www.jusletter-it.eu

Thomas Hrdinka

Regulierung von Kryptowährungen

Crypto currencies carry various risks which cause governments to regulate or even ban them. Building on exemplary weaknesses of Bitcoin, this article aims to highlight various aspects of the need for such regulation in terms of civil and criminal law. (kg)

Category: Articles
Region: Austria
Field of law: Damage. Compensation for Damages.; Blockchain

Citation: Thomas Hrdinka, Regulierung von Kryptowährungen, in: Jusletter IT 26. September 2019

ISSN 1664-848X, jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1. Ausgangssituation
2. Technische Grundlagen
   2.1. Angriffsvektoren gegen Bitcoin
      2.1.1. Kryptographie
      2.1.2. Blockgröße und Transaktionsdauer
      2.1.3. Weitere Angriffsvektoren
3. Rechtsdogmatische Bewertung
   3.1. Finanztechnische Regulative
   3.2. Regulierung auf EU- und internationaler Ebene
   3.3. Haftung und Schadenersatz
   3.4. Strafrechtliche Pönalisierung
   3.5. Beweise
4. Ausblick
5. Literatur

1. Ausgangssituation

[1] Kryptowährungen haben mittlerweile eine in der Informationstechnologie langjährige Geschichte. David Chaum[1] publizierte bereits 1983 seine Ideen zu nicht rückverfolgbaren Zahlungstransaktionen. Er gründete 1990 die Firma DigiCash und setzte mit dem Produkt eCash[2] Meilensteine in der Geschichte des Zahlungsverkehrs. Andere Technologien mit ähnlichen Ideen scheiterten hingegen, da sie ua als staatsfeindlich verfolgt worden sind. Weitere Ideen wie Hash-Cash[3] von Adam Back war ein Proof-of-Work (dazu noch später) basiertes Protokoll, das von Hal Finney weiterentwickelt worden ist. Entwicklungen von Wei Dai (B-Money[4]) und Nick Szabo (Bit Gold[5]) waren tolerant gegenüber byzantinischen Fehlern[6], also Fehlern, die sich beliebig (iSv bösartig) falsch verhalten.

[2] Erst im Oktober 2008 ist Bitcoin[7] von Satoshi Nakamoto (einem Pseudonym[8]) als Proposal publiziert worden, wo aufbauend auf den Arbeiten der Vorgänger Finney, Dai und Szabo ein Konzept vorgestellt worden ist, welches als völlig anonymisiertes Zahlungssystem ohne der Notwendigkeit von Banken konzipiert worden ist. Der erste Bitcoin Client wurde von Nakamoto 2009 als Open Source Software veröffentlicht, zeitgleich die erste Bitcoin Mining Software. Der von Nakamoto erzeugte «Genesis Block» der Blockchain, einer dezentralen Datenbank auf der Bitcoin technisch gründet, enthielt 50 Bitcoins, die erste Bitcoin Transaktion an Finney waren 10

1 *David Chaum*: Blind signatures for untraceable payments, Advances in Cryptology – Crypto «82. Springer-Verlag, 1983, S. 199–203 (1983).

2 *D. Chaum*, *A. Fiat*, *M. Naor*: Untraceable electronic cash. In Proceedings on Advances in Cryptology (Santa Barbara, California, United States). S. Goldwasser, Ed. Springer-Verlag New York, New York, S. 319–327 (1990).

3 *Adam Back:* «Hashcash – A Denial of Service Counter-Measure», technical report (2002).

4 *Wei Dai:* B-Money, http://www.weidai.com/bmoney.txt aufgerufen (1998) 31.12.2017.

5 *Nick Szabo:* Bit gold, https://unenumerated.blogspot.co.at/2005/12/bit-gold.html aufgerufen (2005) 31.12.2017.

6 *L. Lamport*, *R. Shostak*, *M. Pease:* The Byzantine Generals Problem. In: ACM Trans. Programming Languages and Systems. Band 4, Nr. 3, S. 382–401 (1982).

7 *Satoshi Nakamoto:* Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin Foundation, https://bitcoin.org/bitcoin.pdf aufgerufen 31.12.2017, (2008).

8 Es ist bis dato unbekannt, wer hinter diesem Pseudonym steckt. Alle bisher angestellten Vermutungen konnten nicht verifiziert werden. Nakamoto beschreibt in seinen Blogs gute Gründe für seine Tarnung. Es kann auch sein, dass sich dahinter eine Gruppe von Personen verbirgt.

Bitcoins. Der erste belegte Kauf mit Bitcoins war 2010 eine Pizzabestellung (2 Pizzen um 10.000 Bitcoins). Bevor Nakamoto 2010 aus dem Projekt ausstieg, generierte er ca 1 Million Bitcoins.

[3] Die weiteren Jahre waren geprägt durch Nutzung durch sog «Kryptoanarchisten» oder «Cypherpunks»[9], und einem weitgehend stabilen Kurs mit mehr oder weniger Gewinnen oder Verlusten. Bitcoin etablierte sich aber sehr rasch im Darknet, einem Peer-to-Peer Overlay Netzwerk, und zwar als sicheres und anonymes Zahlungsmittel, vor allem für nicht legale Produkte und Dienstleistungen aller Art. «Silkroad» als Drogenumschlagplatz im Darknet erhielt Berühmtheit, insbesondere 2013 nach Verhaftung des Betreibers Ross Ulbricht, wobei zahlreiche Nachahmer folgten. Die jüngsten Entwicklungen von Bitcoin sind von Spekulationen geprägt, und aufgrund der Tatsache, dass der Bitcoin technisch mit 21 Millionen Stück limitiert ist, und bis dato geschätzte 17 Millionen Bitcoins in Umlauf sind, ist ein jähes Ende in naher Zukunft vorhersehbar; als alternatives, anonymes Zahlungsmittel wird der Bitcoin daher immer unattraktiver, auch daher, dass sich die Transaktionsgebühren am hohen Kurs orientierten. Seitdem nämlich der Bitcoin an Börsen als Future, Fonds oder andere Derivate gehandelt werden kann, dh auch auf fallende oder steigende Kurse gesetzt werden kann, ist eine Berg- und Talfahrt des Bitcoin Kurses unübersehbar bemerkbar.

[4] Laut Berichten von EUROPOL[10] werden Kryptowährungen vermehrt eingesetzt im Drogenhandel, der Geldwäsche, und bei der Korruption. Aufgrund dessen, dass verschiedene Staaten sowie die Europäische Union diese Entwicklungen mehr oder weniger kritisch hinterfragen, sind in naher Zukunft Regulative zu erwarten, welche auch andere Kryptowährungen als Bitcoin betreffen können.

2. Technische Grundlagen

[5] Bitcoin implementiert eine sehr komplexe Technologie, die nötig ist, um einerseits unabhängig von einer zentralen Institution wie bspw einer Bank zu sein, andererseits vollkommene Anonymität zu gewährleisten, und letztendlich eine Zahlungstransaktion nachvollziehbar und fälschungssicher zu machen. All diese Forderungen sind in der Pionierarbeit von Satoshi Nakamoto berücksichtigt und implementiert worden. Bitcoin kann abstrakt in 3 Komponenten geteilt werden: Transaktionen, das Consensusprotokoll und das Kommunikationsnetzwerk. Seit der ersten Veröffentlichung des Sourcecodes durch Nakamoto ist der Code, welcher von der Community gewartet und erweitert wird, noch deutlich komplexer und länger geworden.

[6] Elektronische Transaktionen sollen ermöglicht werden, ohne auf das Vertrauen einer Trusted-Third Party angewiesen zu sein. Digitale Münzen, die mit Hilfe digitaler Unterschriften erzeugt werden, ermöglichen zwar eine Eigentumskontrolle, ohne einen vertrauenswürdigen Dritten ist es jedoch schwierig deren unzulässige, mehrfache Verwendung zu verhindern. Zu diesem Zweck wird ein Peer-to-Peer-Netzwerk[11] eingesetzt, das eine öffentliche Historie von Transaktionen aufzeichnet («Blockchain»), die für einen malignen Angreifer solange rechnerisch unattraktiv ist, als die ehrlichen Knoten einen Großteil der gesamten Rechenleistung innehaben. Die Knoten stimmen sich ab und belegen gültige Blöcke, indem sie diese durch weitere Blöcke erweitern und

9 Kunstwort aus Cyber, Cipher und Punks für Technik Freaks die Kryptographie einsetzen.

10 *EUROPOL:* SOCTA 2017, European Union Serious and Organised Crime Threat Assessment, The Hague (2017),

11 Kommunikationsnetz gleichberechtigter Teilnehmer.

ungültige Blöcke ablehnen («Nakamoto Consensus»). Alle Benutzer sind aufgrund der so gewollten Nichtzuordenbarkeit ihrer öffentlichen Schlüssel im Netzwerk anonym.

[7] Die Blockchain baut auf einem Merkle-Tree[12] auf, einem sog Hashtree. Die Besonderheit dabei ist, dass jeder Block im Baum den Hashwert des Vorgängerblocks enthält, usw. Darüber hinaus ist auch die Merkle-Root oder Top-Hash enthalten, der Hashwert des Genesis-Blocks. Der Vorteil dabei ist, dass auch Teilbäume auf Echtheit verifiziert werden können. Versucht nun ein Angreifer einen Block zu verändern, so ändert sich dabei auch sein Hashwert, und jeder Knoten im Netzwerk kann die Fälschung erkennen. Dieses Transaktionsprotokoll, die Bitcoin Blockchain gehört niemandem, denn alle Knoten im Bitcoin Netzwerk besitzen eine Version davon.

[8] Ein Anhängen eines neuen Blocks ist technisch einfach, und jedem Knoten erlaubt. Um das unkontrollierte Anwachsen des Baumes zu begrenzen wird folgende Vorgehensweise gewählt: Neue Bitcoins werden mithilfe von speziellen Miningknoten generiert («Mining» oder Schürfen). Zuerst konsolidiert ein Miner eine oder mehrere Transaktionen in einem Block. Als nächstes bewältigt er für diesen Block eine aufwändige Rechenaufgabe, damit der neue Block vom Netzwerk genehmigt werden kann. Zu diesem Zweck wird ein Hashwert des Blocks erzeugt, und solange dieser Wert nicht kleiner als das aktuelle konsensorientierte Schwierigkeitslevel ist, variiert der Miner einen bestimmten Wert im Block («Nonce-Feld») in der Art, sodass sich auch der Hashwert des Blocks ändert. Dieser Vorgang («Proof-of-Work»[13]) wird solange wiederholt, bis ein größerer Hashwert gefunden ist, und erst dann überträgt der Miner den Block an das Bitcoin Netzwerk. Wenn der Block schließlich vom gesamten Netzwerk akzeptiert wird, erhält der Miner eine Belohnung in Form von neu erzeugten Bitcoins. Danach können andere Miner keine Blöcke mehr an die gleiche Stelle übertragen. Daher sind Miner gefordert, schneller als andere einen Erfolg zu erzielen, um Bitcoin Belohnungen zu erhalten, und unnötige Rechenzeit zu vermeiden.

[9] Das Protokoll ist so konzipiert, dass es immer ca 10 Minuten dauert, um einen Proof-of-Work zu erzeugen. Das legt die Mindestzeit für die Erstellung eines neuen Blocks fest, die auch als Block-Release Timing bezeichnet wird. Nach einer bestimmten Anzahl von Blöcken ändert das Netzwerk die Schwierigkeit so, um sicherzustellen, dass der Prozess noch immer 10 Minuten dauert. Das Block-Release-Timing ist deshalb begrenzt, um die Wahrscheinlichkeit einer Spaltung der Blockchain zu verringern. Es konkurrieren immer mehrere Blockchains gleichzeitig, um als die Haupt-Blockchain angesehen zu werden. Alle Knoten verifizieren neu erzeugte Blöcke, wobei nur jene Blockchain mit der aufwändigsten Proof-of-Work, also idR die längste, gewählt wird; die anderen Blockchains werden verworfen.

2.1. Angriffsvektoren gegen Bitcoin

2.1.1. Kryptographie

[10] Kryptographisch entsprechen die verwendeten Algorithmen ECDSA, SHA256 und RIPEMD160 grundsätzlich dem Stand der Technik, und sind auch in naher Zukunft als sicher anzusehen. Wenn jedoch in Zukunft ein Großteil der Rechenleistung im Bitcoin Netzwerk von

12 *R.C. Merkle:* «Protocols for public key cryptosystems» In: Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122–133 (1980).

13 «Kryptographisches Puzzle», eine Methode/Arbeitsaufgabe, damit ein Dienst nicht übermäßig ge- oder mißbraucht werden kann.

Angreifern übernommen werden sollte, sei es durch massenweisen Betrieb leistungsfähiger Rechner, so ist das gesamte Sicherheitskonzept von Bitcoin und auch anderen Kryptowährungen, die auf einer Blockchain aufbauen, gefährdet. Da dieser Umstand dem Blockchain Konzept zu verdanken ist, lässt sich solch ein Angriff kaum vermeiden, ohne das Consensus Protokoll in seinen Grundfesten zu verändern.

[11] Das Brechen von Hashfunktionen wie SHA256 oder dem schwächeren RIPEMD160 entspricht einem nichtdeterministischen polynomialen (NP) vollständigen Problem, dh es lässt sich nicht effizient berechnen. Der Aufwand zum Brechen mit Hilfe einer Brute-Force Attacke, wie es mit einem heutigen Computer erforderlich wäre, entspricht einem Aufwand[14] $O(2^k)$ für einen Hash der Länge *k*-bit. Es ist jedenfalls bewiesen, dass mit Hilfe des BHT[15] Algorithmus, einer Kombination des Grover[16] Algorithmus mit der Birthday-Attacke[17], eine Lösung mit Aufwand $O(2^{k/3})$ erzielt wird. Die Reduktion ergibt sich durch die Kubikwurzel, und obwohl das keine Reduktion in polynomialer Zeitkomplexität ist, ist das im Hinblick auf Quantencomputer, deren Einsatz genau die Lösung von NP-Problemen ist, ein erheblicher Zeitvorteil.

[12] Mit Hilfe des Shor[18] Algorithmus ist es weiter absehbar, dass auch der digitale Signaturalgorithmus ECDSA gefährdet ist, wenn Quantencomputer zum Einsatz kommen. ECDSA baut darauf auf, dass es zu bestimmten elliptischen Kurven[19] keine Umkehrfunktionen gibt. Aus einem gegebenen öffentlichen Schlüssel könnte ein Quantencomputer mit dem Shor Algorithmus den privaten Schlüssel sehr effizient finden. Statt mit $O(2^{k/2})$ benötigt die Lösung nur $O(k^3)$. Da Bitcoin 256 bit für private Schlüssel nutzt, reduziert sich der Aufwand von $3{,}4 \mathring{u} 10^{38}$ auf lediglich 17 Millionen Möglichkeiten, ein sensationell hoher Geschwindigkeitsgewinn von $2 \mathring{u} 10^{31}$. Wenn nun eine Transaktion an das Netz geschickt wird, bevor diese endgültig in die Blockchain geschrieben wird, ist diese besonders gefährdet, denn ein Angreifer könnte den privaten Schlüssel entschlüsseln, ersetzen und damit alle Bitcoins hinter dieser Transaktion stehlen.

[13] Ein weiteres Problem ist, dass bei Bitcoin eine elliptische Kurve des NIST Standards FIPS 1864[20] genutzt wird, und da nicht bekannt ist, ob die NSA Hintertüren kennt, ist dieser Standard umstritten. Es ist jedenfalls bekannt, dass genau diese Kurve secp265k1 anfällig für Sidechannel[21] Angriffe ist, mit der Konsequenz, dass es auch mit gegenwärtiger Rechenleistung rasch und effizient möglich ist, die privaten Schlüssel einer Wallet aus den öffentlichen Schlüsseln zu errechnen. Andere elliptischen Kurven, wie von der IETF als RFC 7748 standardisierte Curve25519 wären hingegen sicher gewesen.

---

14 Landau Symbol: $f \ O(2^k)$, bedeutet dass die Funktion *f* gemäß der Funktion 2^k, also exponentiell wächst.

15 *G. Brassard, P. Hoyer, A. Tapp*: «Quantum Algorithm for the Collision Problem». Lecture Notes in Computer Science: S. 163–169 (1997).

16 *L. K. Grover:* A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, S. 212 (1996).

17 Erzeugen von Kollissionen idS, dass zwei Klartexte den gleichen Hashwert besitzen. Aufwand statt 2^k nur $2^{k/2}$.

18 *P. W. Shor:* Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In: SIAM Journal on Computing, S. 1484–1509 (1997).

19 Algebraische Kurve der 3. Ordnung; hier Elliptische Kurven über einen endlichen Körper.

20 *NIST*: FIPS 186-4 Digital Signature Standard, National Institute of Standards and Technology, Gaithersburg, S. 19 und 26 (2013).

21 *N. Benger, J. van de Pool, N. P. Smart, Y. Yarom:* «Ooh Aah... Just a Little Bit»: A small amount of side channel can go a long way. In: Batina L., Robshaw M. (eds), Cryptographic Hardware and Embedded Systems – CHES 2014. CHES 2014. Lecture Notes in Computer Science, vol 8731. Berlin, Heidelberg, Springer (2014).

2.1.2. Blockgröße und Transaktionsdauer

[14] Das Protokoll ist insofern begrenzt, als die maximale Größe eines Blocks 1 MB betragen kann und die minimale Größe einer Transaktion etwa 200 Bytes beträgt. Basierend auf diesen Einschränkungen beträgt die maximale theoretische Transaktionsrate nur 7 Transaktionen pro Sekunde, was global gesehen als zu langsam erscheint. Weiter ist die Anzahl der Bitcoins auf 21 Millionen begrenzt worden; was mit dem investierten Geld passiert, wenn diese Grenze erreicht wird, ist nicht absehbar. Dies gleicht einem Pyramidenspiel, denn wer garantiert den Rücktransfer in eine echte Währung, wenn der Bitcoin Kurs zwar aufgrund von Spekulation phantastische Werte erreicht, jedoch niemand zu diesen Bedingungen bereit ist, Bitcoins in eine echte Währung oder andere Gegenwerte zu konvertieren, abgesehen von den begrenzten Transaktionszeitfenstern.

2.1.3. Weitere Angriffsvektoren

[15] Bitcoin ist vom Nakamotokonzept und seiner ersten Implementierung her anfällig für verschiedenste Angriffe, deren Auflistung und Beschreibung den Umfang dieser Publikation sprengen würde. Das Bitcoin Protokoll baut auf Fairness auf, wenn diese nicht gegeben ist, so ist die Stabilität des Systems mitunter nicht mehr gegeben. Nakamoto meinte zwar, dass der Bitcoin solange stabil bleiben wird, als die wirtschaftlichen Anreize aller Miner befriedigt werden. Gemäß der Spieltheorie[22] («Nash-Gleichgewicht») wäre das bei globalem Konsens der Fall, die Stabilität wird jedoch dann schwach, wenn einige oder sogar die Mehrheit sich nicht regelkonform verhält. Ein weiterer Schwachpunkt ist, wenn Miningpools instabil werden, bspw wenn einige Miner andere attackieren, indem sie zu erzeugende Blöcke sabotieren. Ebenso ist das Peer-to-Peer Netzwerk nicht geschützt gegen Denial of Service (DoS) Attacken. Jeder Angreifer kann beliebige Konkurrenz-Knoten sabotieren, um zB das Consensusprotokoll iS seiner eigenen malignen Zwecke zu beeinflussen, wie bspw das Durchsetzen seiner eigenen erzeugten Blockchain, mit eigenen, neuen Bitcoins.

3. Rechtsdogmatische Bewertung

[16] Wie schon in der Einleitung beschrieben, werden Kryptowährungen insb Bitcoin zunehmend für kriminelle Zwecke wie Drogenhandel, Geldwäsche und Korruption genutzt. Ein weiteres Phänomen, wo Bitcoins ebenfalls als anonymes Zahlungsmittel verwendet werden, sind die Verschlüsselungstrojaner («Ransomware»), welche Opfer zB per Email empfangen, und bei Aktivierung die Festplatte verschlüsseln. Die Entschlüsselung ist nur gegen Lösegeld in Form von Bitcoins möglich. Diese Form der Erpressung hat sich im letzten Jahr laut Aussage der Generaldirektion[23] für die Öffentliche Sicherheit verdoppelt.

22 *John Forbes Nash:* Non-cooperative games, Dissertation, Princeton (1950).

23 *Futurezone:* https://futurezone.at/netzpolitik/polizei-whatsapp-ueberwachung-ist-nicht-sinnlos/304.135.064 gelesen 3.1.2018.

[17] Die geschätzte gesamte Schadenssumme weltweit wird im November 2017 auf 1 Million Bitcoins angegeben[24], was ca 6% aller Bitcoins entspricht. Der aktuelle Gegenwert wäre 10 Milliarden Euro. Nicht einberechnet sind dabei Entwendungen aus privaten Client-Wallets. Dass solcherart Entwendungen aus Client-Wallets möglich sind, beweist eine gefundene Sicherheitslücke bei der Wallet Electrum[25].

3.1. Finanztechnische Regulative

[18] Kryptowährungen sind erstmals 2012 von der Europäischen Zentralbank (EZB) als «digitales, nicht reguliertes Geld» klassifiziert[26] worden. Hinsichtlich steuerlicher Behandlung von Bitcoin wurde im Erlass[27] des BMF vom 03.10.2014 die Frage der steuerlichen Beurteilung von Bitcoins als Zahlungsmittel zwischen Unternehmen beantwortet: «Bitcoins sind derzeit nicht als offizielle Währung anerkannt. Es handelt sich daher um ein, einer Finanzanlage oder einem Finanzinstrument vergleichbares, Wirtschaftsgut. Weiter: Hinsichtlich der steuerlichen Erfassung sind Bitcoins wie sonstige betriebliche Wirtschaftsgüter zu behandeln und daraus resultierende Einkünfte daher zum Tarif zu erfassen. Werden Bitcoins jedoch zinstragend veranlagt, stellen sie Wirtschaftsgüter iSd § 27 Abs 3 EStG 1988 dar. Realisierte Wertänderungen unterliegen daher dem Sondersteuersatz gemäß § 27a Abs 1 EStG 1988.»

[19] Der EuGH hat ein Jahr später ein richtungsweisendes Urteil[28] gefällt. Demzufolge wird in Rn 42 und 44 festgestellt, dass, da die virtuelle Währung «Bitcoin» ein vertragliches Zahlungsmittel ist, sie zum einen weder als Kontokorrent noch als Einlage, Zahlung oder Überweisung angesehen werden kann. Zum anderen stellt sie, im Unterschied zu den in Art 135 Abs 1 lit d der Mehrwertsteuerrichtlinie genannten Forderungen, Schecks und anderen Handelspapieren, ein unmittelbares Zahlungsmittel zwischen denjenigen Wirtschaftsteilnehmern dar, die sie akzeptieren. Was zweitens die in Art 135 Abs 1 lit e der Mehrwertsteuerrichtlinie vorgesehenen Steuerbefreiungen betrifft, sieht diese Bestimmung vor, dass die Mitgliedstaaten Umsätze, die sich ua auf «Devisen, Banknoten und Münzen beziehen, die gesetzliches Zahlungsmittel sind», von der Steuer befreien. Letztlich wird in Rn 55 festgestellt, dass die virtuelle Währung «Bitcoin» weder ein Wertpapier darstellt, das ein Eigentumsrecht an juristischen Personen begründet, noch ein vergleichbares Wertpapier.

[20] Letztlich wird in Rz 759 der Richtlinie[29] des BMF vom 05.12.2017 bestimmt, «dass auch der Umtausch konventioneller Währungen in Einheiten der virtuellen Währung «Bitcoin» und umgekehrt steuerfrei ist (vgl EuGH 22.10.2015, Rs C-264/14, Hedqvist). Das «Bitcoin-Mining» (Validierung und Verschlüsselung von Datensätzen (Transaktionen) zum Zwecke der Vermehrung von Bitcoins bzw der Aufrechterhaltung der Sicherheit des gesamten Bitcoin-Systems bzw. -Netzwerkes) ist entweder mangels eines bestimmbaren Leistungsempfängers nicht steuerbar

24 *Futurezone:* https://futurezone.at/digital-life/hacker-haben-schon-eine-million-bitcoin-gestohlen/299.024.231 gelesen 1.1.2018.

25 *Heise:* https://www.heise.de/security/meldung/Bitcoin-und-Litecoin-Klau-bei-Electrum-Electron-Cash-und-Electrum-LTC-moeglich-3936813.html gelesen 9.1.2018.

26 *EZB*: Virtual Currency Schemes, Europäische Zentralbank, Frankfurt (2012).

27 BMF-010203/0312-VI/6/2014.

28 C-264/14, ECLI:EU:C:2015:718.

29 BMF-010219/0375-IV/4/2017.

oder im Falle der Verifizierung eines dezidierten Vorganges gegen Transaktionsgebühren steuerbar, aber steuerfrei».

[21] Zu beachten ist, dass diese Bestimmungen ausschließlich Bitcoin betreffen. Ob auch andere Kryptowährungen davon umfasst sind, wäre, so fern bei diesen eine vergleichbare Technologie und vergleichbare Zahlungsmechanismen verwendet werden wie bei Bitcoin, es mE nach zu bejahen, andernfalls wäre im Einzelfall zu prüfen, ob diese alternative Technologie anderen Regimes wie dem Bankwesengesetz[30], dem E-Geldgesetz[31] oder dem Zahlungsdienstegesetz[32] unterliegen, oder Privatautonomie vorliegt. Eine Klärung durch die FMA[33] wäre aber in jedem Fall geboten, da es sein kann, dass ein anderes Geschäftsmodell als Bitcoin einer Konzession unterliegt. Bspw wird PayPal[34], technisch ein unmittelbarer eCash Ableger, EU-weit als Bank geführt, wobei die zuständige Aufsichtsbehörde die luxemburgische Bankenaufsicht CSSF ist.

3.2. Regulierung auf EU- und internationaler Ebene

[22] Hinsichtlich der Entwicklungen der Cyberkriminalität, hat die Union die 4. Geldwäscherichtlinie[35] erlassen, die mit dem Finanzmarkt-Geldwäschegesetz[36] umgesetzt worden ist. Dieses Bundesgesetz ist auf Kredit- und Finanzinstitute anzuwenden. Der Rat der Europäischen Union einigte sich im Dezember 2017 auf die 5. Geldwäscherichtlinie[37], wobei ebenso Umtausch-Plattformen für virtuelle Währungen sowie von Online Wallets dabei unter diese Regelung fallen, um Nutzer virtueller Währungen über eine geplante zentrale Datenbank leichter identifizieren zu können. Auf diese Weise soll sichergestellt werden, dass diese Börsen bzw Online Wallet Anbieter den Sorgfaltspflichten gegenüber Kunden unterliegen und dazu beitragen, Geldwäsche und Terrorismusfinanzierung zu bekämpfen. Österreich ortete in diesem Vorschlag bezüglich Trusts mangelnde Transparenz, die eine effiziente Bekämpfung von Geldwäsche erfordert[38]: «Austria is strongly concerned that the current text does not enhance transparency on beneficial ownership necessary to avoid the abuse of trusts for the purpose of money laundering and terrorist financing.»

[23] Weitere Regulierungstendenzen sind weltweit zu beobachten, die zukünftig auf die EU sowie auf Österreich Einfluss nehmen werden: im US-Senat ist im November 2017 ein Gesetzesvorschlag[39] eingebracht worden, wo Kryptowährungen unter Geldwäscheverdacht gestellt werden sollen, und anonyme Bitcoin Konten damit illegal werden. Bei Grenzkontrollen ist auch die

30 *BWG*, BGBl 532/1993 idgF.

31 *E-GeldG*, BGBl I 107/2010 idgF.

32 *ZaDiG*, BGBl I 66/2009 idgF.

33 Die FMA kommt zu dem Ergebnis, dass der Kauf und Verkauf von Bitcoins kein konzessionspflichtiges Bankgeschäft gem. § 1 Abs 1 BWG darstellt.

34 PayPal (Europe) S.à r.l. et Cie, S.C.A. www.paypal.com.

35 Richtlinie (EU) 2015/849 des Europäischen Parlaments 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 und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl. L 141/73 vom 5. Juni 2015.

36 *FM-GwG*, BGBl I 118/2016 idgF.

37 ST 15849 2017 INIT – 2016/0208 (COD).

38 ST 15849 2017 ADD 1 – 2016/0208 (COD).

39 *US-Senat:* https://www.congress.gov/bill/115th-congress/senate-bill/1241/text gelesen 3.1.2018.

Durchsuchung elektronischer Geräte nach virtuellem Geld vorgesehen. Das hat auf die EU insofern Auswirkungen, als EUROPOL aus diesem Grund die Kommission zum Handeln auffordert. Anders in der Russischen Föderation: Kryptowährungen, Online Börsen, Mining Pools als auch neuartige Finanzdienstleistungen (als Sandbox Modell in der Eurasischen Wirtschaftsunion[40]) müssen aufgrund eines Präsidialdekrets[41] vom Oktober 2017, bis Juli 2018 reguliert zugelassen werden. Da das russische Krypto-Regulierungsgesetz im Dezember 2018 in die erste Lesung zurückgeschickt worden ist, hat Präsident Putin die Regierung angewiesen, bis Juli 2019 eine Krypto-Regulierung durchzusetzen.

3.3. Haftung und Schadenersatz

[24] Die Durchsetzung von Gewährleistungsansprüchen bei Open Source Software wie Bitcoin ist grundsätzlich möglich, jedoch nicht unproblematisch. Aufgrund der Unentgeltlichkeit der bei Bitcoin verwendeten MIT-Lizenz[42] liegt eine Schenkung[43] gem § 938 ABGB von Werknutzungsrechten[44] aller Verwertungsarten vor, oder je nach Betrachtungsweise ein Vertrag sui generis. Obwohl laut dieser Lizenz Haftung und Schadenersatzansprüche ausgeschlossen werden, haftet der Entwickler in jedem Fall ex contractu (zB Schlechterfüllung) oder ex delicto (siehe nachfolgendes Kapitel). Folglich hat der Nutzer einen eingeschränkten Anspruch wie bei Vorsatz oder grober Fahrlässigkeit gegenüber dem Entwickler. Grobe Fahrlässigkeit ist extremes Abweichen von der gebotenen Sorgfalt, wie zB das Veröffentlichen gänzlich ungetesteter Software oder der Einbau von Verschlüsselungsalgorithmen, die nachweislich nicht dem Stand der Technik entsprechen.

[25] Im Falle von Bitcoin würde ein Anspruch gegen einen Unbekannten Satoshi Nakamoto zwar als völlig aussichtslos erscheinen, jedoch gegenüber anderen am Open Source Projekt Beteiligten, namentlich bekannten Programmierern nicht. Bei Fällen, in denen die Urheber im Quelltext oder an sonstiger Stelle dokumentiert sind, kann die Urhebervermutung des § 12 Abs 1 UrhG angewendet werden. Die subjektive Vorwerfbarkeit gegenüber den Programmierern kann gem § 1299 ABGB der Sachverständigenhaftung begründet werden, denn wer sich als Experte oder Spezialist ausgibt, kann sich nicht mit mangelnder Erfahrung oder Unkenntnis entschuldigen. Die Entwicklercommunity selbst kann auch als GesbR angesehen werden, was eine Solidarhaftung gem § 890 ABGB auslösen kann. Das Schadensausmaß wird zivilrechtlich üblicherweise mit dem Wiederherstellungsaufwand der beschädigten Daten bemessen, wobei bei Kryptowährungen zusätzlich verlorene oder vernichtete Geldwerte hinzukommen.

[26] Die immer wieder bemühte Eigenverantwortung der Bitcoin Nutzer führt aus diesen Gründen ins Leere, denn bei grober Fahrlässigkeit haften die Entwickler und nicht die Nutzer, welche als Laien nicht wissen (können) welches Risiko die geladene Software bergen kann.

40 http://www.eaeunion.org.

41 : -2132, (Instructions following meeting on digital technology in finance), http://kremlin.ru/acts/assignments/orders/55899 gelesen 3.1.2018.

42 Bitcoin wird mit der MIT License zur Verfügung gestellt: https://opensource.org/licenses/mit-license.php aufgerufen 3.1.2018.

43 Vgl § 938 iVm § 943 ABGB: StF: JGS Nr 946/1811 idgF.

44 Vgl § 24 UrhG, BGBl 111/1936 idgF.

3.4. Strafrechtliche Pönalisierung

[27] Delikte in Verbindung mit Kryptowährungen wären ua schwerer Betrug bzw der betrügerische Datenverarbeitungsmißbrauch geregelt in StGB §§ 147 sowie 148a. Auch der Diebstahl[45] wäre ein potenzieller Tatbestand, jedoch wäre zu prüfen, ob die «gestohlene» Kryptowährung eine «bewegliche Sache» ist. Dieser Tatbestand kann bejaht werden, wenn «die Einheiten virtueller Währungen erst einmal erzeugt sind»[46], denn «so handelt es sich um Sachen iSd § 285 ABGB». Es handelt sich somit um unkörperliche und bewegliche Sachen, die verbrauchbar und vertretbar sind. Ist schwerer Betrug gem StGB § 147 Abs 1 Z 1 mit der Benützung eines entfremdeten unbaren Zahlungsmittels oder ausgespähten Daten eines unbaren Zahlungsmittels zwecks Täuschungsabsicht erfüllt, so ist im Unterschied dazu der betrügerische Datenverarbeitungsmißbrauch gem § 148a Abs 1 erfüllt, wenn mit einem Bereicherungsvorsatz das «Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflußt» wird. Dazu ähnliche Bestimmungen finden sich im StGB § 225a der Datenfälschung, wenn elektronische Beweismittel die im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, verändert, unterdrückt oder gelöscht werden. Im Zuge einer Beweissicherung (siehe nachfolgendes Kapitel) würde diese Bestimmung eine Sanktionsmöglichkeit gegen Beweismittelunterdrückung darstellen.

[28] Ein weiterer Tatbestand in diesem Zusammenhang ist die Fälschung unbarer Zahlungsmittel, geregelt im StGB § 241a. Eine Fälschung von Bitcoins wäre dann gegeben, wenn zB durch eine DoS Attacke (StGB § 126b) Mining-Pools angegriffen werden, sodass deren Blockchains sich im Peer-to-Peer Netz nicht durchsetzen können, und die eigene, gefälschte Blockchain stattdessen durch das Consensus-Protokoll bevorzugt wird, ist auch der Tatbestand der Fälschung unbarer Zahlungsmittel gem StGB § 241a erfüllt. Darüber hinaus wäre noch zu erwägen, ob auch der Bereicherungsvorsatz gem StGB § 148a, dem betrügerischen Datenverarbeitungsmißbrauch gegeben ist.

[29] Bitcoin und andere Kryptowährungen stehen in manchen Ländern unter dem Verdacht der Geldwäscherei. Ein Verbot wird nicht nur aus diesem Grund, sondern auch daher erwogen, da sie angeblich pyramidenartig aufgebaut sind. Für die Geldwäsche gem StGB § 165 ist der Vermögensbestandteil ein zentraler Begriff, der sehr allgemein zu verstehen ist. Ein Vermögensbestandteil rührt laut StGB § 165 Abs 5 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». Dazu zählen nicht nur Sachen sondern auch Forderungen, Lizenzen, Beteiligungen und iSv unbaren Zahlungsmittel Kryptowährungen. Wesentlich ist, dass der Tatbestand erfüllt ist, wenn dieser von der in StGB § 165 Abs 1 aufgezählten Vortaten (mit einer mehr als einjährigen Freiheitsstrafe bedrohte Handlung, Urkundenfälschung, Urkundenunterdrückung, Suchtmittelgesetz) herrührt, dh wenn eine Verschleierungsabsicht von Vermögensbestandteilen wie, dass durch viele undurchsichtige Transaktionen, durch falsche Angaben als auch durch Vernichtung von Spuren diese Verschleie-

45 Vgl §§ 127, 128, und allenfalls § 130 Abs 1 StGB, BGBl 60/1974 idgF.

46 *O. Völkel*: Privatrechtliche Einordnung der Erzeugung virtueller Währungen, Ecolex Juli 2017, Manz, S. 639-641 (2017).

rung erfolgt. Gemäß StGB § 165 Abs 1 wird eine «Eigengeldwäscherei» unter Strafe gestellt, die grundsätzlich dann gegeben ist, wenn Verstecken oder Verschleiern von zB Bitcointransaktionen, die aus einer mehr als einjährigen Freiheitsstrafe bedrohten Handlung herrühren. Im Unterschied dazu wird in StGB § 165 Abs 2 die «Fremdgeldwäscherei» unter Strafe gestellt, «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». Wesentlich dabei ist die Wissentlichkeit gem StGB § 5 Abs 3. In Bezug auf Kryptowährungen wären somit sämtliche Transaktionen welche unter dem Eventualvorsatz dolus eventualis in Bezug auf den unter StGB § 165 Abs 1 taxativ aufgezählten Vortaten für Dritte getätigt werden, strafbar. Dieser Tatbestand wird durch Abs 3 höher pönalisiert, wenn jemand Vermögensbestandteile von kriminellen Organisationen (StGB § 278a) oder terroristischen Vereinigungen (StGB § 278b) in deren Auftrag oder Interesse an sich bringt.

[30] Der Tatbestand von Ketten- oder Pyramidenspiele gem StGB § 168a ist dann erfüllt, wenn jemand zB Kryptowährungen als Gewinnerwartungssystem in Gang setzt, «dessen Teilnehmern gegen Einsatz ein Vermögensvorteil unter der Bedingung in Aussicht gestellt wird, daß diesem oder einem damit im Zusammenhang stehenden System unter den gleichen Bedingungen weitere Teilnehmer zugeführt werden, und bei dem die Erlangung des Vermögensvorteils ganz oder teilweise vom bedingungsgemäßen Verhalten jeweils weiterer Teilnehmer abhängt». Diese Bestimmung wäre im Falle von Kryptowährungen nur dann erfüllt, wenn sich jemand bei einem Initial Coin Offering (ICO) vorab Vorteile verschafft, und es weiter nötig ist, neue Teilnehmer anzuwerben, damit das System verbreitet, und dieser Vermögensvorteil zumindest teilweise von diesen neuen Teilnehmern abhängt. Bitcoin ist mE nach an der Grenze dieses Tatbestandes anzusiedeln, da Satoshi Nakamoto sich zu Beginn 1 Mio Bitcoins selbst zugeführt hat, mit einem Limit von 21 Mio. Jedoch konnte es zu Beginn nicht absehbar sein, welche Kurs-Hausse der ursprünglich nahezu wertlose Bitcoin nach 8 Jahren haben wird. Erst nachdem Börsenspekulationen mit Bitcoins möglich geworden sind, könnte das Abhängen vom bedingungsmäßigen Verhalten weiterer Teilnehmer erfüllt sein, was einem Pyramidenspiel nahe kommen würde. Zur Erfüllung des Straftatbestandes des Pyramidenspieles wäre es auch abzuwägen, ob der Initiator überhaupt in der Lage war dieses Verhalten zu beeinflussen. Indizien gemäß des Blogs von Satoshi Nakamoto sprechen jedenfalls dagegen, da bei Bitcoin nie eine Gewinnerwartung versprochen worden ist. Solcherart Gewinnerwartungssysteme iVm Bitcoins sind hingegen jüngst durch unseriöse Dritte in Gang gesetzt worden.

3.5. Beweise

[31] Die strafrechtliche Pönalisierung von Hackern und des Diebstahls von und Betrug mit Bitcoins wird aufgrund der eingesetzten starken Kryptographie, welche Anonymität gewährleistet, nur in den seltensten Fällen möglich sein, und nur dann, wenn der Dienstleister (Online Börse) entsprechende Zugriffsprotokolle auf seinen Servern laufend archiviert, bei den Ermittlungen kooperiert, und sich der Täter im Internet überhaupt rückverfolgen lässt.

[32] Wer die Beweislast trägt ist abhängig davon, ob zivilrechtliche, strafrechtliche oder verwaltungsstrafrechtliche Tatbestände verfolgt werden. Trifft den Betreiber einer Online Börse die Beweislast (gem DSGVO, KSchG) so wäre der Geschädigte bzw die ermittelnde Behörde in einer grundsätzlich stärkeren Position. Im anderen Fall, wenn die Beweislast bei der Behörde oder dem Geschädigten selbst liegt, so wird es ohne ausreichendes, qualifiziertes Beweismaterial in den sel-

tensten Fällen zu einer Verurteilung kommen können. Zur Selbstbelastung bzw Vertuschung von Beweismitteln pönalisiert das StGB im § 225a eine Datenfälschung, wenn elektronische Beweismittel, die im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, verändert, unterdrückt oder gelöscht werden. Gemäß der Strafprozessordnung, trifft auch den Verantwortlichen einer Datenanwendung jedenfalls eine Mitwirkungspflicht[47], und im § 37j KartG[48] ist sogar in Anlehnung an US-Recht des dort gefürchteten «Pretrial discovery» Ansatzes zur Aufklärung der Straftat verpflichtet, dass hohe Ordnungsstrafen drohen, wenn relevante Beweismittel dem Beweisführer entzogen, beseitigt oder zur Benützung untauglich gemacht werden, was bedeutet, dass die Schlüssel oder Passwörter entweder herausgegeben werden, oder die Entschlüsselung vom Beschuldigten selbst vorgenommen wird. Dem steht entgegen, dass kein Beschuldigter, weder im Strafprozess noch im Zivilprozess aufgrund des Grundsatzes nemo tenetur se ipsum accusare verpflichtet werden kann, seine Geheimnisse wie Schlüssel oder Passwörter zu offenbaren, und sich dadurch selbst zu belasten. In Abwägung der Folgen, die solch eine Weigerung zur Kooperation mit sich bringt, wären Beschuldigte gut beraten mitzuwirken, denn wenn gem StPO § 115 eine Beschlagnahme von zB der Server droht, die genau dann nötig ist, wenn seitens der Ermittler Passwörter erraten oder Verschlüsselung gebrochen werden muss, könnte solch einen Eingriff für einen Betrieb teure Konsequenzen haben. Es wäre natürlich im Einzelfall abzuwägen, ob solch eine schwerwiegende Maßnahme einen Exzess darstellt. Das BVwG[49] verneinte in seiner Entscheidung den Einsatz der im Zuge einer Hausdurchsuchung von den Behörden eingesetzten «Spionage-Software», dass diese als a priori und per se rechtswidrig sei. Sohin stellt diese an sich keinen krassen Maßnahmenexzess dar. Die rechtliche Würdigung wird begründet dadurch, «da es zulässig ist, wenn die BWB bei einer Hausdurchsuchung geschäftliche Unterlagen sichtet, kopiert und Beweismittel in ihre Verfügungsmacht bringt, wenn sie dabei forensische Computerprogramme verwendet, um große Datenmengen schnell und effizient sichten zu können und um geschäftliche Unterlagen zu kopieren und diese in einer für sie lesbaren Form in ihre Verfügungsmacht zu bringen». Dieser Beschluss wurde am VwGH[50] angefochten, wobei diese Revision abgewiesen worden ist. Gemäß RS 6 «besteht für den Einsatz forensischer Software eine gesetzliche Grundlage». Weiter wird in RS 7 bestimmt, «soweit die Revisionswerberinnen den konkreten Einsatz der verwendeten Programme als unverhältnismäßig rügen, so wäre dieser Einsatz nur dann nicht mehr durch die gerichtliche Anordnung in den Hausdurchsuchungsbefehlen gedeckt (und damit die rechtliche Zurechnung des Vollzugshandelns zur Justizgewalt unterbrochen), wenn die Verwendung dieser Programme als forensische Software derart unverhältnismäßig gewesen wäre, dass grundsätzlich nicht angenommen werden könnte, sie wäre vom richterlichen Befehl gedeckt».

4. Ausblick

[33] Jede neue Technologie folgt einer vergleichbaren Entwicklung älterer Technologien, und verzögert dazu werden immer neue Regulative zum Schutz Betroffener geschaffen, da jede neue

47 Vgl §§ 141, 142 und 143 StPO, BGBl 631/1975 idgF.

48 Vgl §§ 37 lit j bis m KartG, BGBl I 61/2005 idgF.

49 BVwG: W134 2003810-1; ECLI:AT:BVWG:2014:W134.2003810.1.00.

50 VwGH: Ra 2014/04/0046.

Technologie entsprechend neue, für Nutzer unbekannte, nicht wahrnehmbare oder nicht steuerbare Risiken mit sich bringt. Mit der Verbreitung des Internets ist eine Normenflut einhergegangen, samt neuerdings auch Rechtsmaterialien wie die Netzwerk- und Informationssicherheitsrichtlinie, Datenschutz Grundverordnung oder der Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen[51]. Aufgrund der immer größer werdenden Bedrohungen durch Cyberkriminelle und Cyberterroristen wird an weiteren materiellrechtlichen Gesetzen gearbeitet, und es ist daher keine Frage ob, sondern wann und in welcher Form gesetzliche Regelungen für Kryptowährungen geschaffen werden.

[34] Aufgrund der in dieser Arbeit beschriebenen Umstände, als auch den speziell in Kapitel 3 beschriebenen Schwachstellen, ist aus sicherheitstechnischer Sicht der Bitcoin als mangelhaft einzustufen. Auch wenn aus politischen Gründen Kryptowährungen reguliert, oder sogar verboten werden sollten, so lassen sich zukünftige, innovative Entwicklungen dadurch nicht verhindern. Die Folgen einer Überregulierung wären nämlich die Schaffung alternativer Systeme, in anderer Form und in anderen Ländern, ohne Rechtsschutz, und damit wäre potenziellen Geschädigten auch nicht gedient.

[35] In diesem Zusammenhang ist zu betonen, dass de lege lata ausreichende Tatbestände wie im österreichischen Strafrecht definiert sind, und es weiter auch verwaltungsrechtliche und zivilrechtliche Möglichkeiten gibt, um Cyberkriminelle zu verfolgen. Problematisch ist jedoch, dass aufgrund der eingesetzten starken Kryptographie die Anonymität der Täter geschützt wird, und es daher zu erwarten ist, dass es nur in seltenen Fällen zu einer strafrechtlichen Pönalisierung kommen wird. Das Brechen dieser Kryptographie ermöglicht nämlich das Fälschen der unbaren Zahlungsmittel, hingegen ist eine De-anonymisierung nur dann möglich, wenn zusätzliche täterrelevante Daten vorhanden sind.

[36] Da es keine besondere Eigenschaft von Kryptowährungen ist, dass diese für maligne Zwecke entfremdet werden, wäre der Gesetzgeber gefordert mit Augenmaß[52] abzuwägen, welche einschränkenden Maßnahmen im Interesse aller Beteiligten sinnvoll sind, wie einer effizienteren Verfolgung von Straftätern, der effizienten Beweissicherung, und Rechtsschutz samt nötigen technischen Begleitmaßnahmen, ohne dass ein sicherer, anonymer Zahlungsverkehr dadurch verloren geht.

Dipl.-Ing. Thomas Hrdinka, Zivilingenieur, ZTH Consulting Engineering, Universität Wien, Arbeitsgruppe Rechtsinformatik, thrdinka@zth.at; http://www.zth.at.

---

5. Literatur

A. Stadler, O. Völkel: Bitcoin & Co – das neue Gold, Universität Wien, Veranstaltung (2017).

51 *VO (EU) 910/2014:* vom 28. August 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-VO).

52 *C. Piska, O. Völkel:* Blockchain und Kryptorecht – Regulierungs-Chancen de lege lata und de lege ferenda, Zeitschrift für Energie- und Technikrecht, Pedell, Linz (2017).

Adam Back: «Hashcash – A Denial of Service Counter-Measure», technical report (2002). *allinvain:* https://bitcointalk.org/index.php?topic=16457.0 gelesen 1.1.2018.

C. Piska, *O. Völkel:* Blockchain und Kryptorecht – Regulierungs-Chancen de lege lata und de lege ferenda, Zeitschrift für Energie- und Technikrecht, Pedell, Linz (2017).

Coindesk: https://www.coindesk.com/8-2-million-court-orders-default-judgment-cryptsy-ceo/ gelesen 3.1.2018.

David Chaum: Blind signatures for untraceable payments, Advances in Cryptology – Crypto «82. Springer-Verlag, 1983, S. 199–203 (1983).

D. Chaum, *A. Fiat*, *M. Naor*: Untraceable electronic cash. In Proceedings on Advances in Cryptology (Santa Barbara, California, United States). S. Goldwasser, Ed. Springer-Verlag New York, New York, S. 319–327 (1990).

DerStandard: https://derstandard.at/2000067995278/Nowotny-Regulierung-von-Krypto-Waehrungen-im-Gespraech gelesen 3.1.2018.

Deutsche Wirtschaftsnachrichten: https://deutsche-wirtschafts-nachrichten.de/2017/12/20/betrugs-verdacht-bei-bitcoin-boerse-coinbase/ gelesen 3.1.2018.

EUROPOL: SOCTA 2017, European Union Serious and Organised Crime Threat Assessment, The Hague (2017).

EZB: https://www.ecb.europa.eu/press/key/date/2017/html/ecb.sp170925_2.en.html gelesen 3.1.2018.

EZB: Virtual Currency Schemes, Europäische Zentralbank, Frankfurt (2012).

Futurezone: https://futurezone.at/digital-life/hacker-haben-schon-eine-million-bitcoin-gestohlen/299.024.231 aufgerufen 1.1.2018.

Futurezone: https://futurezone.at/netzpolitik/polizei-whatsapp-ueberwachung-ist-nicht-sinnlos/304.135.064 gelesen 3.1.2018.

G. Brassard, *P. Hoyer*, *A. Tapp*: «Quantum Algorithm for the Collision Problem». Lecture Notes in Computer Science: S. 163–169 (1997).

H. Dobbertin, *A. Bosselaers*, *B. Preneel:* RIPEMD-160: A Strengthened Version of RIPEMD, In Proceedings of FSE, LNCS 1039, S. 71–82, Springer (1996).

Handelsblatt: http://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/krypto-waehrung-bitcoin-faellt-weil-suedkorea-ihn-regulieren-will/20795162.html gelesen 3.1.2018.

Heise: https://www.heise.de/security/meldung/Bitcoin-und-Litecoin-Klau-bei-Electrum-Electron-Cash-und-Electrum-LTC-moeglich-3936813.html gelesen 9.1.2018.

IBM: https://www.ibm.com/blogs/research/2017/11/the-future-is-quantum/?utm_source=ibmqwebsite&utm_medium=web& utm_campaign=ibmq&utm_content=2050qubit
gelesen 2.1.2018.

J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, E. Felten: SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, 2015 IEEE Symposium on Security and Privacy, San Jose, S. 104–121 (2015).

J. Proos, C. Zalka: Shor's discrete logarithm quantum algorithm for elliptic curves, QIC 3, S. 317–344 (2003).

J. F. Nash: Non-cooperative games, Dissertation, Princeton (1950).

Kurier: https://kurier.at/wirtschaft/notenbankchef-nowotny-fordert-bitcoin-mehrwertsteuer/304.720.340 3.1.2018.

N. Benger, J. van de Pool, N. P. Smart, Y. Yarom: «Ooh Aah... Just a Little Bit»: A small amount of side channel can go a long way. In: Batina L., Robshaw M. (eds), Cryptographic Hardware and Embedded Systems – CHES 2014. CHES 2014. Lecture Notes in Computer Science, vol 8731. Berlin, Heidelberg, Springer (2014).

N. Szabo: Bit gold, https://unenumerated.blogspot.co.at/2005/12/bit-gold.html (2005) aufgerufen 31.12.2017.

NIST: FIPS PUB 180-4 – Secure Hash Standard (SHS), National Institute of Standards and Technology, Gaithersburg, S. 12 (2015).

NIST: FIPS 186-4 Digital Signature Standard, National Institute of Standards and Technology, Gaithersburg, S. 19 und 26 (2013).

O. Völkel: Privatrechtliche Einordnung der Erzeugung virtueller Währungen, Juli 2017, Ecolex, S. 639–641 (2017).

R.C. Merkle: «Protocols for public key cryptosystems» In: Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122–133 (1980).

United Nations: World Drug Report 2017, United Nations Office on Drugs and Crime, Vienna (2017).

Wei Dai: B-Money, http://www.weidai.com/bmoney.txt (1998) aufgerufen 31.12.2017.

World Economic Forum: The Global Risks Report 2017, 12th Edition, World Economic Forum,Geneva (2017).