Bitpanda Payments.

VORWORT DES AUTORS

Dieses Fachbuch ist geprägt von Fragen aus meiner beruflichen Praxis. Zuerst in der FMA und jetzt auch bei der Bitpanda GmbH, einer der führenden Krypto-Asset-Handelsplattformen in Europa, wurde mir bewusst, dass die Einordnung von Krypto-Assets in bestehendes Aufsichtsrecht viele Fragen offen lässt und bei weitem nicht geklärt ist. Im Zuge des Fintech-Beirats beim Bundesministerium für Finanzen, Untergruppe ICO, in welche ich damals als Vertreter der FMA entsendet wurde, wurde deutlich, dass auch die Praxis und insbesondere die Wirtschaft mit diesen Einordnungen zu kämpfen hat. Zudem wurde mir bewusst, wie stark das Rechtsverständnis divergiert – sowohl innerhalb der EU als auch global. Dies wurde durch die jüngsten ESMA-Veröffentlichungen (ESMA, Advice on Crypto-Assets, Annex) in aller Deutlichkeit veranschaulicht. Gleichzeitig besteht aber mE großes Potential für Innovation durch Krypto-Assets, insbesondere am Kapital-/Wertpapiermarkt. Die Digitalisierung ist in diesem Bereich noch nicht soweit fortgeschritten, wie es mE sinnvoll und wünschenswert erscheint. Gleichzeitig hindert aber die Rechtsunsicherheit in Zusammenhang mit Krypto-Assets Fortschritt, Innovation und teilweise auch die dahinterstehenden Geschäftsmodelle.

All diese Fragen haben mich schon während des MBA an der WU Executive Academy maßgeblich beschäftigt. Im Austausch mit Lehrenden, aber auch mit Studierenden sowie insbesondere auch mit Mitgliedern aus dem Fintech-Beirat hat sich schnell gezeigt, dass dieses Thema für meine Masterarbeit das Richtige ist. Ich bedanke mich daher bei der WU für die Flexibilität, dass ich dieses Thema wählen konnte und für die tolle Organisation des MBA sowie den reibungslosen Ablauf und die Unterstützung bei allen Schritten, insbesondere bei der Abgabe der Masterarbeit.

Besonderer Dank gilt aber Frau Prof. Kalss, welche immer für Besprechungen zur Verfügung gestanden ist, auch kurzfristig, und mich mit wertvollen Tipps und fachlichem Austausch unterstützt hat. Dieser Dank gilt insbesondere für ihren Einsatz, auch vor dem Hintergrund der Länge der Arbeit. Aus allen Besprechungen konnte ich wertvolle Hinweise und Diskussionspunkte mitnehmen, welche in der Arbeit vertieft und aufgearbeitet wurden. Gleichzeit hat Frau Prof. Kalss mir aber immer vollinhaltlich meine akademische Freiheit gelassen und mir so ermöglicht, nicht nur meine eigenen Schwerpunkte zu setzen, sondern diese auch jeweils umfassend und mit der aus meiner Sicht gebotenen Tiefe aufzuarbeiten.

Die Länge der Arbeit steht auch mit dieser Publikation als Fachbuch beim Finanzverlag in Verbindung. Die Möglichkeit zur Publikation der Masterarbeit in Buchform hat mich zur umfangreichen Aufarbeitung motiviert und ließ mich immer die Extra-Meile gehen. Besonderer Dank geht daher an den Finanzverlag, einerseits für die Möglichkeit zur Publikation dieses Buchs und andererseits für die hervorragende Zusammenarbeit. Auf Grund der Relevanz des Themas für den Finanzmarkt war mir eine Publikation der Masterarbeit als Fachbuch sehr wichtig und es freut mich sehr mit dem Finanzverlag einen idealen Partner dafür gefunden zu haben. Hervorzuheben ist in diesem Zusammenhang der Einsatz von Frau Mag. Löffler-Tüchler und Frau Dr. Buschek-Haunschmidt, welche die vielen Schritte zum Erscheinen dieses Buches perfekt gemeistert und mich entsprechend angeleitet haben.

Weiterer Dank geht an meinen Arbeitgeber Bitpanda für den umfassenden Austausch und die vielen Diskussionen zum Aufsichtsrecht im Allgemeinen sowie teilweise zu Auslegungen in dieser Arbeit bzw zum technischen Verständnis. Besonders auf technischer Ebene war ich für den Input sehr dankbar.

Zusätzlicher Dank ergeht natürlich auch an die FMA, wo ich die grundlegenden Kenntnisse für diese Arbeit erworben habe. Ohne meine berufliche Erfahrung in der FMA wäre ich nicht wo ich bin und auch das Interesse um das Feld der Krypto-Assets wäre womöglich nicht geweckt worden. Besonderer Dank gilt diesbezüglich meiner früheren Chefin, Frau Mag. Susanne Reder, MA, welche mich immer besonders unterstützt und gefördert hat. Ebenso gilt mein besonderer Dank auch meinem Doktorvater ao. Univ.-Prof. Mag. Dr. Raimund Pittl, der mich mit der akademischen Welt vertraut gemacht und meine diesbezügliche Entwicklung maßgeblich geprägt hat. Seine Schmiede in fast 4 Jahren als Studienassistent sowie die Vertiefung im Rahmen der Dissertation haben meine juristischen und wissenschaftlichen Kenntnisse deutlich geprägt und hat damit maßgeblich zum Gelingen dieser Arbeit beigetragen.

Dank gilt aber auch meiner Familie und Freunden sowie Kollegen, welche mich in vielfältiger Weise unterstützt haben. Besonderer Dank ergeht in diesem Zusammenhang an meine Freundin Anna, welche immer Verständnis für die notwendigen Extra-Stunden hatte und mich in vielerlei Form unterstützt hat, insbesondere auch bei der Korrektur dieser Arbeit.

Da die Masterarbeit im Laufe des Juli 2019 abgegeben wurde und zu starke Diskrepranzen zwischen der Masterarbeit und der ersten Auflage dieses Buches vermieden werden sollen, wurden nur notwendige Ausbesserungen vorgenommen. Eine neue Auflage wird wohl auf Grund der Dynamik des Rechtsgebiets innerhalb von wenigen Jahren geboten erscheinen.

Wien, im Oktober 2019 *Christian Steiner*

Hinweis: Die durchgehend männlichen Bezeichnungen dienen allein der sprachlichen Vereinfachung und erfassen selbstverständlich stets auch die jeweiligen weiblichen Bezeichnungen.

2 Krypto-Assets – Begriffe, Überblick und Meilensteine

2.1 Begriffsbestimmungen, Systematik und Definitionen

Schon der Grundbegriff „Krypto-Asset" bietet definitionstechnisch einige Herausforderungen. So ist etwa nicht allgemein anerkannt, was als Krypto-Asset gilt und was nicht.[27] Die meisten Definitionen starten mit den Rahmenbedingungen des ersten – und auch heute noch wichtigsten – Krypto-Assets; dem Bitcoin.[28] Allgemein anerkannt ist, das Krypto-Assets, teilweise auch als virtuelle oder Krypto-Währungen bezeichnet (siehe sogleich), – wie aus dem Namen bereits ersichtlich – mit Kryptographie, zu Deutsch Verschlüsselung, in Verbindung stehen. [29] Dies steht mit dem Gedanken der Dezentralität des Systems in Verbindung – klassische Krypto-Assets weisen einen stark dezentralen Ansatz auf und sind durch das Fehlen von Intermediären gekennzeichnet. Es existiert kein zentraler Server, wo alle Daten gespeichert sind, wie dies etwa bei klassischen Unternehmen der Fall ist. Vielmehr sind die Daten auf alle Mitglieder des Systems (sogenannte *Nodes*)[30] verteilt. Man spricht in diesem Zusammenhang von *Distributed Ledger*.[31] Darunter versteht man vereinfach gesagt, dass sämtliche Daten auf jedem teilnehmenden Node gesichert werden und eben nicht zentral auf einem Server. Genau diese technische Eigenschaft macht eine Verschlüsselung unabdingbar, da sonst jeder im System auf alle Datenpunkte Zugriff hätte. Die Verschlüsselung, genauer gesagt die Kombination aus privatem und öffentlichem Schlüssel, stellt sicher, dass nur derjenige auf seine Krypto-Assets zugreifen kann, der über die Kombination aus beidem verfügt. Die Kryptografie ist somit ein unverzichtbares Sicherheitselement von Krypto-Assets und nicht, wie oft angeführt wird, der Zweck des Systems, etwa um Geldströme zu anonymisieren. Durch den öffentlichen und den privaten Schlüssel wird der Besitz der Krypto-Assets nachgewiesen. Auf Grund des Fehlens einer zentralen Kontrollstelle ist jedoch auch das sogenannte „Double Spending"-Problem zu lösen, das darin besteht, dass keine zentrale Kontrolle der Transaktionen vorliegt und ein Besitzer somit uU zeitgleich zwei Transaktionen ausführen könnte, eine davon ohne das Geld zu besitzen (näher dazu siehe Kapitel 2.2). Aus diesem Grund hat schon *Nakamoto*[32] eine Kontrolle durch das Netzwerk vorgesehen – sogenannte Miner überprüfen die Richtigkeit der Transaktionen.[33] Mining kann – wiederum vereinfacht – als dezentrales Prüfnetzwerk der Transaktionen verstanden werden.[34] Die einzelnen Transaktionen werden jeweils in einen Block gesammelt, die Blöcke werden aneinander gereiht und die jeweils vorherigen Blöcke werden dabei mitgeprüft.[35] Man spricht dabei von der soge-

27 *Wyman*, Cryptocurrencies and public policy (2018), https://www.oliverwyman.com/our-expertise/insights/2018/feb/cryptocurrencies-and-public-policy.html.

28 Siehe dazu Kapitel 2.2 sowie *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf.

29 Eine recht eingängliche Zusammenfassung der verbundenen kryptographischen Methoden findet sich etwa unter *Bitcoin Blog*, Kryptografie des Bitcoins für Anfänger, https://bitcoinblog.de/2013/12/22/kryptografie-des-bitcoins-fuer-anfaenger/.

30 Siehe dazu etwa *Bitcoin Core*, Running a full node, https://bitcoin.org/en/full-node#minimum-requirements.

31 Zu diesem Begriff siehe *Coindesk*, What is a distributed ledger, https://www.coindesk.com/information/what-is-a-distributed-ledger.

32 *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system, aaO, 3f.

33 Im Fall von Bitcoin erfolgt dies mittels sogenanntem Proof-of-Work, näher dazu sowie zu alledem vorher genannten siehe Kapitel 2.2.

34 *BTC Echo*, Wie funktioniert Bitcoin Mining, https://www.btc-echo.de/tutorial/wie-kann-ich-bitcoins-minen/.

35 Auch dazu siehe *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system, aaO; dies ist für die Sicherheit des Systems eine wesentliche Komponente, da jeder weiterer Block die Chance sowie den Aufwand für einen Hacking-Angriff drastisch erhöht (siehe etwa die Kalkulation bei Nakamoto, aaO, S. 7f).

nannten „Blockchain", einer Art Datenbank, welche dezentral gespeichert wird und auf Grund dieser Dezentralität unveränderbar ist.[36] All dies sind wesentliche Elemente eines Krypto-Assets, wobei jedoch nicht geklärt ist, welche Aspekte in welcher Stärke vorliegen müssen oder ob es Ausschlusskriterien gibt. Generell ist die Krypto-Welt vom weitgehenden Fehlen von Standards und anerkannten Begriffen geprägt. Manche Definitionen haben eher auf die Verwendungszwecke abgezielt und greifen mE seit der Welle an mittels ICO hinzugekommen Möglichkeiten zu kurz.[37] Eine weitgehend unumstrittene und mE gelungene Definition (vom Begriff „Währung" abgesehen, siehe dazu sogleich) findet sich in der 5. Geldwäsche-Richtlinie: [38]

> *„virtuelle Währungen" eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist und die nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann;*

Früher wurden Krypto-Assets häufig als Kryptowährungen oder auch als virtuelle Währungen bezeichnet – diese Bezeichnung ist auch heute teilweise noch verbreitet. Da es sich jedoch nicht um eine „Währung" handelt, wurde dieser Begriff allgemein kritisiert und als irreführend bezeichnet.[39] Richtigerweise handelt es sich nicht um ein gesetzliches Zahlungsmittel, welches bekanntlich nur von der OeNB/EZB ausgegeben werden kann.[40] Allerdings spricht der EuGH – in seiner bisher einzigen Rechtsprechung zu Bitcoin – sehr deutlich von einer Währung[41] und auch die einzige europarechtliche Definition spricht von „virtuellen Währungen".[42] Unabhängig von dieser europäischen Ebene hat sich aber in letzter Zeit vermehrt der Überbegriff Krypto-Assets durchgesetzt.[43] Dies erscheint vor dem Hintergrund der Vielzahl an verschiedenen Ausgestaltungen, welche insb durch die ICOs in den Jahren 2017 und 2018 erfolgten (über 2.000)[44] der passendere Begriff. Auch in der „Krypto-Szene" wird das Verständnis geteilt, dass all diese Token nicht als Währungen zu bezeichnen sind, was teilweise zur Unterscheidung in „Kryptowährungen" und Token geführt hat, mittlerweile allerdings weitgehend zur Adaption des Grundbegriffs auf „Krypto-Assets". Dies spiegelt mE auch eine funktionelle Perspektive wider; während Bitcoin 2008 tatsächlich als Zahlungsmittel vorgesehen war, hat sich mittlerweile der Asset-Gedanke mehr durchgesetzt – Krypto-Assets werden faktisch deutlich vermehrt als Wertanlage an

36 Für die wichtigsten Aspekte siehe *Futurezone*, Was ist eigentlich diese Blockchain, https://futurezone.at/digital-life/was-ist-eigentlich-diese-blockchain/270.616.934.

37 Vgl etwa die Definition der *Bank for International Settlements*, Digital Currencies (2015), https://www.bis.org/cpmi/publ/d137.htm. So wird dort etwa – neben virtuell und Peer-to-Peer – angeführt, dass es keine haftende Person geben darf, was schon bei Ethereum mE fragwürdig erscheint.

38 Artikel 1 Abs 2 lit d Z 18 der 5. EU-Geldwäscherichtlinie (RL/2018/843).

39 Etwa *Dobrowolski*, Überblick über die unterschiedlichen aufsichtsrechtlichen Rahmenbedingungen für Initial Coin Offerings, Der Gesellschafter, 3/2018, 147; kritisch auch *OENB*, Sind virtuelle Währungen wie Bitcoin eine Alternative zu klassischen Währungen wie dem Euro?, https://www.oenb.at/FAQ/sonstiges.html.

40 Vgl § 61 NBG.

41 EuGH, 22.10.2015, C-264/14 (Hedqvist).

42 Siehe Artikel 1 Abs 2 lit d Z 18 der 5. EU-Geldwäscherichtlinie (RL/2018/843).

43 So auch *FMA*, Was ist ein ICO?, aaO.

44 Vgl *ICO Data*, Statistik zu ICOs 2017/2018https://www.icodata.io/stats/2017 sowie https://www.icodata.io/stats/2018.

Stelle von Zahlungsmittel angesehen. Außerdem umfasst der Begriff Asset auch Zahlungsmittel[45] und kann gerade deshalb als Überbegriff herangezogen werden.[46]

Auf die zwei bisher wesentlichsten Krypto-Assets (*Bitcoin* und *Ethereum*) wird in den nächsten Kapiteln näher eingegangen, da diese gleichzeitig auch wesentliche Meilensteine in der „Krypto-Asset-Welt" darstellen und mE auch die künftige Entwicklung in diesem Bereich maßgeblich prägen werden. So hat bspw die Entwicklung des Bitcoins die gesamte Entwicklung von Krypto-Assets erst angestoßen. Selbiges gilt für Ethereum in Bezug auf Initial Coin Offerings. Ohne die Möglichkeit der Programmierbarkeit[47] einer Blockchain wären diese schlicht nicht möglich gewesen.

Eine zentrale Rolle in dieser Arbeit wird der Begriff „Initial Coin offering" *(ICO)* innehaben. Der Begriff wurde in Anlehnung an den englischen Begriff für einen Börsegang – Initial Public Offering (IPO) – gewählt.[48] Mit Hilfe von „Smart Contracts", einem Programmcode, welcher vereinbarte Verpflichtungen vollautomatisch abwickelt, wenn gewisse Faktoren („Trigger") erfüllt sind,[49] werden bestehende Krypto-Assets als Finanzierung eingesammelt und neue Token ausgegeben.[50] Die neuen Token stehen idR in Verbindung mit einem konkreten Unternehmen oder Projekt – die Einsatzmöglichkeiten von solchen Token sind grundsätzlich unbeschränkt. Zu Recht weisen Aufsichtsbehörden in aller Regel darauf hin, dass die Token unterschiedlich ausgestaltet sind und deshalb keine allgemeine Einordnung erfolgen kann, sondern vielmehr eine Prüfung im Einzelfall geboten ist.[51] Technisch werden ICO idR auf der Ethereum-Blockchain durchgeführt (zB ERC-20 Token).[52] Wie bereits einleitend erwähnt wurde, werden diese mittels ICO neu geschaffenen Token oft unter dem Begriff „Altcoins" zusammengefasst.[53]

Daraus ist auch erkenntlich, dass keine allgemein gültige Abgrenzung der Begriffe Coin und Token erfolgt. So wird etwa in einem Initial *Coin* Offering idR ein *Token* begeben, welcher dann wiederum (zumindest teilweise) als Alt*coin* bezeichnet wird. Genauer gesagt existiert zwar eine trennscharfe Abgrenzung, diese wird aber im Sprachgebrauch nicht präzise übernommen. Vielmehr werden die Begriffe oft als Synonyme verwendet.[54] Während ein Coin eine eigene Blockchain aufweist, basieren Token auf einer bereits existierenden Blockchain.[55] Im weiteren Verlauf dieser Arbeit soll diese Abgrenzung zwar grds Beachtung finden, wo jedoch gängige Begriffe – wie etwa ICO – bestehen, werden diese herangezogen.

45 Asset wird idR allgemein mit Vermögenswert übersetzt und umfasst somit alle Formen von Kapitalanlagen, unter anderem eben auch Geld/Devisen, etwa *Gründerszene*, Lexikon zum Begriff Asset, https://www.gruenderszene.de/lexikon/begriffe/asset?interstitial_click.

46 Ausdrücklich auch so *FMA*, Was ist ein ICO? aaO.

47 Siehe dazu *Buterin*, aaO, 1.

48 Für viele *Creative Construction*, ICO statt IPO, https://www.creativeconstruction.de/blog/ico-statt-ipo-wie-das-blockchain-basierte-finanzierungsmodell-die-startup-welt-auf-den-kopf-stellt/.

49 Ausführlich zu Smart Contracts vgl etwa *Szabo*, Formalizing and securing relationsships on public networks, https://ojphi.org/ojs/index.php/fm/article/view/548/469; *Christidis et al*, Blockchains and Smart Contracts for the Internet of Things, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408.

50 Vgl auch *FMA*, Was ist ein ICO? aaO.

51 Für viele *FMA*, Was ist ein ICO? aaO.

52 Näher zu diesem Begriff BTC Echo,Was ist ein ERC-20-Token?, https://www.btc-echo.de/tutorial/was-ist-ein-erc-20-token/. Ausführlich vgl *Github*, OpenSource zu ERC-20-Standard, https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md.

53 So etwa *Investopedia*, Definition – Altcoin, https://www.investopedia.com/terms/a/altcoin.asp. Der Begriff wird aber auch unterschiedlich verwendet, siehe etwa *Blockchainwelt*, Was sind Altcoins?, https://blockchainwelt.de/altcoin-definition-und-uebersicht/.

54 Explizit so *FMA*, Was ist ein ICO? aaO.

55 Für viele *Cointrend*, Was sind Token und worin besteht der Unterschied zu Coins?, https://cointrend.de/kryptowiki/token/.

2.2 Bitcoin – Startpunkt der Krypto-Assets

Bitcoin wurde 2008 von Satoshi Nakamoto – ein Pseudonym[56] – erstmals in einem Whitepaper beschrieben.[57] Am 03.01.2009 ging das Bitcoin-Netzwerk erstmals online; Nakamoto erzeugte (mittels „mining") den ersten Block[58].[59] Schon vor Bitcoin wurden mehrfache Versuche durchgeführt, digitales Geld zu erzeugen.[60] In den Medien ist Bitcoin zu Beginn lediglich aus zwei Perspektiven näher behandelt worden, einerseits als Phänomen einer Finanzblase und andererseits als Zahlungsmittel für illegale Aktivitäten (zB im „Darknet"). Erst später wurde die dahinterstehende Technologie („Blockchain", siehe Kapitel 2.1) sowie die Innovation verbunden mit Krypto-Assets näher beleuchtet.[61] Die Geschichte des Bitcoin ist geprägt von extremen Preisschwankungen, sowohl nach oben („Bullrun"/"to the moon") als auch nach unten.[62] Die starke Volatilität von Krypto-Assets im Allgemeinen und von Bitcoin im Speziellen ist sonst auf Finanzmärkten idR nicht zu beobachten. Den bisherigen Höchsttand erreichte Bitcoin am 17.12.2017 mit einem Wert von fast 20.000 US-Dollar; bis 2017 lag der Preis – von minimalen Ausreißern abgesehen – bei ca 1.000 US-Dollar.[63] Dies bedeutete zB eine Preissteigerung von fast 4.000 % im Jahr 2017 und einen Preisverlust von mehr als 70 % im Jahr 2018, was die extreme Volatilität deutlich unterstreicht. Die Bewegungen im Marktpreis sind insbesondere auf regulatorische und steuerrechtliche Einstufungen sowie auf Diebstähle, Hacking-Angriffe und auf das Schließen von Krpyto-Exchanges zurückzuführen[64] – all diese Aspekte beeinflussen auch heute noch den Kurs.

Der mE spannendste Aspekt am Bitcoin ist die Verknüpfung mehrerer Fachgebiete, um eine neue und innovative Möglichkeit für Zahlungsvorgänge zu schaffen. Aus der heutigen ex-post Sicht erscheint die visionäre Idee von Nakamoto, welche wohl auch die Wissenschaft sowie die Finanzpraxis erst später in vollem Maße geschätzt haben, im Jahr 2008 mE bahnbrechend. Durch die interdisziplinäre Verknüpfung von Kryptografie, ökonomischen Anreizen und Informatik wurden die Grundparameter für ein Peer-to-Peer basiertes, globales Zahlungsnetzwerk geschaffen.[65] Der Gedanke der Dezentralität lässt sich zwar bereits auf die Französische Revolution (18. Jahrhundert) zurückführen, ist jedoch mE erst in den letzten Jahren in weiten Teilen der Gesellschaft angekommen, wobei sicherlich die Nachwirkungen der Finanzkrise diese Entwicklungen verstärkt hat.[66] Dies, verbundenen mit einer verstärkten Ablehnung des Staates und politischer sowie wirtschaftlicher Institutionen, hat die Entwicklung von Krypto-Assets geprägt. Andererseits war die Innovationskraft am Finanzmarkt in den letzten Jahrzehnten auch eher gehmäßigt – während mittlerweile Nachrichten in Bruchteilen einer Sekunde weltweit versendet werden können, hat

56 Bis heute ist nicht bekannt wer bzw welche Gruppe hinter diesem Namen verborgen ist. Die Identität ist ein stark diskutiertes Thema in der Szene – es gibt zahlreiche Vermutung: für eine Übersicht *Wikipedia*, Satoshi Nakamoto https://en.wikipedia.org/wiki/Satoshi_Nakamoto.

57 *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf.

58 Siehe dazu die öffentlich abrufbare Blockain, Block 0: https://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

59 Näher dazu *Wallace*, The rise and fall of Bitcoin, https://www.wired.com/2011/11/mf-bitcoin/.

60 Für eine Übersicht siehe *Tschorsch/Scheuermann*, Bitcoin and beyond: A technical Survey on Decentralised Digital Currencies, https://eprint.iacr.org/2015/464.pdf.

61 Etwa *Sinegal* (2018). Blockchain: Die disruptive Macht der Dezentralisierung, http://www.morningstar.at/at/news/168301/blockchain-die-disruptive-macht-der-dezentralisierung.aspx/.

62 Siehe den Chart bei *Coinmarketcap*, Bitcoin Chart https://coinmarketcap.com/currencies/bitcoin/.

63 Vgl die Übersicht unter *Wikipedia*, Geschichte des Bitcoin, https://en.wikipedia.org/wiki/History_of_bitcoin.

64 Dazu *Chohan*, A history of Bitcoin (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875.

65 So auch *Berentsen/Schär*, Bitcoin, Blockhain und Kryptoassets (2017).

66 Näher zu Dezentralität, einem historischen Abriss sowie diverse Perspektiven: *Wikipedia*, Dezentralität, https://en.wikipedia.org/wiki/Decentralization.

sich der Zahlungsverkehr nicht im selben Ausmaß beschleunigt. Selbst heute noch werden „sofort"-[67] oder „Peer-to-Peer" [68]-Transaktionen im Finanzmarkt als großer Innovationsschritt angesehen, obwohl dies Bitcoin bereits vor über 10 Jahren ermöglicht hat.

Dies vorausgeschickt werden in weiterer Folge die wesentlichsten Charakteristika des Bitcoins beschrieben, was stellvertretend auch für die meisten anderen Krypto-Assets gilt. Die Dezentralität wurde bereits oben einleitend erwähnt, soll jedoch im Folgenden näher erläutert werden. Bitcoins werden von keiner zentralen Stelle ausgeben, es fungiert keine juristische Person als Emittent – viel mehr „erzeugt" ein digitales Open-Source[69]-Programm als Belohnung für die Lösung einer Rechenaufgabe Bitcoin und schüttet diese aus. Dies stellt die Incentives für die Ausführungen von Kontrolltätigkeiten im Bitcoin-Netzwerk („Mining") dar; die Ausschüttungen halbieren sich alle 210.000 Blöcke (entspricht etwa alle vier Jahren). Zu Beginn wurden 50 Bitcoins für einen erfolgreich geprüften Block ausgeschüttet, mittlerweile beträgt der „Mining-Reward" 12,5 Bitcoins und reduziert sich 2020 auf 6,125 Bitcoins. Dies erklärt auch den Hintergrund, warum oft von Deflation (= Preissteigerung) im Bitcoin-Netzwerk gesprochen wird. Die maximale Anzahl der Bitcoins liegt bei 21 Millionen; eine Änderung kann nur in demokratischer Form durch Mehrheit der Rechenleistung („Fork") erzielt werden, da niemand das Bitcoin-Netzwerk besitzt oder steuern kann. Das „Minen" (von „mining") dient somit gleich zwei Funktionen im Bitcoin-Netzwerk: einerseits der Schöpfung neuer Werteinheiten und somit der Erhöhung der Geldmenge und andererseits der Kontrolle der Transaktionen, da gerade keine zentrale Instanz die Transaktionen kontrolliert, verwaltet oder beeinflussen kann. Dies unterscheidet das Bitcoin-Netzwerk wesentlich vom sonstigen Finanzmarkt; eine Banküberweisung wird immer zentral von einer Bank gesteuert und verwaltet. Die Zahlung/Übertragung erfolgt somit direkt zwischen den Usern (echtes „Peer-to-Peer"-Netzwerk). Sämtliche Transaktionen werden in einem öffentlichen Verzeichnis aufgezeichnet („Blockchain") – diese Blockchain liegt – wie bereits in Kapitel 2.1 erläutert – nicht zentral auf einem Server, sondern auf jedem am System teilnehmenden Computer.[70] Die Bitcoins werden von Usern selbst – durch die Verwahrung des privaten Schlüssels – gehalten und zwar in Form sogenannter elektronischer Geldbörsen („Wallet"). Daraus resultiert auch die Pseudonymität[71] des Bitcoin-Netzwerks – die Walletadressen sind keiner Person zuordenbar. Dies versucht die 5. Geldwäsche-Richtlinie im Kern zu ändern,[72] wobei die Vorschriften jedenfalls zu kurz greifen, da nur ein kleiner Teil der Wallet-Anbieter zur Identifizierung verpflichtet ist.[73] Jede Verfügung über die dort befindlichen Bitcoins benötigt eine Freigabe durch den Private Key, was – im Gegensatz zum bisherigen Finanzsystem – einen Zugriff Dritter verunmöglicht. Ein Beispiel soll dies veranschaulichen: Ein Gericht stellt fest, dass 10 Bitcoins gestohlen wurden. Man findet den Dieb, das Geld befindet sich noch auf „seinem"

67 Siehe etwa das Projekt TIPS der EZB, welches im November 2018 gestartet ist: ECB, What is TARGET Instan Payment Settlement (TIPS)?, https://www.ecb.europa.eu/paym/target/tips/html/index.en.html.

68 Dies erfolgt auch nicht wirklich Peer-to-peer, sondern immer via zentrale Bankschnittstellen; dem User wird im Frontend aber eine leichte Versendbarkeit, etwa via Telefonnummer, ermöglicht. Rein technisch handelt es sich jedoch um eine zur Telefonnummer hinterlegten IBAN und eine übliche Banktransaktion. Siehe etwa *Zoin*, Was ist Zoin?, https://www.zoin.at/was-ist-zoin/.

69 Somit von jedermann einsehbares und nach gemeinsamen Regeln abänderbares System.

70 Die Datenmenge beträgt derzeit (April 2019) circa 220 Gigabyte: *Statista*, Size of Bitcoin Blockchain https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/.

71 Oft wird fehlerhaft von Anonymität des Bitcoin-Netzwerks geschrieben. Da allerdings sobald die Identifikation/Verknüpfung der Wallet mit der Person einmalig erfolgt ist sämtliche Transaktionen zugeordnet werden können liegt Pseudonymität vor.

72 Für eine Übersicht über die wesentlichsten Änderungen siehe *PFR Rechtsanwälte*, Wichtigste Punkte der 5. Geldwäscherichtlinie, https://www.pfr.at/de/news-medien/news/176-5-geldwaescherichtlinie.

73 So auch im Ergebnis *EBA*, Report with advice for the European Commission on Crypto-Assets, 09.01.2019, https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf, 20ff.

Wallet – die einzige Möglichkeit, das Geld zurückzuerhalten ist die Herausgabe des privaten Schlüssels; keine zentrale Instanz kann das Konto sperren oder eine Rückbuchung durchführen. Am „klassischen" Finanzmarkt würde die Bank auf gerichtliche Anordnung eine Sperre sowie später eine Rückbuchung durchführen. Dies führt teilweise dazu, dass Polizeibehörden zwar wissen wo sich das „Geld" befindet, jedoch nicht darauf zugreifen können.[74] Noch deutlicher wird diese Besonderheit im Fall des Verlustes des privaten Schlüssels – die Bitcoins auf dieser Wallet sind gänzlich verloren und können nicht mehr „wiederhergestellt"/gerettet/verwendet werden.[75] Damit geht auch einher, dass eine getätigte und durchgeführte Transaktion von niemandem (außer dem Empfänger im Sinne einer Rücküberweisung) zurückgesetzt werden kann. All diese technischen Punkte weisen somit auch eine deutlich kritische Komponente auf. Auch die faktische Verwendung von Krypto-Assets und im speziellen Bitcoin für illegale Zahlungen,[76] welche auf Grund der Pseudonimität ermöglicht wird, ist kritisch hervorzuheben. Weiters sind auch technische Aspekte der Blockchain-Technologie mit massiven Herausforderungen verbunden.[77] Zu nennen ist insbesondere die Skalierbarkeit – während das Bitcoin-Netzwerk nur ca 7 Transaktionen pro Minute absolvieren kann, kann etwa das Mastercard-Netzwerk 24.000 verarbeiten.[78] An der Lösung dieser Herausforderung wird jedoch schon länger gearbeitet.[79] Aber auch der extreme Energieverbrauch – das Bitcoin-Netzwerk verbraucht mittlerweile 3,5 Promille des Welt-Stromverbrauchs und weist somit einen höheren Stromverbrauch pro Jahr auf als geschätzt 175 Länder weltweit[80] – ist kritisch zu nennen. Hier versuchen andere Krypto-Assets neue Wege auszuloten[81]

Regulatorisch wurde in den meisten Ländern in Europa[82] sowie – nach umfassender Diskussion – auch in den USA[83] anerkannt, dass keine finanzmarktrechtlichen Vorschriften auf den Bitcoin anwendbar sind. Wie die FMA aber zutreffend klarstellt, bedeutet dies nicht

74 Siehe etwa zur sogenannten WannaCry (Ransomware) *Quartz*, The hackers behind the WannaCry ransomware attack have finally cashed out, https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/.

75 Schätzungen gehen von über einem Drittel aller Bitcoins aus, *Ethereumworldnews*, 36% of BTC in Circulation is Lost, https://ethereumworldnews.com/36-of-btc-in-circulation-is-lost-making-bitcoin-technically-more-scarce/. Der Verlust des privaten Schlüssels kann in vielen Situationen erfolgen – etwa wurde eine alte Festplatte, auf der sich der private Schlüssel befand, verworfen: *Welt*, 32jähriger wirft versehentlich 94 Millionen auf den Müll, https://www.welt.de/wirtschaft/article171372723/32-Jaehriger-wirft-versehentlich-94-Millionen-Euro-auf-den-Muell.html oder im Rahmen eines Todesfall der Private-Key nicht übergeben: *DerStandard*, Krypto Millionär verstorben – Familie sucht Private Keys, https://derstandard.at/ 2000080919325/Krypto-Millionaer-verstorben-Familie-sucht-nach-Private-Keys-fuer-Vermoegen.

76 So etwa *DerStandard,* Bitcoin boomt als Zahlungsmittel im Darknet, https://derstandard.at/2000096604599/Bitcoin-boomt-als-Zahlungsmittel-im-Darknet?ref=rec.

77 Ausführlich zu diversen Herausforderungen: *Bank for international settlement* (2018), Looking beyond the hipe, https://www.bis.org/publ/arpdf/ar2018_5_de.pdf.

78 Siehe etwa *BTC Echo*, Bitcoin vs Mastercard/Visa Transaktionsvolumen, https://www.btc-echo.de/bitcoin-vs-mastercard-visa-transaktionsvolumen/.

79 Sei es in Änderungen an der Blockchain, etwa bei anderen Krypto-Assets (siehe etwa Blockchain-Hero, 17-000 Transaktionen pro Sekunde, https://blockchain-hero.com/17-000-transaktionen-pro-sekunde/) oder durch zusätzliche Innovationen/technische Maßnahmen, etwa durch mehr Transaktionen pro Block oder off-chain-transaktionen (siehe etwa das Lightnings-Network oder allgemein die Diskussion zu diesem Thema, zB *Blocklab*, Diskussion um Skalierung, https://site.blocklab.de/2017/Skalierung/).

80 Für Details: *Powercompare*, Countries that consume more or less electricity than Bitcoin Mining in Late 2018, https://powercompare.co.uk/bitcoin-mining-electricity-map/.

81 Zu nennen sind etwa Proof of Stake/Trust-Verfahren statt Proof-of-Work (Sicherstellung der Systemintegrität durch hohen Rechenaufwand) (vgl etwa *King/Nadal*, PPCoin: Peer-to-peer Crypto-Currency with Proof-of-stake (2012), https://pdfs.semanticscholar.org/0db3/8d32069f3341d34c35085dc009a85ba13c13.pdf).

82 Siehe etwa *EBA*, EBA warns consumer on virtual currencies (2013): https://eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies oder für viele *FMA*, Themenfokus Bitcoin: https://www.fma.gv.at/fma-themenfokusse/fma-fokus-bitcoin-co/.

83 Ausführlich etwa schon *Brito/Castillo*, Bitcoin – A primer for Policymakers (2013), https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf.

allgemein, dass auf Geschäftstätigkeiten in Zusammenhang mit Bitcoin keine Regulierungen anwendbar sind.[84] Lediglich in Deutschland wurde eine Einordnung als „Rechnungseinheit" und somit als Finanzinstrument angenommen.[85] Diese Einordnung hat jüngst ein deutsches Strafgericht verworfen;[86] die BaFin sowie das deutsche Bundesfinanzministerium (BMF) bleiben jedoch bei der Einordnung als Rechnungseinheit/Finanzinstrument.[87] Dies führt – vereinfacht gesagt – dazu, dass jeder Handel, jedes Brokergeschäft, jede Vermittlung uä einer Konzessionspflicht unterliegt.[88] Die weitere Entwicklung diesbezüglich bleibt spannend, wobei mE davon auszugehen ist, dass die Einstufung der BaFin auch in Zukunft laufend hinterfragt und schlussendlich gekippt wird. Auch steuerrechtlich wurde der Bitcoin bereits unterschiedlich eingestuft: Bis zu einem richtungsweisenden Urteil des EuGH sind manche EU-Länder von einer Mehrwertsteuerpflicht von Bitcoin-Transaktionen ausgegangen, was der EuGH auf Grund der Vergleichbarkeit mit Währungen abgelehnt hat.[89]

In Summe besteht aber mittlerweile – von Deutschland abgesehen – Einigkeit, dass der Bitcoin wegen seiner Ausgestaltung nicht unter finanzmarktrechtliche Regulierungen fällt. Zu nennen ist aber die 5. Geldwäsche-Richtlinie, welche die Sorgfaltspflichten zur Bekämpfung von Geldwäscherei auch auf virtuelle Währungen und somit auf Bitcoin erstreckt. Diese wird ab 10. Jänner 2020 anwendbar sein, sofern sie nicht früher national umgesetzt wird.

2.3 Ethereum – maßgebliche Erweiterung des Spektrums

Ethereum basiert auf einer Seite technisch weitgehend auf Bitcoin, während auf der anderen Seite maßgeblich Zusatzmöglichkeiten und Entwicklungen eingefügt wurden. Die wichtigsten Unterschiede, soweit diese relevant für das gegenständliche Thema sind, werden in Folge kurz dargestellt. Das Ethereum-Whitepaper wurde 2014 veröffentlicht,[90] das Netzwerk 2015 live geschalten.[91] Schon der Titel des Whitepapers[92] verdeutlicht, dass mit Ethereum primär ein anderer Zweck als mit Bitcoin verfolgt wird. Während, wie oben dargestellt, Nakamoto primär eine Zahlungsfunktion im Sinn hatte, hat Buterin Ethereum bewusst als Basis eines programmierbaren Netzwerks auf der Blockchain konstruiert.[93] Im Gegensatz zu Bitcoin ist es somit möglich, auf der Ethereum-Blockchain Applikationen zu programmieren und zu verwenden. Diese Weiterentwicklung ermöglichte die Schaffung von ICOs[94] und ist daher von primärerer Relevanz für diese Arbeit. Mit anderen Worten:

84 Etwa wenn in Zusammenhang mit Bitcoins konzessionspflichtige Tätigkeiten gesetzt werden, etwa die Einsammlung von Geld um Bitcoin zu kaufen unter der Verpflichtung den erzielten Erfolg/Verlust wieder herauszugeben (Einlage zur Verwaltung), für andere Fälle siehe *FMA*, Themenfokus Bitcoin https://www.fma.gv.at/querschnittsthemen/fintechnavigator/bitcoin-co/.

85 Siehe *BaFin*, Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer (2013), https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html.

86 Kammergericht Berlin, 25.09.2018, (4) 161 SS 28/18 (35/18).

87 Siehe die parlamentarische Anfragen, zusammengefasst unter: *Private Banking Magazin*, BMF stuft Handel mit Krypto-Assets als erlaubnispflichtig ein, https://www.private-banking-magazin.de/nach-urteil-gegen-verwaltungspraxis-der-bafin-bmf-stuft-handel-mit-krypto-assets-als/.

88 Siehe *BaFin*, aaO.

89 EuGH 22.10.2015, C264/14 (Hedqvist).

90 *Buterin*, A next generation smart contract & decentralized application platform, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

91 30.06.2015, siehe den ersten Block *Etherscan*, Genesis Block, https://etherscan.io/block/0.

92 "Smart contract and decentralized application platform"; beide Komponenten werden in diesem Kapitel näher beleuchtet; siehe aber auch Kapitel 2.4.

93 *Buterin*, aaO.

94 Siehe dazu Kapitel 2.4.