Die Regulierung von Kryptowährung als verfassungsrechtliches Problem

Inauguraldissertation

zur Erlangung der Würde eines Doctor iuris der
Rechtswissenschaftlichen Fakultät der Universität Bern

vorgelegt von

Lars Ruchti
von
Homberg, BE

Die Fakultät hat diese Arbeit am 10. Dezember 2020 auf Antrag der beiden Gutachter Prof. Dr. Axel Tschentscher und Prof. Dr. Mirjam Eggen, als Dissertation angenommen.

Meiner Familie

Vorwort

Mein besonderer Dank gilt meinem Doktorvater, Prof. Dr. Axel Tschentscher, der mich während meiner Dissertation mit großer Fachkenntnis, wertvollen Anregungen und kontinuierlicher Unterstützung unermüdlich begleitet hat. Sein Engagement und seine Geduld haben diese Arbeit entscheidend geprägt und waren wichtige Stützen während meiner Forschung. Ebenso bedanke ich mich herzlich bei meiner Zweitgutachterin, Prof. Dr. Mirjam Eggen.

Sehr dankbar bin ich auch meiner Familie für den Rückhalt und die Unterstützung, die mir geholfen haben, auch in schwierigen Momenten motiviert zu bleiben. Liebe Mutter, Vater und Schwester, danke euch, dass ihr immer ein offenes Ohr für mich hattet und mir immer wieder neuen Ansporn gaben. Ohne euch wäre diese Arbeit nicht möglich gewesen.

Manuskriptschluss dieser Arbeit war am 28. Juni 2020. Judikatur und Literatur wurden bis zu diesem Zeitpunkt berücksichtigt. Die Publikation der Arbeit erfolgte Ende 2024 in Bern.

Bern, im November 2024 Lars Ruchti

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

§	Paragraf
a.A.	anderer Ansicht
Abs.	Absatz
AcP	Archiv für civilistische Praxis (Zeitschrift, Tübingen)
AML/CFT	Anti Money Laundering and Combating the Financing of Terrorism (Anti-Geldwäscherei und Anti-Terrorismusfinanzierung)
AJP	Aktuelle Juristische Praxis (Zeitschrift, Lachen)
Art.	Artikel
Aufl.	Auflage
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
Bd.	Band
BG	Bundesgesetz
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BGer	(Schweizerisches) Bundesgericht
BIZ	Bank für Internationalen Zahlungsausgleich
ca.	circa
CHF	Schweizer Franken
COM	European Commission (=Europäische Kommission [EK])
DNFBP	Designated Non-Financial Business or Profession (=bestimmte nicht-finanzintermediäre Geschäftsfelder und Tätigkeiten)
digma	digma – Zeitschrift für Datenrecht und Informationssicherheit (Zürich)
Diss.	Dissertation
DLT	Distributed Ledger Technology (*Blockchain*)
DPolBl	Deutsches Polizeiblatt (Zeitschrift, Stuttgart)
E/Erw.	Erwägung
EBA	Europäische Bankenaufsichtsbehörde
ECB	European Central Bank (=Europäische Zentralbank [EZB])
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDSB	Europäischer Datenschutzbeauftragter
EFD	Eidgenössisches Finanzdepartement
EFV	Eidgenössische Finanzverwaltung
EK	Europäische Kommission
ESTV	Eidgenössische Steuerverwaltung
et al.	et alii (= und weitere)
etc.	et cetera (= und die übrigen [Dinge])
EU-RL	Europäische Richtlinie
EUROPOL	Europäisches Polizeiamt
EuZ	Zeitschrift für Europarecht (Zürich)
EZB / ECB	Europäische Zentralbank / *European Central Bank*

f./ff.	und folgende (Seite/Seiten)
FATF	Financial Action Task Force / Groupe d'action financière (GAFI)
FIU	Financial Intelligence Unit (= Geldwäschereibekämpfungsfachstelle)
Fn.	Fussnote
FS	Festschrift
h.L.	herrschende Lehre
h.M.	herrschende Meinung
Harv. L. Rev.	Harvard Law Review (Cambridge MA)
Hrsg.	Herausgeberin / Herausgeber
i.e.S.	im engeren Sinne
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinne
J. Marshall J. Info. Tech. & Privacy L.	The John Marshall Journal of Information Technology & Privacy Law (Chicago)
JKP	Jurnal Keuangan dan Perbankan (Zeitschrift, Merdeka Malang)
IMF	International Monetary Fund (= Internationaler Währungsfond [IWF])
JEP	Journal of Economic Perspectives (Pittsburgh)
jM	juris – Die Monatszeitschrift (Saarbrücken)
jusletter.ch	Jusletter (Zeitschrift, Bern)
KGGT	Koordinationsgruppe zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung
Komm.	Kommentar
lat.	lateinisch
lit.	litera (= Buchstabe)
m.E.	meines Erachtens
MHS	multilaterales Handelssystem
MROS	Money Laundering Reporting Office Switzerland (Geldwäschereibekämpfungsfachstelle der Schweiz)
NJW	Neue Juristische Wochenschrift (München/Frankfurt a.M.)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (München/Frankfurt a.M.)
n.Chr.	nach Christus
OR	BG vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht, SR 220)
P2P	*Peer-to-Peer* (= von Person zu Person)
plädoyer	plädoyer – Magazin für Recht und Politik (Bern)
Pra	Die Praxis des Schweizerischen Bundesgerichts (Zürich)
recht	recht – Zeitschrift für juristische Weiterbildung und Praxis (Bern)
Rn.	Randnummer(n)
Rs.	Rechtssache
Rz.	Randziffer(n)

SJZ	Schweizerische Juristenzeitung; Schweizerische Juristen-Zeitung (Zürich)
SNB	Schweizerische Nationalbank
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht (Zürich; bis 1989 SAG)
usw.	und so weiter
vgl.	vergleiche
VSB	Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken
WZG	BG über die Währung und die Zahlungsmittel vom 22. Dezember 1999 (SR 941.10)
z.B.	zum Beispiel
ZBl	Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht (Zürich; früher: Schweizerisches Zentralblatt für Staats- und Gemeindeverwaltung)
zit.	zitiert
ZSR	Zeitschrift für Schweizerisches Recht (Basel)
ZWF	Zeitschrift für Wirtschafts- und Finanzstrafrecht (Wien)

Literaturverzeichnis

AEPPLI ROLAND/BOHNER CHRISTIAN/FÖLLMI TONI (Hrsg.), 75 Jahre Schweizerische Nationalbank: Die Zeit von 1957 bis 1982, FS Nationalbank, Zürich 1982.

ARISTOTELES, Die Nikomachische Ethik, V. Buch, Übersetzung in: GIGON OLOF, Aristoteles. Die Nikomachische Ethik, 5. Aufl., München 2002.

AUER ANDREAS/MALINVERNI GIORGIO/HOTTELIER MICHEL, Droit constitutionnel suisse. Les droits fondamentaux, Bd. II, 3. Aufl., Bern 2013.

AUFFENBERG LUTZ, Bitcoins als Rechnungseinheiten, in: NVwZ 2015, 1184-1188.

BARTONE ROBERTO, Abschaffung des Bargelds? Eine Problemskizze, in: jM 2016, 285-289.

BÄRTSCHI HARALD/MEISSER CHRISTIAN, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Weber Rolf/Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015.

BALTENSPERGER ERNST, Währungsstabilität als Ausdruck gesellschaftlicher Verantwortung. Zentralbankbindung über Verfassungs- und Gesetzesnormen, in: Bagus Philipp/Schwarz Gerhard (Hrsg.), Die Entstaatlichung des Geldes, Zürich 2014.

BÄUERLE MICHAEL, Vertragsfreiheit und Grundgesetz. Normativität und Faktizität individueller Vertragsfreiheit in verfassungsrechtlicher Perspektive, Baden-Baden 2001.

BENES JAROMIR/KUMHOF MICHAEL, The Chicago Plan Revisited, 2012. [erhältlich unter: http://www.ingannati.it/wp-content/uploads/2012/11/Chicago-Plan-Revisited-moneta-di-stato.pdf].

BLOCH JÜRG/GÜTLING NICOLE, GwG-Meldepflichten. Quo vadis? in: SJZ 2018, 565-571.

BÖHME RAINER/CHRISTIN NICOLAS/EDELMAN BENJAMIN/MOORE TYLOR, Bitcoin. Economics, Technology, and Governance, in: JEP 2015, 213-238.

BOLT WILKO/VAN OORDT MARTEEN, On the value of Virtual Currencies, 2016. [erhältlich unter: http://publications.gc.ca/collections/collection_2014/banque-bank-canada/FB3-2-103-12-eng.pdf].

BRANDEIS LOUIS D./WARREN SAMUEL D., The Right To Privacy, in: Harv. L. Rev. 1890, 193-220.

BRITO JERRY, The Case for Electronic Cash. Why Private Peer-to-Peer Payments are Essential to an Open Society, 2019. [erhältlich unter: https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf].

BRITO JERRY/SHADAB HOUMAN/CASTILLO ANDREA, Bitcoin Financial Regulation. Securities, Derivatives, Prediction Markets, and Gambling, in: Colum. Sci. & Tech. L. Rev. 2014, 144-221.

BRUNNER KARL, Konzepte der Geldordnung in einer freiheitlichen Wirtschaftsordnung, in: J. Starbatty/K. Brunner (Hrsg.), Geldordnung und Geldpolitik in einer freiheitlichen Gesellschaft, Tübingen 1982, 7-17.

BULL HANS PETER, Zweifelsfragen um die informationelle Selbstbestimmung. Datenschutz als Datenaskese?, in: NJW 2006, 1617-1624.

BÜLTE JENS, Das neue deutsche Geldwäschegesetz 2017, in: ZWF 2018, 49-54.

BURKHARDT PETER/HÖSLI ANDREAS, Neue strafrechtliche Risiken für Händler bei Barzahlungen über CHF 100'000.-, in: jusletter.ch vom 1. Feb. 2016.

CLAEYS GRÉGORY/DEMERTZIS MARIA/EFSTATHIOU KONSTANTINOS, Cryptocurrencies and monetary policy, 2018. [erhältlich unter: https://www.europarl.europa.eu/cmsdata/150000/BRUEGEL_FINAL%20publication.pdf]

CONTRATTO FRANCA, Sanktionen. Neue Gretchenfrage im Ringen um den Marktzugang in die EU?, SZW 2018, 653-666.

COOK JOSEPH R., Bitcoins. Technological Innovation or Emerging Threat?, in: J. Marshall J. Info. Tech. & Privacy L. 30 (2014), 535-570.

VON DER CRONE HANS-CASPAR/KESSLER FRANZ J./ANGSTMANN LUCA, Token in der Blockchain. Privatrechtliche Aspekte der Distributed Ledger Technologie, in: SJZ 2018, 337-345.

DIETZ RAIMUND, Tausch und Geld. Zur Entstehung der Geldwirtschaft als Ordnung, in: Cassel Dieter (Hrsg.), Entstehung und Wettbewerb von Systemen, Berlin 1996, 45-80.

DITTRICH LARS, Die Bedeutung des Rechts für die Stabilität des Geldes, Tübingen 2016.

EGGEN MIRJAM, Verträge über digitale Währungen, in: jusletter.ch vom 4. Dez. 2017

– Was ist ein Token? Eine privatrechtliche Auslegeordnung, in: AJP 2018, 558-567.

EHRENZELLER BERNHARD/SCHINDLER BENJAMIN/SCHWEIZER RAINER J. (Hrsg.), Die Schweizerische Bundesverfassung. St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014.

EMCH URS/RENZ HUGO/ARPAGAUS RETO, Das Schweizerische Bankgeschäft, 7. Aufl., Zürich 2011.

ENZ BENJAMIN, Die zivilrechtliche Einordnung von Zahlungs-Token wie dem Bitcoin als «Registerwertdaten» und deren Aussonderbarkeit im Konkurs de lege lata und de lege ferenda, in: SJZ 2020, 291-298.

ESSEBIER JANA/BOURGEOIS JANIQUE, Die Regulierung von ICOs, in: AJP 2018, 568-579.

GELLERI CHRISTIAN, Theorie und Praxis des Regiogeldes, in: Weis Mathias/Spitzeck Heiko (Hrsg.), Der Geldkomplex. Kritische Reflexion unseres Geldsystems und mögliche Zukunftsszenarien, Bern/Stuttgart/Wien 2008.

GESELL SILVIO, Die natürliche Wirtschaftsordnung, 8. Aufl., Bern 1938.

GLESS SABINE/KUGLER PETER/STAGNO DARIO, Was ist Geld? Und warum schützt man es? Zum strafrechtlichen Schutz von virtuellen Währungen am Beispiel von Bitcoins, in: recht 2015, 82-97.

GOLDMANN ZACHARY K. /MARUYAMA ELLIE/ROSENBERG ELIZABETH/ SARAVALLE EDOARDO/ SOLOMON-STRAUSS JULIA, Terrorist use of Virtual Currencies. Containing the Potential Threat, 2017. [erhältlich unter: <https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies>]

GRAHAM-SIEGENTHALER BARBARA/FURRER ANDREAS, The Position of Blockchain Technology and Bitcoin in Swiss Law, in: jusletter.ch vom 8. Mai 2017.

GROßE JONAS, Nutzerverfolgung via Blockchain. Die Implikationen der öffentlich einsehbaren Transaktionshistorie von Bitcoin auf die Privatsphäre der Nutzer, digma 2018, 18-22.

HAMID F. AHMAD/TALIB AMEEN, A note on Bitcoin's price volatility, in: JKP 2019, 376-384.

VON HAYEK FRIEDRICH A., Entnationalisierung des Geldes, in: Bosch Alfred/Veit Reinhold (†)/Veit-Bachmann Verena (Hrsg.), Schriften zur Währungspolitik und Währungsordnung, Tübingen 2011, 129-254.

HEIM KATHRIN, VSB 2016. Praxiskommentar zur Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken, 3. Aufl., Zürich 2016.

HELFERRICH KARL, Das Geld, 6. Aufl., Leipzig 1923.

HERRMANN CHRISTOPH, Währungshoheit, Währungsverfassung und subjektive Rechte, Tübingen 2010.

HOFERT EDUARD, Regulierung der Blockchain, Diss. Hamburg, Tübingen 2018.

HUMMLER KONRAD, Das schweizerische Bankgeheimnis. Eine Grundrechtsfrage, in: Hummler Konrad/Schwarz Gerhard (Hrsg.), Das Recht auf sich selbst. Bedrohte Privatsphäre im Spannungsfeld zwischen Sicherheit und Freiheit, Zürich 2003, 175-188.

KLEIN FRITZ/SPREMANN KLAUS, Telegeld. Electronic Money, Smart Cards und E-Commerce werden Realität, Zürich 1998.

KLEMUSCH HOLGER, Hackerwährung oder virtuelles Zahlungsmittel. Lösungsansätze für ein neues polizeiliches Problem, in: DPolBl 2013, 19-23.

JOHNSON M. ERIC/MCGUIRE DAN/WILLEY NICHOLAS, The Evolution of the Peer-to-Peer Sharing Industry and the Security Risks for Users, 2008. [erhältlich unter: https://www.researchgate.net/publication/221179348_The_Evolution_of_the_Peer-to-Peer_File_Sharing_Industry_and_the_Security_Risks_for_Users]

JUNOD CHARLES-ANDRÉ, Art. 38 BV (Juni 1988), in: Aubert Jean-François/Koller Heinrich (Hrsg.), Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft vom 29. Mai 1978, Bd. III, Basel, Loseblatt.

KELLER CLAUDIA/HESS MARTIN, Rechtliche Anforderungen an System- und Datensicherheit und Compliance, in: Weber Rolf/Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 181-205.

KLAUSER PETER, Das schweizerische Bankgeheimnis und die Bekämpfung der Geldwäscherei, in: Quartalsheft SNB 4/95, Zürich 1995, 361-370.

KNAPP GEORG FRIEDRICH, Staatliche Theorie des Geldes, 3. Aufl., München 1921.

KUNZ PETER V./JUTZI THOMAS/SCHÄREN SIMON (Hrsg.), Geldwäschereigesetz (GwG). Bundesgesetz vom 10 Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Stämpflis Handkommentar, Bern 2017.

LASTRA ROSA M./ALLEN JASON G., Virtual currencies in the Eurosystem. Challenges ahead, 2018. [erhältlich unter: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619020/IPOL_STU(2018)619020_EN.pdf]

LECHNER HANS, Währungspolitik, Berlin/New York 1988.

LUHMANN NIKLAS, Die Wirtschaft der Gesellschaft, Frankfurt a.M. 1994.

LUTHER WILLIAM J., Regulating Bitcoin. On What Grounds?, in: H. PEIRCE/B. KLUTSEY (Hrsg.), Reframing Financial Regulation. Enhancing Stability and Protecting Consumers, Airlington: George Mason University 2016, 391-415.

MARTI HANS, Die Wirtschaftsfreiheit der schweizerischen Bundesverfassung, Basel 1976.

MATHYS ROLAND, Was bedeutet Big Data für die Qualifikation als besonders schützenswerte Personendaten? Das Beispiel der Gesundheitsdaten, in: jusletter.ch vom 21. Mai 2015.

MAURER-LAMBROU URS/BLECHTA GABOR P. (Hrsg.), Datenschutzgesetz, Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

MEISSER LUZIUS, Kryptowährung. Geschichte, Funktionsweise, Potential, in: R. Weber/F. Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015.

MENGER CARL, Geld, in: von Hayek Friedrich August (Hrsg.), Carl Menger. Gesammelte Werke, Bd. IV, Schriften über Geld und Währungspolitik, 2. Aufl., Tübingen 1970, 1-116.

MÜLLER LUKAS/REUTLINGER MILENA/KAISER PHILIPPE, Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union, in: EuZ 2018, 80-102.

MÜLLER JÖRG-PAUL/SCHEFER MARKUS, Grundrechte in der Schweiz. Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Aufl., Bern 2008.

NAKAMOTO SATOSHI, Bitcoin. A Peer-to-Peer Electronic Cash System, 2008. [erhältlich unter: https://bitcoin.org/bitcoin.pdf]

NIEDOBITEK MATTHIAS, Art. 37 Nr. 4 GG (Mai 2001), in: Waldhoff Christian/Vogel Klaus (Hrsg.), Bonner Kommentar zum Grundgesetz, Heidelberg, Loseblatt.

NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Strafrecht II, Basler Kommentar, 4. Aufl., Basel 2019.

NOBEL PETER, Gold und Geist, in: Furrer Jürg/Gehrig Bruno (Hrsg.), Aspekte der schweizerischen Wirtschaftspolitik, FS Jaeger, Chur/Zürich 2001, 295-307.

– Goldfieber, in: Ehrenzeller Bernhard/Mastronardi Philippe/Schaffhauser Rene/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Der Verfassungsstaat vor neuen Herausforderungen, FS Hangartner, St. Gallen/Lachen SZ 1998, 845-864.

NOBEL PETER, Zum Fall Wegelin, in: SZW 2013, 529-535.

NORTH MICHAEL, Das Geld und seine Geschichte. Vom Mittelalter bis zur Gegenwart, München 1994.

NUSSBAUM ARTHUR, Das Geld in Theorie und Praxis des deutschen und ausländischen Rechts, Tübingen 1925.

OHLER CHRISTOPH, Die hoheitlichen Grundlagen der Geldordnung, in: JZ 2008, 317-324.

PROCTOR CHARLES, Mann on the Legal Aspects of Money, 7. Aufl., Oxford: Oxford University Press 2012.

PROGRIN-THEUERKAUF SARAH/ZOETEWEIJ-TURHAN MARGARITE/TURHAN OZAN, Interoperabilität der Informationssysteme im Migrationsbereich. Digitale Grenzkontrollen 2019, in: Achermann Alberto/Boillet Véronique/Caroni Martina/Epiney Astrid/Künzli Jürg et al. (Hrsg.), Jahrbuch für Migrationsrecht 2018/2019, Bern 2019, 3-41.

RAHN RICHARD W., The Case for Financial Privacy, in: Hummler Konrad/Schwarz Gerhard (Hrsg.), Das Recht auf sich selbst. Bedrohte Privatsphäre im Spannungsfeld zwischen Sicherheit und Freiheit, Zürich 2003, 167-174.

RAMELET NICOLAS, Geldwäschereibekämpfung bei Barzahlungsgeschäften. Staatliche Sterbehilfe für das Bargeld? in: SZW 2016, 76-83.

RHINOW RENÉ, Art. 31^{quinquies} BV (Februar 1991), in: Aubert Jean-François/Koller Heinrich (Hrsg.), Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft vom 29. Mai 1978, Bd. II, Basel, Loseblatt.

RHINOW RÉNÉ/SCHMID GERHARD/BIAGGINI GIOVANNI/UHLMANN FELIX, Öffentliches Wirtschaftsrecht, 2. Aufl., Basel 2011.

SÁINZ DE VICUÑA ANTONIO, An Institutional Theory of Money, in: Giovanoli Mario/Devos Diego (Hrsg.), International Monetary and Financial Law. The Global Crisis, New York: Oxford University Press 2010, 517-532.

SAMM CARL-THEODOR, »Geld« und »Währung«. Begrifflich und mit Blick auf den Vertrag von Maastricht, in: Weber Albrecht (Hrsg.), Währung und Wirtschaft. Das Geld im Recht, FS Hahn, Baden-Baden 1997, 227-244.

VON SAVIGNY FRIEDRICH CARL, Das Obligationenrecht als Teil des heutigen Römischen Rechts, Bd. I, Aalen 1851.

SCHAR-SCHUPPISSER MARKUS, Standardwerteinheit, Währung, Geld, Genf 1989.

SCHEFER MARKUS, Kerngehalte von Grundrechten. Geltung, Dogmatik, inhaltliche Ausgestaltung, Bern 2001.

SCHMALZ ANNA-LISA, Komplementärwährungen zur Förderung der regionalen Wirtschaft in Städten und Gemeinden, 2013. [erhältlich unter: https://monneta.org/wp-content/uploads/2015/04/KommunaleWaehrungen-24.07.2013.pdf].

SCHMID JEAN-DANIEL/SCHMID ALEXANDER, Bitcoin. Eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, in: jusletter.ch vom 4. Jun. 2012.

SCHMIDT REINER, Geld und Währung, in: Isensee Josef/Kirchhof Paul (Hrsg.), Handbuch des Staatsrechts, Bd. III, Das Handeln des Staates, Heidelberg 1988, 1121-1139.

SCOTT BRETT, How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?, 2016. [erhältlich unter: https://www.econstor.eu/handle/10419/148750].

SIMITIS SPIROS, Bemerkungen zur rechtlichen Sonderstellung des Geldes, in: AcP 159 (1960/1961), 406-466.

VON SPINDLER JOACHIM/BECKER ERNST/STARKE ERNST, Die Deutsche Bundesbank, 4. Aufl., Stuttgart 1973.

SUHR DIETER, Die Geldordnung aus verfassungsrechtlicher Sicht, in: Starbatty Joachim (Hrsg.), Geldordnung und Geldpolitik in einer freiheitlichen Gesellschaft, Tübingen 1982.

– Geld ohne Mehrwehrt. Entlastung der Marktwirtschaft von monetären Transaktionskosten, Frankfurt a.M. 1983.

THELESKLAF DANIEL/WYSS RALPH/VAN THIEL MARK/ORDOLLI STILIANO (Hrsg.), GwG Kommentar. Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, 3. Aufl., Zürich 2019.

TRAN MUOI/BENTOV IDDO/LUU LOI/SAXENA PRATEEK/KANG MIN S., OBSCURO. A Bitcoin mixer using Trusted Execution Environments, 2017. [erhältlich unter: https://eprint.iacr.org/2017/974.pdf].

VISCHER FRANK, Geld- und Währungsrecht. Im nationalen und internationalen Kontext, Basel 2010.

VOGEL MARION, Relevanz et Risiken von virtuellen Währungen am Beispiel von Bitcoin, Hof 2016.

WALDMANN BERNHARD/BELSER EVA MARIA/EPINEY ASTRID (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015.

WEBER ROLF H., E-Commerce und Recht, 2. Aufl., Zürich 2010.

– Elektronisches Geld. Erscheinungsformen und rechtlicher Problemaufriss, Zürich 1999.

WEBER ROLF H./BAUMANN SIMONE, FinTech – Schweizer Finanzmarktregulierung im Lichte disruptiver Technologien. Regulierungsansätze für neue Finanzdienstleistungstechnologien, in: jusletter.ch vom 21. Sep. 2015.

WOLF BURKHARD, Vertragsfreiheit. Das verkannte Verfassungsrecht, in: AJP 2012, 8-11.

ZELLWEGER-GUTKNECHT CORINNE, Digitale Landeswährung. Ein Überblick, in: jusletter.ch vom 31. Okt. 2016.

ZUBERBÜHLER DANIEL, Banken als Hilfspolizisten zur Verhinderung der Geldwäscherei? Sicht eines Bankaufsehers, in: Pieth Mark (Hrsg.), Bekämpfung der Geldwäscherei. Modelfall Schweiz?, Basel/Frankfurt a.M. 1992, 31-66.

ZULAUF URS, Automatischer Informationsaustausch. Das Ende des steuerlichen Bankgeheimnis?, in: SZW 2018, 667-683.

(Sämtliche URLs wurden zuletzt am 22. Mai 2020 besucht.)

Materialienverzeichnis

Schweiz

Bericht des Bundesrats an die Bundesversammlung vom 21. April 1950 über das Volksbegehren betreffend Revision von Art. 39 BV (Freigeldinitiative), BBl 1950 I 893.

Bericht des Bundesrates vom 25. Jun. 2014 zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3678) und Weibel (13.4070).

Botschaft vom 10. Januar 1973 betreffend Änderung der Art. 31^{quinquies} und 32 Abs. 1 der Bundesverfassung (Konjunkturpolitik), BBl 1973 I 117.

Botschaft vom 17. Juni 1996 zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG), BBl 1996 1101.

Botschaft vom 17. März 1997 über die Revision des Nationalbankgesetzes, BBl 1997 II 977.

Botschaft vom 27. Mai 1998 über einen neuen Geld- und Währungsartikel in der Bundesverfassung, BBl 1998 IV 4007.

Botschaft vom 7. Dezember 2007 betreffend die Ratifikation eines Übereinkommens und der Änderung eines Übereinkommens sowie Beitritt zu zwei Änderungsprotokollen der UNO zur Bekämpfung terroristischer Handlungen gegen die nukleare und maritime Sicherheit, BBl 2008 1153.

Botschaft vom 20. November 2013 zur Volksinitiative «Rettet unser Schweizer Gold (Gold-Initiative)», BBl 2013 9329.

Botschaft vom 13. Dezember 2013 zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière [GAFI]), BBl 2014 605.

Botschaft vom 9. November 2016 zur Volksinitiative «Für krisensicheres Geld: Geldschöpfung allein durch die Nationalbank! (Vollgeld-Initiative)», BBl 2016 8475.

Botschaft vom 23. November 2016 zur Genehmigung der multilateralen Vereinbarung der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten und zu ihrer Umsetzung (Bundesgesetz über den internationalen automatischen Informationsaustausch in Steuersachen), BBl 2015 5437.

Botschaft vom 14. Sep. 2018 zur Genehmigung des Übereinkommens des Europarats vom 16.5.2005 zur Verhütung des Terrorismus mit dem dazugehörigem Zusatzprotokoll und Verstärkung des strafrechtlichen Instrumentariums gegen Terrorismus und organisierte Kriminalität, BBl 2018 6427.

Bundesrat, Rechtliche Grundlagen der Distributed Ledger Technologie und Blockchain in der Schweiz. Eine Auslegeordnung mit Fokus auf den Finanzsektor, 2018.

Bundesratsbeschluss vom 29. Juni 1954 betreffend den gesetzlichen Kurs der Banknoten und die Aufhebungen ihrer Einlösung in Gold (SR 951.171).

Eidgenössische Finanzmarktaufsicht, Aufsichtsmitteilung 02/2019. Zahlungsverkehr auf der Blockchain, 2019.

Eidgenössische Finanzmarktaufsicht, FINMA-Rundschreiben 2011/1, Tätigkeit als Finanzintermediär nach GwG. Ausführungen zur Geldwäschereiverordnung (GwV).

Eidgenössische Finanzmarktaufsicht, Wegleitung für Unterstellungsfragen betreffend Initial Coin Offerings (ICOs), 2018.

Eidgenössische Finanzverwaltung, Praxis der Kontrollstelle für die Bekämpfung der Geldwäscherei zu Art. 2 Abs. 3 GwG. Der Geltungsbereich des Geldwäschereigesetzes im Nichtbankensektor (Unterstellungskommentar KSt).

Eidgenössisches Finanzdepartement, Finanzplatz und Finanzmarktpolitik Schweiz, 2006.

Koordinationsgruppe zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung, National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding, 2018.

Nachrichtendienst des Bundes, Prophylax, 2015.

EU

Europäische Bankenaufsichtsbehörde (EBA), Opinion on 'virtual currencies', 2014. [erhältlich unter: https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1].

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament und den Rat. Ein Aktionsplan für ein intensiveres Vorgehen gegen Terrorismusfinanzierung, COM/2016/50 final.

Europäische Kommission, Vorschlag für eine Richtlinie des europäischen Parlamentes und des 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/2016/450 final.

Europäische Kommission, Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 767/2008, der Verordnung (EG) Nr. 810/2009, der Verordnung (EU) 2017/2226, der Verordnung (EU) 2016/399, der Verordnung (EU) 2018/XX [Interoperabilitäts-Verordnung] und der Entscheidung 2004/512/EG sowie zur Aufhebung des Beschlusses 2008/633/JI des Rates, COM/2018/302 final.

Europäische Zentralbank (EZB), Letter vom 16. Dez. 2019 from Yves Mersch, Member of the Executive Board of the European Central Bank (ECB), to Maria Elisabetta Alberti Casellati, President of the Senate of the Italian Republic, Roberto Fico, President of the Italian Chamber of Deputies, and Roberto Gualtieri, Italian Minister for Economy and Finance, requesting that the ECB be consulted on the legislation setting out a new threshold for cash payments.

Europäische Zentralbank (EZB), Virtual currency schemes, 2012. [erhältlich unter: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrency-schemes201210en.pdf].

Europäischer Datenschutzbeauftragter (EDSB), Stellungnahme des EDSB zu einem Vorschlag der Kommission zur Änderung der Richtlinie (EU) 2015/849 und der Richtlinie 2009/101/EG. Zugang zu Informationen über den wirtschaftlichen Eigentümer und Implikationen für den Datenschutz, 2017.

Europäisches Polizeiamt (EUROPOL), EU Drug Market Report. In-depth Analysis, 2016. [erhältlich unter: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TD0216072:EN:HTML].

International

Committee on Payments and Market (BIZ), Digital currencies, Basel 2015.

Financial Action Task Force, Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, FATF Guidance, 2013.

Financial Action Task Force, FATF Guidance on Counter Proliferation Financing. The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, 2018.

Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations, 2012.

Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations, 2018.

Financial Action Task Force, Virtual Assets and Virtual Asset Service Providers. Guidance for a Risk-Based Approach, 2019.

Financial Action Task Force, Virtual Currencies. Guidance for a Risk-based Approach, 2015.

Financial Action Task Force, Virtual Currencies. Key Definitions and Potential AML/CFT Risks, 2014.

Erlassverzeichnis

Schweiz

ABÜ	Übereinkommen vom 17. Dezember 1997 über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr, für die Schweiz in Kraft getreten am: 30. Juli 2000 (SR 0.311.21).
AHÜ	Übereinkommen vom 25. März 1988 über die gegenseitige Amtshilfe in Steuersachen, für die Schweiz in Kraft getreten am: 1. Januar 2017, Amtshilfeübereinkommen (SR 0.652.1).
AKÜ	Übereinkommen vom 31. Oktober 2003 der Vereinten Nationen gegen Korruption, für die Schweiz in Kraft getreten am: 24. Oktober 2009 (SR 9.311.56).
ATFÜ	Internationales Übereinkommen vom 9.12.1999 zur Bekämpfung der Finanzierung des Terrorismus, für die Schweiz in Kraft getreten am 23.10.2003 (SR 0.353.22).
BGS	Bundesgesetz vom 29. Sep. 2017 über Geldspiele, Geldspielgesetz (SR 953.51).
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101).
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz, Datenschutzgesetz (SR 235.1).
MVStI	Multilaterale Vereinbarung vom 29. Oktober 2014 der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten, in Kraft getreten am: 1. Januar 2017 (SR 0.653.1).
StAhiG	Bundesgesetz vom 28 September 2012 über die internationale Amtshilfe in Steuersachen, Steueramtshilfegesetz (SR 651.1).
VStG	Bundesgesetz vom 13. Okt. 1965 über die Verrechnungssteuer, Verrechnungssteuergesetz (SR 642.21).
KGBV	Verordnung vom 11. Februar 2009 über Kontrolle des grenzüberschreitenden Barmittelverkehrs (SR 631.052)
KNVA	Abkommen vom 6. September 1978 zwischen der Schweizerischen Eidgenossenschaft und der internationalen Atomenergieorganisation über die Anwendung von Sicherungsmassnahmen im Rahmen des Vertrages über die Nichtverbreitung von Kernwaffen, für die Schweiz in Kraft getreten am 6. Sep. 1978 (SR 0.515.031).

EU

EGeld-RL Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16.09.2009 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.

4.AMLR 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 (vierte Geldwäsche Richtlinie).

5.AMLR Richtlinie (EU) 2018/843 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 (fünfte Geldwäsche Richtlinie).

BMVo Verordnung (EG) Nr. 1889/2005 des Europäischen Parlaments und des Rates vom 26. Oktober 2005 über die Überwachung von Barmitteln, die in die Gemeinschaft oder aus der Gemeinschaft verbracht werden.

SISVo Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28.11.2019 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006

International

UN-A-61/86 Resolution der UN-Generalversammlung vom 6. Dez. 2006 (Measures to prevent terrorists from acquiring weapons of mass destruction, A/RES/61/86).

UN-S-2178 Resolutionen des UN-Sicherheitsrats vom 24.9.2014 (S/RES/2178)

UN-S-2462 Resolutionen des UN-Sicherheitsrats vom 28.3.2019 (S/RES/2462)

Einleitung

Fragestellung

Die *erste Kryptowährung, Bitcoin*, wurde vor dem Hintergrund der Finanz- und Bankenkrise kreiert, um ein *von Regierungen sowie Banken unabhängiges Zahlungsmittel* zu schaffen, welches allein durch seine Benutzer betrieben werden könnte. Dementsprechend zeichnen sich Kryptowährungen aus, dass die Zahlungsverarbeitung nicht von im Voraus bekannten, zentralisierten Einrichtungen, wie beispielsweise Banken, vorgenommen wird, sondern von einem grundsätzlich offenen sowie allenfalls persönlich unbekannten Kreis von Personen (sogenannte ‹*Miners*›). Kryptowährungen werden deshalb auch als *dezentralisierte Zahlungsmittel* bezeichnet. Die dabei mitschwingende Frage, wie Vertrauen in ein Zahlungsmittel hergestellt werden kann, welches keine verantwortlichen Personen oder sonstige Garantien kennt, lösen Kryptowährungen – nomen est omen – durch den Einsatz von Kryptographie. Mithilfe der *Kryptographie wird sichergestellt, dass Zahlungen nicht manipuliert* und beispielweise an andere Empfänger geleitet werden, und zudem wird auch verhindert, dass Guthaben zweimal gültig ausgegeben werden kann.[1]

Kryptowährungen bestehen aus einer elektronischen Aufzeichnung der Werteinheiten auf einer *spezifisch dafür geschaffenen Datenbank (‹Blockchain›)*. Sie sind vom Buchgeld in staatlicher Währung sowie von elektronischen Transaktionen mit solchem Buchgeld zu unterscheiden. Zunächst stellen *Kryptowährungen eigene Rechnungseinheiten mit eigenem Währungszeichen dar* (beispielsweise BTC). Ferner setzen Kryptowährungen keine Banken zur Verwahrung voraus, sondern können *selbst in elektronischen Geldbörsen – sogenannten ‹Wallets› – aufbewahrt werden*, welche bereits auf einem Smartphone installiert werden können. Darüber hinaus stellen Transaktionen mit Kryptowährung *finale Transaktionen bzw. push-value Vorgänge* dar, d.h. der Empfänger erhält – mit Abschluss des Bezahlvorgangs – unmittelbar den transferierten Wert. Elektronische Transaktionen in staatlicher Währung gelten demgegenüber als pull value Vorgänge, weil keine Vermögensverschiebung an sich bewirkt wird, sondern lediglich einen Berechtigungsnachweis übertragen wird, welcher die Abbuchung eines bestimmten Betrags vom Konto des Absenders gestattet. Insofern weisen Kryptowährungen grössere Ähnlichkeiten mit dem Bargeld auf, welches ebenfalls durch Übergabe die Vermögensverschiebung bewirkt.

---

1 Zum ganzen Absatz siehe S. NAKAMOTO, Bitcoin. A peer-to-peer electronic cash system, 2008, 1 ff., Bitcoin wird dort als elektronisches Zahlungsmittel, welches auf kryptographischem Beweis *statt* Vertrauen basiert, bezeichnet.

Im Unterschied zu Bargeld können Kryptowährungen jedoch einfach und sicher weltweit transferiert werden und eröffnen daher viele *Vorteile sowohl für Privatpersonen wie auch Gewerbetreibende*. Transaktionen mit Kryptowährungen sind nicht nur *schneller und meist günstiger als konventionelle elektronische Überweisungen, sondern schützen auch die Privatsphäre besser*. Darüber hinaus bieten Kryptowährungen als eigenständige Rechnungseinheiten ohne Verbindung zu einer staatlichen Währung *Schutz vor Inflation, Negativzinsen oder sogar einer Währungsreform*.

Als Vermögenswerte sind Kryptowährungen demgegenüber dem grundsätzlichen Risiko des *Missbrauchs für Geldwäscherei, Terrorismusfinanzierung und Steuerhinterziehung* sowie weiteren Delikten ausgesetzt (Proliferation von Massenvernichtungswaffen und Bestechungs- bzw. Korruptionsdelikte). Darüber hinaus eröffnen Kryptowährungen als dezentral operierende Systeme *neuartige Gefährdungslagen*. Insbesondere sind konventionelle Regulierungsansätze, welche auf der *Inpflichtnahme der Finanzintermediäre (v.a. Banken und Zahlungsdienstleister) als «Hilfspolizisten» zur Überwachung des Zahlungsverkehrs und als Gatekeepers beruhen, nicht sachgerecht*.[2] Einerseits kann in Kryptowährung-Systemen *niemand Einfluss auf die Gültigkeit* einzelner Transaktionen ausüben – selbst wenn beispielsweise ein Terrorismusfinanzierungsgeschäft eindeutig vorläge. Andererseits lässt sich der *Zugang zu Kryptowährungen nicht ohne massive Eingriffe in den Internetverkehr an sich kontrollieren*. Die Bedeutung der Funktion der Finanzintermediäre als Gatekeepers ist daher bei Kryptowährungen gegenüber dem konventionellen elektronischen Zahlungsverkehr zumindest reduziert.

Das spezifische Risiko von Kryptowährungen für Geldwäscherei, Terrorismusfinanzierung usw. ergibt sich ferner aufgrund der hohen *Mobilität von Kryptogelder*. Sie können nicht nur *weltweit zur Bezahlung von Waren und Dienstleistungen verwendet werden, sondern auch auf Internetbörsen eingesetzt oder umgetauscht sowie in Kreditguthaben, Geschenkkarten oder zur Gewährung von Krediten investiert* werden. Dadurch kann die Rückverfolgbarkeit (sogenannter ‹Paper Trail›) einzelner Werteinheiten entscheidend erschwert werden. Sodann *bieten gewisse Kryptowährungen (unter anderem Monero) einen darüberhinausgehenden Schutz vor Rückverfolgung, indem das Transaktionsregister und die einzelnen Zahlungsadressen vor jeglicher Einsichtnahme Dritter geschützt sind (Obfuskation)* sowie spezielle Vorkehrungen implementiert sind, welche das

---

2 Dazu siehe D. ZUBERBÜHLER, Banken als Hilfspolizisten zur Verhinderung der Geldwäscherei? Sicht eines Bankaufsehers, in: M. Pieth (Hrsg.), Bekämpfung der Geldwäscherei. Modellfall Schweiz, 1992, 29-66 (29 ff.); P. KLAUSER, Das schweizerische Bankgeheimnis und die Bekämpfung der Geldwäscherei, Quartalsheft SNB 4/95, Basel/Frankfurt a.M. 1995, 1 ff.

Netzwerk vor noch intensiveren Überwachungsmethoden (Netzwerkaufklärung) schützen.

Schlussendlich geht von Kryptowährungen ein – zumindest theoretisches – Risiko aus, dass es zu einer *Verdrängung der staatlichen Währung als Zahlungsmittel* kommt und demzufolge die *Effektivität währungspolitischer Massnahmen* im Bereich der Geldmengensteuerung beeinträchtigt würde und so die Gewinnaussichten der Nationalbank aufgrund des entgangenen *Münzgewinns bzw. Seigniorage schmälerte*.

Die vorliegende Arbeit widmet sich dem Spannungsverhältnis zwischen dem Nutzen von Kryptowährungen sowie ihren Risiken im Bereich von Geldwäscherei, Terrorismusfinanzierung usw. Der *Fokus der Arbeit liegt auf dem Benutzer bzw. auf dem privaten Umgang mit Kryptowährung*. Dies entspricht der Konzeption von Kryptowährung als von Banken und Regierungen unabhängiges, dezentralisiertes Geld. Regulierungen im Geldwäschereirecht haben, ohne dass sie unmittelbare Normadressaten darstellten, direkte Auswirkungen auf die Rechtspositionen der Benutzer von Zahlungsmitteln. Dementsprechend lautet die Forschungsfrage, *welche Regulierungen für Kryptowährungen, die sich auf den blossen Benutzer auswirken, grundrechtlich gerechtfertigt sind.*

Gang der Untersuchung

Die Klärung der Untersuchungsfrage setzt zunächst ein Verständnis von Geld und dessen Bedeutung für das Individuum und für die Gesellschaft voraus. Der erste Teil der Arbeit widmet sich daher zunächst der Frage, was Geld bzw. Währung ausmacht. Danach wird auf das Phänomen komplementärer Währung eingegangen und dargelegt, *dass Kryptowährungen als Zahlungsmittel die geldmässigen Funktionen erfüllen können und daher als privates, komplementäres Geld zu qualifizieren sind*. Hierbei erfolgt eine erste Abgrenzung des Untersuchungsgegenstands, insofern als Kryptowährungen, welche weitere, über die Funktion als Zahlungsmittel hinausgehende Eigenschaften besitzen, nicht als Kryptogelder bezeichnet werden und im Rahmen der vorliegenden Arbeit nicht weiter berücksichtigt werden. Darüber hinaus erfolgt eine Abgrenzung von Kryptogeld gegenüber weiteren, elektronischen Geldformen sowie eine Abgrenzung gegenüber möglichen Regulierungsschwerpunkten, welche die gewöhnlichen Benutzer von Kryptogeld nur am Rande betreffen.

Der *zweite Teil der vorliegenden Arbeit behandelt die Frage, wie das geltende Recht Kryptogeld erfasst*. Zunächst wird untersucht, ob überhaupt eine *verfassungsmässige Kompetenz* des Bundes für eine Regulierung von Kryptogeld

besteht. In Betracht fallen dabei grundsätzlich das Geld- und Währungsmonopol (Art. 99 BV), die Gesetzgebungskompetenz auf dem Gebiet von Banken, Versicherungen und weiteren Finanzdienstleistungen (Art. 98 BV) sowie die Kompetenz im Bereich des Strafrechts (Art. 123 BV). Ferner erfolgt eine Darstellung der geltenden *gesetzlichen Vorschriften*, welche Auswirkungen auf den blossen Umgang mit Kryptogeld haben können. Im Zentrum stehen dabei die Vorschriften des Geldwäschereirechts. Ferner sehen internationale Vereinbarungen im Bereich der Bekämpfung von Steuerdelikten eine Bekanntgabe von Daten über die Benutzer von Kryptogeld an staatliche Behörden vor.

Im *dritten Teil* wird schliesslich auf die Regulierung von Kryptogeld *de lege lata* eingegangen. Mögliche Regulierungsvarianten werden dabei anhand des Massstabs von Einschränkung von Grundrechten (Art. 36 BV) beurteilt.

Die Regulierung von Kryptogeld befindet sich in einem *Spannungsfeld zwischen den gewichtigen individuellen Vorteilen und dem besonderen Gefährdungspotential hinsichtlich der Risiken für Geldwäscherei, Terrorismusfinanzierung und Steuerhinterziehung*. Der Nutzen einer Regulierung von Kryptogeld lässt sich am bestehenden Gefährdungspotential für Geldwäscherei und weiteren, damit verwandten, Delikten messen. Die Gefährdung durch Kryptogeld lässt sich vorderhand darauf zurückführen, dass keine Identifikation vorausgesetzt ist (*Anonymität*) und Vermögenswerte schnell und weltweit verschoben werden können (*Schnelligkeit*). Kryptogelder besitzen darüber hinaus eine hohe *Mobilität*, weil sie Peer-to-Peer einsetzbar sind und weil es unter anderem bei Internettauschbörsen einfach und rasch konvertiert werden kann. Es besteht folglich das Risiko, dass die Möglichkeit von schnellen, anonymen, grenzüberschreitenden Transaktionen, welche Kryptogelder ermöglichen, genutzt wird, um eine illegitime Herkunft oder einen illegitimen Verwendungszweck der Vermögenswerte zu verschleiern.

Demgegenüber kommen Kryptogelder hinsichtlich individueller Freiheitsaspekte eine besondere Bedeutung zu, zumal deren Benutzung sowohl auf Seiten der Konsumenten wie auch der Gewerbetreibenden als *Erscheinung* grundrechtlich geschützter *Handlungsoptionen* gelten oder für deren *Wahrung* von Interesse sein kann. Zunächst ist Kryptogeld als *Ausdruck von Staatsunabhängigkeit* als Grundentscheidung für einen eigenen Lebensplan aufzufassen. Staatsunabhängigkeit hat in dieser Hinsicht den praktischen Mehrwert, dass sich das Individuum gegen staatliche Einflüsse, insbesondere auf den Wert des Geldes bzw. vor Kaufkraftverlust sowie Negativzinsen, schützen kann. Die Benutzung von Kryptogeld ist Ausdruck wie auch Garant ungehinderter *Persönlichkeitsentfaltung* und hat somit grundrechtliche Relevanz. Die freie Wahl des Zahlungsmittels ist ausserdem ein Aspekt *privatautonomer Gestaltung* von Rechtsbeziehungen und wird durch die Vertragsinhaltsfreiheit als Teil der Privatautonomie sowie der Wirtschaftsfreiheit

geschützt. Ferner stellen Kryptogelder aufgrund der Anonymität bzw. „Pseudonymität" probate Mittel hinsichtlich der *Verwirklichung der informationellen Selbstbestimmung* dar, zumal sie die persönliche Datenspur minimieren. Insofern ist Kryptogeld für die Verwirklichung gleich mehrerer Grundrechte von Bedeutung.

Zunächst wird eine *Obergrenze für die mögliche Annahme von Bitcoins* durch Händler zur Diskussion gestellt (CHF 10'000). Der Entscheid über die Verwendung von Kryptogeld im Rahmen einer privatwirtschaftlichen Erwerbstätigkeit ist Gegenstand der Wirtschaftsfreiheit und lässt sich auf die *Vorteile von Bitcoin für Händler* zurückführen. Dazu zählen insbesondere die Möglichkeit eine kostengünstige elektronische Bezahloption für Kunden anbieten zu können, bei denen sie nicht das Rückbuchungsrisiko tragen müssen, welches pull-value basierte Zahlungsmittel wie Kreditkarten auszeichnen. Sie profitieren aber auch von den allgemeinen Vorteilen von Bitcoin, wie der Resilienz des Netzwerks und des voraussetzungslosen Zugangs zu einem elektronischen Zahlungssystem. Der Ausschluss des Genusses dieser Vorteile stellt ein Eingriff in die Wirtschaftsfreiheit dar. Am Eingriff in die Wirtschaftsfreiheit bestehen allerdings *gewichtige öffentliche Interessen*, welche dem Interesse an der Benutzung von Bitcoin vorgehen könnten. Dazu zählen die *Verhinderung von Terrorismusfinanzierung, Geldwäscherei* usw. Für die Zumutbarkeit der Massnahme spricht darüber hinaus der Umstand, dass die hohe Bagatell- bzw. Freigrenze von CHF 10‘000.- die allermeisten Geschäfte mit Konsumenten (B2C) nicht einschränkt.

In einem weiteren Schritt wird die entsprechende Beeinträchtigung der Konsumenten aufgrund der *Bitcoin-Annahmeobergrenze* untersucht. Mangels Anwendbarkeit der Wirtschaftsfreiheit in Rechtsprechung und Lehre auf Konsumentenbelange kommt immerhin die Anwendbarkeit der *allgemeinen persönlichen Freiheit* (Art. 10 Abs. 2 BV) in Betracht. Dabei kann gezeigt werden, dass eine Bitcoin-Annahmeobergrenze unterschiedlichste Teilgehalte der persönlichen Freiheit betrifft, wie beispielsweise als *Konsum eines identitätsstiftenden Produkts* oder als *Mittel von besonderer praktischer Bedeutung*. Der Bagatellvorbehalt der persönlichen Freiheit führt allerdings dazu, dass die Beeinträchtigung nur im Fall der persönlichen Vorsorge eine genügende Belastungsintensität erreicht, und die im Ergebnis, angesichts des beträchtlichen verbliebenen Freiraums für Konsumenten, gerechtfertigt ist.

Im dritten Teil werden ferner mögliche *Regulierungen von Monero, welcher stellvertretend für weitere anonyme, dezentrale Zahlungsmittel steht*, untersucht. Zunächst kommt auch bei Monero eine *Annahmeobergrenze* als Kontrolle eines möglichen, sogenannten ‹Exit-Point› für Kryptogeld in Betracht. Um eine Differenzbetrachtung zur Bitcoin-Annahmeobergrenze zu ermöglichen, wird von einer gleichen Bagatellgrenze ausgegangen (CHF 10‘000.-). Die Annahmeobergrenze

für Monero erweist sich allerdings im Unterschied zu Bitcoin für Gewerbetreibende als ein *quasi-Technologieverbot*, das auch nicht durch das erhöhte Gefährdungspotential für Geldwäscherei, Terrorismusfinanzierung usw. eines anonymen Zahlungsmittels wie Monero gerechtfertigt werden kann. Insofern ist der Eingriff für Gewerbetreibende letztlich als Verletzung der Wirtschaftsfreiheit zu qualifizieren.

Im Unterschied dazu erreicht die *Monero-Annahmeobergrenze* für Konsumenten unter den Gesichtspunkten der *informationellen Selbstbestimmung* sowie der persönlichen Freiheit keine vergleichbare Belastungsintensität. Konsumenten sind von der Annahmeobergrenze von CHF 10'000.- ungleich weniger betroffen als Gewerbetreibende, zumal Beträge von Transaktionen mit Kunden (B2C) in der Regel nicht diese Grenze erreichen. Sie kommen daher selbst unter der Geltung der Monero-Annahmeobergrenze in den Genuss der Vorteile von anonymen Geldtransaktionen. Durch Verwendung von Monero lässt sich insbesondere die Erstellung von Zahlungsprofilen entgehen, welche Rückschlüsse auf höchstpersönliche Informationen wie Gesundheitszustand und politische sowie religiöse Ansichten zulassen. Insofern verbleibt ein genügend grosser Freiheitsraum, der die Beeinträchtigung aufzuwiegen vermag. Zum selben Resultat führen auch die Erwägungen hinsichtlich der Monero-Annahmeobergrenze und der *persönlichen Freiheit*. Selbst ein bloss kleiner Nutzen vermag die Beeinträchtigung der persönlichen Freiheit zu rechtfertigen, zumal gewichtige öffentliche Interessen betroffen sind und ein genügend grosser Freiheitsraum den Konsumenten verbleibt.

Schlussendlich wird die Grundrechtskonformität eines neuartigen Instruments zur Verhinderung von Terrorismusfinanzierung, Geldwäscherei usw. untersucht, nämlich einer *Meldepflicht der Identität der Inhaber von Kryptogeld-Adressen*, wie es die fünfte Geldwäscherichtlinie der EU bereits für gewöhnliche Bankkonten vorschreibt und für Kryptogeld zumindest absehbar ist. Zur Zielsetzung der fünften Geldwäscherichtlinie gehört ferner die *Identifikation von Transaktionen*, welche auch nur *geringe Beträge* beinhalten, die aber im *Zusammenhang mit Terrorismusfinanzierung, Geldwäscherei* etc. stehen.

Die Meldepflicht für Kryptogeld-Adressen wird zunächst am Beispiel von Monero hinsichtlich der Auswirkungen auf die *informationelle Selbstbestimmung* (Art. 13 Abs. 2 BV) untersucht. Weil es sich bei Monero um ein anonymes Zahlungsmittel handelt bzw. die Monero-Blockchain obfuskiert – d.h. verschleiert – ist, wird die vorgeschlagene Regulierung um das Erfordernis erweitert, dass Finanzintermediäre dem Staat die *Mittel zur Einsichtnahme* in die ansonsten verborgenen Monero-Wallets durch Überreichung sogenannter *‹View-Keys›* zur Verfügung stellen müssen. Eine derart erzwungene, umfassende Deanonymisierung der Inhaber von Monero-Wallets ist als schweren Eingriff in die informationelle

Selbstbestimmung zu werten, weil diese Informationen in ihrer Kombination eigentliche *Zahlungsprofile der Betroffenen* darstellen. Im Rahmen der Erforderlichkeit kann jedoch unter anderem gezeigt werden, dass weniger einschneidende Alternativen keine gleichwertige Effektivität aufweisen. Im Ergebnis vermögen die gewichtigen öffentlichen Interessen, die weitgehende Beeinträchtigung der informationellen Selbstbestimmung nicht zu rechtfertigen, weshalb eine Verletzung der informationellen Selbstbestimmung vorliegt.

Darüber hinaus sind die Auswirkungen auf die informationelle Selbstbestimmung bei einer Meldepflicht für Bitcoin-Adressen bzw. –Wallets sowie für Angaben zur Identität des Inhabers zu untersuchen. Weil die Bitcoin-Blockchain grundsätzlich öffentlich ist, können staatliche Stellen direkt auf Informationen zugreifen und bedürfen dafür nicht eines View-Key. Insofern besteht jedoch die Gefahr, dass der Staat – aber auch Dritte – eine umfassende Überwachung sämtlicher Wallets und Transaktionen anstrebt. Dies kann zu Ungewissheit der Individuen darüber führen, ob sie ein *Ziel einer heimlichen Überwachung darstellen, was zu einer nachhaltigen abschreckenden Wirkung (chilling effect)* auf die Benutzung von Bitcoin führt. Darüber hinaus besteht das Risiko von diskriminierenden Behandlungen, zumal Filter angesichts der grossen Zahl an Transaktionen und Wallets eingesetzt werden müssten, da in Anbetracht der Zielsetzung, sämtliche – d.h. unabhängig von den involvierten Beträgen – Terrorismusfinanzierungsaktivitäten sowie Geldwäschereidelikte aufzuspüren, nicht an die Überschreitung eines bestimmten Betrags (sogenannter Bagatellbetrag) angeknüpft werden kann. Aus diesen Gründen erweist sich die Bitcoin-Meldepflicht als einen nicht-gerechtfertigten Eingriff in die informationelle Selbstbestimmung.

Teil I:
Einführung in den Untersuchungs-gegenstand

Kapitel 1: Kryptowährung als komplementäres Geld

In den folgenden Absätzen wird zunächst das *Phänomen Geld bzw. Währung* sowie dessen Bedeutung für das Individuum und die Gesellschaft kurz dargestellt (**I.**). Anschliessend werden *alternative Zahlungsmittel* (sogenanntes Komplementärgeld) und mögliche Beweggründe für ihre Verwendung überblicksweise aufgezeigt (**II.**). Schlussendlich erfolgt eine Abgrenzung von Kryptowährung als reines Zahlungsmittel, welches im Folgenden als *Kryptogeld* bezeichnet wird, gegenüber weiteren möglichen Ausprägungen (**III.**). 1

I. Währung und Geld

1. Begriffsbestimmung

Geld wird im allgemeinen Sprachgebrauch tendenziell als Oberbegriff zu Währung gesehen, zumal als Geld bzw. als Geldmittel unterschiedliche Währungen in Betracht kommen. Als *Geld zählen demnach sämtliche Medien, welche im Austausch für eine erhaltene Sache oder Dienstleistung hingegeben werden und vom Vertragspartner als vollständige Abgeltung dafür verstanden werden*. Zum Geld (i.w.S.) können daher auch gegenständliche Vermögenswerte zählen, welche im Normalfall nicht als Zahlungsmittel eingesetzt werden, aber aufgrund ihrer Standardisierung bzw. einfachen Messbarkeit sich gut dazu eignen – beispielsweise Zigaretten. 2

Kryptowährung kann grundsätzlich als Geld bezeichnet werden, zumal es im Austausch für Waren und Dienstleistungen als Gegenleistung eingesetzt und vom Vertragspartner als Abgeltung dafür verstanden wird. 3

Der *Begriff der Währung* wird demgegenüber üblicherweise im Zusammenhang mit der Beschreibung der materiellen Beschaffenheit eines Zahlungsmittels oder der in einem bestimmten Land geltenden Rechnungseinheit verwendet.[3] Beispielsweise wird zwischen Metallwährung, Goldwährung und Papierwährung sowie zwischen Dollar, Pfund, Franken als Währungen bzw. als unterschiedliche 4

---

3 C-T. SAMM, »Geld« und »Währung«. Begrifflich und mit Blick auf den Vertrag von Maastricht, in: A. Weber (Hrsg.), Währung und Wirtschaft. Das Geld im Recht, FS Hahn, Baden-Baden 1997, 227-244 (235 f.).

Rechnungseinheiten – auch Standardwerteinheiten bzw. Werteinheiten genannt – unterschieden.[4]

5 In diesem Sinne kann Kryptowährung als zur Abgrenzung gegenüber anderen Währungen verwendet werden, welche *nicht auf Kryptografie zur Sicherstellung der Systemintegrität beruhen*.

6 Dass Kryptowährungen im Allgemeinen weniger als Geldmittel oder Währung und augenscheinlich mehr als Anlageform zur Renditeerzielung betrachtet werden, kann auch *auf verfestigte Ansichten darüber, dass Geld primär ein staatliches Konstrukt sei*, zurückgeführt werden. Einen stückweisen Aufschluss darüber gibt die Geschichte des Geldes, welche den wachsenden Einfluss des Staates im Bereich des Geldwesens deutlich macht.

2. Geschichtlicher Überblick

7 In welchem Zeitpunkt der Geschichte das erste Geld entstanden ist, ist bis heute nicht restlos geklärt und ist ausserdem Gegenstand von Meinungsverschiedenheiten.[5] Indes besteht darüber Einigkeit, dass die *Geldgeschichte eine Chronologie der Entsubstantialisierung* von Geldmitteln und der Machtausdehnung des Staates darstellt.[6] Die Geldgeschichte zeigt jedoch auch, dass der Staat nicht beliebige Sachen zu Geld machen kann, sondern dass ein Mindestmass an Akzeptanz des Zahlungsmittels beim Publikum notwendig ist.

8 Unumstritten ist zunächst, dass die steinzeitliche Subsistenzwirtschaft, die keinen wirtschaftlichen Austausch beinhaltete (sogenannte Intraproduktion),[7] durch die *Tauschwirtschaft der antiken Kulturen abgelöst wurde, in welcher zunächst besonders verkehrsfähige Naturalgüter als Geld dienten*. Ausschlaggebend für die Verkehrsfähigkeit eines Gutes war die Relevanz für den persönlichen Gebrauch, d.h. dessen Beliebtheit. Daher wurden vorzugsweise diejenigen Sachen als Geld eingesetzt, die im Alltag Verwendung fanden und daher einen Nutzwert aufwiesen (beispielsweise Getreide, Stoffe, Pelze, Vieh und Werkzeuge). Darüber hinaus

---

4 Zu diesem und dem vorherigen Absatz, M. SCHAR-SCHUPPISSER, Standardwerteinheit, Währung, Geld, Genf 1989, 68 ff.

5 L. DITTRICH, Die Bedeutung des Rechts für die Stabilität des Geldes, Tübingen 2016, 18; J. BENES/M. KUMHOF, The Chicago Plan revisited, 2012, 12.

6 F. KLEIN/K. SPREMANN, Telegeld. Electronic Money, Smart Cards und E-Commerce werden Realität, Zürich 1998, 25 f.; R. DIETZ, Tausch und Geld. Zur Entsteheung der Geldwirtschaft als Ordnung, in: D. Cassel (Hrsg.), Entstehung und Wettbewerb von Systemen, Berlin 1996, 45-80 (72); SAMM, Geld (Fn. 3), 228.

7 H. LECHNER, Währungspolitik, Berlin/New York 1988, 258 f.

waren aber auch bereits die Eignung zur Zählung bzw. Messung sowie eine gewisse Haltbarkeit erwünschte Attribute eines allgemeinen Zahlungsmittels.[8]

In den antiken Kulturen entstanden ferner bereits die Anfänge des Metallgelds. 9
Diese Phase der Geldgeschichte ist dadurch gekennzeichnet, dass in erster Linie Edelmetalle – d.h. Gold und Silber – und zur Ergänzung des Geldsystems durch kleine Stücke unedle Metalle – Kupfer, Bronze, Zinn und Eisen – als Zahlungsmittel verwendet wurden. *Von der Frühphase des Metallgelds, welche sich durch gegenständlich geformte, uneinheitliche Tauschwerte – beispielsweise Schmuckstücke – als Geld auszeichnete, verlief die Entwicklung vor dem Hintergrund des Aufkommens der Münzprägung rasch hin zu einem standardisierten Tauschmittel.* In diese Phase fällt auch der Bruch mit dem vorherigen Geltungsgrund, nämlich der Nützlichkeit für den persönlichen Bedarf. Für die Fungibilität oder Verkehrsfähigkeit eines Zahlungsmittels entscheidend war nunmehr die Eignung für den Zahlungsverkehr, d.h. eine hohe Wertbeständigkeit und eine einfache Teilbarkeit bzw. Zählbarkeit. Nach wie vor waren aber die Seltenheit und Schönheit des verwendeten Metalls massgebend.[9]

Die Anfänge eines Münzwesens werden für Europa zwischen dem achten und 10
sechsten Jahrhundert v. Chr. gesehen. In der Phase des Übergangs von prämonetären Formen – d.h. Schmuckgeld, Barrengeld usw. – hin zum Münzgeld als Tauschmittel akzentuiert sich der staatliche Einfluss auf das Geld und markiert den Beginn des Einflusses des Staates auf das Geldwesen. Eine *staatliche Währungsordnung gewährt dem Staat die sogenannte Münzhoheit oder das Münzrecht, d.h. die Kompetenzen, Münzen zu prägen, den Münzfuss bzw. Metallgehalt festzulegen und Münzstätten einzurichten sowie Fälschungen und unerlaubte Einfuhren zu bestrafen*.[10] Nur zwischenzeitlich, d.h. nach dem Niedergang des weströmischen Reiches und den Münzreformen von Pippin und Karl der Grosse (ca. 476-750 n.Chr.), war das Geldwesen bzw. die Münzprägung in Europa wieder in rein privaten Händen.[11] Die Schaffung einer staatlichen Währungsordnung,

8 C. HERRMANN, Währungshoheit, Währungsverfassung und subjektive Rechte, Tübingen 2010, 7 f.

9 K. HELFERRICH, Das Geld, 6. Aufl., Leipzig 1923, 18 f.; HERRMANN, Währungshoheit (Fn. 8), 10.

10 M. NORTH, Das Geld und seine Geschichte. Vom Mittelalter bis zur Gegenwart, München 1994, 10; HERRMANN, Währungshoheit (Fn. 8), 10 ff.

11 HERRMANN, Währungshoheit (Fn. 8), 13; HELFFERICH, Geld (Fn. 9), 31.

welche vorwiegend auf militärische Motive zurückzuführen ist, illustriert ferner den stärker werdenden Machtanspruch des Staates.[12]

11 Den Herrschern, welchen das Münzrecht grundsätzlich zustand, übten dieses Recht in der Regel nicht selbst aus, sondern veräusserten dieses an zahlreiche weltliche – d.h. Herzöge, Grafen, Städte etc. – sowie geistliche Gewalten – v.a. Bistümer – in ihrem Herrschaftsgebiet weiter. Diese Zersplitterung des Münzrechts führte zu einer Vielzahl an Münzen mit unterschiedlichem Erscheinungsbild und Edelmetallgehalt (sogenannter Feingehalt) in einem Herrschaftsgebiet, was den kaufmännischen Verkehr stark erschwerte. Darüber hinaus schuf die *Monopolisierung des Geldwesens beim Staat das Risiko einer fiskalischen Ausnutzung des Geldwesens und bewirkte damit oftmals einen Vertrauensverlust in das Geld*. Insbesondere schwächten Münzverschlechterungen – d.h. die Reduktion des Feingehalts unter Beibehaltung des Nominalwerts –, Fälschungen sowie Münzverrufungen – d.h. Ungültigkeitserklärung oder offizielle Abwertung des Nominalwerts – das Vertrauen in damalige Geldmittel.[13]

12 Als Folge resultierten wegen dieser auf *Edelmetallen basierenden Währungen – sogenannte Edelmetallwährung – Nachteile hinsichtlich der Geldversorgung der Wirtschaft*. Ungewöhnliche hohe Ab- oder Zuflüsse von Edelmetallen – beispielsweise bei Entdeckung neuer Vorkommen – sorgten dafür, dass die Geldmenge mehrheitlich nicht gleichmässig mit der Produktion bzw. der Warenmenge verlief. Die Folge davon war, dass die Wirtschaft abwechselnd durch deflationäre und inflationäre Phasen bestimmt war, obwohl Veränderungen teilweise nur auf der Geldseite eingetreten waren.[14]

13 Schlussendlich bereiten Edelmetallwährungen ganz praktische Probleme. Grössere Beträge weisen ein hohes Gewicht auf und sind naturgemäss mühsam über weite Distanzen zu transportieren. Bereits *seit dem 13. Jahrhundert wurden daher in oberitalienischen Handelsstädten Wertpapiere, welche das Metallgeld vertreten, für den Handel eingesetzt*. Die Bezahlung mit diesen Wechseln erübrigte den Transfer von Münzgeld und ermöglichte, durch die Absicherung der im Wertpapier verbrieften Ware, die Gewährung von Krediten.[15]

---

12 S. SIMITIS, Bemerkungen zur rechtlichen Sonderstellung des Geldes, in: AcP 1960/1961, 406-466 (419).

13 HERRMANN, Währungshoheit (Fn. 8), 13 ff.; HELFFERICH, Geld (Fn. 9), 31 ff.; S. GLESS/P. KUGLER/D. STAGNO, Was ist Geld? Und warum schützt man es? Zum strafrechtlichen Schutz von virtuellen Währungen am Beispiel von Bitcoins, in: recht 2015, 82-97 (84).

14 NORTH, Geld (Fn. 10), 78 ff; siehe ferner DITTRICH, Stabilität (Fn. 5), 10.

15 HERRMANN, Währungshoheit (Fn. 8), 18 f.; NORTH, Geld (Fn. 10), 111 ff.

Ab Mitte des 17. Jahrhunderts entwickelten sich diese Wertpapiere durch die Möglichkeit der direkten Übertragung und des Schuldversprechens auf den Inhaber zu Inhaberpapieren und damit zu eigentlichen Banknoten. Die Ausgabe von Banknoten in Europa wurde von privaten Banken betrieben, war aber meist von einer staatlichen Bewilligung abhängig, welche allerdings die von diesen Banken herausgegebenen Banknoten nicht zu einem gesetzlichen Zahlungsmittel machte.[16] 14

Diese Banknoten bzw. Wertpapiere waren die Vorläufer der nächsten Etappe im Prozess der Entsubstantialisierung des Geldes, welche durch das reine Papiergeld (in Frankreich ab 1720 sowie um 1790 – *Assignaten*) gekennzeichnet ist.[17] *Papiergeld zeichnet sich dadurch aus, dass es keinen über den Funktionswert hinausgehenden Wert aufweist, d.h. insbesondere keinen Stoffwert sowie keinen abgeleiteten Wert – etwa durch hinterlegte Güter – besitzt*. Seit den Anfängen der Geldgeschichte war die Werthaltigkeit entweder aufgrund des Nutzens für den täglichen Bedarf, des Stoffwertes oder aufgrund von hinterlegten Werten für die Akzeptanz als Zahlungsmittel grundsätzlich unverzichtbar. In der Abkehr vom Prinzip der Werthaltigkeit werden zwar einerseits geldtheoretische Vorteile hinsichtlich der Tendenz zum Austausch, d.h. der Polarität, gesehen, allerdings auch eine gewichtige Problematik.[18] Weil eine äussere Begrenzung der Herstellung praktisch gänzlich fehlt, kann so viel Geld geschaffen werden, wie die Notendruckmaschinen dies zulassen. Der Staat hat ein Interesse an der Inverkehrsetzung von Papiergeld, zumal er den Nennwert minus die minimalen Herstellungskosten als Gewinn einfahren kann. Ferner kann der Staat einfacher zu einer Währungsreform greifen, d.h. den Nennwert von Zahlungsmitteln verringern oder diese sogar gänzlich ausser Kurs setzen.[19] 15

Die anfängliche Akzeptanz des frühen Papiergeldes im Publikum – insbesondere die der französischen Assignaten und Mandaten – beruhte weniger auf den geldtheoretischen Vorteilen, sondern aufgrund der gesetzlichen Bestimmungen, welche dem Papiergeld nunmehr einen gesetzlichen Kurs sowie einen Zwangskurs – auch interne Inkonvertibilität genannt – verliehen und deren Geltung durch Androhung sogar der Guillotine abgesichert wurde.[20] Weil die Geltung eines 16

16 NORTH, Geld (Fn. 10), 113.

17 HELFERRICH, Geld (Fn. 9), 66 f.; NORTH, Geld (Fn. 10), 135 ff.

18 KLEIN/SPREMANN, Telegeld (Fn. 6), 21; SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 138 ff.

19 Siehe dazu S. GESELL, Die natürliche Wirtschaftsordnung, Bern 1938, 119 ff.

20 C. MENGER, Das Geld, in: F.A. von Hayek (Hrsg.), Carl Menger Gesammelte Werke, 2. Aufl., Tübingen 1970, 1-116 (100); Für die Begriffsverwendung «Zwangskurs»

bestimmten Zahlungsmittels als Geld unter diesem Gesichtspunkt eher als eine staatliche Entscheidung denn als eine des Publikums angesehen werden kann, wird staatliches Papiergeld auch als Fiatgeld, d.h. «Es-sei-Geld», bezeichnet. Obwohl sich kaum «ein stärkerer Eingriff in die wirtschaftliche Freiheit, wie ein Verbot an die Verkäufer, ihre Waren gegen ein anderes als das vom Staat bezeichnete Gut abzulassen, […] ausdenken [lässt]»,[21] konnte sich seit der Französischen Revolution dieses Recht des Staates im Grossen und Ganzen halten.[22] Indessen zeigte sich, dass die Androhung staatlicher Zwangsmittel nicht genügte, um das Vertrauen des Publikums in ein stoffwertloses Zahlungsmittel über längere Zeit aufrechtzuerhalten. Die Industriestaaten gingen daher ab 1870 allmählich dazu über, den Wert ihrer jeweiligen Währung in Gewicht von Edelmetall – meist Gold (Goldwährung) – auszudrücken sowie die interne Konvertibilität von Banknoten in Edelmetalle zu garantieren (Goldkernwährung), d.h. den Austausch gegen den Gegenwert in Gold.[23]

17 Das System der Goldumlaufwährung durch Münzen mit Einlösepflicht für Banknoten bestand formell für die Schweiz von 1891 bis zum Inkrafttreten der aktuellen BV. In der Praxis wurde die Einlösepflicht für Banknoten allerdings immer wieder suspendiert und 1954 durch Bundesratsbeschluss auf unbestimmte Zeit aufgehoben.[24] Im Gegenzug wurde die Nationalbank zunächst verpflichtet, die Parität des Schweizer Frankens zum Goldwert aufrechtzuerhalten (sogenannte Goldparität). Im Rahmen des Systems von Bretton Woods, an welchem sich auch die Schweiz beteiligte, war die Konvertibilität in Gold nur für den Dollar vorgesehen, zu dem der Kurs des Schweizer Frankens nicht zu sehr abweichen durfte (Fixkurssystem). Mit dem Zusammenbruch des Systems von Bretton Woods wurde der Schweizer Franken zu einer Goldkernwährung jedoch ohne Umtauschpflicht der Nationalbank und mit flexiblen Wechselkursen im Aussenverhältnis, d.h. zu anderen Währungen. Durch den 1992 erfolgten Beitritt der Schweiz zum

und «gesetzlicher Kurs» siehe CH.-A. JUNOD, Art. 39 BV (Juni 1988), in: J-F. Aubert/H. Koller (Hrsg.), Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft vom 29. Mai 1978, Bd. 3, Loseblatt, Fn. 5 f.

21 HELFERRICH, Geld (Fn. 9), 335.

22 HERRMANN, Währungshoheit (Fn. 8), 19 f.

23 HELFERRICH, Geld (Fn. 9), 67 ff.; HERRMANN, Währungshoheit (Fn. 8), 16 f.

24 Bundesratsbeschluss vom 29. Juni 1954 betreffend den gesetzlichen Kurs der Banknoten und die Aufhebungen ihrer Einlösung in Gold (SR 951.171); CH.-A. JUNOD, Art. 39 aBV (Fn. 20), Rz. 3 ff.

IWF und aufgrund dessen Verbot der Goldbindung erwies sich die verbliebene verfassungsrechtliche Ordnung (Goldparität) als Verstoss gegen Völkerrecht.[25]

Der formelle Widerspruch zum Völkerrecht wurde erst mit dem *Inkrafttreten der totalrevidierten BV im Januar 2000 aufgelöst, welche eine moderne Währungsordnung ohne Goldparität schuf*. Gold fungiert seither nur noch als blosse Währungsreserve, welche die Nationalbank zur Erfüllung ihrer verfassungsmässigen Pflichten frei verwenden kann. Darüber hinaus wurde die Ausgabe von reinem Papiergeld auf eine verfassungsmässige Grundlage gestellt, während den Bedenken gegenüber solchem Geld durch die Gewährung der Unabhängigkeit der Nationalbank sowie deren Verpflichtung auf die Gesamtinteressen des Landes, Rechnung getragen wurden (Art. 99 Abs. 2 BV).[26] 18

Die neu geschaffene Währungsordnung gemäss Art. 99 BV lässt mit der Erwähnung, dass das Geld- und Währungswesen Sache des Bundes ist, keinen Zweifel mehr, dass das Banken-Buchgeld vom Bundesmonopol miterfasst ist.[27] Banken-Buchgeld ist aus der Überlegung entstanden, dass Banken niemals gleichzeitig und vollständig sämtliche ihrer Verbindlichkeiten erfüllen müssen und daher das ihnen anvertraute Geld teilweise als Kredit weitergeben können. *Banken können also Geld schaffen, welches zwar kein gesetzliches Zahlungsmittel darstellt (vgl. Art. 2 WZG), das jedoch – weil es die Rechtsordnung erlaubt – in gesetzliche Zahlungsmittel konvertiert werden kann*. Ausdruck dieser Möglichkeit ist die Verwendung derselben Rechnungseinheit (beispielsweise CHF). Aufgrund der Konvertibilität hat die Schaffung von Banken-Buchgeld jedoch Auswirkungen auf die Geldmenge und muss daher zur Wahrung des Publikumsvertrauens grundsätzlich regulierbar sein. 19

Vom Banken-Buchgeld, welches heutzutage als rein elektronisches Geld in Erscheinung tritt, ist das elektronische Geld, welches auf Chip- oder Prepaidkarten besteht, zu unterscheiden (sogenanntes Chipkartengeld). Chipkartengeld lässt sich wie Bargeld einsetzen, zumal es vom Benutzer selbst aufbewahrt und meist einfacher transferiert werden kann als das Banken-Buchgeld, welches eine Anweisung 20

25 C. KAUFMANN/F. UTZ, Art. 99 BV, in: B. Waldmann/E. Belser/A. Epiney (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015, Rz. 1 ff.; P. NOBEL, Goldfieber, in: B. Ehrenzeller et al. (Hrsg.), Verfassungsstaat vor neuen Herausforderungen, FS Hangartner, St. Gallen/Lachen SZ 1998, 845-864 (853); Botschaft vom 17. Mrz. 1997 über die Revision des Nationalbankgesetzes, BBl 1997 II 977, 995.

26 P. NOBEL, Gold und Geist, in: J. Furrer/B. Gehrig (Hrsg.), Aspekte der schweizerischen Wirtschaftspolitik, FS Jaeger, Chur/Zürich 2001, 295-307 (300 ff.); Botschaft vom 20. Nov. 2013 zur Volksinitiative «Rettet unser Schweizer Gold (Gold-Initiative)», BBl 2013 9329, 9330 ff.

27 Siehe hingegen zur aBV, CH.-A. JUNOD, Art. 39 aBV (Fn. 20), Rz. 19.

an die Bank zur Ausführung von Transaktionen voraussetzt. Gewisse Formen von Chipkartengeld bestehen seit mehr als 20 Jahren und es existieren daher viele Ausprägungen sowie technische Unterschiede in der jeweiligen Ausgestaltung. Im Wesentlichen unterscheidet sich Chipkartengeld von Kryptowährung nach den folgenden zwei Gesichtspunkten. Einerseits ist *Chipkartengeld in einer staatlichen Währungseinheit denominiert und ist daher grundsätzlich an eine bestimmte Währungsordnung gebunden. Andererseits stellen Chipkartengelder keine dezentralen Zahlungsmittel dar*, zumal eine Bestätigung der Echtheit und Gültigkeit von Chipkartengeld durch eine zentrale Stelle erfolgt oder, weil ohne eine Bestätigung durch eine solche Stelle, erhaltenes Chipkartengeld nicht wieder ausgegeben werden kann.[28]

21 Darüber hinaus finden mit Kreditkarten sowie unter Zuhilfenahme sogenannter Online-Zahlungsdienstleister, wie beispielsweise PayPal, ebenfalls elektronische Geldtransaktionen seit mehr als 20 Jahren statt. Sie lassen sich jedoch von Zahlungen mit Kryptowährungen unterscheiden. Transaktionen mit Kreditkarte oder mittels Online-Zahlungsdienstleister verwenden i.d.R. diejenige Währungseinheit, welche am Ort der Niederlassung des Benutzers gilt. Ferner sind *solche Transaktionen im Unterschied zu Transaktionen mit Kryptowährung keine push-value Vorgänge, bei welchen der Empfänger direkt begünstigt wird, sondern blosse Anweisungen. Vermögensverschiebungen werden bei Kreditkarten und Netzgeld, wie beispielweise Paypal, durch sich entsprechende Belastungen und Gutschriften durch die Bank bei den Konten der Vertragspartner bewerkstelligt*, wobei die Anweisung bzw. das Vorweisen der Kreditkarte als Zustimmung zur Vornahme dieser Buchungen dient. Für diese Zahlungsmittel gilt daher, dass über Guthaben nur mit der Zustimmung des Dienstleistungsanbieters verfügt werden kann und, dass Benutzer grundsätzlich das Kreditrisiko tragen, dass der Anbieter das geschuldete Guthaben nicht auszahlen kann.

22 Schlussendlich ist auf die mögliche Entwicklung zu einer vollständig digitalen Landeswährung hinzuweisen. Die Idee einer digitalen Landeswährung, bei der elektronische Werteinheiten gesetzliche Zahlungsmittel darstellen würden, wurde bereits vor bald 30 Jahren diskutiert.[29] Diese Idee hat aber durch die Verbreitung von Kryptowährungen und der Idee von Vollgeld, d.h. durch die Zentralbanken

---

28 Siehe zu diesem und dem vorherigen Absatz, F. VISCHER, Geld- und Währungsrecht. Im nationalen und internationalen Kontext, Basel 2010, Rz. 22 ff.; R. WEBER, Elektronisches Geld. Erscheinungsformen und rechtlicher Problemaufriss, Zürich 1999, 56 ff.

29 C. ZELLWEGER-GUTKNECHT, Digitale Landeswährung. Ein Überblick, in: jusletter.ch vom 31.10.16, Rz. 1 ff.

geschaffenes Buchgeld,[30] erneute Aktualität erfahren. *Eine digitale Landeswährung wäre im Unterschied zu Kryptowährungen jedoch in eine staatliche Währungsordnung eingebunden und insbesondere von währungspolitischen Massnahmen betroffen*.

3. Individuelle Interessen an Geld

An Geld bzw. Geldmittel bestehen unabhängig der Erscheinung individuelle Interessen. Diese Interessen orientieren sich überwiegend an den drei Grundfunktionen von Geld. 23

3.1 Geld als Tauschmittel

Geld zeichnet sich primär dadurch aus, dass es als Tauschmittel die Korrelation einzelner Güter ermöglicht. Der Verkäufer erhält Geld in der Höhe des Tauschwertes der verkauften Ware, das er selbst wieder im Austausch einsetzen kann. Dadurch werden die Möglichkeiten des Austauschvorgangs Gut gegen Gut um die Variante Gut gegen Geld ergänzt. *Insofern kommt Geld als universelles Tauschmittel* hinsichtlich der Befriedigung der persönlichen Bedürfnisse ein grosses Gewicht zu. Ohne ein universelles Tauschmittel wäre die Suche nach einem geeigneten Vertragspartner bedeutend schwieriger oder gar unmöglich, da dieser genau gegenteilige Bedürfnisse haben müsste, damit ein Vertrag zustande kommt (sogenannte doppelte Bedürfniskoinzidenz). Dem Besitzer von Geld erweitert es folglich seine individuellen Handlungsmöglichkeiten: Er kann selbst entscheiden, was er zu welchem Zeitpunkt von welchem Anbieter nachfragt und was nicht. Geld wird deshalb auch als «geprägte Freiheit» oder «Joker unter den Waren» angesehen.[31] Auch die Redewendung «Geld regiert die Welt» bzw. «Geld ist der einzige Herr aller Dinge» (lat.: *pecunia unum regimen est rerum omnium*) kann unter anderem auf die besondere Stellung des Geldes zurückgeführt werden. 24

3.2 Geld als Wertaufbewahrungsmittel

Darüber hinaus *eignet sich Geld für die Speicherung von Wert insbesondere über die zeitliche Dimension hinweg*. Geld wird deshalb auch als «Anwartschaft aus 25

30 Botschaft vom 9. Nov. 2016 zur Volksinitiative «Für krisensicheres Geld: Geldschöpfung allein durch die Nationalbank! (Vollgeld-Initiative)», BBl 2016 8475, 8491 ff.

31 BVerfG 97, 350 (371) – Euro; HERRMANN, Währungshoheit (Fn. 8), 289; GESELL, Wirtschaftsordnung (Fn. 19), 138 ff.; D. SUHR, Geld ohne Mehrwert. Entlastung der Marktwirtschaft von monetären Transaktionskosten, Frankfurt a.M. 1983, 59.

Tausch zum Tausch» bezeichnet.[32] Individuen können daran aus unterschiedlichen Motiven ein Interesse haben: Im Vordergrund steht das Bedürfnis, Vorsorge für sich und die nächsten Angehörigen treffen zu können. Dies kann entweder eine Vorsorge für ganz spezielle (Not-) Lagen sein – beispielsweise bei unvorhergesehenem Erwerbsausfall – aber auch im Rahmen allgemeiner persönlicher Vorsorge, d.h. hinsichtlich der Altersvorsorge.

26 *Geld, insbesondere elektronisches Geld, eignet sich besonders gut, um Vorsorge treffen zu können*. Geld beansprucht im Vergleich zu Wertgegenständen nur wenig Raum und kann daher vergleichsweise einfach und kostengünstig aufbewahrt werden. Darüber hinaus kann Geld nicht verderben und ist im Unterschied zu den meisten anderen Gegenständen keinem Alterungsprozess ausgesetzt.

3.3 Geld als Wertmassstab

27 Geld erfüllt ferner die sogenannte Wertmassstabsfunktion. Obwohl diese Funktion alltägliche Verwendung findet, so ist sie am wenigsten im Bewusstsein der Benutzer verankert. *Als Wertmassstab lässt sich Geld, ähnlich eines echten Massstabs, an fast alle Gegenstände anlegen, um ihren Wert zu bestimmen*. Insofern erlaubt die Wertmassstabsfunktion, dass sich komplett unterschiedliche Objekte miteinander vergleichen lassen.[33]

28 Die Wertmassstabsfunktion beschränkt sich grundsätzlich jedoch nicht nur auf die Messung von Objekten, sondern kann auch auf Rechte oder blosse Erwartungen angewandt werden. Darüber hinaus lässt sich im Einzelfall auch der Wert einer Unterlassung mithilfe der Wertmassstabsfunktion quantifizieren. *Die Wertmassstabsfunktion hat demnach Bedeutung für das persönliche Nutzenkalkül*.

3.4 Geld als Medium zwischenmenschlicher Freiheiten

29 Schlussendlich erscheint Geld in tatsächlicher sowie rechtlicher Hinsicht als Voraussetzung für die Ausübung grundrechtlich garantierter Freiheiten. Einerseits ist die Möglichkeit der Benutzung von Geld notwendig, zumal in einer arbeitsteiligen Wirtschaft der Bezug von Waren und Dienstleistungen vom Monopol des Geldes abhängt. Ein Ausschluss der Benutzung von Geld käme daher dem Ausschluss vom Bezug fast aller Waren und Dienstleistungen gleich und damit von weiten Teilen des öffentlichen Lebens. Insofern stellt Geld ein notwendiges Medium dar,

---

32 D. SUHR, Die Geldordnung aus verfassungsrechtlicher Sicht, in: J. Starbatty (Hrsg.), Geldordnung und Geldpolitik in einer freiheitlichen Gesellschaft, Tübingen 1982, 114.

33 SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 187.

um in den Genuss derjenigen Freiheiten zu kommen, welche sich nur im Austausch mit anderen Individuen verwirklichen lassen.[34]

Andererseits ist die freie Entscheidung über die rechtsgeschäftliche Gestaltung von Verträgen Ausdruck von Privatautonomie und damit von grundsätzlicher Bedeutung für die ungehinderte Persönlichkeitsentfaltung, wie sie durch die persönliche Freiheit (Art. 10 Abs. 2 BV) garantiert ist. Entscheidungsfreiheit in Form der Vertragsfreiheit kann sich jedoch nur in Geldwirtschaften entfalten.[35] 30

4. Gesellschaftliche Interessen

Bereits ARISTOTELES hat auf die Notwendigkeit des Vorhandenseins eines allgemeinen Tauschmittels in einer Gemeinschaft bzw. für die Existenz der Gemeinschaft überhaupt hingewiesen.[36] Die Vorteile für die Gemeinschaft folgen auch bei ARISTOTELES aus den drei Grundfunktionen von Geld. Geld als allgemeines Tauschmittel ist zunächst Voraussetzung für eine arbeitsteilige Wirtschaft.[37] Eine arbeitsteilige Wirtschaft erlaubt die Spezialisierung der Wirtschaftssubjekte in der Herstellung einzelner Güter bzw. der Bereitstellung von Dienstleistungen. Aus der Spezialisierung der Wirtschaftssubjekte folgt insbesondere eine Beschleunigung des technischen Fortschritts sowie eine Steigerung der Produktivität, wovon die ganze Gesellschaft profitiert. 31

Zweitens haben an der Wertaufbewahrungsfunktion von Geld auch andere Wirtschaftssubjekte als die Individuen wie beispielsweise die Gemeinwesen und die Unternehmen ein Interesse. Auch sie sind interessiert, Kaufkraft zu speichern und bei Bedarf zu einem späteren Zeitpunkt einzusetzen.[38] 32

Schlussendlich transformiert sich die Wertmassstabsfunktion von Geld in einer gesamtwirtschaftlichen Perspektive in der Koordinationsfunktion für Märkte bzw. in den Preismechanismus. Geld bzw. *Geldwirtschaft ist Voraussetzung dafür, dass sich für ein bestimmtes Gut ein bestimmter Preis bilden kann und nur in diesem Rahmen kann der Preismechanismus zum Tragen kommen*. Preisgesteuerte Märkte 33

---

34 SUHR, Geldordnung (Fn. 32), 115; SUHR, Mehrwehrt (Fn. 31) 116 f.

35 N. LUHMANN, Die Wirtschaft der Gesellschaft, Frankfurt a.M. 1994, 241 f.

36 ARISTOTELES, Die Nikomachische Ethik, V. Buch, in: G. Olof, Aristoteles. Die Nikomachische Ethik, München 2002, 215.

37 LECHNER, Währungspolitik (Fn. 7), 258 ff.; C. OHLER, Die hoheitlichen Grundlagen der Geldordnung, in: JZ 2008, 317-324, 317; HERRMANN, Währungshoheit (Fn. 8), 40 ff.; SIMITIS, Sonderstellung (Fn. 12), 415.

38 R. SCHMIDT, Geld und Währung, in: J. Isensee/P. Kirchhof (Hrsg)., Handbuch des Staatsrechts, Bd. 3 (Das Handeln des Staates), Heidelberg 1988, 1121-1139 (1125).

senken die Transaktions- und Informationskosten in einer Volkswirtschaft und steigern damit ihre Leistungsfähigkeit.[39]

II. Komplementäre Zahlungsmittel

1. Definition

34 Als Komplementärwährung kann die Vereinbarung innerhalb einer Gemeinschaft bzw. eines bestimmten Nutzerkreises betrachtet werden, ein anderes Medium nebst dem offiziellen Geld als Zahlungsmittel zu akzeptieren.[40]

35 Als komplementäres Zahlungsmittel gilt daher dasjenige Medium, welches in der Vereinbarung bzw. in einer alternativen Währungsverfassung zu einem Geldzeichen erklärt wurde.

2. Bedeutung

36 Komplementäre Zahlungsmittel sind in der Regel als Ergänzung zum staatlichen Geld und mit der Absicht, ein bestimmtes Anliegen zu fördern oder gewissen Defiziten staatlichen Gelds zu begegnen, konzipiert. Der Hauptanwendungsfall für komplementäre Zahlungsmittel ist die Förderung und Stabilisierung der regionalen Wirtschaft insbesondere in Zeiten wirtschaftlicher Rezession. In Betracht kommen aber auch weitere Anliegen wie soziale und ökologische Motive.[41]

3. Erscheinungen

37 Alternative Zahlungsmittel sind so beschaffen, dass sie ihren, vom Urheber angedachten Zweck erfüllen können. *Da der angestrebte Zweck von Fall zu Fall unterschiedlich* ist, sind auch die Erscheinungsformen von komplementären Währungen sehr verschieden und nicht abschliessend aufzählbar.

38

---

39 Siehe VISCHER, Währungsrecht (Fn. 28), Rz. 11.

40 A-L. SCHMALZ, Komplementärwährungen zur Förderung der regionalen Wirtschaft in Städten und Gemeinden. Ein innovativer Ansatz für Kommunen, 2013, 15, erhältlich unter: <https://monneta.org/wp-content/uploads/2015/04/KommunaleWaehrungen-24.07.2013.pdf>.

41 C. GELLERI, Theorie und Praxis des Regiogeldes, in: M. Weis/H. Spitzeck (Hrsg.), Der Geldkomplex. Kritische Reflexion unseres Geldsystems und mögliche Zukunftsszenarien, Bern/Stuttgart/Wien 2008, 156-185 (174 ff.); SCHMALZ, Komplementärwährungen (Fn 40), 16 f.

Ein bekanntes und erfolgreiches Beispiel von Komplementärgeld stellt das 1933 ausgegebene Wörgler Freigeld bzw. Wörgler Arbeitswertscheine dar, welches auf die Theorien von SILVIO GESELL zurückgeht.[42] Das Wörgler Freigeld soll durch die Ausgestaltung als sogenanntes Schwundgeld – auch als Schrumpfgeld oder Geld mit inkorporierten Nennwertverlust bezeichnet – die Umlaufgeschwindigkeit des Zahlungsmittels steigern und damit die Wirtschaft ankurbeln. Das in der Schweiz bekannteste Beispiel einer komplementären Währung hingegen, das WIR-Geld, welches auf eine ähnliche Motivation zurückzuführen ist, kommt ohne diesen inkorporierten Nennwertverlust aus.

4. Risiken und Nachteile

Die Risiken und Nachteile von Komplementärwährung werden abzüglich der Risiken, welche durch Verwechslung mit einem staatlichen Geldzeichen entstehen könnten, v.a. in den nachteiligen Auswirkungen hinsichtlich der *Effektivität von geldpolitischen Massnahmen* der Nationalbank gesehen. Ferner hat insbesondere die Geldwäschereigesetzgebung entsprechende Risiken bei der Ausgabe von komplementären Zahlungsmitteln identifiziert.[43] 39

Darüber hinaus kann die Existenz von komplementären Zahlungsmitteln in einer Volkswirtschaft dazu führen, dass die staatliche Währung vom Publikum weniger nachgefragt wird. In einem solchen Fall könnte die Nationalbank gezwungen sein, nur in einem reduzierten Umfang neue Geldeinheiten in den Wirtschaftskreislauf einzubringen, was die Seigniorage bzw. Münzgewinn und damit den Ertrag, welcher aus der Geschäftstätigkeit der Nationalbank resultiert, beeinträchtigt. Ferner erhöhen miteinander konkurrenzierende Geldsorten in einer Volkswirtschaft die Informationskosten des Publikums, zumal ihr jeweiliger Wert in der Regel nicht beständig ist.[44] 40

Schlussendlich besteht zumindest das theoretische Risiko, dass wegen einer reduzierten Nachfrage nach staatlicher Währung aufgrund einer erhöhten Nutzung 41

42 GESELL, Wirtschaftsordnung (Fn. 19), 235 ff.

43 Dazu weiter hinten Rz. 89 f.; G. CLAEYS/M. DEMERTZIS/K. EFSTATHIOU, Cryptocurrency and monetary policy. Monetary Dialogue July 2018, 2018, 15; Bundesrat, Rechtliche Grundlagen der Distributed Ledger-Technologie und Blockchain in der Schweiz. Eine Auslegeordnung mit Fokus auf den Finanzsektor, 2018, 87 ff.; EZB, Virtual currency schemes, 2012, 33 ff.

44 DITTRICH, Stabilität (Fn. 5), 27; GELLERI, Regiogeld (Fn. 41), 182; K. BRUNNER, Konzepte der Geldordnung in einer freiheitlichen Wirtschaftsordnung, in: J. Starbatty/K. Brunner (Hrsg.), Geldordnung und Geldpolitik in einer freiheitlichen Gesellschaft, Tübingen 1982, 7-17 (14).

komplementärer Zahlungsmittel, die *Stabilität von bargeldlosen Zahlungsabwicklungssystemen, welche auf staatlicher Währung basieren, beeinträchtigt wird*.[45]

III. Kryptowährung als komplementäres Zahlungsmittel

42 Als Kryptowährung fallen über 2000 Varianten sogenannter „Kryptomünzen" (‹Crypto Tokens›) grundsätzlich in Betracht.[46] Indes sind nicht sämtliche Kryptomünzen als reines Zahlungsmittel bzw. Geld konzipiert und werden daher im Folgenden nicht als Kryptogeld bzw. Kryptowährung i.e.S. bezeichnet (**1.**). Kryptomünzen, welche mehr als ein blosses Zahlungsmittel darstellen, gelten daher als Kryptowährung i.w.S aber nicht als Kryptogeld (**2.**).

1. Kryptowährung als Geld (‹Zahlungstoken›)

43 Als reines Zahlungsmittel können diejenigen Kryptomünzen aufgefasst werden, welche tatsächlich oder in der Absicht des Urhebers als reines Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen Verwendung finden oder der Geld- und Wertübertragung dienen. Anders ausgedrückt, erschöpft sich der Wert bzw. die Nützlichkeit von Zahlungstokens in den Anwendungen auf der Blockchain (sogenannte ‹Native Tokens›).[47]

2. Kryptowährung i.w.S.

44 Die Zahlungstokens bzw. Kryptowährung i.e.S. oder Kryptogeld sind von den übrigen Formen von Kryptomünzen abzugrenzen, welche zwar faktisch *als Zahlungsmittel genutzt werden können, darüber hinaus noch weitergehende Ansprüche vermitteln*. Für eine Abgrenzung ist gemäss der Praxis der FINMA auf die wirtschaftliche Funktion des jeweiligen Tokens abzustellen.[48]

---

45 Zu diesem und dem vorherigen Absatz, BIZ, Digital currencies, Basel 2015, 15 f.; R. LASTRA/J. ALLEN, Virtual currencies in the Eurosystem. Challenges ahead, 2018, 26 ff., erhältlich unter: <http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619020/IPOL_STU(2018)619020_EN.pdf>.

46 Siehe für eine Übersicht: <https://coinmarketcap.com/all/views/all/>.

47 FINMA, Wegleitung für Unterstellungsfragen betreffend Initial Coin Offerings (ICOs), 2018, 3; Bundesrat, Grundlagen (Fn. 43), 67 ff.

48 Bundesrat, Grundlagen (Fn. 43), 100 ff.

2.1 Anlagetokens

Die Qualifikation als Anlagetoken ist davon abhängig, ob die jeweilige Kryptowährung einen Vermögenswert bzw. Wertrecht ausserhalb der Blockchain repräsentiert. Dieser Vermögenswert kann unter anderem eine bestimmte Sache oder aber auch ein Unternehmensanteil oder einen Anteil an einem Ertrag sein.[49] 45

In der Regel stellen Anlagetokens daher Effekten gemäss Art. 1 Abs. 2 lit. b FinfraG dar. 46

2.2 Nutzungstokens

Nutzungstokens gewähren dem Inhaber das Recht, in den Genuss einer bestimmten Dienstleistung oder eines Produkts zu kommen oder sich an einer dezentralen Organisation (DAO) beteiligen zu können (sogenannter ‹Work Token›).[50] Üblicherweise handelt es sich um ein digitales Produkt oder um eine Dienstleistung, welche durch eine Internetplattform erbracht wird. Denkbar sind allerdings auch nicht-digitale Güter und Angebote. 47

Weil das durch Nutzungstokens verkörperte Recht in der Regel keinen Bezug zum Kapitalmarkt aufweist, stellen Nutzungstokens keine Effekten dar.[51] 48

2.3 Hybride Tokens

Kryptomünzen können auch als Mischformen der genannten Kategorien bestehen. So sind insbesondere Anlagetokens und auch Nutzungstokens denkbar, welche zusätzlich als Zahlungsmittel genutzt werden. Ausserdem können sich Anlagetokens zu Nutzungstokens entwickeln, beispielsweise wenn Token zur Finanzierung des Aufbaus einer Plattform ausgegeben werden, welche nicht betriebsbereit ist.[52] 49

Als Mischformen haben hybride Tokens üblicherweise Effektenqualität.[53] 50

---

49 FINMA, Wegleitung (Fn. 47), 3.

50 M. EGGEN, Was ist ein Token? Eine privatrechtliche Auslegeordnung, AJP 2018, 558-567 (560 f.).

51 L. MÜLLER/M. REUTLINGER/P. KAISER, Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union, in: EuZ 2018, 80-102 (91); Bundesrat, Grundlagen (Fn. 43), 88 f.

52 Bundesrat, Grundlagen (Fn. 43), 89.

53 FINMA, Wegleitung (Fn. 46), 3.

2.4 Colored Coins

51 Schwierig ist eine Abgrenzung im Falle sogenannter ‹Colored Coins›, die ursprünglich als reine Zahlungstokens konzipiert waren, durch – nachgelagerte – Nutzerübereinkünfte aber Funktionen erhalten haben, welche für Anlage- oder Nutzungstokens typisch sind.

52 In der Mehrheit der Fälle ist die Abstellung auf die Absicht des Urhebers und damit eine Qualifikation als reines Zahlungstoken angebracht, zumal die Nutzerübereinkunft keine einklagbaren Rechte gewährt und sie meist auf einen eng begrenzten Personenkreis sowie Anwendungsbereich beschränkt bleiben – beispielsweise für virtuelle Gegenstände von Online-Mehrspieler-Rollenspiele.[54]

53 Für Colored Coins ist es daher meist angezeigt, sie nicht als Effekten zu behandeln.

3. Konsequenzen hinsichtlich des Untersuchungsgegenstands

54 Anlagetokens, Nutzungstokens und hybride Tokens gewähren dem Inhaber Vorteile, welche über die gewöhnlichen Rechte von Inhabern von Geldmitteln hinausgehen. Diese Tokens repräsentieren vermögenswerte Positionen, welche weder in der Substanz noch in der Funktion als Zahlungsmittel angelegt sind (sogenannte ‹Non-Native Tokens›). *Modernes Fiatgeld wird demgegenüber als stoffwertloses Geld bezeichnet, weil es keinen speziellen Bezug zu einzelnen, bestimmten, intrinsischen (Stoffwert) oder extrinsischen – d.h. abgeleitete – Werten hat*.[55] Der Wert bzw. Geltungsgrund von modernem Geld besteht vielmehr darin, dass es seine Funktion als stabiles universelles Schuldtilgungsmittel erfüllt.[56]

55 Aus dem Gesagten folgt, dass eine Beschränkung des Untersuchungsgegenstands auf Zahlungstokens, d.h. auf Kryptowährung i.e.S. (Kryptogeld), angebracht ist, zumal die *übrigen Formen – d.h. Anlagetokens, Nutzungstokens sowie hybride Tokens – Elemente aufweisen, welche atypisch für modernes Geld, d.h. Fiat-Geld bzw. Papiergeld, sind und sie daher als Effekte (Art. 2 lit. b FinfraG) qualifiziert werden können*. Reine Kryptogelder stellen demgegenüber – gemäss

54 Siehe auch E. HOFERT, Regulierung der Blockchain, 2018, Diss. Hamburg, Tübingen 2018, 37 f.

55 Siehe M. SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 73.

56 Siehe D. SUHR, Mehrwert (Fn. 31), 59 ff.

h.L. sowie der Praxis der FINMA – faktische bzw. immaterielle Vermögenswerte sui generis dar, welchen keine Effektenqualität zukommt.[57]

Kapitel 2: Kryptogeld als disruptive Technologie

I. Eigenschaften

Kryptogelder lassen sich weiter unterteilen in vollkommen anonymes Kryptogeld und solche, die lediglich als „pseudonymes" Kryptogeld gelten. Die Frage der Anonymität bei Zahlungsvorgängen ist für die Frage zentral, ob und inwieweit eine Regulierung gerechtfertigt ist. Im Folgenden wird daher zwischen bloss pseudonymen Kryptogeld (‹Bitcoin›) einerseits (**2.1**) und vollkommen anonymen Kryptogeld (‹Monero›) andererseits (**2.2**) unterschieden. Zunächst ist auf die allgemein gültigen Eigenschaften von Kryptogelder einzugehen (**1.**). 56

1. Allgemeine Eigenschaften

1.1 Dezentralität

Kryptogeld im hier verstandenen Sinn zeichnet sich massgeblich durch Dezentralität aus. Die Dezentralität wird durch kryptographische Verfahren ermöglicht und hat unterschiedliche Ausprägungen. 57

Zunächst erlauben Kryptogelder eine dezentrale Zahlungsverarbeitung. *Dezentralität in der Zahlungsverarbeitung bedeutet, dass der Kreis, der an der Verarbeitung beteiligten Personen, grundsätzlich offen* ist. Dies setzt voraus, dass ein für jedermann zugängliches Netzwerk besteht (sogenannte ‹permissionless Blockchain›).[58] 58

Ferner setzt Dezentralität voraus, dass *weder der Staat noch einzelne Private auf die Ausgabe von Geldeinheiten, die Zahlungsverarbeitung oder die Geldmengensteuerung usw. einen bestimmenden Einfluss ausüben* können. Vielmehr müssen Entscheidungen in diesen Angelegenheiten allein dem Programmcode obliegen, um als echtes Kryptogeld zu gelten. 59

---

57 H. BÄRTSCHI/C. MEISSER, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: R. Weber/F. Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 139 ff.; Bundesrat, Grundlagen (Fn. 43), 100.

58 Der Bundesrat, Grundlagen (Fn. 43), 25.

60 Darüber hinaus bedeutet Dezentralität *Disintermediation von Banken und anderen Dienstleistungsanbieter im Finanzbereich*. Kryptogeld kann vom Benutzer selbst aufbewahrt werden und Transaktionen mit Kryptogeld bedürfen nicht der Mitwirkung von Finanzintermediären oder Banken zu ihrer Durchführung.

61 Schlussendlich sollte der Programmcode von Kryptogeld open-source sein, d.h. dass er öffentlich einsehbar ist und in abgeänderter Form von anderen Personen weiterverwendet werden darf. Die *Einsehbarkeit des Programmcodes ist wichtig, um die Einhaltung der übrigen Voraussetzungen überprüfen zu können und hat auch Auswirkungen auf die Zensurresistenz* insofern eine allfällige Weiterentwicklung des Programmcodes – allenfalls als neues Kryptogeld mit einer anderen Rechnungseinheit – nicht von der Zustimmung einzelner Personen abhängt.

62 Ausdruck der Dezentralität ist die Verwendung eigener Währung- bzw. Rechnungseinheiten (beispielsweise Bitcoin: BTC oder Monero: XMR).

1.2 Immaterialität

63 Die Immaterialität stellt ein weiteres begriffsbestimmendes Element von Kryptogeld dar und hat Auswirkungen in zweifacher Hinsicht. Zunächst folgt aus der Immaterialität, dass Kryptogeld grundsätzlich keine körperliche Gestalt aufweist, sondern als elektronische Repräsentation einer Rechnungseinheit primär als digitale Aufzeichnung in Erscheinung tritt. Im Vordergrund steht allerdings die Voraussetzung, dass *Transaktionen mit Kryptogeld vollständig elektronisch durchgeführt werden können, d.h. ohne, dass die physische Übergabe einer Sache oder eines Legitimationsnachweises vorausgesetzt wäre*.[59]

64 Das Gesagte gilt jedoch nicht absolut, d.h. der zur Verfügung über das Guthaben notwendige, private Schlüssel – eine lange Zeichenkette aus Buchstaben und Zahlen, da Kryptogeld auf Public Key Cryptography basiert – kann beispielsweise ausgedruckt werden (sogenanntes ‹Paper Wallet›) und wie ein Geldschein dem Empfänger übereicht werden. Als Gegeneinschränkung ist jedoch festzuhalten, dass dieser Schlüssel vollständige Kontrolle verleiht, so lange das Guthaben nicht auf eine andere Zahlungsadresse transferiert wird und insofern das Risiko besteht, dass der ursprüngliche Schlüsselinhaber jenen Inhalt noch kennt und die Gelder veruntreuen könnte.

[59] FATF, Virtual Currencies. Key Definitions and Potential AML/CFT Risks, 2014, 4.

1.3 Universalität

Kryptogeld muss grundsätzlich universell einsetzbar sein. Universalität setzt zu- 65
nächst voraus, dass *erhaltene Geldstücke ohne weitere Validierung gleich wieder ausgegeben werden können* (Mehrweg-Token-System).[60]

Darüber hinaus müssen Kryptogelder *konvertibel sein, d.h. ihr Einsatz ist nicht* 66
nur auf einen ganz spezifischen Bereich beschränkt, wie beispielsweise bei einer bestimmten Warenhauskette. Alternativ genügt aus einer anti-geldwäschereimässigen Perspektive allerdings die Existenz eines Schwarzmarkts, wo nicht-konvertible Währungen gegen konvertible Währungen getauscht werden können.[61]

Ferner setzt Universalität voraus, dass *jeder Empfänger von Kryptogeld sein* 67
kann, der sich dazu bereit erklärt, und dass die Benutzung von keinen weiteren Voraussetzungen als den dafür notwendigen technischen Hilfsmittel abhängt. Dieser Gedanke ergibt sich bereits aus dem Aspekt der Dezentralität bzw. Disintermediation, nämlich dass keine zentrale Stelle über die Zulassung einer Person zur Benutzung von Kryptowährung entscheiden kann.

1.4 Funktionalität

68

Schlussendlich setzt der Begriff von Kryptogeld voraus, dass es sich um funktionales Geld handelt, d.h. dass *das Medium die geldmässigen Funktionen zumindest im Grossen und Ganzen erfüllt.* Dazu gehören in jedem Fall die Werttausch-, Wertaufbewahrungs- sowie Wertmassstabsfunktion, welche weiter unten im Detail erörtert werden.[62]

Kryptogeld kommt daher keinen weiteren, intrinsischen oder extrinsischen Wert zu als 69
denjenigen Wert, welches es aufgrund der Erfüllung dieser Funktionen bzw. ihrer Nützlichkeit zukommt. Der Wert bzw. Geltungsgrund von Kryptowährung ist anders ausgedrückt rein konsensueller Natur («bonitas conventionalis»).[63]

2. Spezielle Eigenschaften

60 Zum Begriff Mehrweg-Token-System siehe R. WEBER, Geld (Fn. 28), 57 f.; R. WEBER, E-Commerce und Recht, 2. Aufl., Zürich 2010, 595 f.; siehe auch J-D. SCHMID/A. SCHMID, Bitcoin. Eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, in: jusletter.ch vom 4. Jun. 2012, Rz. 6 ff.

61 FATF, Virtual Currencies (Fn. 59), 5.

62 Siehe dazu hinten Rz. 111 ff.

63 Siehe dazu M. SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 76.

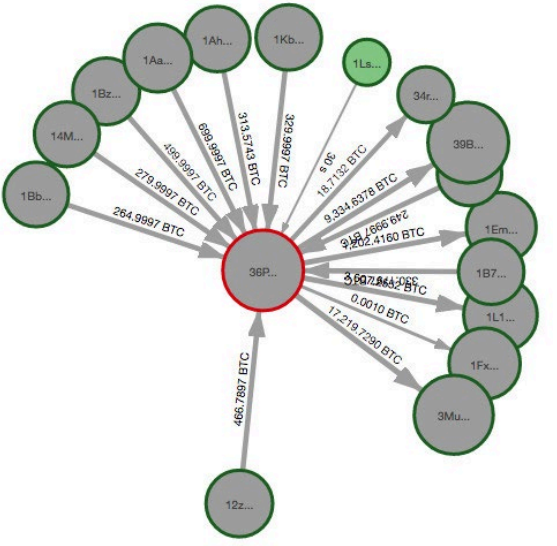
2.1 Bitcoin

70 Ungeachtet der genauen technischen Ausgestaltung im Einzelfall zählen sämtliche Kryptogelder als pseudonymes Kryptogeld, welche die oben genannten Kriterien für Kryptogeld erfüllen und die sich für die Zahlungsverarbeitung auf eine *öffentliche einsehbare Datenbank (Blockchain) stützen und Zahlungsabsender sowie Zahlungsempfänger mittels eines unveränderlichen Pseudonyms, d.h. einer Zahlungsadresse, identifizieren*. Ausserdem ist das Netzwerk von pseudonymem Kryptogeld nicht speziell gegen Überwachung – wie beispielsweise die Verknüpfung von Transaktionen mit IP-Adressen – geschützt.

71 Aufgrund der Öffentlichkeit der Blockchain können bei pseudonymen Kryptowährungen Transaktionen und die dabei verwendeten Einheiten von Kryptogeld über Jahre hinweg nachverfolgt werden. Dadurch eröffnet sich die Möglichkeit, eine Datenbank zu führen, welche Transaktionen bzw. bestimmte Geldeinheiten enthält, die im Zusammenhang mit einem Delikt stehen oder ein ausgewiesenes Risiko für Terrorismusfinanzierung oder ähnliches beinhalten – sogenannte ‹Tainted Coins›. Ferner können spezielle forensische Methoden – beispielsweise Clustering – auf der Blockchain dazu verwendet werden, Transaktionen bzw. Zahlungsadressen mit einer bestimmten Person in Verbindung zu bringen. Insbesondere besteht durch den *Abgleich mit weiteren, ausserhalb der Blockchain liegenden Datensätzen die Möglichkeit einer vollständigen Deanonymisierung* der auf der Blockchain gespeicherten Transaktionsdaten. Beispielsweise können Videoaufzeichnungen von Überwachungskameras bei Automaten oder Geschäften ausgewertet werden oder die Lieferadresse bei Händlern nachgefragt werden, bei denen inkriminiertes Kryptogeld ausgegeben wurde.[64]

64 Siehe zum ganzen Absatz J. GROßE, Nutzerverfolgung via Blockchain. Die Implikationen der öffentlich einsehbaren Transaktionshistorie von Bitcoin auf die Privatsphäre der Nutzer, fokus 2018, 18-22 (18 ff.).

Beispielansicht eines forensischen Tools für Bitcoin (‹Clustering›): 72



2.2 Monero

Die vollständig anonymen Kryptogelder, welche im Rahmen dieser Untersuchung unter dem Begriff Monero zusammengefasst werden, haben aufgrund ihrer besonderen technischen Ausgestaltung (‹Stealth Addresses›, ‹Ring Confidential Transactions› [RingCT])[65] *Vorkehrungen implementiert, welche eine Deanonymisierung durch forensische Techniken ausschliessen*. Sie zeichnen sich dadurch aus, dass die Blockchain und damit auch die Transaktionshistorie und die Kontostände im Vergleich zu Bitcoin nicht öffentlich einsehbar sind. Ausserdem sind die Netzwerke von anonymen Kryptogelder vor Netzwerküberwachung bzw. Netzwerkaufklärung geschützt.[66] 73

Weil die getätigten Transaktionen auf der Monero-Blockchain im Unterschied zur Bitcoin-Blockchain nicht öffentlich einsehbar sind, besteht keine Möglichkeit risikobehaftete Transaktionen zu markieren (Tainted Coins). Dies ist für den Empfänger von Monero ein Vorteil, zumal er nicht das Risiko trägt, dass die 74

65 <https://getmonero.org/resources/moneropedia/stealthaddress.html>; <https://www.getmonero.org/resources/moneropedia/ringCT.html>.

66 <https://www.getmonero.org/resources/moneropedia/kovri.html>.

Geldeinheiten vorbelastet und insofern weniger fungibel wären, was den Wert der jeweiligen Geldeinheiten beeinträchtigt. Darüber hinaus setzt sich der Empfänger von Monero nicht dem Risiko aus, dass er unbewusst vorbelastete Geldeinheiten annimmt und dadurch selbst in den Verdacht gerät, Geldwäscherei oder Terrorismusfinanzierung usw. zu betreiben.

II. Disruptive Wirkungen von Kryptogeld

1. Revolution der Peer-to-Peer Zahlungen

75 Kryptogeld stellt eine eigentliche *Revolution der Peer-to-Peer Zahlungsmittel* dar, zumal lange davon ausgegangen wurde, dass elektronische Peer-to-Peer Bezahlvorgänge wegen der Anfälligkeit für Manipulationen in dezentralen Systemen, d.h. eine Wiederverwendung erhaltener Geldzeichen ohne Validierung durch eine zentrale Stelle, nicht realisierbar seien.

76 Bitcoin und Monero lösen diese Problematik mithilfe von Proof-of-Work (PoW). Manipulation der Blockchain sind zwar theoretisch möglich, lohnen sich wirtschaftlich angesichts des notwendigen Aufwands jedoch nicht.

77 Elektronische Peer-to-Peer Zahlungsmittel haben starke disruptive Wirkung im Bereich der Zahlungsverarbeitung und damit auf die individuelle Autonomie, da sie Finanzintermediäre wie Banken und Zahlungsdienstleister, wie beispielsweise Kreditkarteninstitutionen und Zahlungstransferanbieter, für elektronische Zahlungen und Kontoführung überflüssig machen (‹Disintermediation›). Mit Kryptowährungen können insbesondere grenzüberschreitende Zahlungen einfach, sicher und schnell ausgeführt werden. Darüber hinaus ist der Zugang zu Kryptogeld prinzipiell offen für jedermann – insbesondere auch für Personen, welche vom Finanzsystem ausgeschlossen sind (‹Unbanked›). Andererseits können durch Irrtum oder Betrug veranlasste Transaktionen nicht ohne Mitwirkung des Empfängers rückgängig gemacht werden, und es besteht keine Möglichkeit des Ersatzes von verlorenem oder gestohlenem Kryptogeld.

2. Regulierung der Finanzintermediäre

78 Die Möglichkeit, Transaktionen weltweit und mittels einer dezentral organisierten Struktur auszuführen, hat ferner disruptive Wirkung im Bereich der Geldwäschereiregulierung, zumal der konventionelle Regulierungsansatz auf der Prämisse beruht, dass identifizierbare Personen oder Unternehmen existieren, welche einen bestimmenden Einfluss auf die Zahlungsverarbeitung haben (sogenannte ‹Gatekeeper›). Die geltende Gesetzgebung verpflichtet die Finanzintermediäre

unter anderem dazu, sämtliche Transaktionen zu überwachen und falls angezeigt, verdächtige Transaktionen und Kunden zu melden. Die Nichtbeachtung dieser Pflicht kann zum Entzug der Bewilligung sowie zu strafrechtlichen Sanktionen führen (Art. 305ter StGB).[67]

Die Zahlungsverarbeitung bei Kryptogelder erfolgt demgegenüber dezentral und ist offen für weitere Teilnehmer, welche sich an der Zahlungsverarbeitung beteiligen möchten (Miner). *Die konzeptionelle Offenheit stützt sich auf die Kryptographie und hat zur Folge, dass die Miner sich nicht zu identifizieren brauchen und in einem nicht oder nur schwach reguliertem Land operieren können sowie jederzeit austauschbar sind*. Darüber hinaus haben einzelne Miner keinen Einfluss auf die Entscheidung über die Gültigkeit einer Zahlung. Die dem konventionellen Regulierungsansatz zugrunde liegende Prämisse ist daher im Bereich von Kryptogeld à priori nicht gegeben und es muss daher nach alternativen Lösungen gesucht werden. 79

Ferner können auch neuere Regulierungsansätze für bestimmte Internetangebote, wie Netzsperren für Internetcasinos (Art. 86 BGS)[68], nicht auf Kryptogelder angewandt werden, da *IP-Adressen-Sperren oder Manipulationen von DNS-Einträgen in einem Peer-to-Peer Netzwerk als praktisch wirkungslos betrachtet werden*.[69] 80

3. Staatliches Währungsmonopol und Geldschöpfung

Kryptogeld könnte ausserdem im Zusammenhang mit dem staatlichen Währungsmonopol disruptive Wirkungen zeitigen. Die Koexistenz eines alternativen Geldmittels in einer Volkswirtschaft kann dazu führen, dass die Nachfrage nach der staatlichen Währung zurückgeht. Der Staat bzw. die Nationalbank kann in einer solchen Situation grundsätzlich weniger staatliche Währung neu in Umlauf bringen, was den Münzgewinn bzw. die Seigniorage schmälert. 81

Die Existenz eines alternativen Zahlungsmittels in einer Volkswirtschaft, welches der Kontrolle der Nationalbank entzogen ist, könnte zur Folge haben, dass die *Effektivität geldpolitischer Massnahmen reduziert ist*. Für das Individuum 82

---

67 ZUBERBÜHLER, Hilfspolizisten (Fn. 2), 33 ff.

68 Bundesgesetz vom 29. Sep. 2017 über Geldspiele, Geldspielgesetz (BGS, SR 953.51).

69 Siehe M. JOHNSON/D. MCGUIRE/N. WILLEY, The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users, 2008, erhältlich unter: <https://www.researchgate.net/publication/221179348_The_Evoltion_of_the_Peer-to-Peer_File_Sharing_Industry_and_the_Security_Risks_for_Users>.

hingegen stellt die Unbeeinflussbarkeit ein Vorteil dar, da es Kryptogeld dazu verwenden kann, um sich gegen die Nachteile, welche aus möglichen Massnahmen – beispielsweise Negativzinsen oder sogar Währungsreform – drohen, zu schützen.[70]

III. Abgrenzung des Untersuchungsgegenstands sowie Problemaufriss

1. Abgrenzung gegenüber weiteren möglichen Regulierungsschwerpunkten mit Kryptogeld

83 Finanzmarktrechtliche und geldwäschereirechtliche Regulierungen von Kryptogeld können unterteilt werden in solche, die in erster Linie die Finanzintermediäre betreffen – und allenfalls vermögensrechtliche Interessen und Gleichbehandlungsansprüche der Kunden gegenüber jenen schützen – sowie in *Regulierungen, die sich zwar primär an Finanzintermediäre als unmittelbare Normadressaten richten, jedoch zugleich massgebliche Auswirkungen auf die Benutzer von Kryptogeld und deren Umgang mit Kryptogeld als Zahlungsmittel haben*. Regulierungen, die keine oder nur sehr geringe grundrechtliche Relevanz für die gewöhnlichen Benutzer aufweisen, sind für die vorliegende Untersuchung nicht von Interesse. Ausserdem kann auf eine zivilrechtliche sowie steuerrechtliche Einordnung von Kryptogeld verzichtet werden. Folgende Fragestellungen im Zusammenhang mit Kryptogeld werden daher nicht weiter untersucht:

1.1 Finanzmarktrecht

a. Betrieb eines Zahlungssystems (Art. 81 FinfraG)

84 Kryptogelder können als Zahlungssystem im Sinne von Art. 81 FinfraG gelten, da sie gestützt auf einheitliche Regeln und Verfahren Zahlungsverpflichtungen abrechnen und abwickeln. Es stellte sich die Frage, ob die Anforderungen, welche das FinfraG für Zahlungssysteme stellt, auch für Kryptogelder als dezentralisierte Zahlungssysteme gelten sollen. *Die Frage, ob und wie ein dezentral betriebenes Zahlungssystem reguliert werden kann, steht im Zentrum der Untersuchung, allerdings liegt der Fokus der vorliegenden Arbeit auf den Beeinträchtigungen der*

---

70 Zu diesem und dem vorherigen Absatz: R.J. Cook, Bitcoins. Technological Innovation or Emerging Threat? in: J. Marshall J. Info. Tech. & Privacy L. 2014, 535-570 (553 ff.).

Benutzer. Das FinfraG hat demgegenüber das primäre Ziel, die Funktionsfähigkeit und Stabilität von Finanzmarktinfrastrukturen zu sichern (Art. 1 Abs. 2 FinfraG).

Die Funktionsfähigkeit und Stabilität von Kryptogeld-Infrastrukturen wird durch die Dezentralität sichergestellt, bzw. genauer gesagt, durch die Möglichkeit der Beteiligung einer – möglichst – grossen Zahl von Personen und Computern an der Zahlungsverarbeitung. Kryptogelder weisen daher eine hohe Ausfallsicherheit sowie Zensurresistenz auf. 85

b. Betrieb einer Kryptobörse (Art. 26 FinfraG)

Börsen und multilaterale Handelssysteme (MHS) könnten auch *Zahlungstoken zum Handel zulassen*, obwohl das FinfraG grundsätzlich lediglich auf Finanzmarktinfrastrukturen, welche mit Effekten oder Derivaten handeln, anwendbar ist (Art. 1 FinfraG).[71] 86

Die Frage, ob das FinfraG – d.h. einzelne Bestimmungen oder in seiner Gesamtheit – auch auf Börsen und MHS, welche nur den Handel mit reinen Zahlungstoken zulassen, anwendbar ist, muss im Rahmen der vorliegenden Arbeit nicht entschieden werden; zumal – wie bereits erwähnt – *der Fokus auf Beschränkungen der Benutzer im Umgang mit Kryptogeld liegt*. 87

c. Entgegennahme von Zahlungstoken-Einlagen (FIDLEG)

Die Entgegennahme von fremden Zahlungstokens als Einlage gemäss Art. 3 lit. a Ziff. 6 FIDLEG – beispielsweise im Rahmen von Crowdfunding – kann nach Ansicht des Bundesrats ein Finanzinstrument im Sinne dieses Gesetzes darstellen.[72] Die Vorschriften des FIDLEG kämen in diesem Fall zur Anwendung (insbesondere Art. 7 ff. FIDLEG). Allerdings können Einlagen mit Kryptowährung durch sogenannte ‹Multi-Signature-Keys› (kurz: *multisig-Keys* bzw. *multisig*-Schlüssel) *geschützt werden und dem Treuhänder so die exklusive Verfügungsmacht über die Vermögenswerte genommen werden*. Es stellte sich die Frage, ob Einlagen mit Kryptogeld, insbesondere diejenigen, welche mithilfe von *multisig*-Schlüssel 88

71 MÜLLER/REUTLINGER/KAISER, Regulierung (Fn. 51), 89; Bundesrat, Grundlagen (Fn. 43), 108.

72 Bundesrat, Grundlagen (Fn. 43), 123; siehe auch KGGT, National Risk Assessment (NRA). Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding, 9 ff.

geschützt sind, als Einlagen zu qualifizieren sind.[73] Diese Fragestellung betrifft den Umgang mit Kryptogeld nur am Rande und wird daher nicht weiterverfolgt.

1.2 Emission von Kryptogeld

89 Die Emission von nicht in Bargeld bestehenden Zahlungsmitteln stellt gemäss Art. 4 Abs. 1 lit. b GwV eine Dienstleistung für den Zahlungsverkehr und damit eine finanzintermediäre Tätigkeit dar. Diese Bestimmung will sicherstellen, dass die *Rückverfolgbarkeit von Vermögenswerten nicht durch den Erwerb eines neuen Zahlungsmittels vereitelt werden kann*. Die geldwäschereirechtliche Problematik, d.h. die Frage nach der Herkunft der Vermögenswerte, bezieht sich daher nur dann auf Kryptogeld, falls es zum Erwerb eines neuen Zahlungsmittels eingebracht wird. In der Praxis dürften solche Vorgänge jedoch nur in wenigen Ausnahmefällen relevant werden und sind daher nicht zu den Alltagsgeschäften von Konsumenten zu zählen. Es rechtfertigt sich daher die Ausklammerung dieser Fragestellung in der vorliegenden Untersuchung.

90 Die Emission von Kryptogeld (sogenannter [I]nitial [C]oin [O]ffering) könnte eine Ausgabe von nicht in Bargeld bestehenden Zahlungsmittel im Sinne von Art. 4 lit. b GwV und damit eine dem GwG unterstellte Dienstleistung für den Zahlungsverkehr darstellen.[74] Die Schaffung bzw. Verbreitung von *Kryptogeld durch ICO ist durch den oben genannten Grundsatz der Dezentralität zwar nicht prinzipiell ausgeschlossen, aber wäre ungewöhnlich*.

1.3 Bankengesetz

91 Eine weitere mögliche Fragestellung betrifft die Qualifikation von anvertrauten Kryptogelder als Einlage gemäss BankG. Wie bei beim Crowdfunding lässt sich die Frage stellen, ob es sich bei den auf die Plattform bzw. Bank eingezahlten Geldern *um Publikumseinlagen nach dem Bankengesetz (Art. 1a BankG) handelt und somit eine bewilligungspflichte Banktätigkeit vorliegen könnte*. Diese Fragestellung wird im Rahmen dieser Arbeit jedoch nicht weiterverfolgt.[75]

1.4 Zivil- und steuerrechtliche Behandlung von Kryptogeld

92 Die *herrschende Lehre und die FINMA qualifizieren Kryptogeld als faktische, immaterielle Vermögenswerte*. Ob Kryptogeld darüber hinaus beispielsweise als

---

73 HOFERT, Blockchain (Fn. 54), 37 f.; siehe auch MÜLLER/REUTLINGER/KAISER, Entwicklungen (Fn. 51), 90.

74 FINMA, Wegleitung (Fn. 47), 6; siehe auch J. ESSEBIER/J. BOURGEOIS, Die Regulierung von ICOs, in: AJP 2018, 568-579 (573).

75 Siehe dazu BÄRTSCHI/MEISSER, Währungen (Fn. 57), 126 ff.

Forderung oder Anerkennungsanspruch gegenüber weiteren Blockchain-Teilnehmern zu qualifizieren wäre, wird nicht untersucht. Auch weitere zivilrechtliche Fragestellungen, wie z.B. die Pfandtauglichkeit von Kryptogeld, die Einbringlichkeit zur Mindestkapitalisierung von Unternehmen usw., brauchen im Rahmen der vorliegenden Arbeit nicht beantwortet zu werden.[76]

Ferner kann auf eine Darstellung der steuerrechtlichen Aspekte von Kryptogeld, beispielsweise hinsichtlich der Umsatzsteuer, Vermögenssteuer usw. sowie deren Bemessungen, verzichtet werden.[77] 93

Eine Ausnahme davon stellt die Bekämpfung von Steuerhinterziehung auf internationaler Ebene dar. Kryptogeld wird nämlich immer wieder als Mittel zur Begehung von Steuerhinterziehung genannt.[78] Ausserdem steht die Bekämpfung von grenzüberschreitender Steuerhinterziehung in einem sachlichen Zusammenhang mit der Bekämpfung von Geldwäscherei. 94

2. Problemaufriss

Die Regulierung von Kryptogeld befindet sich in einem Spannungsverhältnis zwischen persönlicher Freiheit und einem wettbewerbsfähigen Finanzplatz auf der einen Seite sowie Sicherheit und den völkerrechtlichen Vorgaben, welche die Schweiz aufgrund ihrer internationalen Einbindung betreffen auf der anderen Seite. 95

2.1 Freiheit vs. Sicherheit

Dreh- und Angelpunkt der vorliegenden Untersuchung bildet der Grundrechtskatalog der BV. Die *Benutzung von Kryptogeld ist zunächst als Ausdruck privatautonomer Gestaltung des eigenen Lebens aufzufassen*. Ausserdem ist die 96

---

76 Siehe dazu B. ENZ, Die zivilrechtliche Einordnung von Zahlungs-Token wie dem Bitcoin als «Registerwertdaten» und deren Aussonderbarkeit im Konkurs de lege lata und de lege ferenda, in: SJZ 2020, 291-298 (291 ff.); H.C. VD. CRONE/F. KESSLER/L. ANGSTMANN, Token in der Blockchain. Privatrechtliche Aspekte der Distributed Ledger Technologie, in: SJZ 2018, 337-345 (340 ff.); M. EGGEN, Token (Fn. 50), 560 ff.; M. EGGEN, Verträge über digitale Währungen, in: jusletter.ch vom 4. Dez. 2017, Rz. 17 ff.; B. GRAHAM-SIEGENTHALER/A. FURRER, The Position of Blockchain Technology and Bitcoin in Swiss Law, in: jusletter.ch vom 8. Mai 2017, Rz. 40 ff.

77 Siehe dazu, BÄRTSCHI/MEISSER, Währungen (Fn. 57), 156 ff.

78 Siehe statt vieler EBA, Opinion on 'virtual currencies', 2014, 34; zurückhaltend: W. J. LUTHER, Regulating Bitcoin. On What Grounds, in: H. Peirce/B. Klutsey (Hrsg.), Reframing Financial Regulation. Enhancing Stability and Protecting Consumers, Arlington 2016, 391-415 (400).

Vertragsfreiheit, und genauer die Vertragsinhaltsfreiheit, bei Beschränkungen der Wahl des Zahlungsmittels betroffen. Weil der Fokus auf den Benutzern von Kryptogeld liegt, stellt sich unter anderem die Frage, ob auch nicht-gewerblich tätige Personen, d.h. der Konsumentenseite, die Berufung auf die Vertragsfreiheit offensteht, welche die herrschende Lehre als Teilgehalt der Wirtschaftsfreiheit anerkannt.

97 Darüber hinaus gibt es spezifische Grundrechte, die von einer Regulierung von Kryptogeld betroffen sein können. Dazu zählen unter anderem die informationelle Selbstbestimmung, die Wirtschaftsfreiheit sowie die persönliche Freiheit. Daraus folgt, dass die Benutzung von Kryptogeld nur aufgrund von legitimen öffentlichen Interessen und nicht unverhältnismässig stark eingeschränkt werden darf (Art. 36 BV).

98 Als Gründe für die Einschränkung der Benutzung von Kryptogeld besteht das Risiko der Begehung schwerer Straftaten, wie beispielsweise Terrorismusfinanzierung, Geldwäscherei oder sogar Proliferation von Massenvernichtungswaffen. Die vorliegende Arbeit widmet sich der Frage, welche Regulierungen zur Verhinderung dieser Delikte verfassungsrechtlich bzw. grundrechtlich gerechtfertigt sind.

99 Darüber hinaus liesse sich an eine Regulierung von Kryptogeld aus Gründen des Konsumentenschutzes sowie der Stabilität als Infrastruktur im Zahlungsverkehr denken. Ferner wurde der hohe Stromverbrauch, welcher zur Absicherung der dezentral geführten Datenbank notwendig ist (PoW), als Grund für eine mögliche Regulierung genannt. Diese Regulierungsmotive werden nicht weiter untersucht, zumal der Fokus der vorliegenden Arbeit auf Beschränkungen der Benutzer im Umgang mit Kryptogeld liegt.

2.2 Finanzplatz Schweiz und internationale Einbindung

100 Die Regulierung von Kryptogeld befindet sich ferner in einem Spannungsfeld zwischen dem *Interesse an einem wettbewerbsfähigen Finanzplatz und den völkerrechtlichen Verpflichtungen*, welche auch die Schweiz, insbesondere aufgrund ihrer Einbindung in internationalen Organisationen und Institutionen, betreffen.

101 Die Wettbewerbsfähigkeit und Standortattraktivität des Finanzplatzes Schweiz sind wegen dessen gesamtwirtschaftlicher Bedeutung von hohem Stellenwert für den Wirtschaftsstandort. Die Schweizer Bevölkerung und Wirtschaft profitiert von einem leistungsstarken Finanzplatz unter anderem aufgrund der gebotenen

Beschäftigung, der generierten Wertschöpfung und Steuersubstrate.[79] Der Finanzplatz Schweiz ist allerdings in einem umkämpften globalen Standortwettbewerb mit den übrigen internationalen Finanzzentren eingebunden.

Die Attraktivität und Wettbewerbsfähigkeit des Finanzplatzes Schweiz sollen auch bei zukünftigen technologischen Umwälzungen gewahrt werden. Für Geschäftsmodelle, welche auf neuartigen Technologien basieren, sollen demnach keine weiteren Schranken gelten, als für konventionelle Geschäftsmodelle. Die *Schweiz setzt dazu auf einen prinzipienbasierten und technologieneutralen Rechtssetzungs- und Regulierungsansatz, welcher zwar Ausnahmen zulässt, diese indes an die Voraussetzung der Wettbewerbsneutralität anknüpft*.[80] 102

Die Schweiz ist allerdings bei der Regulierung des eigenen Finanzsektors nicht frei. Kriminelle Akteure nutzen das globale Finanzsystem sowie spezifische rechtliche Strukturen in unterschiedlichen Staaten, um die wahren Eigentümer, die Herkunft oder die Verwendung von Vermögenswerten zu verschleiern und gleichzeitig ihre Verfügungsmöglichkeiten darüber zu erhalten. *Verschiedene internationale Organisationen – bei denen die Schweiz ausserdem Mitglied ist (UNO, Europarat und G20 (FATF)) – überwachen daher internationale Finanzmärkte auf Missbräuche und Defizite insbesondere im Hinblick auf die Verhinderung von Terrorismusfinanzierung und Geldwäscherei*. Ausserdem stehen die Verhinderung der Verbreitung von Massenvernichtungswaffen bzw. ‹Non-Proliferation of Weapons of Mass Destruction› (NPWMD) sowie Bestechungsdelikte, insbesondere jene von fremden Amtsträgern, unter Beobachtung internationaler Organisationen. Die Empfehlungen und Entscheide der FATF spielen dabei eine entscheidende Rolle. Die FATF führt sogenannte Black- und Greylists, welche Länder mit Defiziten benennen und die massgebend sind für den Marktzugang von inländischen Finanzdienstleistern im Ausland und sogar für Rettungspakete des IWFs sowie der Weltbank sind.[81] Auch die EU – bei der die 103

79 Eidgenössisches Finanzdepartement, Finanzplatz und Finanzmarktpolitik Schweiz, 2006, 3 ff.

80 R.H. WEBER/S. BAUMANN, FinTech – Schweizer Finanzmarktregulierung im Lichte disruptiver Technologien. Regulierungsansätze für neue Finanzdienstleistungstechnologien, in: jusletter.ch vom 21. Sep. 2015, Rz. 53; Bundesrat, Grundlagen (Fn. 43), 8 ff.

81 M. LIEBI/L. CONOD, Art. 4 GwG, in: P.V. Kunz/T. Jutzi/S. Schären (Hrsg.), Geldwäschereigesetz, Stämpflis Handkommentar, Bern 2017, Rz. 1 ff.; U. EMCH/H. RENZ/R. ARPAGAUS, Das Schweizerische Bankgeschäft, 7. Aufl., Zürich 2011, Rz. 440 ff.; siehe A. PERRAS, Terrorfinancier endlich verurteilt, in: DerBund vom 19.2.2020, 4.

Schweiz ein besonderes Interesse am Marktzugang hat – hat die Empfehlungen der FATF als Mindeststandard übernommen.[82]

[82] Europäische Kommission, Vorschlag für eine Richtlinie des europäischen Parlamentes und des 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) 450 final, 18.

Teil II:
Die Regulierung von Kryptogeld de lege lata

Kapitel 1: Kryptogeld in der Bundesverfassung

Eine *bundesrechtliche Regulierung von Kryptogeld setzt eine Kompetenzgrundlage in der Bundesverfassung voraus*. Eine solche Kompetenznorm könnte zunächst im Geld- und Währungsmonopol (Art. 99 Abs. 1 BV) bestehen (**I.**). Ferner könnte die Kompetenz zur Regulierung privatwirtschaftlicher Tätigkeit im Finanzbereich (Art. 95 und 98 Abs. 2 BV) (**II.**) oder die Gesetzgebungskompetenz im Bereich des Strafrechts (Art. 123 BV) in Betracht kommen (**III.**). 104

I. Geld- und Währungsmonopol (Art. 99 Abs. 1 BV)

Die *Währungsverfassung umfasst sämtliche Normen mit verfassungsmässigem Rang, welche die Geldordnung im Staat definieren*. Sie geben Auskunft, wie der Staat seine aus der Geldhoheit fliessenden Kompetenzen ausübt.[83] Für die Währungsverfassung stellt das Geld- und Währungsmonopol (Art. 99 Abs. 1 BV) die bedeutsamste Bestimmung dar. Ferner zählt zur Währungsverfassung das Bargeldmonopol (Art. 99 Abs. 1 BV) sowie die Bestimmung des WZG, welche unter anderem als Währungseinheit für die Schweiz den Franken festlegt (Art. 1 WZG). Es stellt sich die Frage, ob Kryptogeld von der Währungsverfassung überhaupt erfasst ist. 105

1. Unterscheidung Geldmonopol und Währungsmonopol

Art. 99 Abs. 1 BV gewährt dem Bund eine ausschliessliche und umfassende Kompetenz im Bereich des Geld- und Währungswesens. Man kann sich daher fragen, *ob eine Unterscheidung zwischen Geldmonopol sowie Währungsmonopol entlang der in der – deutschen Fassung – der BV getroffenen begrifflichen Differenzierung geboten* ist. 106

Die Botschaft des Bundesrats zum neuen Geld- und Währungsartikel in der BV (Art. 99 BV) sieht eine Unterscheidung vor, zumal der Anwendungsbereich des Währungsmonopols weiter als derjenige des Geldmonopols gezogen wird. Nach Ansicht des Bundesrats bezieht sich der verfassungsrechtliche Geldbegriff auf den engen Anwendungsbereich der staatlich anerkannten Zahlungsmittel (siehe Art. 2 WZG). Demgegenüber erfasse der Begriff der Währung bzw. das Währungsmonopol Geld in seiner abstrakten Funktion als Rechnungseinheit.[84] 107

---

83 D. SUHR, Geldordnung (Fn. 32), 92.

84 Botschaft vom 27. Mai 1998 über einen neuen Geld- und Währungsartikel in der Bundesverfassung, BBl 1998 IV 4007, 4028 ff.

Dem *Währungsmonopol käme daher ein weiterer Anwendungsbereich zu, nämlich für sämtliche Gegenstände, die aufgrund ihrer Standardisierung wie Geld genutzt werden können und im Verkehr als solches benutzt werden* – beispielsweise ausländische Währungen oder sogar Zigaretten (sogenanntes usuelles Geld).

108 Allerdings hebt die Botschaft den zuvor eng gezogenen Anwendungsbereich des Geldmonopols gleich wieder auf, indem sie ausführt, dass als Geld im Sinne der Verfassung und damit zum Geldmonopol auch Geldmittel zu zählen sind, welche aufgrund ihres Volumens die Gefahr einer Beeinträchtigung des staatlichen Geldschöpfungsprozess bereiten.[85] Das *Geldmonopol umfasst nach Ansicht der Botschaft somit auch diejenigen Rechnungseinheiten, welche aufgrund ihrer Verbreitung bzw. ihrer regen Benützung wie ein Geldmittel behandelt werden sollen* und geht somit von einem weiten Anwendungsbereich aus, der auch das usuelle Geld umfassen kann.

109 Daraus folgt, dass das Währungsmonopol mit dem Geldmonopol zusammenfallen kann und daher eine genaue Einordnung a priori nicht möglich ist. Insofern *rechtfertigt es sich, das Währungs- und Geldmonopol als Einheit zu behandeln und nach Kriterien zu fragen, welche die Aspekte des Währungsmonopols und des Geldmonopols miteinander verbinden*.

110 Darüber hinaus zeigt ein Vergleich mit der französischen sowie italienischen Fassung der BV, dass eine Unterscheidung zwischen Währungsmonopol und Geldmonopol nicht angezeigt ist. In den *beiden romanischen Sprachen operiert die BV alleine mit den Begriffen «la monnaie» und «settore monetario» und meint jeweils sowohl das Währung- wie auch das Geldmonopol*.[86] Für das deutsche Grundgesetz wurde ferner explizit postuliert, «dass ‹das Währungs-, Geld- und Münzwesen› eine unteilbare Gesetzgebungsmaterie darstellt, die dementsprechend nur einheitlich gedeutet werden kann.»[87] Im Folgenden wird daher vom Währungsmonopol gesprochen, um den umfassenden Charakter dieser Kompetenz deutlich zu machen. Das Geldmonopol ist dabei jedoch stets mitgemeint.

---

85 Botschaft Währungsartikel (Fn. 84), 4029 f.

86 Art. 99 BV in der französischen sowie italienischen Fassung.

87 M. NIEDOBITEK, Art. 73 Nr. 4 GG (Mai 2001), in: C. Waldhoff/K. Vogel (Hrsg.), Bonner Kommentar zum Grundgesetz, Heidelberg, Loseblatt, Rz. 48; a. A.: HERRMANN, Währungshoheit (Fn. 8), 73.

2. Mögliche Perspektiven

2.1 Funktionale Betrachtungsweise

Die Qualifikation eines Mediums als Geld setzt gemäss der funktionalen Betrachtungsweise eine Erfüllung der drei zentralen geldmässigen Funktionen (Tauschmittelfunktion, Wertmassstabsfunktion sowie Wertaufbewahrungsfunktion) voraus. In einer *funktionalen Betrachtungsweise brauchen nicht alle drei Funktionen vollständig erfüllt zu sein*, zumal Zielkonflikte zwischen den einzelnen Aspekten bestehen und deren jeweilige Bedeutung historisch immer wieder unterschiedlich bewertet wurde.[88] 111

a. Tauschmittelfunktion

Die Frage der Erfüllung der Tauschmittelfunktion hängt im Wesentlichen davon ab, ob das Medium fungibel ist. *Die Fungibilität ist abhängig von der Eignung des Mediums zur Übertragung bzw. zum Austausch (Liquidität) sowie der örtlichen Bereitschaft zur Annahme (Universalität)*. Der Grad der Liquidität lässt sich am Aufwand an Energie, Arbeit und Kosten messen, welche notwendig sind, um einen Gegenstand zum Austausch zu bringen (sogenannte Transaktions- und Informationskosten). Eine absolute Liquidität liegt vor, wenn der Gegenstand jederzeit und ohne zusätzlichen Mehraufwand sowie ohne Werteinbusse für den Austausch zur Verfügung steht. Die Universalität bestimmt sich nach der Anzahl der möglichen Vertragspartner, bei welchen die Bereitschaft vorhanden ist, das jeweilige Geldmittel zu akzeptieren.[89] 112

Kryptogelder stellen (elektronische) *Mehrweg-Token-Systeme dar, welche eine sofortige Wiederverwendung einzelner Geldeinheiten ohne vorgängige Validierung erlauben*.[90] Sie erleiden keine Werteinbusse im Austausch. Ausserdem kann der Inhaber von Kryptogelder direkt über diese verfügen (sogenannte finale oder ‹Peer-to-Peer› Zahlung) und ist nicht wie Kontoinhaber bei Buchgeld auf Anweisungen zur Zahlungsausführung beschränkt. Diese Möglichkeit besteht, weil die Benutzer von Kryptogeld im Unterschied zum Banken-Buchgeld es grundsätzlich selbst halten können – beispielweise bereits auf einem Smartphone. 113

Demgegenüber stellen Kryptogelder keine gesetzlichen Zahlungsmittel dar und es fehlt ihnen daher die universelle Schuldtilgungswirkung sowie die 114

88 C. PROCTOR, Mann on the Legal Aspects of Money, 7. Aufl., Oxford 2012, Rz. 1.08; vgl. MENGER, Geld (Fn. 20), 18.

89 SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 216 ff.

90 Zum Begriff Mehrweg-Token-System siehe vorne Rz. 65.

grundsätzliche Annahmepflicht (sogenannter ‹gesetzlicher Kurs›). Dies *beeinträchtigt zunächst ihre Liquidität, weil die Tilgungswirkung von einer vertraglichen Vereinbarung abhängt*. Ferner ist auch die Universalität reduziert, weil die Annahme grundsätzlich freiwillig ist und in der Regel keine staatlichen Abgaben, d.h. Gebühren, Steuern usw., damit gezahlt werden können. Allerdings ist als Gegeneinschränkung festzuhalten, dass der Einsatzbereich für Kryptogelder, im Unterschied zu vielen gesetzlichen Zahlungsmittel nicht auf einen bestimmten Staat beschränkt ist, sondern grundsätzlich weltweit ist. Ausserdem kann durch vertragliche Abrede die Erfüllung bzw. Tilgungswirkung einer Schuld in Kryptogeld vereinbart werden, was immerhin zwischen den Parteien Wirkungen entfaltet.

115 Zweifellos erfordern Kryptogelder – im Vergleich zu staatlichem Geld – ein Mehraufwand hinsichtlich der Informationsgewinnung, insbesondere hinsichtlich der Wertbestimmung, zumal Löhne, Steuern und weitere Preise in der Regel in staatlicher Währung ausgedrückt sind. *Die Informationskosten für den Einsatz von Kryptogeld sind daher meist höher als beim Einsatz von gesetzlichen Zahlungsmitteln*. Kryptogeld ermöglicht jedoch gleich wie gewöhnliches Geld die Entkoppelung der Notwendigkeit eines direkten Güteraustausches für die Bedürfnisbefriedigung.[91]

116 Die Erfüllung der Tauschmittelfunktion setzt keine hundertprozentige Liquidität des in Frage stehenden Mediums voraus.[92] *Kryptogeld, d.h. Bitcoin und Monero, erfüllen daher Voraussetzungen, welche die Tauschmittelfunktion an Geld stellt*.

b. Wertmassstabsfunktion

117 Die Erfüllung der Funktion des Wertmassstabs bzw. Rechnungseinheit hängt im Wesentlichen von der Standardisierung und Konsistenz des in Frage stehenden Mediums ab. *Standardisierung setzt voraus, dass die Rechnungseinheit im ganzen Währungsgebiet über längere Zeit uniform ist, damit sich Leistungen wertmässig universell vergleichen lassen*.[93] Staatliche Währungen kommen diesem Erfordernis dadurch nach, dass das Gesetz die Grundsätze der Währung, d.h. die Einheit und die Stückelung, definiert (siehe Art. 1 WZG). Die Wertmassstabsfunktion setzt ferner voraus, dass das Referenzmaterial, d.h. das Trägermaterial für die

91 Siehe dazu vorne Rz. 24.

92 Vgl. SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 102.

93 SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 135 ff.

Standardwerteinheit, möglichst keinen Eigenwert aufweist, der die Messung beeinflussen könnte.[94]

Die Standardisierung bei Kryptogelder erfolgt im Unterschied zum staatlichen Geld nicht aufgrund gesetzlicher Anordnung, sondern aufgrund des Programmcodes. Hinsichtlich der Konsistenz ist der Programmcode eine verlässliche Grösse, zumal Änderungen im Programmcode von Bitcoin in der Regel eine Mehrheit der beteiligten Miner voraussetzen, welche nur sehr schwer zu erreichen ist. Ferner stellen Kryptogelder präzise Wertmassstäbe dar, zumal die kleinste Teilmenge bei Bitcoin der Satoshi mit acht Nachkommastellen – mit einem Wert von ca. CHF 0.000084 (Tageskurs vom 28. Mai 2020) – darstellt und Monero sogar bis auf zwölf Nachkommastellen teilbar ist. Theoretisch können aber mit Kryptogelder beliebig kleinere Teilmengen ermöglicht werden. Darüber hinaus weisen Kryptogelder, als reine elektronische Werteinheiten, keinen Eigenwert auf, d.h. weder einen intrinsischen noch einen extrinsischen Wert, welcher die Messung beeinflussen könnte.[95] Kryptogelder erfüllen daher die Voraussetzungen der Standardisierung und Konsistenz und stellen insofern Rechnungseinheiten dar.[96] 118

c. Wertaufbewahrungsfunktion

Die Wertaufbewahrungsfunktion beschreibt die Möglichkeit von Geld, Kaufkraft über einen bestimmten Zeitraum für den Inhaber zur Verfügung zu halten. Geld kann diese Voraussetzung nur erfüllen, wenn das *Trägermaterial, welches das Geldzeichen trägt bzw. die Standardwerteinheit repräsentiert, beständig* ist. Darüber hinaus stellt sich die Frage, ob der Geldwert, d.h. die durch das Geldzeichen verkörperte Kaufkraft ungefähr gleich hoch bleiben muss. 119

Kryptogeld stellt eine elektronische Aufzeichnung auf einer spezifisch dafür geschaffenen Datenbank (Blockchain) dar, auf welche mithilfe von PKI (‹Public-Key-Infrastructure›) zugegriffen, d.h. über das Kryptogeld verfügt werden kann. Die *Standardwert- bzw. Rechnungseinheiten von Kryptogelder werden folglich durch rein elektronische Aufzeichnung repräsentiert, die keine Körperlichkeit haben und daher keine Abnutzung erleiden können*. Darüber hinaus kann die PKI-Zugangsberechtigung, d.h. der ‹Private Key›, beliebig oft – elektronisch oder auch nicht-elektronisch (sogenanntes ‹Paper Wallet›) – vervielfältig werden, während die Werteinheiten von Kryptogeld aufgrund der dezentralen Blockchain 120

---

94 PROCTOR, Mann (Fn. 88), Rz. 1.09; SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 138.

95 Siehe vorne Rz. 69; vgl. auch SIMITIS, Geld (Fn. 12), 416.

96 Siehe dazu ferner L. AUFFENBERG, Bitcoins als Rechnungseinheiten, in: NVwZ 2015, 1184-1188 (1186 ff.).

auf zahlreichen Computern weltweit abgespeichert sind und daher das Risiko von Datenverlusten sehr gering gehalten werden kann. Kryptogelder erfüllen demnach die Voraussetzung der Beständigkeit des Trägermaterials.

121 Ob Kryptogelder darüber hinaus wertbeständig sind, lässt sich nicht allgemein beantworten, zumal sehr viele Ausprägungen existieren. Einerseits gibt es Kryptogeld, welches einen inkorporierten Wertverlust – auch Schwundgeld, Schrumpfgeld oder umlaufgesichertes Geld genannt – aufweist.[97] Bei diesen speziellen Geldformen wurde bewusst das Augenmerk auf die Erfüllung der Tauschmittelfunktion gelegt, während die Funktion der Wertaufbewahrung zurückgestellt wurde.[98] Meines Erachtens sind auch solche Geldformen funktionales Geld, da die Verminderung des Nennwerts publik ist und darüber hinaus Möglichkeiten bestehen können, den periodischen Wertverlust dieser Gelder zu verhindern oder abzumildern.

122 Bei gewöhnlichen Kryptogelder – d.h. ohne inkorporierten Wertverlust – stellt sich andererseits die Frage, ob *sie angesichts ihrer teilweisen volatilen Wechselkurse, die Voraussetzung der Wertstabilität erfüllen*. Es wird angenommen, dass bei Wertverlusten, welche die gewöhnlichen Zinssätze übersteigen, die grundsätzliche Eignung als Wertaufbewahrungsmittel verloren geht.[99] Kryptogelder – und insbesondere Bitcoin – verzeichneten teilweise Kursschwankungen von über 15% zum US-Dollar innert 30 Tagen.[100] Dies könnte zur Annahme verleiten, dass Bitcoin bzw. Kryptogeld im Allgemeinen die Funktion der Wertaufbewahrung nicht erfülle und der zukünftigen Benutzung als Zahlungsmittel im Weg steht.[101]

123 Gegen eine solche Ansicht sprechen verschiedene Einwände. Zunächst kann ein volatiler Wechselkurs auch Wertgewinne ermöglichen, welche die Verluste ausgleichen können, wobei nur diese für die Funktion als Wertaufbewahrung abträglich sind, während jene willkommen sind. Darüber hinaus *verzeichnen staatliche Währungen sogar noch volatilere Kursbewegungen, ohne dass ihnen die Geldqualität abgesprochen wird*.[102] Darüber hinaus ist die Volatilität des Wechselkurses immer von der Leistungsfähigkeit zweier Währungen abhängig. Die

97 Siehe dazu vorne Rz. 38.

98 Bericht des Bundesrats an die Bundesversammlung vom 21. Apr. 1950 über das Volksbegehren betreffend Revision von Art. 39 BV (Freigeldinitiative), BBl 1950 I 893, 898.

99 Botschaft vom 10. Jan. 1973 betreffend Änderung der Art. 31^{quinquies} und 32 Abs. 1 der Bundesverfassung (Konjunkurpolitik), BBl 1973 I 117, 131.

100 <https://bitvol.info/> (Woche vom Mo. 13.6.2011).

101 Siehe dazu etwa W. BOLT/M. VAN OORDT, On the value of Virtual Currencies, 2016, 3 ff.

102 <https://www.boerse.de/statistik/Euro-Dollar/EU0009652759>.

Volatilität ist daher keine genaue Angabe über die Leistungsfähigkeit einer einzigen Währung. Ferner muss berücksichtigt werden, dass Kryptowährungen als sicherer Hafen und teilweise auch als attraktive Geldanlage in den Jahren nach der Finanzkrise galten und die Wechselkursvolatilitäten unter anderem auf Finanzspekulation sowie auf die Minderleistung konventioneller Geldanlageformen zurückzuführen waren.[103]

Die Eignung von Kryptogeld zur Wertaufbewahrung müsste daher anhand ihrer Kaufkraft bewertet werden. *Einen Konsumentenpreisindex für Kryptogeld existiert allerdings nicht*. Darüber hinaus würde die Anlegung dieses Massstabs die Eignung vieler gewöhnlicher staatlichen Währungen in Frage stellen. Beispielsweise verlor der – als «sicheren Hafen» geltende – Schweizer Franken zwischen 1972 und 2018 ca. 161% an Wert.[104] Daraus folgt, dass wegen ihrer teilweisen volatilen Kursbewegungen Kryptogelder nicht die Qualität als Wertaufbewahrungsmittel abzusprechen ist. 124

Zusammenfassend lässt sich festhalten, dass *Kryptogelder die drei zentralen geldmässigen Funktionen in genügender Weise erfüllen*. Aus einer funktionalen Perspektive fallen Kryptogelder daher unter das Währungsmonopol gemäss Art. 99 Abs. 1 BV. 125

2.2 Technische Betrachtungsweise

Kryptogeld als elektronische Repräsentation einer Rechnungseinheit könnte sich als *funktionales elektronisches Geld (sogenanntes E-Geld) erweisen*. 126

E-Geld wird als «jeden elektronisch – darunter auch magnetisch – gespeicherten monetären Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge […] durchzuführen», verstanden (Art. 2 Ziff. 2 EU-RL 2009/110/EG).[105] Der Begriff des E-Geldes erfasst zwei unterschiedliche Ausprägungen. Einerseits das sogenannte hardwarebasierte E-Geld (Kartengeld oder Prepaid-Cash), welches in der Regel auf eine Chipkarte oder einem ähnlichen Speichermedium geladen werden kann und meist zur mobilen Bezahlung von Kleinbeträgen Verwendung 127

103 Siehe A. HAMID/A. TALIB, A note on Bitcoin's price volatility, in: JKP 2019, 376-384 (376 ff.).

104 <http://www.portal-stat.admin.ch/lik_rechner/d/lik_rechner.htm> (Landesindex der Konsumentenpreise, LIK-Teuerungsrechner).

105 Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16.09.2009 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 (*EGeld-RL*).

findet. Andererseits das sogenannte Netzgeld – auch softwarebasiertes E-Geld – bei welchem üblicherweise nicht der Nutzer selbst die Geldeinheiten besitzt, sondern eine Zugangsberechtigung zu einer Plattform, welche ihm die Verfügung über die Vermögenswerte erlaubt (beispielsweise Paypal).[106]

128 Kryptogelder können als elektronisch gespeicherte Geldwerte betrachtet werden, indes stellen sie *als reine immaterielle Vermögenswerte keine Forderung gegenüber einem Emittenten dar, der gegen Zahlung ausgestellt würde*.[107] Wie bereits erwähnt, basiert die Annahme von Kryptogeld rein auf dem Konsens der Parteien und verlustiges Kryptogeld kann gerade mangels eines Emittenten bzw. einer Ansprechperson nicht erstattet werden. Darüber hinaus haben Kryptogelder als eigenständige Währungen eine eigene Währungseinheit (BTC bzw. XMR) während E-Geld und Netzgeld in der Regel in einer etablierten staatlichen Währung ausgedrückt ist. Folglich stellen Kryptogelder keine E-Gelder dar.

2.3 Staatstheoretische Betrachtungsweise

129 In der staatstheoretischen Betrachtungsweise, welche im Wesentlichen durch die Arbeit von GEORG FRIEDRICH KNAPP begründet ist, steht die *staatliche Qualifikation eines Mediums als Geld im Vordergrund*.

130 Von einem *rechtspositivistischen Standpunkt ausgehend*, kommt Geldqualität nach der staatlichen Theorie nur denjenigen Zahlungsmitteln zu, die vom Staat selbst oder zumindest unter dessen Aufsicht ausgegeben werden, die durch Gesetzesanordnung in einer Rechnungseinheit denominiert sind und die aufgrund des Gesetzes als universales Austauschmittel auf dem Gebiet des jeweiligen Staates fungieren, mithin gesetzliche Zahlungsmittel darstellen.[108]

131 Für die Qualifikation von Kryptogeld als Geld folgt, dass Kryptogelder in einer staatstheoretischen Betrachtungsweise kein Geld darstellen, da sie weder durch den Staat ausgegeben werden noch die Ausgabe vom Staat beaufsichtigt wird. Ferner sind Kryptogelder nicht aufgrund gesetzlicher Anordnung in eine Rechnungseinheit denominiert, sondern der Programmcode enthält die zentralen Grundsätze von Kryptogelder. Schlussendlich stellen Kryptogelder keine gesetzlichen Zahlungsmittel (sogenannte(r) ‹Legal Tender›) dar (vgl. Art. 2 WZG). Daran ändert

---

106 Bericht des Bundesrates vom 25. Jun. 2014 zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3678) und Weibel (13.4070), 7 ff.; R. WEBER, E-Commerce (Fn. 60), 592.

107 Siehe dazu vorne Rz. 63 ff.

108 G.F. KNAPP, Staatliche Theorie des Geldes, 3. Aufl., München/Leipzig 1921, 26 ff.; PROCTOR, Mann (Fn. 88), Rz. 1.17; SIMITIS, Sonderstellung (Fn. 12), 420.

auch der Umstand nichts, dass mit Bitcoin bereits kommunale Steuern und Abgaben in bestimmten Gemeinden bezahlt werden können.[109]

Kryptogelder erfüllen nicht alle Voraussetzungen für eine Qualifikation als Geld gemäss der staatlichen Theorie. In einer *staatstheoretischen Perspektive handelt es sich bei Kryptogeld also nicht um Geld*. 132

2.4 Gesellschaftstheoretische Betrachtungsweise

Die gesellschaftstheoretische Betrachtungsweise stellt die Akzeptanz des Zahlungsmittels in einer Gesellschaft in den Vordergrund der Untersuchung («bonitas conventionalis oder consensualis»).[110] Entscheidend ist die *Erwartung des Individuums bei der Akzeptanz eines Geldmittels als Begleichung für eine Schuld, dass es dieses Geldmittel gegenüber seinen zukünftigen Vertragspartnern ebenfalls als Schuldtilgungsmittel* einsetzen kann. FRIEDRICH CARL VON SAVIGNY prägte diese Theorie vor dem Hintergrund des Aufkommens von Papiergeld und der damit zusammenhängenden Frage, wie Vertrauen in ein an sich wertloses Stück Papier bestehen kann.[111] ARTHUR NUSSBAUM erweiterte diese These um den Gedanken, dass gerade in Krisenzeiten nicht offiziell anerkannte Tauschmittel zu Geld werden oder umgekehrt, staatliches Geld unter Umständen nicht mehr als Zahlungsmittel akzeptiert wird und es deshalb seinen Status als Geld verlieren kann.[112] 133

Wie bereits erwähnt stellen Kryptogelder rein private Zahlungsmittel dar, welche nicht auf ein bestimmtes Gebiet oder ein bestimmtes Land beschränkt sind, sondern weltweit von vielen Personen benutzt werden, die in Kryptogelder einen Nutzen und damit einen Wert sehen.[113] Hierin manifestiert sich der Gedanke von VON SAVIGNY, dass Geldmittel nur diejenigen Sachen sein können, an denen ein «allgemeiner Glaube» hinsichtlich des Wertes besteht. Die *zunehmende Bereitschaft von Privaten weltweit, Kryptogelder als Bezahlung anzunehmen, spricht für das Vorliegen von Vertrauen in den Wert bzw. die Funktionsfähigkeit von Kryptogelder*. Ferner hat sich anhand von Kryptogeld auch die These NUSSBAUMS verwirklicht, insofern Kryptogelder als Antwort der Zivilgesellschaft auf die durch 134

109 Siehe auch SCHMID/SCHMID, Bitcoin (Fn. 60), Rz. 18 f.

110 Siehe zu diesem Geltungsgrund SCHAR-SCHUPPISSER, Standardwerteinheit (Fn. 4), 76.

111 F.C. VON SAVIGNY, Das Obligationenrecht. Als Teil des heutigen Römischen Rechts, Band I, Aalen 1851, 407 f.

112 A. NUSSBAUM, Das Geld in Theorie und Praxis des deutschen und ausländischen Rechts, Tübingen 1925, 6 ff.; siehe auch SIMITIS, Sonderstellung (Fn. 12), 418 ff.; MENGER, Geld (Fn. 20), 92.

113 Siehe zum Nutzen eines mit Leichtigkeit einsetzbaren Zahlungsmittels, KLEIN/SPREMANN, Telegeld (Fn. 6), 21.

die Finanzkrise offenbarten Defizite des Finanzsystems aufgefasst werden können und Kryptogelder besonders rege in Volkswirtschaften Verwendung finden, in denen die staatliche Währungsordnung nicht stabil ist.[114]

135 In einer gesellschaftstheoretischen Betrachtungsweise stellen Kryptogelder folglich Geld dar.

2.5 Institutionstheoretische Betrachtungsweise

136 Sowohl die staatstheoretische wie auch die gesellschaftstheoretische Betrachtungsweise gehen auf eine Zeit zurück, in der der Wert eines Zahlungsmittels stark vom verwendeten Trägermaterial abhing (Metallismus) und der Staat den Wert des Geldes mehrheitlich autonom und in Relation zu Gold (Goldparität) festsetzte. Ferner orientierten sich diese älteren Theorien am Vorbild von physisch greifbaren Zahlungsmitteln, welche die Entwicklungen hin zum elektronischen Buchgeld nicht berücksichtigen. Die modernere, institutionelle Theorie begegnet diesen Defiziten, indem sie die *traditionellen Geldfunktionen als Ausgangspunkt der Betrachtung nimmt, die Geldqualität jedoch massgeblich von der Frage der institutionellen Einbindung abhängig macht*.[115]

137 Geld wird im Sinne der institutionstheoretischen Betrachtungsweise als Kredit gegenüber einem Schuldner verstanden, welcher aufgrund einer normativen Ordnung, die die Wertstabilität, Fungibilität, Funktionalität – d.h. die Fähigkeit zur Erfüllung monetärer Verpflichtung – und Verfügbarkeit sicherstellt, vom Publikum als Tauschmittel und als Wertaufbewahrungsmittel akzeptiert wird.[116] Der Begriff der Institution bezieht sich auf die Voraussetzung, dass die Akzeptanz von Geld von einem Regelwerk abhängt und nicht auf den Wert oder den Nutzen zurückzuführen ist.[117] Als Institution gelten diejenigen Organisationen, Strukturen oder auch nur Regeln, welche aufgrund ihrer Beständigkeit und Widerstandsfähigkeit auf eine gewisse Dauer angelegt sind.

138 Der Programmcode bzw. die Kryptographie von Kryptogelder könnte als Regelwerk bzw. normative Ordnung und in einem weiteren Sinn als Institution aufgefasst werden, zumal die oben beschriebenen Aspekte dadurch zumindest

---

114 B. SCOTT, How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance, 2016, 6.

115 Zu diesem und dem folgenden Absatz: A. SÁINZ DE VICUÑA, An Institutional Theory of Money, in: M. Giovanoli/D. Devos (Hrsg.), International Monetary and Financial Law. The Global Crisis, New York 2010, Rz. 25.01 ff.; PROCTOR, Mann (Fn. 88), Rz. 1.31.

116 SÁINZ DE VICUÑA, Money (Fn. 115), Rz. 25.01.

117 PROCTOR, Mann (Fn. 88), Rz. 1.32.

teilweise verwirklicht werden. Beispielsweise wird die Wertstabilität bei Bitcoin mittels einer inhärenten Geldmengenbeschränkung im Programmcode zu erreichen versucht. Andererseits stellen Kryptogelder keine Kredite dar – insbesondere nicht gegenüber Zentralbanken –, zumal es aufgrund der Dezentralität keinen Emittenten gibt und folglich gar keine Schuldnerposition begründet werden kann. Darüber hinaus setzt die institutionelle Betrachtungsweise nicht nur einen normativen, sondern einen gesetzlichen Rahmen voraus, da die Akzeptanz eines Zahlungsmittels von der Fähigkeit bzw. Möglichkeit abhängt, monetäre Verpflichtungen allgemein rechtsgültig erfüllen zu können oder – im Fall von Buchgeld – zumindest in solche Zahlungsmittel einzutauschen.[118] Eine allgemeine rechtsgültige Wirkung kann nur aufgrund gesetzlicher Anordnung erfolgen. Die Akzeptanz von Kryptogeld ist demgegenüber auf allein allfällige Parteiabsprachen zurückzuführen, welche ihrerseits auf dem Nutzen beruhen, das das Kryptogeld dem Inhaber stiftet.[119]

In einer institutionstheoretischen Perspektive stellen Kryptogelder folglich kein Geld dar. 139

3. Ergebnis mit Rücksicht auf Art. 99 Abs. 1 BV

Die Untersuchung der möglichen Perspektiven auf Kryptogeld zeigte, dass es zwar funktionales Geld darstellt und vom Publikum als solches angesehen wird, es jedoch aus einer staatlichen Optik und auch aus einer institutionstheoretischen Perspektive kein Geld darstellt. Darüber hinaus handelt es sich bei Kryptogeld in einer technischen Betrachtungsweise nicht um E-Geld, sondern um neuartige Währungen mit besonderen Merkmalen. Es stellt sich die Frage, von welcher Betrachtungsweise Art. 99 Abs. 1 BV in Bezug auf die Qualifikation als Geld ausgeht. 140

Die *Wortwahl von Art. 99 BV («-wesen») impliziert zunächst einen sehr weiten Anwendungsbereich des Währungsmonopols*. Es liesse sich daher darauf schliessen, dass alles, was funktionales Geld darstellt, unter den Begriff des Währungswesens Art. 99 BV fiele. 141

Demgegenüber könnte die Aussage der Botschaft zum Geld- und Währungsartikel, dass «[erst] die staatliche Währungsordnung die Voraussetzungen für die Existenz von Geld [schaffe]»,[120] als Hinweis auf die Geltung der 142

118 SÁINZ DE VICUÑA, Money (Fn. 115), Rz. 25.19.
119 BIZ, Currencies (Fn. 45), 4 f.
120 Botschaft Währungsartikel (Fn. 84), 4030.

staatstheoretischen Betrachtungsweise oder allenfalls der institutstheoretischen Perspektive verstanden werden.

143 In Anbetracht der Zielsetzung von Art. 99 Abs. 1 BV, welche unter anderem in der Versorgung der Volkswirtschaft mit einem stabilen Zahlungsmittel besteht, erscheint eine *Kombination der erwähnten Perspektiven zur Bestimmung, welche Gegenstände davon erfasst sind, sachgerecht*. In diesem Sinne bildet die institutstheoretische Betrachtungsweise den Ausgangspunkt, zumal die staatliche Betrachtungsweise nur die gesetzlichen Zahlungsmittel erfasst und nicht das Banken-Buchgeld und daher zu kurz greift. Darüber hinaus fallen jedoch auch diejenigen Zahlungsmittel unter Art. 99 Abs. 1 BV, welche im Sinne der gesellschaftstheoretischen Betrachtungsweise Geld darstellen und die aufgrund ihrer regen Nutzung eine Gefahr für die Wirksamkeit der geldpolitischen Massnahmen der Nationalbank darstellen.[121]

144 Kryptogeld stellt im Lichte der institutstheoretischen Betrachtungsweise kein Geld dar, insbesondere weil es nicht in eine rechtliche Ordnung im oben erwähnten Sinne eingebunden ist.[122] Ferner haben Kryptogelder – d.h. Bitcoin als am meisten verbreitetes Beispiel – wegen ihrer vergleichsweise geringen Marktkapitalisierung keine nachteiligen Auswirkungen auf die Effektivität geldpolitischer Massnahmen. *Art. 99 Abs. 1 BV kommt daher als verfassungsmässige Kompetenznorm für eine Regulierung von Kryptogeld nicht in Betracht*.

II. Regelungskompetenz für Finanzdienstleistungen (Art. 98 Abs. 2 BV)

145 Dem Bund kommt aufgrund von *Art. 98 Abs. 2 BV eine umfassende Gesetzgebungskompetenz im Bereich der übrigen Finanzdienstleistungen* zu, d.h. für solche, die nicht unter das Bank- und Börsenwesen gemäss Art. 98 Abs. 1 BV fallen.

146 Als übrige Finanzdienstleistungen gelten sämtliche Dienstleistungen, welche einen Bezug zu Finanzgeschäften aufweisen. Als Finanzgeschäfte zählen die Annahme, Aufbewahrung, Anlage oder Übertragung von Vermögenswerten mit Instrumenten, die dem Finanzsektor zugeordnet werden können.[123] Zumal Kryptogelder eigenständige Währungen darstellen, kann Guthaben von Kryptogeld bei

121 Siehe ferner Botschaft Währungsartikel (Fn. 84), 4030 f.

122 Siehe zu dieser Voraussetzung vorne Rz. 136 ff.

123 C. KAUFMANN/F. UTZ, Art. 98 BV, in: B. Waldmann/E. Belser/A. Epiney (Hrsg.), Basler Kommentar, Basel 2015, Rz. 23.; R. WYSS, Art. 2 GwG, in: D. Thelesklaf/R. Wyss/M. van Thiel et al. (Hrsg.), GwG Kommentar. Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, Zürich 2019, Rz. 25.

Dritten als eine Art Devise betrachtet werden. Devisen gehören zu Vermögenswerten, welche üblicherweise im Finanzsektor gehandelt werden. Aufbewahrung und andere vergleichbare *Geschäfte mit Kryptogeld können daher typischerweise dem Finanzsektor zugeordnet werden und zählen insofern zu den übrigen Finanzdienstleistungen im Sinne von Art. 98 Abs. 2 BV*. Daraus folgt, dass gewöhnliche Wallet-Dienstleistungen, d.h. sogenannte ‹Custody Wallet-Anbieter› und deren Angebote, von Art. 98 BV erfasst sind und reguliert werden können.

Im *Umkehrschluss folgt daraus jedoch, dass, sofern keine Finanzdienstleistung vorliegt, keine Gesetzgebungskompetenz* des Bundes aus Art. 98 BV besteht. In Ermangelung einer anderweitigen Kompetenzgrundlage könnte daher der private Umgang mit Kryptogeld, wozu selbstverständlich das eigene Halten von Kryptogeld gehört, nicht reguliert und insofern auch nicht überwacht werden. 147

III. Regelungskompetenz im Bereich des Strafrechts (Art. 123 BV)

Die Bundesverfassung enthält ferner eine Gesetzgebungskompetenz für den Bund im Bereich des materiellen Strafrechts (Art. 123 Abs. 1 BV). Kraft dieser Bestimmung kann der Bund *sozialschädliches Verhalten mit einer Strafe bedrohen und kann damit den nachträglichen Schutz von Rechtsgütern* sicherstellen. Der Bund hat von dieser Kompetenz Gebrauch gemacht und bestimmte Handlungen, die unter anderem Kryptogeld betreffen, wegen ihren sozialschädlichen Auswirkungen unter Strafe gestellt. Dazu gehört insbesondere die Geldwäscherei (Art. 305^{bis} StGB), die Finanzierung des Terrorismus (Art. $260^{quinquies}$ StGB) sowie die Bestechungsdelikte (Art. 322^{ter} ff. StGB). 148

Die Gesetzgebungskompetenz für den Bereich des materiellen Strafrechts *erschöpft sich allerdings in der Strafbarkeitserklärung bestimmter, sozialschädlicher Handlungen*. Insbesondere besteht keine darüber hinaus gehende Kompetenz, Massnahmen zu erlassen, welche proaktiv auf die Verhinderung der zuvor genannten Delikte gerichtet sind und Personen betreffen, bei welchen keine konkreten Verdachtsmomente bestehen. 149

IV. Fazit zur Kompetenzgrundlage in der BV

Als Zwischenfazit lässt sich festhalten, dass der Bund *Handlungen mit Kryptogeld regulieren kann, die in einem weiteren Sinne zu den Finanzdienstleistungen gezählt werden können*. Daher könnten beispielsweise Angebote, die auf die sichere Aufbewahrung von fremdem Kryptogeld gerichtet sind als Gegenstand von Art. 98 Abs. 2 BV einer Regulierung zugeführt werden. 150

151 Weil Kryptogeld vom Benutzer gehalten werden kann und auch keine Finanzintermediäre zur Ausführung von Transaktionen bedürfen, könnte der *Anspruch an den Staat gestellt werden, dass dieser Transaktionen und Konten mit Kryptogeld überwacht, bei denen keine Finanzdienstleistungen involviert* sind.[124] Insbesondere könnte der Staat bei Bitcoin, wegen der Öffentlichkeit der Blockchain, Transaktionen und Kontostände relativ einfach auf allfällige Risiken für Geldwäscherei, Terrorismusfinanzierung usw. überprüfen. Solche Massnahmen erweisen sich jedoch mangels einer konkreten, verfassungsmässigen Kompetenzgrundlage als verfassungswidrig.

Kapitel 2: Kryptogeld im Geldwäschereirecht

152 Die Geldwäschereigesetzgebung will hauptsächlich verhindern, dass Vermögenswerte illegaler Herkunft in den normalen Wirtschaftskreislauf integriert werden können. Die Vorschriften des GwG und der dazugehörenden Verordnungen werden auch als «*AML/KYC (anti-money laundering/know-your-customer)*»-Regeln bezeichnet. Die *Identifikation des Kunden sowie die Herstellung der Rückverfolgbarkeit jeder ausgeführten Transaktion (‹Paper Trail›) gehören zu den zentralen Pflichten der Finanzintermediäre aufgrund der Geldwäschereigesetzgebung*.

I. Erfasste Tätigkeiten mit Kryptogeld

153 Im Folgenden wird eine Übersicht der de lata *GwG-Vorschriften aufgezeigt, welche für Kryptogeld anwendbar sind und die Auswirkungen auf den reinen Benutzer von Kryptogeld*, haben. Die Kategorie der Händler bildet einen Sondertatbestand, der keine eigentliche finanzintermediäre Tätigkeit darstellt.

1. Finanzintermediation

154 Die *Finanzintermediation kann als Grundtatbestand des GwG nebst der speziellen Kategorie der Händler* (Art. 8 GwG) betrachtet werden. Die Spezialtatbestände – d.h. Kassageschäfte sowie Geld- und Wertübertragungsgeschäfte – stellen immer auch finanzintermediäre Tätigkeiten dar.[125]

---

124 Siehe zur Disintermediation vorne Rz. 60; zur Verfassungsgrundlage für die Regulierung von Finanzdienstleistungen vorne Rz. 145 ff.

125 S. SCHÄREN, Art. 2 GwG, in: P.V. Kunz/T. Jutzi/S. Schären (Hrsg.), Geldwäschereigesetz (GwG). Bundesgesetz vom 10 Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Stämpflis Handkommentar, Bern 2017, Rz. 53 f.

1.1 Persönlicher Anwendungsbereich

Grundsätzlich zählen zu den Finanzintermediären im Sinne des GwG Personen und Unternehmen, die berufsmässig fremde Vermögenswerte annehmen, aufbewahren oder helfen, sie anzulegen oder zu übertragen. Das GwG unterscheidet dabei zwischen zwei Kategorien von Finanzintermediären: In die erste Kategorie fallen Personen und Unternehmungen, welche wegen ihrer Tätigkeit einer spezialgesetzlichen Regulierung sowie Beaufsichtigung unterliegen – sogenannter «Banken- und Versicherungssektor» bzw. Finanzintermediäre i.e.S. (Art. 2 Abs. 2 GwG).[126] In die zweite Kategorie gehören Personen und Unternehmungen, welche anlässlich ihrer berufsmässigen Ausübung von Dienstleistungen im Finanzsektor unterstellungspflichtig sind – sogenannter «Nichtbankensektor» oder Finanzintermediäre i.w.S. (Art. 2 Abs. 3 GwG). 155

Für die Finanzintermediäre i.w.S. bzw. für den Nichtbankensektor gilt, dass *die finanzintermediäre Tätigkeit berufsmässig ausgeübt werden muss, damit sie unter das GwG fällt*. Die einmalige Vornahme einer unterstellungspflichtigen Tätigkeit führt daher nicht zu einer Bewilligungspflicht gemäss dem GwG. Allgemeine Kriterien zur Bestimmung der Berufsmässigkeit enthält Art. 7 GwV. Demgegenüber fallen Unternehmen, die zum Banken- und Versicherungssektor bzw. zu den Finanzintermediären i.e.S. zu zählen sind, stets unter das GwG.[127] 156

Im Zusammenhang mit der Erbringung von Dienstleistungen mit Kryptogeld sind daher vom persönlichen Anwendungsbereich des GwG regelmässig die *Banken gemäss Art. 2 Abs. 2 lit. a GwG sowie Finanzintermediäre i.w.S. erfasst, welche Dienstleistungen für den Zahlungsverkehr gemäss Art. 2 Abs. 3 lit. b GwG erbringen*. 157

Es stellte sich allenfalls die Frage, ob Kryptogelder Zahlungssysteme im Sinne von Art. 81 FinfraG darstellen und insofern als Finanzintermediäre nach Art. 2 Abs. 2 lit. d^{ter} GwG aufgefasst werden sollten. Diese Frage ist jedoch – auch wegen der vergleichsweisen geringfügigen Auswirkungen auf die Rechtsstellung der Nutzer – von der vorliegenden Untersuchung ausgenommen.[128] Ausserdem kann bei Kryptogeld als dezentrale Zahlungssysteme, niemand für Funktionsfähigkeit und Stabilität von Kryptogeld verantwortlich gemacht werden, da dies ausserhalb des Einflussbereich einzelner Personen oder Unternehmen liegt. Eine Ausnahme davon wäre im (theoretischen) Fall gegeben, wo ein sogenannter Mining Pool – d.h. ein informeller Zusammenschluss mehrerer Miner – mehr als 50% der Rechenleistung des Netzwerks kontrollieren 158

126 Siehe FINMA-Rundschreiben 2011/1, Tätigkeit als Finanzintermediär nach GwG. Ausführungen zur Geldwäschereiverordnung (GwV), 2010, Rz. 1.

127 SCHÄREN, Art. 2 GwG (Fn. 125), Rz. 52.

128 Siehe dazu vorne Rz. 84 f.

würde. Die grossen Mining Pools sind jedoch in der Mehrheit im Ausland angesiedelt und können selbst auch anonym bleiben.

1.2 Sachlicher Anwendungsbereich

159 Im Grundtatbestand setzt das GwG eine finanzintermediäre Tätigkeit voraus. Als finanzintermediäre Tätigkeit gilt die berufsmässige Annahme, Aufbewahrung oder Hilfe bei der Anlage sowie Übertragung fremder Vermögenswerte. *Finanzintermediäre Tätigkeiten im Sinne des GwG weisen ein Risiko hinsichtlich des Missbrauchs für Geldwäscherei auf, zumal mit ihrer Hilfe die Rückverfolgbarkeit von Vermögenswerten erschwert oder verunmöglicht werden kann*.

160 Der Grundtatbestand ist subsidiär zu den – nicht abschliessend aufgezählten – Spezialtatbeständen anwendbar und absichtlich mit *abstrakten Rechtsbegriffen gefüllt, um künftige Entwicklungen und technologische Neuerungen, welche auch neuartige Geschäftsmodelle hervorrufen können, zu erfassen*.[129] In jedem Fall muss aber die in Frage stehende Tätigkeit ein tatsächliches Geldwäschereirisiko aufweisen, damit eine Unterstellung unter das GwG gerechtfertigt ist.[130]

161 Als finanzintermediäre Tätigkeit mit Kryptogelder im Grundtatbestand fällt nach dem Gesagten insbesondere deren Aufbewahrung in Betracht. Einrichtungen, welche die Aufbewahrung von Kryptogeld im Namen ihrer Kunden anbieten, werden als als Anbieter elektronischer Geldbörsen bezeichnet (siehe Art. 2 Abs. 1 Ziff. 3 lit. h 5.AMLR).[131] Solche Dienstleistungen mit elektronischen Wallets stellen in der Regel einen benutzerfreundlicheren Zugang zu Kryptogeld bereits als gegenüber der Standard-Software.

162 Von Anbietern gewöhnlicher elektronischer Geldbörsen (verwaltete Wallets) sind die Anbieter sogenannter ‹Custodial Wallet› bzw. ‹Custody Wallets› zu unterscheiden.[132] Bei Letzteren wird der private kryptographische Schlüssel, welcher zur Verfügung über das Kryptogeld notwendig ist, dem Dienstleistungsanbieter übertragen bzw. dem Kunden gar nie ausgehändigt. Custodial Wallets stellen ein benutzerfreundliches Mittel dar, um Kryptogeld zu verwenden, zumal der private kryptographische Schlüssel

---

129 Zur Technologieneutralität siehe vorne Rz. 102; SCHÄREN, Art. 2 GwG (Fn. 125), Rz. 54 ff.

130 Siehe zu diesem Erfordernis BGer 2A.62/2007 vom 30.9.2007, E. 8.

131 Richtlinie (EU) 2018/843 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.

132 Zum Begriff Custody Wallet-Anbieter bzw. Custodial Wallet-Anbieter siehe FINMA, Wegleitung (Fn. 47), 7.

von Dienstleistungsanbietern verwahrt wird und daher der Kunde nicht in Gefahr läuft, den Schlüssel zu verlieren oder irrtümlicherweise Dritten bekanntzugeben. Darüber hinaus sind Custody Wallets einfacher zugänglich, weil eine Kombination aus Benutzername und Passwort für den Zugang zu Kryptogeld ausreicht.

Das Dienstleistungsangebot elektronischer Geldbörsen stellt eine finanzintermediäre Tätigkeit dar, weil es die Annahme und Aufbewahrung fremder Vermögenswerte beinhaltet sowie ein reales Risiko zum Missbrauch für Geldwäschereizwecke darstellt. Beispielsweise besteht das Risiko, dass der Eigentümer, der auf elektronische Geldbörsen eingebrachten Vermögenswerten nicht der Inhaber der elektronischen Geldbörse ist (Strohmann-Problematik). 163

Elektronische Wallets fallen weder in die im GwG erwähnten Kategorien der Kassageschäfte noch in die der Dienstleistungen für den Zahlungsverkehr bzw. den Geld- und Wertübertragungsgeschäfte. Allerdings erweisen sie sich als *fortdauernde Geschäftsbeziehung zwischen Finanzintermediär und Kunden, also als eine dauernde Geschäftsbeziehung gemäss Art. 2 lit. d GwV-FINMA*. Die GwV-FINMA kann als Mindeststandard für die Beurteilung der Reglemente von Selbstregulierungsorganisationen (SRO) betrachtet werden.[133] 164

2. Geldwechsel (Kassageschäft)

Nach Art. 2 lit. b GwV-FINMA gelten als *Kassageschäfte «alle Bargeschäfte, insbesondere der Geldwechsel*, der An- bzw. Verkauf von Edelmetallen, der Verkauf von Reiseschecks, die Umwandlung und Auszahlung in Bargeld von Kassa- und Anleihensobligationen und dergleichen, sofern mit diesen Geschäften keine dauernde Geschäftsbeziehung verbunden ist[.]» 165

Als Kassageschäfte gelten daher Dienstleistungen, welche einem Kunden erbracht werden, der keine dauernde Geschäftsbeziehung mit dem Finanzintermediär unterhält und beispielsweise nur am Schalter erschienen ist (sogenannte Laufkundschaft).[134] Als Kassageschäfte können daher auch Geldwechselgeschäfte oder andere Geschäfte an einem Automaten in Betracht fallen. 166

---

133 Die Kategorie der direkt unterstellten Finanzintermediäre (DUFIs) wurde per Anfang Februar 2020 aufgehoben; R. Wyss, Art. 4 GwG, in: D. Thelesklaf/R. Wyss/M. van Thiel et al. (Hrsg.), GwG Kommentar. Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, Zürich 2019, Rz. 12.

134 K. Heim, VSB 2016 Praxiskommentar zur Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken, 3. Aufl., Zürich 2016, 49 f.; Botschaft vom 17. Juni 1996 zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor

167 Für Kryptogeld steht im Rahmen der Kassageschäfte der Geldwechsel im Vordergrund, welcher nach Art. 2 Abs. 3 lit. c GwG i.V.m. Art. 5 Abs. 1 lit. a GwV als Handelstätigkeit zu qualifizieren ist und unter das GwG fällt. Das Geldwechselgeschäft wird gemeinhin als den direkten Umtausch eines bestimmten Betrags in einer Währung gegen einen äquivalenten Betrag in eine andere Währung verstanden. *Die Verordnung stellt dem Geldwechsel diejenigen Mittel gleich, welche eine ähnlich hohe Universalität und Fungibilität wie Geld aufweisen und deshalb gerne an Zahlungsstatt hingegeben oder angenommen werden* – dazu zählen Edelmetalle, Reisechecks, Inhaberpapiere und -obligationen sowie Checks.

168 Kryptogeld kann weltweit bei Händler und Internetplattformen für die Bezahlung von Waren und Dienstleistungen eingesetzt werden.[135] Darüber hinaus kann es bei speziellen Automaten oder bei Tauschbörsen im Internet gegen andere Kryptowährung aber auch gegen staatliche Währungen getauscht werden. Es geniesst daher mindestens die Universalität und Fungibilität von Reisechecks und ist in dieser Hinsicht allenfalls sogar mit Edelmetallen vergleichbar. *Kryptogeld ist daher gleich wie die erwähnten Barmittel zu behandeln*. Grundsätzlich kommen daher folgende Fälle des Geldwechsels in Betracht, in denen Kryptogeld involviert ist:

1. Tausch von Kryptogeld in staatliche Währung oder umgekehrt;
2. Tausch einer Kryptogeld-Währung in eine andere Kryptogeld-Währung (beispielsweise Bitcoin in Monero oder umgekehrt);
3. Kauf oder Verkauf von Edelmetallen mit bzw. gegen Kryptogeld;
4. Kauf von Reisechecks mit virtueller Währung;
5. Auszahlung von Inhaberpapieren, Kassa- und Anleihensobligationen sowie Checks in Kryptogeld.

169 *Kassageschäfte setzen ferner voraus, dass durchgehend höchstens zwei Parteien beteiligt* sind, nämlich der Finanzintermediär sowie der Kunde.[136] Sind mehr als zwei Parteien beteiligt oder besteht für den Finanzintermediär keine Möglichkeit sich darüber zu vergewissern, so liegt kein Kassageschäft vor und der

(Geldwäschereigesetz, GwG), BBl 1996 1101, 1122; R. AEPPLI/C. BOHNER/T. FÖLLMI (Hrsg.), 75 Jahre Schweizerische Nationalbank. Die Zeit von 1957 bis 1982, FS Nationalbank, Zürich 1982, 266 f.

135 Siehe <www.coinmap.org>.

136 Bundesrat, Grundlagen (Fn. 43), 147; HEIM, VSB 2016 (Fn. 134), 49.

Finanzintermediär muss sich an den höheren Voraussetzungen, welche für das Geld- und Wertübertragungsgeschäfts gelten, orientieren.[137]

Der akzessorische Geldwechsel – d.h. die Erbringung des Geldwechselgeschäfts als reine Nebenleistung – zählt bis zur Grenze der Berufsmässigkeit nicht als Geldwechselgeschäft. Diese Ausnahmeregelung betrifft vor allem Hotels, Reisebüros, Tankstellen usw., die für ihre Kunden auch Fremdwährungen entgegennehmen, das Retourgeld aber in Franken erstatten.[138] Dies könnte aber auch Angebote mit Kryptogeld betreffen. 170

Die Beschränkung der Kassageschäfte auf Zweiparteienverhältnisse erweist sich im Bereich von Kryptogeld als problematisch, zumal die Strohmann-Problematik bei den übrigen Barmitteln dadurch entschärft ist, dass sie nur einmal existieren und physisch – allenfalls über Landesgrenzen – bewegt werden müssen. Demgegenüber kann *der zur Verfügung über Kryptogeld notwendige kryptographische Schlüssel ohne Weiteres vervielfältigt werden und Personen weltweit mitgeteilt werden, welche sodann als Berechtigte auftreten könnten*. Der im Bericht des Bundesrates geäusserte Standpunkt, dass der Finanzintermediär mit geeigneten Massnahmen sicherstellen muss, dass es sich um das Wallet eines Kunden und nicht einer Drittperson handelt, greift m.E. daher zu kurz.[139] Es müsste überprüft werden, ob die am Schalter erscheinende Person eine ausschliessliche Verfügungsmacht über das Wallet innehat. Weil aber beliebig viele Kopien der Berechtigung erstellt werden können, kann kein solcher Nachweis erbracht werden. 171

Der mögliche Anwendungsbereich von Kassageschäften mit Kryptogeld reduziert sich daher auf diejenigen Fälle, die nicht die Konvertierung von Kryptogeld in andere Vermögenswerte zum Gegenstand haben. Dies trifft auf den Fall eins in der Variante des Wechsels von Barmitteln zu Kryptogeld und auf den Fall drei, in der Variante des Verkaufs von Edelmetallen gegen Kryptogeld, sowie auf den Fall fünf zu. In der Praxis dürfte allerdings bloss der erste Fall relevant werden. Der Finanzintermediär könnte in solchen Situationen eine *neue Kryptogeldadresse generieren und den umgerechneten Betrag in Kryptogeld darauf transferieren*. Unter dem Aspekt der Technologieneutralität würden so vergleichbare Bedingungen zwischen Kryptogeld und konventionellen Barmitteln geschaffen. Allerdings kann das gewechselte Kryptogeld weltweit rascher, d.h. elektronisch transferiert werden 172

137 Siehe zum Geld- und Wertübertragungsgeschäft hinten Rz. 173 ff.; Bundesrat, Grundlagen (Fn. 43), 147.

138 EFV, Praxis der Kontrollstelle für die Bekämpfung der Geldwäscherei zu Art. 2 Abs. 3 GwG. Der Geltungsbereich des Geldwäschereigesetzes im Nichtbankensektor (Unterstellungskommentar Kst), 2008, Rz. 23.

139 Siehe Bundesrat, Grundlagen (Fn. 43), 147.

als die übrigen Barmittel und weist daher eine höhere Geschwindigkeit sowie Mobilität auf.[140]

3. Geld- und Wertübertragungen

173 Als Geld- und Wertübertragungsgeschäft gilt der *Transfer von Vermögenswerten durch Entgegennahme von Bargeld, Edelmetallen, virtuellen Währungen, Schecks oder sonstigen Zahlungsmitteln und, entweder die Auszahlung einer entsprechenden Summe in Bargeld, Edelmetallen oder virtuellen Währungen,* oder, die bargeldlose Übertragung oder Überweisung über ein Zahlungs- oder Abrechnungssystem (Art. 4 Abs. 1 lit. c i.V.m. Art. 4 Abs. 2 GwV). Die GwV-FINMA setzt ausserdem einen Auslandsbezug voraus, d.h. rein inländische Geschäfte gelten wegen des niedrigeren Geldwäschereirisikos nicht als Geld- und Wertübertragungsgeschäfte (Art. 2 lit. c GwV-FINMA).[141]

174 Das Geld- und Wertübertragungsgeschäft unterscheidet sich von zuvor behandelten Kassageschäften bzw. Geldwechselgeschäften durch ein Dreiparteienverhältnis. An Geld- und Wertübertragungen sind in der Regel der Finanzintermediär, der Kunde sowie ein Begünstigter beteiligt. Wie bereits erwähnt, *muss der Finanzintermediär von einem Dreiparteienverhältnis ausgehen, solange er nicht die berechtigte Annahme treffen kann, dass nur er und eine weitere Partei an der Transaktion beteiligt sind*.[142]

175 Als Geld- und Wertübertragung mit Kryptogeld fallen einerseits Geldwechselgeschäfte in Betracht und andererseits Transaktionen zwischen elektronischen Geldbörsen bei Finanzintermediären. Darüber hinaus erwähnt die FINMA-Aufsichtsmitteilung 02/2019 die Möglichkeit, Überweisungen an externe Wallets – auch von Drittpersonen – vorzunehmen, «sofern die Verfügungsmacht des Dritten über die externe Wallet durch geeignete technische Massnahmen überprüft [ist]. Problematisch m.E. dabei ist, dass *zur Verminderung von Geldwäscherei- und Terrorismusfinanzierungsrisiken sichergestellt werden müsste, dass der Dritte eine exklusive Verfügungsmacht innehat, dies jedoch in der Realität, insbesondere bei externen Wallets, nicht überprüft werden* kann.[143]

---

140 Siehe dazu vorne Rz. 113.

141 FINMA, Geldwäschereiverordnung-FINMA (GwV-FINMA). Erläuterungsbericht, 2010, 25.

142 Siehe auch Bundesrat, Postulate (Fn. 106), 15 f.

143 Siehe zur Möglichkeit der Vervielfältigung der Zugangsberechtigung vorne Rz. 171.

4. Handelsgeschäfte (Art. 8*a* GwG)

In eine *Spezialkategorie fallen die Handelsgeschäfte gemäss Art. 8a GwG, weil dabei keine finanzintermediäre Tätigkeit* involviert ist. Die Unterstellung gewöhnlicher Händler, d.h. von Gewerbetreibenden, welche primär mit dem Angebot von Waren oder Dienstleistungen einen Erwerb erzielen, stellt einen von der FATF angestossenen und von der EU weiterentwickelten Paradigmenwechsel dar.[144] 176

Gemäss Art. 8*a* Abs. 1 GwG sind *Händler im Rahmen eines einzelnen Handelsgeschäfts dem GwG unterstellt, sofern sie als Bezahlung «mehr als 100'000.- Franken in bar entgegennehmen*[.]» Die Händler können sich der Verpflichtung jedoch entziehen, wenn sie die Zahlung über einen Finanzintermediär abwickeln (Art. 8*a* Abs. 5 GwG). 177

Kryptogeld wird dem Bargeld in unterschiedlichen geldwäschereirechtlichen Bestimmungen gleichgestellt (Art. 4 Abs. 2 GwV und Art. 2 lit. c GwV-FINMA). Folgerichtig müssten Händler bei der Annahme von umgerechnet CHF 100'000.- in Kryptogeld gleichermassen verpflichtet werden. *Allerdings steht dieser Ansicht der eindeutige Wortlaut von Art. 8a GwG entgegen*. Einerseits wird explizit auf die Annahme von Franken abgestellt. Kryptogelder haben aber eigene Währungseinheiten und sind nicht in Franken denominiert. Andererseits ist mit dem Fehlen eines Zusatzes, wie beispielsweise «umgerechnet», davon auszugehen, dass der Gesetzgeber bewusst keine wertmässige Grenze für sämtliche mit dem Bargeld vergleichbaren Mitteln festlegen wollte. Art. 8*a* GwG in der geltenden Fassung ist folglich nicht auf die Annahme von Kryptogeld durch Händler anwendbar.[145] 178

II. Rechtsfolgen der Unterstellung nach GwG

1. Identifizierung der Vertragspartei

Die grundlegendste Sorgfaltspflicht der Finanzintermediäre gemäss GwG stellt die Identifizierungspflicht der Vertragspartei dar (Art. 3 GwG). Gemäss dieser 179

144 A. SCHOTT/M. KESSLER, Art. 8*a* GwG, in: P.V. Kunz/T. Jutzi/S. Schären (Hrsg.), Geldwäschereigesetz (GwG). Bundesgesetz vom 10 Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Stämpflis Handkommentar, Bern 2017, Rz. 2 ff.

145 Siehe für Vorschläge einer de ferenda Regulierung hinten Rz. 208 ff.; der Vorentwurf für eine Revision des GwG sieht ein Schwellenwert von nur noch CHF 15'000 für Edelmetall sowie Edelsteinhändler vor, siehe Art. 8a Abs. 4bis E-GwG (2019) (BBl 2019 5555).

Norm muss der *Finanzintermediär anhand eines beweiskräftigen Dokuments überprüfen, ob es sich beim Kunden um diejenige Person handelt, die er zu sein vorgibt*. Sie soll verhindern, dass Finanzdienstleistungen gegenüber unbekannten Personen erbracht werden. Die Kenntnis der Identität des Kunden ist darüber hinaus im Hinblick auf die Erfüllung der übrigen Sorgfaltspflichten notwendig, insbesondere hinsichtlich der Eruierung der Hintergründe und des Zwecks von Geschäftsbeziehung (Art. 6 GwG) sowie hinsichtlich der Verdachtsmeldungen (Art. 9 GwG).

180 Die Identitätsfeststellung ist nicht zwingend an eine persönliche Vorsprache gekoppelt. Zugelassen sind auch andere Technologien, insbesondere Video- und Online-Identifizierungen, welche eine gleichwertige Sicherheit für die Umsetzung der Sorgfaltspflichten bieten.[146] Dadurch eröffnet sich die *Möglichkeit, Finanzdienstleistungen an Personen erbringen zu können, welche beispielsweise im Ausland ansässig sind und nicht persönlich erscheinen*. Dienstleistungsanbieter im Bereich von Kryptogeld können daher weltweit Kunden akquirieren und diese können von den Vorteilen des Finanzplatzes Schweiz profitieren. Demgegenüber bedeutet es aber auch, dass persönliche Daten bei jeder Geschäftsbeziehung mit einem schweizerischen Finanzintermediär bearbeitet werden müssen.

2. Identifizierung der wirtschaftlich Berechtigten

181 Gemäss den 2012 revidierten FATF-Empfehlungen sieht das GwG vor, dass Finanzintermediäre die an Vermögenswerten und die an juristischen Personen tatsächlich berechtigten Personen identifizieren müssen (Art. 4 GwG).[147] Mit der *Feststellung der wirtschaftlich Berechtigten soll verhindert werden, dass sich Personen hinter rechtlichen Strukturen verstecken, um nicht selbst identifiziert zu werden* und damit beispielsweise Erlöse aus kriminellen Handlungen zu verschleiern. Mit Art. 4 GwG sollen folglich vorhandene, rechtliche Verfügungsmöglichkeiten über Vermögenswerte offengelegt werden.[148]

182 Grundsätzlich ist der *Finanzintermediär selbst dazu angehalten, die wirtschaftlich berechtigten Personen zu ermitteln*. Er kann nur darauf verzichten,

---

146 G. DOBRAUZ-SALDAPENNA/C. DERUNGS, Art. 3 GwG, in: P.V. Kunz/T. Jutzi/S. Schären (Hrsg.), Geldwäschereigesetz (GwG). Bundesgesetz vom 10 Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Stämpflis Handkommentar, Bern 2017, Rz. 45 ff.

147 FATF, The FATF Recommendations. International Standards on Combating Money Laundering and the Financing of Terrorism & Profileration, 2012, Empfehlungen Nr. 10 ff.

148 WYSS, Art. 4 GwG (Fn. 133), Rz. 2; LIEBI/ CONOD, Art. 4 GwG (Fn. 81), Rz. 4.

wenn es sich um eine börsenkotierte Gesellschaft oder eine von einer solchen Gesellschaft kontrollierte Tochtergesellschaft handelt, zumal diese meist aufgrund börsenrechtlicher Vorschriften zur Offenlegung der Eigentumsverhältnisse verpflichtet sind (Art. 4 Abs. 1 GwG). Ausserdem hat der Finanzintermediär in gewissen Fällen die Pflicht, auf eine Erklärung des Vertragspartners über die wirtschaftlich berechtigten Personen zu bestehen (Art. 4 Abs. 2 GwG). Ausser in den Fällen der Kassageschäfte von erheblichem Wert muss der Finanzintermediär eine solche Erklärung einholen, wenn er einerseits Zweifel hegt, dass die Vertragspartei mit der wirtschaftlich berechtigten Person identisch ist (Art. 4 Abs. 2 GwG) und andererseits, wenn Verdachtsmomente für eine mögliche Geldwäscherei oder Terrorismusfinanzierung vorliegen (Art. 59 Abs. 3 GwV-FINMA).

Im Bereich von Kryptogeld ist die Feststellung der wirtschaftlich berechtigten Personen allerdings mit Problemen behaftet. Wie bereits weiter oben erwähnt, reicht die Kenntnis des privaten Schlüssels aus, um über ein bestimmtes Guthaben von Kryptogeld verfügen zu können.[149] Daher kann zwar der Nachweis relativ einfach erbracht werden, dass eine bestimmte Person über ein bestimmtes Guthaben bzw. Wallet verfügen kann, *jedoch kann nicht bewiesen werden, dass keine Kopien des privaten Schlüssels existieren, und somit nicht weitere Personen am Kryptogeld-Guthaben bzw. am Wallet wirtschaftlich berechtigt sind*. Die Missbrauchsgefahr von Kryptogeld für Geldwäscherei und andere kriminelle Zwecke wird immerhin durch das Misstrauen gemildert, welches darin besteht, dass die weiteren Personen bzw. Strohmänner, welche Kenntnis vom privaten Schlüssel haben, das Kryptogeld möglicherweise veruntreuen könnten. 183

3. Pflicht zur Abklärung der Hintergründe und Zwecke

Finanzintermediäre trifft die Pflicht, die Art und der Zweck der Geschäftsbeziehung mit Kunden zu eruieren (Art. 8 Abs. 1 GwG). Ausserdem müssen sie und die Händler die Hintergründe und den Zweck von einzelnen Transaktionen überprüfen, wenn die zuvor gemachte Überprüfung der Geschäftsbeziehung Anhaltspunkte für Geldwäscherei oder Terrorismusfinanzierung liefert oder auch nur ungewöhnlich erscheint (Art. 6 Abs. 2 und Art. 8 Abs. 2 GwG). Der *Umfang der geforderten Überprüfungspflicht variiert daher je nach Kunde und Transaktion* im Einzelfall. 184

Weil die Kontrolldichte abhängig vom Risiko des jeweiligen Kunden oder der jeweiligen Transaktion ist, kann die *Vorschrift als Anwendungspflicht des* 185

[149] Siehe vorne Rz. 120.

risikobasierten Ansatzes bei Kundenbeziehungen gelten.[150] Der Finanzintermediär muss die Kriterien für die Bestimmung von Risiko-Transaktionen sowie Kundenbeziehungen grundsätzlich selbst festlegen. Er hat allerdings in jedem Fall die durch die Geldwäschereigesetzgebung festgelegten Kriterien zu beachten. Dazu gehören beispielsweise die besonders exponierten Personen – sogenannte PEP – (Art. 6 Abs. 2 GwG) oder Personen, welche in Ländern ansässig sind, die von der FATF als ‹high risk› oder nicht-kooperativ eingestuft werden (Art. 13 Abs. 2 GwV-FINMA).

186 Die Pflicht zur Anwendung eines risikobasierten Ansatzes hat in der Praxis allerdings dazu geführt, dass Finanzintermediäre und Banken eher auf gewisse Beziehungen ganz verzichten, als den zusätzlichen Aufwand auf sich zu nehmen, der dadurch gefordert wäre (‹De-Risking›). Zunächst sind davon Banken– und sogar Zentralbanken – betroffen, welche deswegen kaum mehr Korrespondenzbanken für die Ausführung von Auslandstransaktionen finden. Darüber hinaus betrifft es gewöhnliche Personen, beispielsweise weil sie einer Tätigkeit nachgehen, bei der meistens viel Bargeld involviert ist oder, wenn sie in einem Hochrisiko-Land niedergelassen sind. Schlussendlich sind auch Unternehmen und gemeinnützige Organisationen betroffen, welche in einem Hochrisiko-Land ihre Geschäftstätigkeit ausüben möchten. Die Folgen reichen von Verzögerungen bei der Auszahlung oder bei der Ausführung von Transaktionen, vom ungenügenden Zugang zu finanziellen Dienstleistungen (‹Underbanked›) bis hin zum kompletten Ausschluss von Bank- bzw. Finanzdienstleistungen (‹Unbanked›).[151]

187 In dieser Hinsicht besteht ein gewisses *Risiko, dass dedizierte Anbieter von Dienstleistungen mit Kryptogeld oder sogar gewöhnliche Personen, welche regelmässig Kryptogeld verwenden, von einer Bankkundenbeziehung unter Hinweis auf den gebotenen, zusätzlichen Aufwand wegen der Einhaltung der Sorgfaltspflichten ausgeschlossen* werden.[152] Freilich entstehen durch Kryptogelder neuartige Gefährdungslagen hinsichtlich der Geldwäscherei und der Terrorismusfinanzierung,

---

150 R. Wyss, Art. 6 GwG, in: D. Thelesklaf/R. Wyss/M. van Thiel et al. (Hrsg.), GwG Kommentar. Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, Zürich 2019, Rz. 3.

151 TheEconomist vom 8. Jul. 2017, „The Great Unbanking", 47 f.

152 S. Golstein, Australian banks allegedly blocking cryptocurrency transactions, freezing accounts, in: financemagnets.com vom 31. Dez. 2017, erhältlich unter: <https://www.financemagnates.com/cryptocurrency/news/australian-banks-allegedly-blocking-cryptocurrency-transactions-freezing-accounts/>; S. Haig, Aussie banks still cold to cryptocurrency business despite regulation, in: news.bitcoin.com vom 14. Apr. 2019, erhältlich unter: <https://news.bitcoin.com/aussie-banks-cold-cryptocurrency-businesses/>.

deren Erkennung und Vermeidung für Banken und Finanzintermediäre einen zusätzlichen Aufwand darstellt. Es kann allerdings nicht ausgeschlossen werden, dass Geschäftsbeziehungen abgelehnt werden, um unliebsame Konkurrenz vom Markt fernzuhalten oder die Verbreitung eines alternativen Zahlungsmittels behindert wird, welches nicht von Banken abhängig ist.

4. Dokumentationspflicht (Art. 7 GwG)

Die Dokumentationspflicht sieht vor, dass Finanzintermediäre und Händler für sämtliche durchgeführte Transaktionen sowie über *alle gemachten Abklärungen, welche durch die GwG-Sorgfaltspflichten vorgeschrieben sind, Belege zu erstellen haben* (Art. 7 GwG). Letzteres betrifft insbesondere die Unterlagen und Dokumentationen, welche zur Identifizierung der Vertragspartei sowie zur Feststellung des wirtschaftlich Berechtigten verwendet wurden.[153] Hinsichtlich der Transaktionen ist die Dokumentationspflicht relevant, um die geforderte Rückverfolgbarkeit von Vermögenswerten (Paper Trail) zu gewährleisten. 188

Die gemäss Art. 7 GwG erstellte Dokumentation ist *für die Dauer von zehn Jahren vom Finanzintermediär aufzubewahren* bzw. für Strafverfolgungsbehörden zur Verfügung zu halten (Art. 7 Abs. 2 und 3 GwG). Strafverfolgungsbehörden können die Herausgabe dieser Informationen gemäss den Voraussetzungen, welche die StPO für Zwangsmassnahmen (Art. 197 Abs. 1 StPO) vorsieht, verlangen. 189

Zumal eine Herausgabe der durch Finanzintermediäre gesammelten Unterlagen an staatliche Stellen nur in einzelnen, begründeten Fällen erfolgt, unterliegt die Dokumentationspflicht – und insofern die Geldwäschereigesetzgebung – dem risikobasierten Ansatz. Der *risikobasierte Ansatz im Geldwäschereirecht soll gewährleisten, dass der Staat in der Regel nicht Kenntnis der Finanzdaten von unschuldigen und unverdächtigen Personen erhält*. 190

Die Rückverfolgbarkeit kann nur dann gewährleistet werden, falls dem Finanzintermediär, der das Wallet betreut, welches eine Zahlung erhalten soll, Angaben über den Absender mitgeteilt werden. Die FINMA hat daher im Rahmen der Geltung des technologieneutralen Ansatzes bekräftigt, dass *Art. 10 GwV-FINMA, welcher Finanzintermediäre verpflichtet, bei einem Zahlungsauftrag die Angaben zum Auftraggeber und zum Begünstigten zu übermitteln, auch für Kryptogelder* 191

153 Siehe dazu vorne Rz. 179 f. und 181 ff.; siehe dazu T. MÜLLER, Art. 7 GwG, in: P.V. Kunz/T. Jutzi/S. Schären (Hrsg.), Geldwäschereigesetz (GwG). Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Stämpflis Handkommentar, Bern 2017, Rz. 9 ff.

gelte. Damit könne der die Zahlung empfangende Finanzintermediär die Angaben auf ihre Richtigkeit überprüfen und beispielsweise mit Sanktionslisten abgleichen. Kann ein Finanzintermediär nicht die benötigten Angaben übermitteln oder empfangen, so darf er nur Zahlungen zwischen eigenen Kunden und deren Wallets ausführen.[154]

5. Meldepflicht (Art. 9 GwG)

192 Eine mit dem risikobasierten Ansatz und der Dokumentationspflicht verbundene Aufgabe stellt die Meldepflicht für Finanzintermediäre und Händler gemäss Art. 9 GwG dar. Weil staatliche Behörden nur in Ausnahmefällen Zugang zu persönlichen Finanzdaten haben, stellt die *Meldepflicht eine Schnittstelle zwischen den Sorgfaltspflichten des Finanzintermediärs und den Massnahmen von Strafverfolgungsbehörden* dar.[155]

193 Finanzintermediäre und Händler sind verpflichtet, bereits beim Vorliegen eines einfachen Verdachts in Bezug auf die kriminelle Herkunft oder Verwendungszecke von Vermögenswerten eine Meldung zu erstatten.[156] Die *Meldepflicht soll sowohl die Einziehung von inkriminierten Vermögenswerten wie auch die Identifizierung der dahinter stehenden Personen erleichtern, damit diese der Strafverfolgung zugeführt werden können*.[157] Dementsprechend ist der Finanzintermediär aufgrund von Art. 10a GwG angehalten, weder betroffene Personen noch Dritte über erfolgte Meldungen zu unterrichten. Ferner ist der Finanzintermediär sogar verpflichtet, Kundenaufträge, welche gemeldete Vermögenswerte betreffen – auch solche im Zusammenhang mit Terrorismusfinanzierung –, weiter auszuführen (Art. 9a GwG).

194 Aus dem Gesagten folgt, dass die *Meldestelle für Geldwäscherei ab Erhalt einer Verdachtsmeldung von einem Finanzintermediär bis zur Grenze des begründeten Verdachts, ab welcher sie der zuständigen Strafverfolgungsbehörde Anzeige erstatten muss (Art. 23 Abs. 4 GwG), heimliche Untersuchungen durchführt*. Heimliche Untersuchungen durch staatliche Behörden stellen eine Gefahr für die unbeeinflusste Persönlichkeitsentfaltung dar und berühren die persönliche Freiheit

154 FINMA, Aufsichtsmitteilung 02/2019. Zahlungsverkehr auf der Blockchain, 2019, 2 f.; Siehe FATF, Virtual Assets and Virtual Asset Service Providers. Guidance for a Risk-Based Approach, 2019, Rz. 187 ff.

155 R. Wyss, Art. 9 GwG, in: D. Thelesklaf/R. Wyss/M. van Thiel et al. (Hrsg.), GwG Kommentar. Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, Zürich 2019, Rz. 3.

156 BGer Urteil vom 21.3.18, 1B_433/2017, E. 4.9.

157 R. Wyss, Art. 9 GwG (Fn. 155), Rz. 3 f.

(Art. 10 Abs. 2 BV). Weil persönliche Finanzdaten in die Untersuchung einfliessen, wäre ferner die informationelle Selbstbestimmung betroffen (Art. 13 Abs. 2 BV). Diese Daten können im Rahmen eines Strafverfahrens vollumfänglich Verwendung finden.

Für Bitcoin als nicht anonymes Zahlungsmittel gilt, dass die Geldwäschereifachstelle, d.h. für die Schweiz die MROS (Money Laundering Reporting Office) als FIU (‹Financial Intelligence Unit›) und Strafverfolgungsbehörden, auf die *Blockchain und damit auf ein umfassendes Transaktionsregister direkten Zugriff haben*. Daher können sie im Unterschied zu konventionellen Bankkonten unmittelbar Adressen einsehen, welche entweder Gelder von der gemeldeten Adresse erhalten oder an diese transferiert haben. Ferner lassen sich durch forensische Methoden weitere, auch nicht gemeldete Adressen, die von ein und derselben Person benutzt werden, miteinander in Verbindung bringen. Gegenüber dem konventionellen Zahlungsverkehr entfallen daher die unter Umständen langwierigen Herausgabebegehren an weitere Finanzintermediäre und Banken für weitere Unterlagen bezüglich der getätigten Transaktionen. Demgegenüber lässt sich Monero wegen der Obfuskation bzw. Anonymität der Blockchain nicht mithilfe forensischer Methoden überwachen und Dritte, wozu auch FIUs zählen, bedürfen einer Berechtigung (sogenannter ‹View Key›), um fremde Kontostände oder Transaktionen einzusehen. 195

6. Ausnahme: de-minimis Regel (Art. 7a GwG)

Die zuvor genannten Sorgfaltspflichten müssen nicht bei jedem Geschäft in demselben Mass berücksichtigt werden. Grundsätzlich ist vom Risiko der jeweiligen Transaktion bzw. der Geschäftsbeziehung für Geldwäscherei, Terrorismusfinanzierung auszugehen. In diesem Sinne bestimmt das geltende Recht, dass Finanzintermediäre bei Transaktionen, bei denen *nur Vermögenswerte von geringem Wert betroffen sind und keine Anhaltspunkte für Geldwäscherei oder Terrorismusfinanzierung vorliegen, von der Einhaltung der Sorgfaltspflichten befreit sind*. Diese sogenannte de-minimis Regel ist Ausdruck des risikobasierten Ansatzes, zumal bei geringen Beträgen, das Risiko für Geldwäscherei, Terrorismusfinanzierung etc. allgemein klein ist. Andererseits sieht das geltende Recht auch Verschärfungen vor, beispielweise in den bereits erwähnten Fällen von PEP oder Überweisungen in Risikoländer.[158] 196

Die Ausnahmeregelung für kleine Beträge muss grundsätzlich auch für Transaktionen und Geschäftsbeziehungen mit Kryptogeld gelten. Allerdings ist zu 197

158 Siehe dazu vorne Rz. 184 ff.

berücksichtigen, dass die *Erstellung von Kryptogeld-Adressen wesentlich vereinfachter und rascher vonstatten geht, als beispielsweise Bankkontos mit gefälschten Identitäten eröffnet werden können*. Um nicht aufzufallen, könnten die transferierten Kryptogeld-Beträge daher beliebig klein gehalten werden. Es muss daher nach weiteren möglichen Anzeichen gefragt werden, welche als Kriterium für die Auslösung einer Verdachtsmeldung wegen Geldwäscherei oder Terrorismusfinanzierung bei Kryptogeld in Betracht fallen.

198 Ein mögliches Kriterium stellt die Häufigkeit von Transaktionen dar, welche eine bestimmte Kryptogeld-Adresse generiert. Transaktionen könnten auch mit der Uhrzeit abgeglichen werden, um ungewöhnliche Verhaltensmuster erkennen zu können. Dienstleistungsanbieter von elektronischen Wallets könnten ferner die getätigten Zugriffe auf das Wallet mit der verwendeten IP-Adresse abgleichen, um Mehrfachnutzungen oder die Verwendung in Hochrisikoländer – oder deren Umgehung mithilfe VPN-Dienstleistungen – erkennen zu können. Darüber hinaus könnte *bei Bitcoin, zumal die gesamte Transaktionshistorie öffentlich ist, Kryptogeld bis zum Ursprung zurückverfolgt werden, d.h. anhand der Transaktionshistorie festgestellt werden, ob Anzeichen für Geldwäscherei oder Terrorismusfinanzierung vorliegen*. Bei Bitcoin bestünde ferner die Möglichkeit, schwarze Listen mit bekannten Adressen und Transaktionen zu erstellen, welche die Finanzintermediäre zum Abgleich mit den Transaktionen ihrer Kunden verwenden könnten und die festgestellte, oder zumindest wahrscheinliche, Risiken für Geldwäscherei oder Terrorismusfinanzierung enthielten. Für Monero folgt aus dem Gesagten e contrario jedoch, dass die Möglichkeiten zur Erkennung besagter Risiken vergleichsweise stark reduziert sind.

III. Fazit zum Geldwäschereirecht

199 Das geltende Geldwäschereirecht erfasst das Phänomen Kryptogeld grundsätzlich und knüpft an finanzintermediäre Tätigkeiten mit Kryptogeld, welche sich mit Dienstleistungen im konventionellen Zahlungsverkehr vergleichen lassen, entsprechende Rechtsfolgen an. Darüber hinaus werden die geltenden geldwäschereirechtlichen Sorgfaltspflichten allerdings nicht vollständig der dezentralen Konzeption von Kryptogeld gerecht. Beispielsweise brauchen sich tatsächlich wirtschaftlich berechtigte Personen nicht hinter rechtlichen Strukturen zu verstecken, um ihre Eigentümerstellung über Kryptogeld-Guthaben zu verschleiern. Ferner kann Kryptogeld weltweit von Person zu Person verschoben werden, ohne dass Finanzintermediäre oder Banken von dieser Transaktion Kenntnis erhalten.

Kapitel 3: Kryptogeld und Steuerhinterziehung

Kryptogelder sind als *immaterielle Vermögenswerte bzw. als «geldwerte Rechte» Thema des Steuerrechts und insofern des Steuerstrafrechts*. Im Hinblick auf die Fokussierung der vorliegenden Arbeit auf die Benutzer von Kryptogeld stehen die direkten Steuern im Zentrum des Interesses. Für die steuerliche Behandlung von Kryptogeld in der Schweiz ist daher die Vermögenssteuer (Art. 13 Abs. 1 StHG) sowie die Einkommenssteuer (Art. 7 Abs. 1 StHG) relevant. In einigen ausländischen Rechtsordnungen ist ferner eine Kapitalgewinnsteuer auf Wertgewinne von Kryptogeld-Guthaben geschuldet. 200

Steuerbare Tatbestände sind von den Steuerpflichtigen zu deklarieren, da die Nicht-Vornahme der Meldung ein Steuerdelikt darstellt. In der Schweiz ist das Verschweigen von Vermögen oder Einkünften als einfache Steuerhinterziehung zu qualifizieren, welche mit einer Geldbusse abhängig von der Höhe des hinterzogenen Steuerbetrags bestraft wird (Art. 56 Abs. 1 StHG). Im Ausland können für ein entsprechendes Unterlassen allerdings auch Freiheitsstrafen gesprochen werden (siehe etwa § 370 AO).[159] Bei *Kryptogeld, welches selbst gehalten wird, hat die Selbstdeklaration eine zentrale Bedeutung, da keine Drittparteien bestehen, welche die Steuertatbestände bescheinigen*. Anders liegt der Fall bei verwalteten Wallets. 201

Die Schweiz hat sich gegenüber bestimmten Staaten dazu verpflichtet, Informationen zu teilen, die im Rahmen von Steuerverfahren und auch Steuerstrafverfahren eingesetzt werden können. Gleichzeitig hat die Schweiz entsprechende Gegenrechte erhalten. Ein *Informationsaustausch findet insbesondere aufgrund der ‹multilateralen Vereinbarung der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten› („Globaler Standard")* statt.[160] Ausserdem besteht mit dem FATCA-Abkommen eine Vereinbarung, welche eine automatische Datenbekanntgabe an US-Steuerbehörden vorsieht. Ferner leistet die Schweiz in bestimmten Fällen Amtshilfe in Steuersachen, sofern ein entsprechendes Doppelbesteuerungsabkommen oder ein Steuerinformationsabkommen mit dem ersuchenden Land besteht.[161] Amtshilfe in Steuersachen kann seit 2017 auch 202

159 Abgabenordnung (AO) vom 16. Mrz. 1976, 610-1-3 [Deutschland].

160 Multilaterale Vereinbarung vom 29. Okt. 2014 der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten (MVStI, SR 0.653.1).

161 Siehe Übereinkommen vom 25. Jan. 1988über die gegenseitige Amtshilfe in Steuersachen, mit Änderung vom 27. Mai 2010 (SR 0.652.1), für die Schweiz in Kraft getreten am: 1. Jan. 2017, Amtshilfeübereinkommen (AHÜ, SR 0.652.1).

Gruppenanfragen umfassen, bei denen keine einzelnen, bestimmten Personen bezeichnet werden müssen (siehe Art. 14*a* StAhiG).[162]

203 Die Schweiz leistet ferner Rechtshilfe im Bereich von Steuerstrafverfahren. Für die *Gewährung von internationaler Rechtshilfe ist grundsätzlich das Bundesgesetz für internationale Strafsachen ausschlaggebend*. In Steuersachen kann Rechtshilfe geleistet werden, wenn zumindest ein Abgabebetrug vorliegt (Art. 3 Abs. 3 IRSG). Ein Abgabebetrug setzt Arglistigkeit voraus, die jedoch auch bei blossem Schweigen unter Umständen vorliegen kann.[163]

204 Allerdings können *Informationen, die die Schweiz im Rahmen des automatischen Informationsaustauschs oder im Rahmen eines Amtshilfeverfahrens einem ausländischen Staat übermittelt hat, von diesem auch in einem Steuerstrafverfahren wegen Steuerbetrug oder Steuerhinterziehung Verwendung finden*.[164] Darüber hinaus dürfen die Daten nur für die Bekämpfung von Geldwäscherei sowie Terrorismusfinanzierung verwendet werden oder es muss die Zustimmung der Schweiz für die anderweitige Verwendung der Daten vorliegen (Art. 22 Abs. 4 AHÜ).[165] Gleichzeitig dürfen vom Ausland in die Schweiz übermittelte Daten nur zur Anwendung und Durchsetzung des schweizerischen Steuerrechts genutzt werden (Art. 21 Abs. 1 AIAG). Ein allfälliger weiterer Gebrauch der Daten – beispielsweise für die Bekämpfung von Geldwäscherei, Terrorismusfinanzierung oder Korruption – ist zwar möglich, allerdings an enge Voraussetzungen geknüpft. Einerseits muss die weitere Verwendungsart im schweizerischen Recht vorgesehen und nach dem anwendbaren Abkommen zulässig sein. Andererseits muss unter Umständen die Zustimmung der zuständigen ausländischen Behörde zur anderweitigen Nutzung vorliegen (Art. 21 Abs. 2 AIAG).

205 *Wallets bzw. Konten mit Kryptogeld, welche einem Finanzintermediär anvertraut sind, unterliegen mangels Anwendbarkeit der Ausnahmetatbestände (Art. 3 f. AIAG) dem automatischen Informationsaustausch*. Finanzintermediäre müssen daher umfassende Angaben von im Ausland steuerpflichtigen Personen, welche bei ihnen ein verwaltetes Wallet unterhalten, automatisch der Eidgenössischen Steuerverwaltung (ESTV) mitteilen. Dazu gehören Name, Anschrift,

---

162 Bundesgesetz vom 28. Sep. 2012 über die internationale Amtshilfe in Steuersachen, Steueramtshilfegesetz (StAhiG, SR 651.1).

163 BGE 125 II 250, 252, E.3.b. – *Rechtshilfe Steuerstrafverfahren*.

164 Medienmitteilung des Bundesrats vom 29. Aug. 2018, „Keine Ausdehnung der Rechtshilfe bei Fiskaldelikten".

165 Notifikation der Schweiz vom 4. Mai 2017 nach Abschnitt 7 Abs. 1 Buchstabe d zur Multilateralen Vereinbarung vom 29. Okt. 2014 der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten (MVStI).

Geburtsdatum sowie Geburtsort, Kontosaldo etc. (Abschnitt 2 Ziff. 2 MVStI). Die ESTV leitet diese Daten an die zuständigen ausländischen Behörden weiter (Art. 15 AIAG). Umgekehrt erhält die ESTV Daten von ausländischen Behörden über in der Schweiz steuerpflichtige Personen, die sie den zuständigen nationalen Steuerbehörden weiterleitet (Art. 21 Abs. 1 AIAG). Die Einholung darüberhinausgehender Informationen muss allerdings im Amtshilfe- oder allenfalls Rechtshilfeverfahren erfolgen.

206 Demgegenüber besteht für schweizerische Finanzintermediäre keine Pflicht, Daten von Inländern den Schweizer Steuerbehörden bekanntzugeben. Im Gegenteil, das schweizerische Bankgeheimnis bzw. «Bankkundengeheimnis» gemäss Art. 47 BankG schränkt die Möglichkeit von Banken und weiteren Finanzdienstleistern ein, Informationen über ihre Kunden Steuerbehörden und weiteren Behörden, aber auch an Private, bekanntzugeben. *Das Bankgeheimnis ist nur ab der Schwelle der Vortaten zu Geldwäscherei und Terrorismusfinanzierung durchbrochen*. Mit der seit zu Beginn von 2016 geltenden Betrachtung der qualifizierten Steuervergehen als Vortaten zu Geldwäscherei muss die Bank daher bei begründetem Verdacht des Vorliegens eine Meldung machen (Meldepflicht), oder, im Fall von Zweifel, darf sie ohne Verletzung des Bankgeheimnisses ihren Verdacht zumindest melden (Melderecht).[166] Das Bankgeheimnis ist auf Wallet-Dienstleistungen mit Kryptogeld (Art. 47 Abs. 1 i.V.m. Art. 1b Abs. 1 BankG) anwendbar.

207 Aus dem Gesagten folgt, dass *Wallets von in der Schweiz steuerpflichtigen Personen bei inländischen Finanzintermediären besser vor der Kenntnis der Steuerbehörden geschützt sind als Wallets bei ausländischen Finanzintermediären, welche Daten im Rahmen des automatischen Informationsaustauschs bekannt geben müssen*. Erschwerend für die Identifikation und die Besteuerung von inländischen Wallets wirkt ausserdem, dass Kryptogeld-Guthaben nicht der Verrechnungssteuer unterliegt (Art. 4 Abs. 1 VStG e contrario).[167] Im Gegensatz dazu können Ausländer, die Wallet-Dienstleistungen in der Schweiz nutzen, dies wegen der erwähnten internationalen Abkommen nicht vor ihrem Fiskus verheimlichen. Ausserdem kann die ESTV Finanzinformationen von ausländischen Kunden, die nach einem Abkommen übermittelt werden sollen, gegenüber Finanzinformationen von inländischen Kunden einfacher, d.h. voraussetzungslos, mittels Zwangsmassnahmen beim Finanzintermediär beschaffen (Art. 13 Abs. 1 i.V.m. Art. 8

166 U. ZULAUF, Automatischer Informationsaustausch. Das Ende des steuerlichen Bankgeheimnisses?, in: SZW 2018, 667-683 (679); siehe dazu ferner J. BLOCH/N. GÜTLING, GwG-Meldepflichten. Quo vadis? in: SJZ 2018, 565-571 (566).

167 Bundesgesetz vom 13. Okt. 1965 über die Verrechnungssteuer, Verrechnungssteuergesetz (VStG, SR 642.21).

Abs. 2 StAhiG).[168] Im Ergebnis kommt die internationale Bekämpfung von Fiskaldelikten daher einer De-Anonymisierung von Wallet-Dienstleistungen in den genannten Situationen gleich.

168 Botschaft vom 23. November 2016 zur Genehmigung der multilateralen Vereinbarung der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten und zu ihrer Umsetzung (Bundesgesetz über den internationalen automatischen Informationsaustausch in Steuersachen), BBl 2015 5437, 5515.

Teil III:
Die de lege ferenda Regulierung von Kryptogeld

Kapitel 1: Bitcoin-Annahmeobergrenze

Eine mögliche Kryptogeld-Regulierung könnte darin bestehen, dass Händler ana- 208
log Art. 8a GwG nur eine begrenzte Summe von Kryptogeld pro Geschäft annehmen dürften. Ein V*erbot von betragsmässig hohen Handelsgeschäften könnte das Risiko für Geldwäscherei und Terrorismusfinanzierung mit Kryptogeld minimieren, zumal dem GwG nicht unterstellte Handelsgeschäfte zur Herkunftsverschleierung (‹Layering›) genutzt werden könnten*. In diesem Sinne könnte Kryptogeld, welches – beispielweise wegen Datendiebstahl (Art. 143 StGB) oder Erpressung (Art. 156 StGB) – unmittelbar oder – falls die inkriminierten Vermögenswerte zuvor in Kryptogeld eingetauscht wurden – mittelbar aus einer Straftat herrührt, „reingewaschen" werden.

Die Kryptogeld-Annahmeobergrenze orientiert sich unter anderm am generel- 209
len Barzahlungsverbot für Grundstücks- und Fahrniskäufe wie es der bundesrätliche Vorentwurf zum GwG noch vorsah.[169] Im Verlaufe der parlamentarischen Beratung wurde das Barzahlungsverbot ab CHF 100'000.- umgewandelt in die *Verpflichtung der Händler, für die Einhaltung der Anti-Geldwäscherei-Sorgfaltspflichten bei Überschreiten dieses Betrags selbst zu sorgen* oder die Bezahlung über einen anerkannten Finanzintermediär abwickeln zu lassen. Wie erläutert, bestehen bei Kryptogeld jedoch keine Finanzintermediäre im klassischen Sinne und die Einhaltung der GwG-Sorgfaltspflichten wäre für Händler und weitere Personen anspruchsvoller als dies beim Bargeld der Fall ist.

Als O*bergrenze für die Annahme von Bitcoin könnte ein umgerechneter Betrag* 210
von CHF 10'000.- zur Anwendung kommen. Dies stellt die betragsmässige Grenze dar, ab welcher einreisende Personen zur Auskunftserteilung verpflichtet sind (Art. 3 KGBV).[170] Ausserdem entspricht der gemachte Vorschlag ungefähr dem

---

169 Botschaft vom 13. Dez. 2013 zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière (GAFI), BBl 2014 605, 629 ff.

170 Verordnung vom 11. Februar 2009 über die Kontrolle des grenzüberschreitenden Barmittelverkehrs (KGBV, SR 631.052); siehe auch Art. 3 Abs. 1 Verordnung (EG) Nr. 1889/2005 des Europäischen Parlaments und des Rates vom 26. Oktober 2005 über die Überwachung von Barmitteln, die in die Gemeinschaft oder aus der Gemeinschaft verbracht werden (BMVo).

Betrag, welcher in der vierten europäischen Geldwäsche-RL (4.AMLR) für Händler vorgeschrieben ist (Art. 2 Abs. 1 Ziff. 3 lit. e i.V.m. Art. 11 lit. c 4.AMLR).[171]

211 Die Annahmeobergrenze für Bitcoin bei Waren- oder Dienstleistungsgeschäften schränkt sowohl die Handlungsoptionen der Verkäufer bzw. Händler wie auch der Käufer bzw. Konsumenten ein. *Gemäss etablierter schweizerischer Rechtsauffassung können sich nur Personen auf die Wirtschaftsfreiheit (Art. 27 BV) berufen, die mit Gewinnabsicht handeln*.[172] *Üblicherweise ist daher nur die Angebotsseite, d.h. die Händler, berechtigt, sich auf die Gehalte der Wirtschaftsfreiheit zu berufen*, während die Nachfrageseite, d.h. die Konsumenten, nicht in den Genuss dieser Garantien kommt. In einem ersten Schritt ist daher abzuklären, ob die Wirtschaftsfreiheit der Händler durch die Annahmeobergrenze verletzt ist (**I.**). Demgegenüber ist auf Seiten der Käufer bzw. der Konsumenten der Frage nachzugehen, ob die persönliche Freiheit (Art. 10 Abs. 2 BV) als subsidiäres Auffanggrundrecht Schutz vor einer derartigen Einschränkung bietet (**II.**).

I. Wirtschaftsfreiheit (Art. 27 BV)

1. Anwendbarkeit auf Kryptogeld

212 Es stellt sich zunächst die *Frage, ob Art. 94 Abs. 4 i.V.m. 100 Abs. 3 BV so auszulegen ist, dass Gesetzgebungen, welche in die dort erwähnten Kategorien fallen – d.h. das Geld- und Kreditwesen, die Aussenwirtschaft sowie die öffentlichen Finanzen – der Kontrolle unter dem Aspekt der Wirtschaftsfreiheit entzogen* sind. Wie bereits erwähnt, ist Kryptogeld ein Geldmittel und könnte daher zum

171 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 (vierte Geldwäsche EU-RL); in den EU-Mitgliedsstaaten haben sich jedoch teilweise noch tiefere Schwellenwerte etabliert: siehe EZB, Letter vom 16. Dez. 2019 from Yves Mersch, Member of the Executive Board of the European Central Bank (ECB), to Maria Elisabetta Alberti Casellati, President of the Senate of the Italian Republic, Roberto Fico, President of the Italian Chamber of Deputies, and Roberto Gualtieri, Italian Minister for Economy and Finance, requesting that the ECB be consulted on the legislation setting out a new threshold for cash payments.

172 BGE 102 Ia 104, 121, E. 7 – *Magazine zum Globus*; F. UHLMANN, Art. 27 BV, in: B. Waldmann/E. Belser /A. Epiney (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015, Rz. 18.

Geldwesen im Sinne von Art. 100 Abs. 4 BV zu zählen sein. Staatliche Interventionen zum Schutz der eigenen Währung bzw. des staatlichen Geldes sind ausserdem – zumindest aus der Perspektive des Staates – sinnvoll, zumal aufgrund einer grösseren Verbreitung mehr Einnahmen durch Münzgewinn generiert werden können und die Massnahmen zur Geldmengensteuerung effektiver sind.

213 Die Auffassung, dass die oben angeführten Gegenstände der Wirtschaftsfreiheit entzogen seien, lässt sich auf den Wortlaut von Art. 100 Abs. 3 BV zurückführen. Allerdings liefe eine solche Auslegung der ursprünglichen Motivation des Konjunkturartikels zuwider, welche vor einem unterschiedlichen historischem Hintergrund erfolgte und ihre praktische Relevanz fast gänzlich verloren hat.[173] *Mit der Ausnahme sollten nämlich spezifische konjunkturpolitische Massnahmen ermöglicht werden, die aber gegen den Grundsatz der Gleichbehandlung der Gewerbegenossen als Teilgehalt der Wirtschaftsfreiheit verstiessen*. Die Erklärung der Zulässigkeit solcher Eingriffe wurde obsolet, als durch Massnahmen der Globalsteuerung einzelne Wirtschaftsakteure nicht mehr bei der Konjunktursteuerung begünstigt wurden. Die Massnahmen zur Globalsteuerung sind daher in der Regel wettbewerbsneutral und somit unproblematisch unter dem Aspekt der Wirtschaftsfreiheit.[174]

214 Aus dem Gesagten folgt, dass *Art. 100 Abs. 3 BV keine Ausnahme von der Wirtschaftsfreiheit, sondern eine Ausnahme vom Grundsatz der Gleichbehandlung der Gewerbegenossen beinhaltet* und die Wirtschaftsfreiheit daher auch in den erwähnten Kategorien zur Anwendung kommt.

215 Es lässt sich noch die *Frage aufwerfen, ob Art. 100 Abs. 3 BV im Sinne einer ausgeglichenen konjunkturellen Entwicklung erlaubt, staatliches Geld gegenüber alternativen Zahlungsmitteln bevorzugt zu behandeln bzw. die Benützung alternativer Zahlungsmittel zu behindern*. Dies würde voraussetzen, dass Massnahmen gegen Kryptogeld tatsächlich positive Wirkungen auf die Konjunktur zeitigen. Wie weiter oben bereits erwähnt, ist aber die Verbreitung von Kryptogeld zu gering, um einen massgeblichen Einfluss auf gesamtwirtschaftliche Zusammenhänge ausüben zu können.[175] Ausserdem ist fraglich, ob Massnahmen gegen ein alternatives Zahlungsmittel positive Auswirkungen auf die konjunkturelle Entwicklung hätten. Ferner müsste Kryptogeld als Gewerbegenosse zum staatlichen

---

173 M. OESCH/B. KAMMERMANN, Art. 100 BV, in: B. Waldmann/E. Belser /A. Epiney (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015, Rz. 29 ff.

174 R. RHINOW, Art. 31^{quinquies} BV (Februar 1991), in: J-F. Aubert/H. Koller (Hrsg.), Kommentar zur Bundesverfassung der schweizerischen Eidgenossenschaft vom 29. Mai 1874, Band II, Loseblatt, Rz. 73 ff.

175 Siehe dazu vorne Rz. 143 f.

Geld mit sämtlichen getroffenen Massnahmen ebenfalls als zur Steuerung der Konjunktur notwendig aufgefasst werden.

216 Als Zwischenfazit lässt sich festhalten, dass mit Mitteln der Auslegung nicht begründet werden kann, dass Massnahmen im Bereich von Kryptogeld generell unter die Ausnahme für konjunkturpolitische Massnahmen (Art. 100 Abs. 3 BV) fielen. Die *Wirtschaftsfreiheit kommt daher im Bereich privater Zahlungsmittel und insofern für Einschränkungen des Umgangs mit Bitcoin grundsätzlich zur Anwendung*.

2. Schutzbereich der Wirtschaftsfreiheit (Art. 27 BV)

217 Träger der Wirtschaftsfreiheit gemäss Art. 27 BV sind sowohl die mit Schweizer Bürgerrecht ausgestatteten *natürlichen Personen wie auch die in der Schweiz ansässigen juristischen Personen des Privatrechts*.[176]

218 Daraus folgt, dass sich *gegen eine Annahmeobergrenze für Bitcoin von umgerechnet CHF 10'000.- sowohl die natürlichen Personen wie auch die juristischen Personen des Zivilrechts grundsätzlich auf die Garantie der Wirtschaftsfreiheit* berufen können.

219 Die in Art. 27 BV enthaltene Garantie stellt die individualrechtliche Seite der Wirtschaftsfreiheit der schweizerischen Verfassungsordnung dar. In dieser Funktion soll diese vorwiegend die freie berufliche und wirtschaftliche Entfaltung des Individuums schützen. *Als Schutzobjekt der Wirtschaftsfreiheit gilt die freie privatwirtschaftliche Betätigung in einem umfassenden Sinne*. Sie schützt nicht nur vor Beschränkungen der Berufswahl und des Berufszugangs, sondern, darüber hinaus, vor sämtlichen Berufsausübungsbeschränkungen.[177]

220 Die Wirtschaftsfreiheit gemäss Art. 27 BV steht nach bundesgerichtlicher Rechtsprechung sowie einem Teil der Lehre nur Gewerbetreibenden im Rahmen ihrer gewerblichen Tätigkeit zu. Nach ständiger Rechtsprechung des Bundesgerichts ist die Anrufung der Wirtschaftsfreiheit daher vom sogenannten Erwerbsmoment abhängig.[178] *Der Erwerbsmoment bildet die Absicht des Individuums oder des Unternehmens, mit einer bestimmten, privatwirtschaftlichen*

---

176 K.A. VALLENDER, Art. 27 BV, in: B. Ehrenzeller/B. Schindler/R.J. Schweizer (Hrsg.), Die Schweizerische Bundesverfassung. St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014, Rz. 46.

177 VALLENDER, Art. 27 BV (Fn. 176), Rz. 7 ff.

178 R. RHINOW/G. SCHMID/G. BIAGGINI/F. UHLMANN, Öffentliches Wirtschaftsrecht, 2. Aufl., Basel 2011, § 5 Rz. 30 ff.

Tätigkeit einen Gewinn zu erzielen. Ob der anvisierte Erfolg tatsächlich eintritt, oder ob noch weitere Motive als die Gewinnerzielung hinter der Geschäftstätigkeit stecken, ist für die Anwendbarkeit der Wirtschaftsfreiheit nicht von Belang. Allein in Situationen, in denen eine gewerbetreibende Person für den privaten Gebrauch Waren oder Dienstleistungen bezieht, kann die Wirtschaftsfreiheit gemäss Art. 27 BV nicht angerufen werden.[179] Liegt eine gewinnorientierte Tätigkeit im oben beschriebenen Sinn vor, so fallen aufgrund der Freiheit unternehmerischer Betätigung, als Teilgehalt der Wirtschaftsfreiheit, sämtliche dazugehörigen Handlungen und Entscheide in den Schutzbereich der Wirtschaftsfreiheit.

Händler, welche Waren oder Dienstleistungen verkaufen, verfolgen in der Regel eine gewinnorientierte, private Erwerbstätigkeit. *Ein Verbot, mehr als umgerechnet CHF 10'000.- in Bitcoin annehmen zu dürfen, schränkt sie in ihrer Freiheit der unternehmerischen Betätigung* ein. Genauer gesagt, wird die freie Wahl der Gewerbetreibenden zur Bestimmung der Gegenleistung für beim Verkauf oder Kauf von Waren oder Dienstleistungen und damit die Vertragsfreiheit eingeschränkt. 221

Eine Bitcoin-Annahmeobergrenze von CHF 10'000.- berührt folglich den Schutzbereich der Wirtschaftsfreiheit (Art. 27 BV). 222

3. Eingriff

Der Eingriff besteht darin, dass die Sorgfaltspflichten für Händler gemäss A*rt. 8a GwG durch das Verbot ergänzt wird, Bitcoins mit einem Wert von umgerechnet mehr als CHF 10'000.- annehmen zu dürfen*. Als Einschub in eine generell-abstrakte Norm ist der Eingriff als rechtsförmig zu qualifizieren.[180] Darüber hinaus verkürzt die Bitcoin-Annahmeobergrenze die Wirtschaftsfreiheit unmittelbar, da die Beeinträchtigung der Händler so beabsichtigt ist. 223

Eine Annahmeobergrenze für Bitcoins im Wert über CHF 10'000.-, welche für alle Händler gilt, schränkt deren Vertragsfreiheit ein. Die Vertragsfreiheit ist durch die Obergrenze in ihrem Teilgehalt der Gestaltungsfreiheit und die Wirtschaftsfreiheit daher in der Freiheit unternehmerischer Betätigung betroffen. Die Einschränkung ist allerdings auf einen ganz bestimmten Aspekt bezogen, nämlich die Bezahlung mit Bitcoin, und gelangt erst bei Überschreitung eines relativ hohen Bagatellbetrags von CHF 10'000.- zur Anwendung. Dieser *Bagatellbetrag deckt* 224

179 A. AUER/G. MALINVERNI /M. HOTTELIER, Droit constitutionnel suisse. Les droits fondamentaux, 3. Aufl., Bern 2013, Rz. 933; H. MARTI, Die Wirtschaftsfreiheit der schweizerischen Bundesverfassung, Basel 1976, Rz. 87.

180 Siehe zur gesetzlichen Grundlage sogleich Rz. 229.

fast sämtliche mögliche Handelsgeschäfte mit Kunden über Waren und Dienstleistungen grösstenteils ab (B2C).

225 Demgegenüber sind Geschäfte mit wertvolleren Gegenständen, wie beispielsweise Schmuck, Edelmetalle, Kunstobjekten, Fahrzeugen usw., oder mit Immobilien von der Bitcoin-Annahmeobergrenze betroffen. Während die Geschäftstätigkeit im Immobilienhandel voraussichtlich nur wenig zusätzlich erschwert ist, sind von einer Annahmeobergrenze Bereiche, in denen *regelmässig an viele persönlich unbekannte Personen Verkäufe getätigt werden, ungleich härter betroffen*. Insbesondere besteht das Risiko, dass wegen des zusätzlichen Zeitaufwandes Geschäfte, welche regelmässig an persönlich unbekannte Personen teure Gegenstände verkaufen – beispielsweise Juweliere – an Laufkundschaft verlieren. Dies betrifft jedoch nur eine kleine Anzahl der Gewerbetreibenden.

226 Die Annahmeobergrenze hat ferner Konsequenzen auf die überwiegende Mehrheit der Geschäfte zwischen Gewerbetreibenden (B2B), zumal der Bagatellbetrag von CHF 10'000.- regelmässig bei solchen Geschäften überschritten wird. Allerdings sind die Vorteile von Bitcoin-Transaktionen zwischen Gewerbetreibenden – im Unterschied zu Monero-Transaktionen – im Vergleich zu konventionellen elektronischen Überweisungen nur geringfügig und es bestehen Mittel Bitcoin einfach zu konvertieren und damit Ausweichmöglichkeiten für den Grundrechtsträger.[181] Folglich ist der Eingriff in dieser Hinsicht nur als leicht zu qualifizieren.

227 Schlussendlich weist das Verbot der Bezahlung von Beträgen von umgerechnet mehr als CHF 10'000.- mit Bitcoin, als Beschränkung der Vertragsinhaltsfreiheit, keine besondere Nähe zu Persönlichkeit auf. Die die Intensität des Eingriffs ist daher als nur leicht zu qualifizieren.

4. Genügende gesetzliche Grundlage

228 Eine Annahmeobergrenze für Bitcoin kann de lege ferenda in einem eingeschobenen Absatz in Art. 8*a* GwG mit folgendem Wortlaut eingeführt werden:

229

> Sorgfaltspflichten für Händlerinnen und Händler […]
>
> [1bis] Sie [Händlerinnen und Händler] dürfen pseudonyme virtuelle Währungen höchstens bis zu einem umgerechneten Wert von CHF 10'000.- annehmen. […]

181 Siehe zu Monero hinten Rz. 322.

Diese *de lege ferenda Norm ist ausreichend präzise formuliert und erfüllt daher die Anforderungen hinsichtlich der Normdichte*. Als Einschub in Art. 8*a* GwG handelt es sich um eine formell-gesetzliche Grundlage. Damit wird auch der Anforderung an die Normstufe Genüge getan. Sie würde selbst den Ansprüchen an einen schweren Eingriff entsprechen. 230

5. Legitime Eingriffsinteressen

Die Annahmeobergrenze soll zunächst der Verhinderung von Geldwäschereidelikten (Art. 305bis StGB) dienen. Die Geldwäschereibekämpfung dient dem Schutz von Polizeigütern, d.h. dem Schutz der öffentlichen Ordnung und ist damit als eine Aufgabe des Gemeinwesens zu qualifizieren. Wie bereits geschildert, hat sich die Schweiz auch völkerrechtlich zur Bekämpfung von Geldwäschereitaten verpflichtet.[182] 231

Als weiteres *polizeiliches Interesse gilt die Verhinderung bzw. die Bekämpfung von Terrorismus und der Terrorismusfinanzierung*. Der Straftatbestand der «Finanzierung des Terrorismus» (Art. 260^{quinquies} StGB) sieht dafür eine Freiheitsstrafe bis zu 5 Jahren oder eine Geldstrafe vor. Auch in diesem Bereich unterstreichen zahlreiche internationale Übereinkommen sowie Resolutionen des UN-Sicherheitsrats – welche die Schweiz praktisch ausnahmslos ratifizierte – die ausserordentliche Bedeutung dieses Anliegens für die Staatengemeinschaft.[183] Im Unterschied zur Geldwäscherei können hierunter auch Vermögenswerte mit legalem Ursprung fallen. 232

In einem weiteren Sinne kann auch das *Interesse an der Bekämpfung von Korruption als legitimes Eingriffsinteresse genannt werden*. Korruption bzw. Bestechung stellen nämlich, gleich nach den Drogendelikten (21%), die zweitmeist begangene Vortat für Geldwäschereidelikte dar.[184] Die Schweiz ist Signaturstaat des OECD-Übereinkommens über die Bekämpfung der Bestechung ausländischer 233

182 Siehe dazu vorne Rz. 100 ff.

183 Siehe etwa Internationales Übereinkommen vom 9.12.1999 zur Bekämpfung der Finanzierung des Terrorismus, für die Schweiz in Kraft getreten am 23.10.2003 (SR 0.353.22); Botschaft vom 14. Sep. 2018 zur Genehmigung des Übereinkommens des Europarats vom 16.5.2005 zur Verhütung des Terrorismus mit dem dazugehörigem Zusatzprotokoll und Verstärkung des strafrechtlichen Instrumentariums gegen Terrorismus und organisierte Kriminalität, BBl 2018 6427, 6428 ff. (Ratifikation ausstehend); Resolutionen des UN-Sicherheitsrats vom 28.3.2019 und 24.9.2014, UN-S-2462 und UN-S-2178; siehe EMCH/RENZ/ARPAGAUS, Bankgeschäft (Fn. 81), Rz. 385 ff.

184 EUROPOL, EU Drug Market Report. In-depth Analysis, 2016, 30.

Amtsträger im internationalen Geschäftsverkehr sowie der UNO-Konvention gegen die Korruption.[185]

234 Darüber hinaus stellt die Bekämpfung der Proliferation von Massenvernichtungswaffen und damit verwandten Gütern ein weiteres öffentliches Interesse dar, das durch zahlreiche völkerrechtliche Regimes und Übereinkommen hervorgehoben wird.[186] Durch ihre Teilnahme hat sich die Schweiz verpflichtet, die Nicht-Weiterverbreitung bzw. die vollständige Beseitigung solcher Waffen voranzutreiben. *Proliferation von Massenvernichtungswaffen in der Schweiz – wozu auch dazugehörige Finanzgeschäfte zählen – könnten eine Reihe von Sanktionen nach sich ziehen, welche vom Verlust der Glaubwürdigkeit der Politik sowie des Wirtschaftsstandortes, über Beeinträchtigung der aussen- und handelspolitischen Beziehungen bis hin zu Klagen sowie Retorsionsmassnahmen reichen*.[187]

235 Korruption und die Proliferation von Massenvernichtungswaffen zählen nach Ansicht der UNO sowie der FATF zu den «weiteren Gefahren», welche für das internationale Finanzsystem bestehen.[188] Sowohl die *Verhinderung der Proliferation von Massenvernichtungswaffen wie auch die Korruptionsbekämpfung weisen einen engen sachlichen Bezug zur Verhinderung von Terrorismusfinanzierung und Geldwäscherei auf*. Beispielsweise kann die Terrorismusfinanzierung letztendlich zum Kauf von Massenvernichtungswaffen verwendet werden. Ferner ist die Bestechung als Vortat zur Geldwäscherei aufzufassen.[189] Ausserdem können sowohl für Terrorismusfinanzierung, Korruption und Proliferationsgeschäfte Vermögenswerte aus legalem Ursprung Verwendung finden. Diese Delikte stellen demnach

185 Übereinkommen über die Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr vom 17. Dez. 1997, für die Schweiz in Kraft getreten am 30. Jul. 2000 (SR. 0.311.21); Übereinkommen der Vereinten Nationen gegen Korruption vom 31. Okt. 2003, für die Schweiz in Kraft getreten am 24. Okt. 2009 (SR 0.311.56).

186 Siehe etwa Abkommen vom 6. September 1978 zwischen der Schweizerischen Eidgenossenschaft und der internationalen Atomenergieorganisation über die Anwendung von Sicherungsmassnahmen im Rahmen des Vertrages über die Nichtverbreitung von Kernwaffen, für die Schweiz in Kraft getreten am 6. Sep. 1978 (SR 0.515.031).

187 Nachrichtendienst des Bundes, Prophylax, 2015, 5 ff.; FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. 2018, 11 ff.

188 Resolution der UN-Generalversammlung (A/RES/61/86) vom 6. Dez. 2006 (Measures to prevent terrorists from acquiring weapons of mass destruction); EMCH/RENZ/ARPAGAUS, Bankgeschäft (Fn. 81), Rz. 394.

189 M. PIETH, Art. 322^{septies} StGB, in: M. Niggli/H. Wiprächtiger (Hrsg.), Strafrecht II, Basler Kommentar, 4. Aufl., Basel 2019, Rz. 36.

keine neuartigen Gefährdungslagen für das Finanzsystem dar und werden daher nur erwähnt, sofern sie Auswirkungen auf den Gang der Untersuchung haben. Andernfalls sind mit der Erwähnung von Geldwäscherei, Terrorismusfinanzierung usw. immer auch diese Delikte mitangesprochen.

Es *liegen also anerkannte öffentliche Interessen an der Annahmeobergrenze für Bitcoin vor*. Es stellt sich die Frage, ob die öffentlichen Interessen einen solchen Eingriff zu rechtfertigen vermögen. 236

6. Verhältnismässigkeit

6.1 Eignung

Gegen die Eignung der Bitcoin-Annahmeobergrenze kann vorgebracht werden, dass sie fast vollständig wirkungslos bleibt. Bitcoin ist wegen der Öffentlichkeit der Blockchain grundsätzlich kein probates Mittel um die Herkunft oder den Verwendungszeck von Vermögenswerten zu verschleiern, zumal eine Art Paper Trail aufgrund der Daten in der Blockchain besteht.[190] Sachkundige Geldwäscher oder Terrorismusfinanzierer würden daher entweder immer knapp unter dem Schwellenwert bleiben oder vom Gebrauch von Bitcoins gänzlich absehen. Ausserdem können Bitcoins in eine andere, insbesondere anonyme, Kryptowährung – d.h. Monero – gewechselt und wieder rückgetauscht werden und so die Rückverfolgbarkeit praktisch aufgehoben werden. Dieser Ansicht kann entgegengehalten werden, dass eine Kontrolle von Exit Points, wozu insbesondere finanzintermediäre Tätigkeiten aber eben auch Handelsgeschäfte zählen, gerade bei Kryptogeld zumindest einen minimalen Nutzen stiften. Da Kryptogeld einfach, schnell und weltweit übertragen werden kann sowie die Eigentümer sich nicht zwingend zu identifizieren brauchen, *reduziert die Bitcoin-Annahmeobergrenze die Zahl der möglichen, unkontrollierten Exit-Points für Kryptogeld, die als Tore zum „legalen" bzw. konventionellen Wirtschaftskreislauf angesehen werden können. Durch die Errichtung einer Hürde, wie die Bitcoin-Annahmeobergrenze, ist daher zumindest die Attraktivität von Bitcoin zur Geldwäscherei, Terrorismusfinanzierung usw. gemindert und ist daher geeignet.* 237

6.2 Erforderlichkeit

Als ein in sachlicher Hinsicht milderes Mittel könnte eine analoge Heranziehung von Art. 8a Abs. 1 GwG dienen. Dies würde bedeuten, dass *anstelle des Annahmeverbots die Pflicht der Händler träte, die Geldwäscherei-Sorgfaltspflichten* 238

190 Siehe dazu vorne Rz. 70 ff.

hinsichtlich der erhaltenen Bitcoins selbst vorzunehmen. Eine solche Massnahme wäre für die Händler – trotz des zusätzlichen Zeitaufwandes – weniger einschneidend, da ihnen die Annahme grundsätzlich offen stünde, sie allerdings Abklärungen über die Herkunft oder den Verwendungszweck vornehmen müssten. Die Verpflichtung der Händler zur Abklärung des Bestehens von Geldwäscherei- und Terrorismusfinanzierungsrisiken ist jedoch weniger gut geeignet als die vollständige Ausschaltung des Risikos durch ein Annahmeverbot, da eine fundierte Prüfung ein beträchtliches Fachwissen voraussetzen würde. Ausserdem lassen sich Anhaltspunkte, welche für Geldwäscherei im konventionellen Bereich sprechen, nicht ohne Weiteres auf Bitcoin bzw. Kryptogeld übertragen. Ferner wäre der im Hinblick auf die Abklärung der geldwäschereimässigen Risiken erforderliche Zeitaufwand kaum mit den Ansprüchen der Laufkundschaft zu vereinbaren.[191]

239 Zum selben Resultat führte auch eine Regulierung, welche Händler verpflichten würde, Finanzintermediäre bzw. bestimmte *Fachstellen zur Begutachtung des Geldwäschereirisikos beiziehen zu müssen*. Diese Fachstellen könnten sich auf die Analyse von Blockchain-Daten spezialisieren und allenfalls die Benutzung von Mixern bzw. Tumblern oder sonstige ungewöhnliche Anhaltspunkte, welche für Geldwäscherei oder ähnliches sprechen, besser erkennen.[192] Auch diese Stellen könnten jedoch im Vergleich zu einem Verbot nur in vermindertem Masse die Abwesenheit von Geldwäscherei oder Steuerhinterziehung garantieren. Ferner bestünde ein gewisses Risiko, dass vor allem solche Fachstellen gewählt würden, welche eher grosszügig die Unbedenklichkeit von Transaktionen hinsichtlich Geldwäscherei, Terrorismusfinanzierung usw. ausweisen. Die Wirksamkeit wird ferner dadurch eingeschränkt, dass eine gründliche Überprüfung, beispielsweise der Transaktionshistorie, zeitlich intensiv ist und daher nur nachträglich – d.h. im Anschluss an den Verkauf – erfolgen könnte. Insofern könnten Geldwäscherei und Terrorismusfinanzierung im besten Fall nur aufgedeckt und nicht verhindert werden. Mangels adäquater Wirksamkeit fällt diese Alternative also ausser Betracht.

240 Ferner kommt eine Beschränkung der Annahmeobergrenze auf Geschäfte mit Kunden (B2C) in Betracht, da Gewerbetreibende in der Regel Rechnungsführung- und Buchführungspflichten (Art. 957 Abs. 1 OR) unterstehen. Dies würde für Händler eine grosse Erleichterung bedeuten, zumal die Annahmeobergrenze von CHF 10'000.- die überwiegende Mehrheit der B2B-Geschäfte erfasst und verbietet. Eine *Regulierungsvariante, welche B2B-Geschäfte generell von der Geltung der Annahmeobergrenze ausnimmt, trägt allerdings nicht im selben Mass zur*

191 Siehe dazu N. RAMELET, Geldwäschereibekämpfung bei Barzahlungsgeschäften. Staatliche Sterbehilfe für das Bargeld? in: SZW 2016, 76-83 (82 f.).

192 Siehe M. TRAN/I. BENTOV/L. LUU et al., OBSCURO. A Bitcoin Mixer using Trusted Execution Environments, 2017 (Version vom: 31.12.18), 2 f.

Verhinderung von Geldwäscherei, Terrorismusfinanzierung usw. bei, wie eine Regulierung, die für beide Formen gilt. Da B2B-Transaktionen grundsätzlich höhere Beträge aufweisen, ist das Risiko der Gefährdung durch die genannten Delikte folglich gesteigert. Darüber hinaus ist die Rechnungslegung, insbesondere wenn keine vertiefte, unabhängige Überprüfung bzw. Revision verlangt ist, kein Garant für eine einwandfreie Geschäftstätigkeit. Ferner ist zu berücksichtigen, dass die Eigentümerstellung von Unternehmen, die einer Rechnungslegungspflicht unterstehen, durch zwischengeschaltete, insbesondere länderübergreifende, rechtliche Strukturen verschleiert werden kann.

Als milderes Mittel steht ferner eine Annahmeobergrenze nur für bestimmte, d.h. der Geldwäscherei besonders anfällige, Geschäftszweige zur Diskussion. Diese müssten sicherlich die von den FATF-Empfehlungen genannten Branchen wie Immobilienhändler, Edelstein- und Edelmetallhändler, Treuhänder usw. (sogenannte DNFBP) umfassen.[193] Eine nur *branchenweise geltende Annahmeobergrenze ist aber nicht gleich wirksam wie eine allgemein gültige Obergrenze*. Ausserdem konnten sich in der EU aufgrund der FATF Empfehlungen umfassende, branchenunabhängige Barzahlungsvorschriften etablieren, an welchen sich die Schweiz im Interesse des Marktzugangs orientieren muss.[194] 241

In Betracht fällt darüber hinaus eine *Bewilligungspflicht für die Annahme von Bitcoin von umgerechnet über CHF 10'000.- für Händler*. Es wäre jedoch sehr schwierig, taugliche Kriterien für die Bewilligungserteilung zu finden. Grundsätzlich bietet sich als Grundlage für eine solche Ausnahmebewilligung die de-minimis Ausnahme an (Art. 7a GwG), welche auch die FATF-Empfehlungen gewähren.[195] Allerdings liessen sich die Risiken kaum bereits im Vorfeld abschätzen. Wie zuvor ausgeführt, scheidet eine Lösung, welche anhand der betroffenen Branche unterscheidet, aus. Eine Bewilligungspflicht für die Annahme von mehr als CHF 10'000.- ist angesichts des Restrisikos nicht gleich wirksam, wie ein absolutes Verbot der Annahme bei Erreichen der Bagatellgrenze. 242

Als Zwischenergebnis lässt sich also festhalten, dass *zwar mildere Mittel vorhanden sind, diese aber nicht die gleiche Wirksamkeit aufweisen wie ein* 243

193 FATF, Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, 2013, Rz. 51 ff.

194 F. CONTRATTO, Sanktionen. Neue Gretchenfrage im Ringen um den Marktzugang in die EU?, SZW 2018, 653-666 (658); RAMELET, Geldwäschereibekämpfung (Fn. 191), 77 ff.

195 FATF, Inclusion (Fn. 193), Rz. 55 ff.; FATF, Virtual Currencies. Guidance for a Risk-based Approach, 2015, Rz. 45.

Annahmeverbot von Bitcoin ab umgerechnet CHF 10'000.-. Die Massnahme ist folglich erforderlich.

6.3 Zumutbarkeit

244 Gegen die Zumutbarkeit einer Bitcoin-Annahmeobergrenze sprechen zunächst die dadurch *bewirkten Beeinträchtigungen der Geschäftstätigkeit von Händlern*. Händler müssen die Kunden darauf hinweisen, dass nur bestimmte Zahlungsmittel je nach Wert des Gegenstands akzeptiert werden können. Darüber hinaus muss das Personal auf die Beachtung dieser Unterschiede geschult werden. Aufgrund der Bitcoin-Annahmeobergrenze können sich Händler und deren Personal strafbar machen, zumal die Geldwäscherei (Art. 305bis StGB) nach bundesgerichtlicher Rechtsprechung auch im Unterlassungsfall strafbar ist und eine Garantenstellung aus der Bitcoin-Annahmeobergrenze abgeleitet werden könnte.[196] Diese Konsequenz ist stossend angesichts des Umstands, dass Händlern eine Pflicht auferlegt wird, welche die Vermeidung von Risiken zum Gegenstand hat, die weder in der eigenen Geschäftstätigkeit noch in der Geschäftstätigkeit ihres Wirtschaftssektors begründet sind. Allerdings gilt es zu berücksichtigen, dass bis zum Erreichen der Bagatellgrenze keine Beeinträchtigungen bestehen. Händler ziehen daher grundsätzlich Nutzen von den Vorteilen, welche Bitcoin bietet. So profitieren sie insbesondere von schnelleren Transaktionen, denen kein Rückbuchungsrisiko (sogenanntes ‹Chargeback-Risiko›) anhaftet, d.h. eine Stornierung der Transaktion nach erfolgter Auslieferung. Ausserdem profitieren auch Händler von der Widerstandsfähigkeit des Netzwerkes gegenüber Angriffen sowie gegenüber Zensur. Nicht zuletzt können dank des voraussetzungslosen Zugangs zu Bitcoin theoretisch mehr Kunden angesprochen werden, als dies mit Bargeld oder mit, durch sehr restriktiven Zugang gekennzeichneten, Kreditkarten möglich ist.

245 Ferner sprechen die Auswirkungen auf den Wert von Bitcoin gegen die Annahmeobergrenze. Eine Bitcoin-Annahmeobergrenze hat zur Folge, dass der mögliche Einsatzbereich von Bitcoin reduziert ist auf die Begleichung von Zahlungen bis umgerechnet maximal CHF 10'000.-. Dies beeinträchtigt die Universalität und damit die Eignung als Zahlungsmittel von Bitcoin. Mit der Beeinträchtigung der Eignung als Zahlungsmittel geht ein Wertverlust einher, zumal Kryptogeld ausschliesslich ein Wert aufgrund der Erfüllung der geldmässigen Funktionen

196 BGE 136 IV 188, 191 f. E. 6.2 – *Geldwäscherei* (=Pra 2011, Nr. 79); siehe zur Strafbarkeit im Unterlassungsfall: P. BURKHARDT/A. HÖSLI, Neue strafrechtliche Risiken für Händler bei Barzahlungen über CHF 100'000, in: jusletter.ch vom 1. Feb. 2016, Rz. 35 ff.

zukommt.[197] Die Annahmeobergrenze führt in diesem Sinne zu einer *Entwertung eines unter die Wirtschaftsfreiheit fallenden Gegenstands*.

Demgegenüber spricht für die Zumutbarkeit der Annahmeobergrenze für Bitcoin, dass an der Verhinderung von Terrorismusfinanzierung – und an der Verhinderung der Proliferation von Massenvernichtungswaffen – ein erhebliches, globales Interesse besteht. Dasselbe gilt, in vermindertem aber stetig zunehmendem Masse, für die Korruptionsbekämpfung sowie Steuerhinterziehung. Illegitime Machenschaften mit Bitcoin stellen *ein Reputationsrisiko für den Finanzplatz Schweiz dar und können darüber hinaus auch internationale Sanktionen für die Schweiz und einzelne Akteure nach sich ziehen* – z.B. Aufnahme auf „Schwarze" oder „Graue Listen" oder Ausschluss von in US-Dollar denominierten Zahlungen sowie Klagen usw.[198] Es bestehen also substantielle Interessen an der Verhinderung solcher Delikte. 246

In einer Gesamtbetrachtung der gemachten Argumente ist zunächst festzuhalten, dass die erwähnten Beeinträchtigungen der freien Geschäftstätigkeit von Händlern nur leicht gegen die Zumutbarkeit sprechen, da *der hohe Bagatellbetrag von CHF 10'000.- bedeutet, dass die überwiegende Mehrheit der Geschäfte mit Privatkunden (B2C) von der Annahmeobergrenze nicht betroffen ist* und insofern gar keine Beeinträchtigung besteht. Diese Überlegung lässt sich auch auf das Argument der möglichen Strafbarkeit von Händler sowie Personal übertragen. Die mögliche Strafbarkeit ist zwar als einschneidend, allerdings angesichts des hohen Bagatellbetrags als wenig praxisrelevant einzustufen. Ausserdem kann von Geschäftszweigen, die regelmässig mit solchen Beträgen handeln – beispielweise Juweliere – eine grundsätzlich erhöhte Wachsamkeit eingefordert werden. Ferner ist auch das Argument der begrenzten Wirksamkeit sowie das Argument, Händler für branchenfremde Risiken verantwortlich zu machen, nur leicht zu gewichten, zumal viele Regulierungen solche Defizite aufweisen. 247

Demgegenüber kommt hinsichtlich der Zumutbarkeit der Bitcoin-Annahmeobergrenze den *verfolgten öffentlichen Interessen aufgrund ihrer internationalen Beachtung und der daraus folgenden Bedeutung für den Finanzplatz Schweiz ausserordentliches Gewicht zu*. Das Interesse an der Verhinderung von 248

197 Siehe zur Werthaltigkeit vorne Rz. 69; siehe auch KLEIN/SPREMANN, Telegeld (Fn. 6), 21.

198 EMCH/RENZ/ARPAGAUS, Bankgeschäft (Fn. 81), Rz. 443; Botschaft vom 7. Dez. 2007 betreffend die Ratifikation eines Übereinkommens und der Änderung eines Übereinkommens sowie Beitritt zu zwei Änderungsprotokollen der UNO zur Bekämpfung terroristischer Handlungen gegen die nukleare und maritime Sicherheit, BBl 2008 1153, 1170; Nachrichtendienst des Bundes, Prophylax (Fn. 187), 7.

Terrorismusfinanzierung, Geldwäscherei usw. überwiegt daher dem Interesse an einer ungehinderten Ausübung der Wirtschaftsfreiheit.

249 Aus dem Gesagten folgt, dass eine *Bitcoin-Annahmeobergrenze von CHF 10'000.- für Handelsgeschäfte zumutbar wäre*.

7. Kerngehalt

Der Kerngehalt der Wirtschaftsfreiheit besteht aus einem persönlichkeitsbezogenen sowie einem institutionellen Gehalt. Nach ersterem sind insbesondere Sklaverei und Zwangsarbeit verboten. Auch der Zwang zum Erlernen oder Ausüben eines bestimmten Berufs fällt unter diesen Gesichtspunkt und ist unvereinbar mit der Wirtschaftsfreiheit. Der *institutionelle Gehalt der Wirtschaftsfreiheit schützt den freien Markt, d.h. den Grundsatz des freien Austauschs von Gütern zwischen Personen*. Staatliche Eingriffe in den freien Markt, insbesondere solche, die den Marktmechanismus beseitigen oder Betätigungsfelder für die Privatwirtschaft substantiell reduzieren, verletzen den institutionellen Kerngehalt der Wirtschaftsfreiheit.[199] Wie bereits erwähnt, folgt weder aus Art. 99 noch 100 BV einen Ausschluss der Rechtsgewährleistung im Bereich der privaten Zahlungsmittel.[200]

250 Angesichts der zur Diskussion stehender Regulierung ist der persönlichkeitsbezogene Gehalt nicht einschlägig. Allerdings könnte der institutionelle Kerngehalt durch die vorgeschlagene Regulierung betroffen sein. Wie in anderen Bereichen besteht *auch im Bereich privater Zahlungsmittel das Risiko, dass staatliche Eingriffe den Marktmechanismus bzw. die Betätigungsfelder für Private beseitigen* und insofern in den Kerngehalt eingreifen.

251 Es stellt sich die Frage, ob es überhaupt einen Marktmechanismus zwischen Währungen gibt. Unter dem Marktmechanismus versteht man das Zusammenspiel von Angebot und Nachfrage und dessen Auswirkung auf den Preis eines Gutes. Obwohl in der klassischen volkswirtschaftlichen Literatur nur wenig behandelt, können *unterschiedliche Währungen zueinander in Konkurrenz treten und damit*

199 M. SCHEFER, Kerngehalte von Grundrechten. Geltung, Dogmatik, inhaltliche Ausgestaltung, Bern 2001, 291, 467 ff.; J.P. MÜLLER/M. SCHEFER, Grundrechte in der Schweiz. Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, Bern 2008, 1078 f.

200 Siehe vorne Rz. 212 ff.

einen Marktmechanismus beinhalten.[201] Dieser Marktmechanismus zwischen Währungen fällt unter den Schutz der Wirtschaftsfreiheit.

Eine auf Händler beschränkte Annahmeobergrenze von umgerechnet CHF 10'000.- führt allerdings kaum zu einer vollständigen Beseitigung des Marktmechanismus oder der möglichen Betätigungsfelder für Private. Das Vorhandensein einer bzw. mehrerer Alternativen zur nationalen Währung ist nach wie vor möglich. *Das Recht Privater, eigene Geldmittel nach Vorbild von Bitcoin herauszugeben, wird durch die vorgeschlagene Regulierung nicht geschmälert*. Ausserdem bedeutet eine Obergrenze, keinen unerlaubten staatlichen Eingriff auf den Preismechanismus zwischen Währungen. Obwohl dadurch die Attraktivität von Bitcoin geschmälert wird, sind die Auswirkungen auf den Wert von Bitcoin in jedem Fall zu gering, um eine Betroffenheit des Kerngehalts annehmen zu können.[202] 252

Es liesse sich hingegen argumentieren, dass sich eine überbordende Regulierung im Bereich von Bitcoin auf grundsatzwidrige Motive stützt, nämlich, dass der Staat die eigene, staatliche Währung bevorzugen möchte – v.a. aus Gründen des Notenbankgewinns (Seigniorage).[203] Dies könnte im Einzelfall tatsächlich zutreffen, jedoch bestehen durchaus auch grundsatzkonforme Motive hinter dem Eingriff.[204] *Die alleinige Koexistenz allfälliger grundsatzwidriger Motive führt nicht dazu, dass ein Eingriff in den Kerngehalt der Wirtschaftsfreiheit besteht*. 253

Im Ergebnis liegt also *keine Betroffenheit des Kerngehalts* der Wirtschaftsfreiheit wegen der Bitcoin-Annahmeobergrenze vor. 254

8. Fazit

Eine für Händler geltende Annahmeobergrenze von umgerechnet CHF 10'000.- für Bitcoin verletzt die Wirtschaftsfreiheit (Art. 27 BV) nicht, zumal die Bitcoin-Annahmeobergrenze ein geeignetes und erforderliches Mittel darstellt und zudem die staatlichen Interessen an der Verhinderung von 255

201 Siehe aber F.A. VON HAYEK, Entnationalisierung des Geldes, in: A. Bosch/R. Veit(†)/V. Veit-Bachmann (Hrsg.), Schriften zur Währungspolitik und Währungsordnung, Tübingen 2011, 129-254.

202 Siehe zu den Auswirkungen auf den Wert vorne Rz. 245.

203 BIZ, Digital currencies (Fn. 45), 2015, 16; siehe auch E. BALTENSPERGER, Währungsstabilität als Ausdruck gesellschaftlicher Verantwortung. Zentralbankbindung über Verfasssungs- und Gesetzesnormen, in: P. Bagus/G. Schwarz (Hrsg.), Die Entstaatlichung des Geldes, Zürich 2014, 70.

204 Siehe zu den legitimen öffentlichen Interessen vorne Rz. 231 ff.

Terrorismusfinanzierung, Geldwäscherei usw. dem Interesse an der ungehinderten Ausübung der Wirtschafsfreiheit überwiegen. Unter dem *Gesichtspunkt der Wirtschaftsfreiheit (Art. 27 BV) steht der Einführung einer Bitcoin-Annahmeobergrenze folglich keine Hindernisse entgegen*.

II. Persönliche Freiheit (Art. 10 Abs. 2 BV)

256 Zu den Betroffenen einer Bitcoin-Annahmeobergrenze zählen auch die potentiellen Kunden der Händler, d.h. die Konsumenten. Sie könnten *mangels einer eigentlichen Konsumfreiheit in der schweizerischen Rechtsordnung immerhin in ihrer allgemeinen persönlichen Freiheit* (Art. 10 Abs. 2 BV) berührt sein.[205]

1. Schutzbereich

257 Auf die allgemeine persönliche Freiheit gemäss Art. 10 Abs. 2 BV können sich anerkanntermassen alle natürlichen Personen berufen. Die Trägerschaft juristischer Personen ist hingegen umstritten. Nach bundesgerichtlicher Rechtsprechung können sich immerhin die Personenvereinigungen auf die persönliche Freiheit berufen. Die herrschende Lehre lehnt die Grundrechtsträgerschaft juristischer Personen ab.[206] Da die Wirtschaftsfreiheit gegenüber der persönlichen Freiheit einen sachlich spezifischeren Anwendungsbereich aufweist sowie juristische Personen meist einer gewerbsmässigen Tätigkeit nachgehen und sich insofern auf die Wirtschaftsfreiheit (Art. 27 BV) berufen können, wird *im Folgenden exemplarisch die Betroffenheit natürlicher Personen untersucht*.

1.1 Grundentscheidung für den eigenen Lebensplan

a. Geschützte Verhaltensweise

258 Laut bundesgerichtlicher Rechtsprechung schützt die persönliche Freiheit im Sinne von Art. 10 Abs. 2 BV alle elementaren Erscheinungen der Persönlichkeitsentfaltung. Dazu können auch ganz alltägliche Handlungen bzw. Vorgänge gehören, sofern sie Ausdruck der Grundentscheidung für einen eigenen Lebensplan sind und damit für die Persönlichkeit besondere Bedeutung aufweisen. Als

205 Siehe vorne Rz. 211.

206 R. SCHWEIZER, Art. 10 BV, in: B. Ehrenzeller/B. Schindler/R. J. Schweizer (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich 2014, Rz. 10 f.

Ausdruck einer solchen Grundentscheidung gilt unter anderem der Konsum identitätsstiftender Produkte.[207]

Die Qualifikation von *Bitcoin als ein identitätsstiftendes Produkt – und damit als Ausdruck der Grundentscheidung für den eigenen Lebensplan – scheint angesichts seiner Ursprünge sowie Attribute als angezeigt*. Die Unabhängigkeit von staatlichen Institutionen – insbesondere der Nationalbanken – ist ein erklärtes Ziel des mutmasslichen Erfinders von Bitcoin.[208] Ausserdem geniessen Kryptogelder vor allem in libertären und krypto-anarchischen Kreisen (sogenannte ‹Cypherpunks›) die grösste Bekanntheit und Verbreitung. Diese Bewegungen zeichnen sich unter anderem durch eine gelebte oder zumindest angestrebte, mehr oder weniger weit gehende Staatsferne als lebensphilosophische Grundhaltung aus.[209] Staatsferne ist auch auf das Geldwesen zu erstrecken, d.h. der Staat darf auch dort nicht tätig werden, weil Private die Aufgabe der Versorgung der Volkswirtschaft mit Geldmittel gleich gut oder sogar besser als der Staat erfüllen können.[210] Ferner legen Anhänger dieser Bewegungen Wert auf die Wahrung der Privatsphäre und des Schutzes persönlicher Daten.[211] Eine angestrebte staatsferne Lebensweise sowie der Schutz der Privatsphäre, wozu Bitcoin bzw. Kryptogeld ein vorzügliches Mittel darstellt, haben einen Bezug zur Persönlichkeit und können Einfluss auf deren freie Entfaltung haben. Die Benutzung von Bitcoin als Ausdruck bzw. Alltagspraxis des Lebensplans steht daher unter dem Schutz von Art. 10 Abs. 2 BV. 259

b. Mindestgewicht der Beeinträchtigung

Zumal es sich beim Konsum eines identitätsstiftenden Produkts um ein Element der persönlichen Freiheit im Grundtatbestand handelt, reicht eine bloss minimale Belastungsintensität nicht aus, um den Schutzbereich der persönlichen Freiheit zu eröffnen. Die *Beeinträchtigung muss daher die Grenze für Bagatellfälle bzw. den Bagatellvorbehalt im Sinne von Art. 10 Abs. 2 BV überschreiten*.

---

207 A. TSCHENTSCHER, Art. 10 BV, in: B. Waldmann/E. Belser/A. Epiney (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015, Rz. 36.

208 Siehe NAKAMOTO, Bitcoin (Fn. 1), 1 ff; L. MEISSER, Kryptowährung. Geschichte, Funktionsweise, Potential, in: R. Weber/ F. Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich 2015, 74 ff.

209 M. VOGEL, Relevanz & Risiken von virtuellen Währungen am Beispiel von Bitcoin, Hof 2016, 15.

210 VON HAYEK, Entnationalisierung (Fn. 201), 129 ff.

211 L. BRANDEIS/S. WARREN, The Right to Privacy, in: Harv. L. Rev. 1890, 193-220 (213 ff.).

260 Aufgrund der Annahmeobergrenze von umgerechnet CHF 10‘000.- für Händler wird nur ein kleiner Teilbereich der möglichen Handlungsoptionen der Konsumenten mit Bitcoin entzogen. Zunächst ist die Möglichkeit, Zahlungen zwischen Privatpersonen ausführen zu können (P2P), gar nicht betroffen, weil nur im Rahmen von gewerbsmässigen Handelstätigkeiten die Annahmeobergrenze zum Tragen kommt. Ferner kommt selbst im Rahmen von Käufen bei gewerbsmässig-tätigen Händler die Annahmeobergrenze nur selten zur Anwendung, weil die Bagatellgrenze von CHF 10'000.- die allermeisten Gegenstände erfasst. Schlussendlich kommen auch andere Tätigkeiten mit Bitcoin als identitätsstiftendes Produkt in Betracht, die von der Annahmeobergrenze nicht betroffen sind. Dazu zählen die Möglichkeiten der Beteiligung an Bitcoin als Zahlungsverarbeiter, d.h. als Miner, als Betreiber eines Mining Pools für eine Gruppe von Miner oder als Entwickler. *Die Annahmeobergrenze für Bitcoin stellt daher nur eine leichte Beeinträchtigung des Umgangs mit einem identitätsstiftenden Produkt dar und erreicht insofern nicht die von Art. 10 Abs. 2 BV vorausgesetzte Intensität der Massnahme,* um den Schutzbereich der persönlichen Freiheit zu tangieren.

1.2 Besondere praktische Bedeutung

261 Gemäss bundesgerichtlicher Rechtsprechung fällt darüber hinaus jede Handlung in den Schutzbereich von Art. 10 Abs. 2 BV, die nach den konkreten Umständen von besonderer praktischer Bedeutung ist. Dieses Kriterium wurde vom Bundesgericht insbesondere hinsichtlich der Umstände von Inhaftierungen angewandt.[212] Es lässt sich jedoch auch auf andere Situationen übertragen.

a. Verwendung als Vorsorgekapital

aa. Geschützte Verhaltensweise

262 *Bitcoin könnte ferner hinsichtlich der persönlichen Vorsorge von besonderer praktischer Bedeutung* sein. Individuen könnten nämlich ein Interesse daran haben, Bitcoin-Vorsorge- oder Sparkapital aufzubauen. Als reine Eigentumsbeschränkung, die kaum die Schwere einer formellen Enteignung erreicht, wäre eine Annahmeobergrenze jedoch unter der Eigentumsfreiheit (Art. 26 BV) entschädigungslos hinzunehmen.

263 Bitcoin könnte unter anderem wegen der Unabhängigkeit von Nationalbanken und Politik bzw. aufgrund des Umstands, dass die Geldmengensteuerung vorprogrammiert ist, eine besondere Bedeutung hinsichtlich der persönlichen Vorsorge darstellen. Staatliche Währung ist im Unterschied zu Kryptowährung politischen

212 TSCHENTSCHER, Art. 10 (Fn. 207), Rz. 38.

und wirtschaftlichen Zielsetzungen unterworfen, welche sich in der Regel negativ auf die Kaufkraft und damit negativ auf den Sparer und Rentner auswirken. *Selbst bei normalem Geschäftsgang der Nationalbank erfolgt, aufgrund der von der SNB selbst gesetzten, «optimalen» Inflationsrate von zwei Prozent, eine entsprechende jährliche Entwertung von Sparguthaben*. Da Zinsen auf Sparkonten im heutigen Zinsumfeld nur noch einen Bruchteil der Inflationsrate ausmachen – und sogar auch für durchschnittliche Sparer ins Negative abzugleiten drohen –, resultiert schon nach wenigen Jahren ein beträchtlicher Verlust an Kaufkraft.[213] Bitcoin wird demgegenüber als deflationäres Zahlungsmittel bezeichnet, weil immer weniger neue Geldeinheiten in derselben Zeitspanne neu in Umlauf gebracht werden.

Die bereits unter Normalbedingungen zu erwartete Entwertung von zwei Pro- 264
zent ist in historischer Perspektive und im internationalen Vergleich allerdings nur marginal. *Eine Währungsreform in Form eines sogenannten Währungsschnitts kann Inflationsraten bzw. Entwertungen von über 100% jährlich zur Folge* haben.[214] Eine Absicherung gegen solche Massnahmen gibt es unter anderem wegen der Geltung des Nominalwertprinzips allerdings nicht.[215] Als Ausweichmöglichkeiten kommen Investitionen in Sachwerte, ausländischen Währungen oder Finanzprodukte in Frage. Ausländische, staatliche Währungen unterliegen aber ausnahmslos zumindest der Kontrolle der jeweiligen Nationalbank und weisen daher dasselbe Risiko auf. Sachwerte haben eine schlechtere Liquidität und Fungibilität wie Geldmittel. Bei Finanzprodukten, welche in staatlicher Währung denominiert sind, bestehen die gleichen Risiken wie bei staatlicher Währung und es kommen weitere wie beispielsweise das Gegenparteirisiko hinzu. Individuen haben also ein *berechtigtes Interesse daran haben, ihre Vorsorge bzw. ein Teil davon in Bitcoin anzulegen, welcher keinen währungspolitischen Einflüssen – wie Negativzinsen oder sogar dem Risiko einer Währungsreform – ausgesetzt ist*.

bb. Mindestgewicht der Beeinträchtigung

Die Annahmeobergrenze für Bitcoin bedeutet à priori nicht, dass die Vorteile von 265
Bitcoin hinsichtlich der persönlichen Vorsorge vollständig verloren gehen. Allerdings könnte die Verwendung von Bitcoin als Vorsorgeguthaben durch die

213 V. ADE, „Für Bankkunden drohen höhere Abgaben", in: Finanz und Wirtschaft Zeitung vom 18. Sep. 2019, 11; Siehe HERRMANN, Währungshoheit (Fn. 8), 292 ff.; J. VON SPINDLER/E. BECKER/E. STARKE, Die Deutsche Bundesbank, 4. Aufl., Stuttgart 1973, 19 f.

214 Siehe OGer ZH, Urteil vom 25.5.2012, PS120042, E. 3.2.

215 HERRMANN, Währungshoheit (Fn. 8), 335 ff.

Annahmeobergrenze derart eingeschränkt sein, dass es den Bagatellvorbehalt von Art. 10 Abs. 2 BV übersteigt.

266 Die *Annahmeobergrenze führt zu einer erheblichen Beeinträchtigung des Vorsorgecharakters von Bitcoin-Guthaben, zumal die üblichen Verwendungsmöglichkeiten im Alter schnell die Bagatellgrenze von CHF 10'000.- erreichen*. Beispielsweise könnte der Wunsch bestehen, eine für den Lebensabend geeignete Immobilie oder ein geeignetes Fahrzeug zu erwerben, was aber aufgrund des in dieser Hinsicht tiefen Freibetrags der Annahmeobergrenze ausgeschlossen ist. Darüber hinaus besteht eine grosse Wahrscheinlichkeit, dass bei Geltung einer Annahmeobergrenze auch der Umtausch von Bitcoin in eine staatliche Währung stark reguliert ist, d.h. ansonsten zugängliche Ausweichmöglichkeiten abgeschnitten oder zumindest erheblich erschwert sind, wie beispielsweise wenn zuerst der Nachweis erbracht werden muss, dass es sich unzweifelhaft um Mittel legalen Ursprungs handelt.

267 Ferner haben Eingriffe dieser Art zur Folge, dass beim Individuum ein Gefühl der *Unsicherheit entstehen kann, ob und inwiefern es Bitcoin zukünftig noch einsetzen kann*. Dadurch wird der mögliche Vorsorgecharakter von Bitcoin nachhaltig geschädigt und kann sogar eine prohibitive Wirkung auf die Verwendung als Vorsorgekapital haben.

268 Schlussendlich ist auch hier zu erwähnen, dass Massnahmen gegenüber Bitcoin, die sich negativ auf die Eignung als Zahlungsmittel auswirken, Einfluss auf den Wert bzw. die Kaufkraft haben. Weil die Tauschmittelfunktion von Bitcoin durch eine Annahmeobergrenze beeinträchtigt wird verliert Bitcoin an Wert. Dieser *Wertverlust vermindert die Attraktivität des Zahlungsmittels Bitcoin und beeinträchtigt insbesondere die Interessen von Sparern, zumal der Wert ihres Sparguthabens eng mit den zur Verfügung stehenden Einsatzmöglichkeiten im Zusammenhang steht*. Weil von einer auf die Schweiz beschränkten Annahmeobergrenze die zu erwartenden Auswirkungen auf den Wert von Bitcoin jedoch gering sind, erscheint dieser Aspekt im Vergleich zu den direkten Auswirkungen, d.h. des Verbots der Bezahlung von Gütern und Dienstleistungen ab CHF 10'000.- mit Bitcoin, von untergeordneter Bedeutung.

269 Aus der Annahmeobergrenze von CHF 10'000.- folgt eine ausreichend *starke Beeinträchtigung der Nutzung von Bitcoin als Vorsorgeguthaben als Gegenstand von besonderer praktischer Bedeutung*. Der Schutzbereich der persönlichen Freiheit ist insofern eröffnet.

b. Transparenz bei Spenden

aa. Geschützte Verhaltensweise

Besondere *praktische Bedeutung könnte Bitcoin im Zusammenhang mit Spenden und Zuwendungen haben*, zumal die fehlende Transparenz bei konventionellen Geldspenden unter anderem als Grund genannt wird, warum das Vertrauen in das Spendenwesen bzw. in Organisationen, die sich über Spenden finanzieren, nachlässt.[216] Aufgrund der Öffentlichkeit der Bitcoin-Blockchain kann der Spendengeber theoretisch seine Spende vom Verlassen seiner Wallet über die gemeinnützige Organisation bis hin zum Endempfänger rückverfolgen. Dadurch *sinkt das Risiko für Missbrauch bzw. Veruntreuung von Spenden, was gleichzeitig das Vertrauen in die Effektivität der Spende und in die jeweilige Organisation erhöht*.[217] Das Ausrichten einer Bitcoin-Spende hat also eine besondere praktische Bedeutung. 270

bb. Mindestgewicht der Beeinträchtigung

Eine Annahmeobergrenze von umgerechnet CHF 10'000.- bedeutet, dass nur betragsmässig hohe Spenden davon erfasst sind und daher nicht von der Transparenz der offenen Bitcoin-Blockchain profitieren können. Allerdings zeigen Statistiken, dass die *tatsächlich ausgerichteten Spenden pro Jahr und Haushalt mit ca. CHF 450.- nur einen Bruchteil des erlaubten Höchstbetrags ausmachen und insofern von der Annahmeobergrenze in der überwiegenden Anzahl der Fälle gar nicht betroffen sind*.[218] Ferner ist zu berücksichtigen, dass auch andere Mittel und Wege bestehen, um sich über die Effektivität einer Spende zu vergewissern. 271

Die *Annahmeobergrenze für Bitcoin erreicht unter diesem Gesichtspunkt nicht die von Art. 10 Abs. 2 BV vorausgesetzte Intensität* der Beeinträchtigung. 272

---

216 W. SHAWCROSS, „Trust in charities is at an all-time low. Time to change", in: theguardian.com vom 28. Jun. 2016, erhältlich unter: <https://www.theguardian.com/commentisfree/2016/jun/28/trust-charities-low-charitable-work-public>.

217 L. SHIN, „Want To Follow Your Donation In Real Time? Bitcoin Non-Profit BitGive Launches Donation Tracker", in: Forbes.com vom 8. Dez. 2016, erhältlich unter: <https://www.forbes.com/sites/laurashin/2016/12/08/want-to-follow-your-donation-in-real-time-bitcoin-non-profit-bitgive-launches-donation-tracker/>; Beispiel einer Bitcoin-Spenden-Plattform: Givetrack <www.givetrack.org>.

218 Bundesamt für Statistik, Haushaltsbudgeterhebung 2012-2014, erhältlich unter <https://www.bfs.admin.ch/bfsstatic/dam/assets/1400581/master>.

c. Finanzielle Exklusion

aa. Geschützte Verhaltensweise

273 Bitcoin könnte ferner eine besondere praktische Bedeutung haben für Personen und Organisationen, welche von finanzieller Exklusion betroffen sind, sowie für Personen, welche an von finanzieller Exklusion betroffene Personen, Organisationen oder Unternehmen Geldzahlungen tätigen möchten. Finanzielle Exklusion liegt vor, wenn gar keinen oder nur einen eingeschränkten Zugang zu finanziellen Dienstleistungen vorhanden ist. *Finanzielle Exklusion belangt v.a. Personen in abgelegenen geografischen Lagen aber auch solche, die vom sogenannten ‹De-Risking› der Banken und Finanzdienstleister – d.h. der Ausschaltung von möglichen Haftbarkeiten durch Abbruch von Kundenbeziehung, die ein besonderes Risiko darstellen und daher besondere, auch kostspielige Massnahmen erforderten (Art. 6 GwG) – betroffen sind*.[219]

274 Als Beispiele von finanzieller Exklusion aufgrund von De-Risking können illustrativ die Beispiele von Wikileaks und der NRA dienen. Bei beiden Beispielen handelt es sich um gemeinnützige Organisationen, die keiner gewerblichen Tätigkeit nachgehen und sich daher nicht auf die Wirtschaftsfreiheit berufen können. Wikileaks hat sich die Veröffentlichung von als geheim klassifizierten Dokumenten zur Aufgabe gemacht und wurde deshalb von diversen Zahlungsdienstleistungsanbieter boykottiert. Dies hatte zur Folge, dass Wikileaks keine Spendengelder über Kreditkarten annehmen konnte und Spendenwillige vorübergehend keine Spende an Wikileaks tätigen konnten.[220] Bitcoin-Spenden erlangten insofern für Wikileaks selbst wie auch für diejenigen Personen, welche Wikileaks unterstützen wollten, eine besondere praktische Bedeutung. Im Falle der NRA wurden die im Staat NY ansässigen Finanzdienstleister vom Gouverneur, welcher die Oberaufsicht über sie innehatte, angewiesen, ihre Geschäftsbeziehungen zur NRA zu überprüfen und ggf. abzubrechen, ohne dass irgendwelche Gesetzesverstösse festgestellt wurden. Als Begründung enthielt die Anordnung lediglich den Hinweis auf einen möglichen negativen Einfluss auf das Ansehen der Unternehmen sowie Bedenken bezüglich der öffentlichen Sicherheit bei Geschäftsbeziehungen mit der

---

219 Siehe dazu vorne Rz. 184 ff.

220 H. KLEMUSCH, Hackerwährung oder virtuelles Zahlungsmittel. Lösungsansätze für ein neues polizeiliches Problem, in: DPolBl 2013, 19-23 (21); J. BRITO/H. SHADAB/A. CASTILLO, Bitcoin Financial Regulation. Securities, Derivatives, Prediction Markets, and Gambling, in Colum. Sci. & Tech. L. Rev. 2014, 144-221 (217 f.).

NRA.[221] Die NRA machte vor Gericht geltend, dass, ohne die Möglichkeit einfach, d.h. elektronisch, Spenden zu erhalten, ihre Existenz grundlegend gefährdet sei.[222] Die Beispiele zeigen, dass für Organisationen aber auch *Personen, welche auf Einnahmen angewiesen, aber vom konventionellen elektronischen Zahlungsverkehr ausgeschlossen sind, die Möglichkeit des Erhalts von Bitcoin-Zahlungen eine besondere praktische Bedeutung hat*.[223]

bb. Mindestgewicht der Beeinträchtigung

Auf Seiten des Zahlung- bzw. Spendenempfängers stellt die Beschränkung, maximal umgerechnet CHF 10‘000.- annehmen zu dürfen, keine genügende Beeinträchtigung dar, zumal die *allermeisten Gegenstände und Dienstleistungen sowie die üblichen Spendenbeträge weit unter diese Betragsgrenze fallen* und daher von der Bitcoin-Annahmeobergrenze gar nicht betroffen sind. 275

Demgegenüber liegt auf Seiten des Zahlers eine indirekte Beschränkung der Möglichkeit vor, Zahlungen von umgerechnet über CHF 10'000.- in Bitcoin an Personen, Organisationen oder Unternehmen, welche von finanzieller Exklusion betroffen sind, vornehmen zu können. Auch hier gilt, dass die *Beeinträchtigung angesichts der hohen Bagatellgrenze als wenig intensiv ausfällt und daher das von Art. 10 Abs. 2 BV geforderte Mindestgewicht nicht erreicht*. 276

Aus dem Gesagten folgt, dass weder für Zahlungsempfänger, die von finanzieller Exklusion betroffen sind noch für die Zahler, welche an solche Empfänger Geldzahlungen ausführen möchten, *keine ausreichende Belastungsintensität im Sinne von Art. 10 Abs. 2 BV vorliegt*. 277

---

221 Büro des Gouverneur des Staates NY, Insurance Companies, Banks, and Other Financial Institutions Encouraged to Review Relationships with the NRA and Similar Organizations, 2018, erhältlich unter: <https://www.governor.ny.gov/news/governor-cuomo-directs-department-financial-services-urge-companies-weigh-reputational-risk>; J. BRITO, The Case for Electronic Cash. Why Private Peer-to-Peer Payments are Essential to an Open Society, 2019, 18 ff.

222 *National Rifle Association of America v. Cuomo et al*, N.D.N.Y 18-CV-00566-TJM-CFH, eingereicht am: 20.7.18, Rz. 128; A. FRANKEL, „NRA v. N.Y., A timely reminder that officials can’t use their power to squelch speech”, reuters.com vom 7. Aug. 2018, erhältlich unter: <https://www.reuters.com/article/us-otc-nra/in-nra-v-n-y-a-timely-reminder-that-officials-cant-use-their-power-to-squelch-speech-idUSKCN1NC2TI>.

223 Illustrativ zum Ausschluss vom konventionellen Zahlungsverkehr, P. NOBEL, Zum Fall Wegelin, in: SZW 2013, 529-535 (530 ff.).

1.3 Privatautonomie

a. Geschützte Verhaltensweise

278 Als weiterer Teilgehalt der persönlichen Freiheit im Grundtatbestand könnte die Privatautonomie betroffen sein. Die Privatautonomie ist im Hinblick auf die ungestörte, freie Persönlichkeitsentfaltung von zentraler Bedeutung. Als *Mittel zur Durchsetzung der Privatautonomie in wirtschaftlichen Belangen garantiert der Staat den Bürgern grundsätzlich das Institut des Vertrags und insofern die Vertragsfreiheit*. Die grundsätzlich freie, privatautonome Gestaltung von Rechtsbeziehungen gehört zum Grundverständnis eines liberalen Rechtstaats, welcher auf marktwirtschaftlichen Prinzipien beruht. Darüber hinaus ist die Privatautonomie für die Ausübung weiterer Grundrechte gedanklich vorausgesetzt.[224] Es rechtfertigt sich daher die Vertragsfreiheit grundsätzlich auch Konsumenten zu erstrecken, die Frage der Betroffenheit jedoch vom Bagatellvorbehalt von Art. 10 Abs. 2 BV abhängig zu machen.

279 Die Privatautonomie schützt nicht nur die Wahl der Geschäftspartner, sondern auch die freie Gestaltung des Inhalts des Vertrags, wozu folgerichtig die Wahl über die Art und Weise der Bezahlung gehört. Die *Annahmeobergrenze für Bitcoin bedeutet jedoch eine Einschränkung dieser Vertragsinhaltsfreiheit*.

b. Mindestgewicht der Beeinträchtigung

280 Es stellt sich somit die *Frage, ob das Verbot der Bezahlung mit Bitcoin von Beträgen über umgerechnet CHF 10'000.- für einzelne Rechtsgeschäfte eine genügende Intensität* der Beeinträchtigung der Privatautonomie erreicht.

281 Wegen der *Annahmeobergrenze wird nur ein kleiner Teilbereich der Gestaltungsfreiheit von Rechtsbeziehungen beschränkt und damit der Privatautonomie bzw. Vertragsfreiheit entzogen*. Einfache Beschränkungen insbesondere der Inhaltsfreiheit sind alltäglich – wie beispielsweise Barzahlungsverbote ab einer bestimmten Grenze im europäischen Ausland zeigen –[225] und erreichen nicht das vorausgesetzte Mindestgewicht für Beeinträchtigungen im Rahmen von Art. 10 Abs. 2 BV.

282

---

224 B. WOLF, Vertragsfreiheit. Das verkannte Verfassungsrecht, AJP 2002, 8-11 (7 ff.); siehe ferner M. BÄUERLE, Vertragsfreiheit und Grundgesetz. Normativität und Faktizität individueller Vertragsfreiheit in verfassungsrechtlicher Perspektive, Baden-Baden 2001, 280 ff.

225 Siehe EZB, Letter (Fn. 171); RAMELET, Geldwäschereibekämpfung (Fn. 191), 82 f.

Als vorläufiges Ergebnis lässt sich festhalten, dass die *Annahmeobergrenze für Bitcoin, aufgrund deren Auswirkungen im Hinblick auf die persönliche Vorsorge, die persönliche Freiheit betrifft*.

2. Eingriff in die persönliche Freiheit

Unmittelbare Adressaten der Annahmeobergrenze von CHF 10'000.- sind einzig die Händler im Rahmen ihrer gewerbsmässigen Tätigkeit. Obwohl Privatpersonen bzw. Konsumenten in der Bestimmung nicht erwähnt werden, sind sie dennoch durch die Annahmeobergrenze direkt betroffen. Die *Annahmeobergrenze stellt auch für die Konsumentenseite eine rechtsförmige Massnahme dar, welche zielgerichtet eine vormals bestehende Freiheit – nämlich das Bezahlen von Schulden bei Gewerbetreibenden mit Bitcoin über umgerechnet CHF 10'000.- – unmittelbar aufhebt*. 283

Für einen schweren Eingriff in die persönliche Freiheit müsste der künftig mögliche Gebrauch des Sparguthabens zumindest stark erschwert sein. Diese Voraussetzung könnte erfüllt sein, zumal die Bitcoin-Annahmeobergrenze insbesondere der Anschaffung eines alters- oder invalidengerechten Fahrzeugs oder einer Immobilie im Weg steht, und der mögliche Vorsorgecharakter mit Bitcoin wegen der Annahmeobergrenze generell zurückgedrängt ist.[226] Darüber hinaus spricht die grosse Anzahl potentiell betroffener Personen für das Vorliegen eines schweren Eingriffs. Demgegenüber spricht – wegen des hoch angesetzten Bagatellbetrags – für einen leichten Eingriff, dass keine vollständige Entwehrung einer Freiheit, sondern nur ein kleiner Teilbereich der möglichen Handlungsoptionen entzogen wird. Die Auswirkungen auf die Privatautonomie sind folglich nur gering. Aus demselben Grund ist ausserdem der Kreis tatsächlich betroffener Personen wesentlich kleiner, als dass es die Zahl der Bitcoin-Benutzer vordergründig vermuten lässt. Schlussendlich bleiben Möglichkeiten bestehen, um Bitcoin-Vorsorgeguthaben weiterhin zu gebrauchen. Es könnte beispielsweise für Ausgaben bis CHF 10'000.- verwendet werden, bei in- oder ausländischen Tauschbörsen in staatliche Währung getauscht oder sogar auf Internetbörsen eingesetzt werden. *Es liegt also keine prohibitiv-wirkende Beeinträchtigung des zukünftigen Gebrauchs von Bitcoin-Vorsorgeguthaben vor und die Beeinträchtigung hat nur wenig Bezug zur Persönlichkeitsentfaltung des Grundrechtsträgers*. Folglich besteht nur ein leichter Eingriff in die persönliche Freiheit wegen der Bitcoin-Annahmeobergrenze von umgerechnet CHF 10'000.- 284

226 Siehe zur Beeinträchtigung des Vorsorgecharakters vorne Rz. 262 ff.

3. Genügende gesetzliche Grundlage

285 Die für die Einschränkung grundrechtlich geschützter Interessen notwendige gesetzliche Grundlage entspricht der Bestimmung, welche für die Bitcoin-Annahmeobergrenze unter der Wirtschaftsfreiheit (Art. 27 BV) diskutiert wurde:

286 > Sorgfaltspflichten für Händlerinnen und Händler […]
>
> [1bis] Sie [Händlerinnen und Händler] dürfen pseudonyme virtuelle Währungen höchstens bis zu einem umgerechneten Wert von CHF 10'000.- annehmen. […]

287 Diese Bestimmung ist *ausreichend konkret, zumal die Auswirkungen der freiheitsbeschränkenden Massnahmen absehbar sind* bzw. die Folgen von Fehlverhalten mit einem den Umständen entsprechenden Grad an Gewissheit voraussehbar sind. Ferner weist die Bestimmung, als de ferenda Absatz von Art. 8 GwG, eine genügende Normstufe auf.

4. Legitimes Eingriffsinteresse

288 Die Bitcoin-Annahmeobergrenze dient der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung, Korruption sowie der Proliferation von Massenvernichtungswaffen. Ausserdem trägt sie zur Verhinderung von Steuerhinterziehung bei. Es bestehen also anerkannte, staatliche Interessen am Eingriff.

5. Verhältnismässigkeit

5.1 Eignung

289 Gegen die Bitcoin-Annahmeobergrenze für die Verhinderung von Terrorismusfinanzierung, Geldwäscherei usw. kann vorgebracht werden, dass sachkundige Täter Ausweichstrategien zu nutzen wissen und sie daher nicht geeignet ist, den öffentlichen Interessen Geltung zu verschaffen. Beispielsweise könnten Bitcoins auf ausländischen, nicht-regulierten oder dezentralen Tauschbörsen in Währungen getauscht werden, welche nicht von einer Annahmeobergrenze betroffen sind. Dagegen lässt sich einwenden, dass die *Annahmeobergrenze immerhin zu einer besseren Kontrolle der Exit-Points – wozu auch Handelsgeschäfte mit Bitcoin gehören – von Kryptogelder führen*.[227] Die Bitcoin-Annahmeobergrenze ist folglich geeignet.

---

227 Siehe zur grundsätzlich besseren Kontrolle vorne Rz. 237.

5.2 Erforderlichkeit

Als ein sachlich milderes Mittel steht zunächst eine Regelung zur Diskussion, welche bei Erreichen eines bestimmten Grenzwerts kein Annahmeverbot, sondern lediglich die Unterstellung des Händlers unter die geldwäschereirechtlichen Sorgfaltspflichten, vorsieht. Insofern wäre bei Erreichen des Grenzwerts der Erwerb für den Konsumenten nicht gänzlich ausgeschlossen, er müsste sich aber die Bearbeitung seiner persönlichen Daten gefallen lassen (Art. 13 Abs. 2 BV). Hinsichtlich der persönlichen Freiheit wäre die Alternative zwar milder, jedoch gilt, dass sie nicht die gleiche Wirksamkeit aufweist wie ein Annahmeverbot, zumal ein Restrisiko hinsichtlich der Nicht-Erkennung von Geldwäscherei- oder Terrorismusfinanzierungsrisiken besteht. 290

Auch für die *Pflicht zur Heranziehung eines Finanzintermediärs zur Überprüfung auf allfällige Geldwäscherei- und andere Risiken* gilt, dass die Wirksamkeit gegenüber einem absoluten Annahmeverbot eingeschränkt ist, zumal selbst besonders befähigten Stellen Fehler unterlaufen können sowie Händler und Fachstellen ein Interesse daran haben, Transaktionen als unbedenklich zu deklarieren.[228] Diese Alternative fällt daher ausser Betracht. 291

Denkbar wäre allenfalls eine *Beschränkung des Annahmeverbots von Bitcoin auf Personen, welche keinen Wohn- und Steuersitz in der Schweiz besitzen*. In personeller Hinsicht stellt dies ein milderes Mittel dar, weil ein grosser Kreis von Personen von der Regelung ausgenommen wäre. Personen mit ausländischem Steuersitz, auf welche die völkerrechtlichen Abkommen gerichtet sind und deren allfällige Steuerhinterziehung dem internationalen Ansehen der Schweiz besonders abträglich ist, wären aber nach wie vor erfasst. Ausserdem liesse sich argumentieren, dass Inländer bereits wegen ihrer Anwesenheit bzw. Niederlassung eher auffallen würden, falls Anzeichen für Terrorismusfinanzierung, Geldwäscherei usw. vorlägen und daher bei dieser Personengruppe das Risiko grundsätzlich tiefer ist. Diese Erleichterung ist allerdings nicht gleich wirksam wie ein generelles Bitcoin-Annahmeverbot. Es besteht insbesondere die Gefahr, dass Inländer, d.h. von der Regulierung ausgenommene Personen, vermehrt als Strohmänner bzw. „Geldesel" genutzt würden.[229] Ferner kann zumindest bezweifelt werden, dass bei im Inland niedergelassenen Personen, Anzeichen für Geldwäscherei und weitere Delikte grundsätzlich besser erkannt werden. 292

---

228 Siehe zu den gegenteiligen Interessen vorne Rz. 239.

229 Siehe dazu A. HOPF-SULC, „Wie Schweizer als «Geldesel» Kriminellen helfen", in: DerBund vom 26. Feb. 2019.

293 Im Ergebnis existiert also *gegenüber einer Bitcoin-Annahmeobergrenze von umgerechnet CHF 10'000.- kein milderes Mittel in Bezug auf die persönliche Freiheit (Art. 10 Abs. 2 BV)*, welches das Interesse an der Verhinderung von Geldwäscherei, Terrorismusfinanzierung, Steuerhinterziehung usw. gleich wirksam zu fördern vermag. Die Bitcoin-Annahmeobergrenze ist daher eine erforderliche Massnahme.

5.3 Zumutbarkeit

294 Gegen die Zumutbarkeit einer Bitcoin-Annahmeobergrenze unter der persönlichen Freiheit spricht insbesondere, dass die Regulierung nur einen lückenhaften Schutz gewährt, d.h. dass *Konsumenten unnötigerweise damit belastet werden, während die Regulierung im Hinblick auf die Verhinderung von Terrorismusfinanzierung, Geldwäscherei etc. keinen nennenswerten Nutzen stiftet*. Davon betroffen sind insbesondere Personen, welche Bitcoin – wegen der Unabhängigkeit von Zentralbanken und Banken – als Vorsorgeguthaben verwenden möchten. Die Annahmeobergrenze bedeutet für sie eine Beschränkung der zukünftigen Verwendungsmöglichkeiten und allenfalls einen Wertverlust.

295 Für die Zumutbarkeit der Annahmeobergrenze spricht demgegenüber, dass viele Bereiche, in denen Bitcoin einsetzbar ist, von der Regelung gar nicht betroffen sind. Dazu zählt insbesondere die Möglichkeit von Privatpersonen, untereinander Bitcoin austauschen zu können (Peer-to-Peer) und verbietet insbesondere nicht Überweisungen an Familie und Freunde zur Bestreitung des Lebensunterhalts. Ausserdem sind nur Vorgänge von der Bitcoin-Annahmeobergrenze erfasst, die Geschäfte mit gewerbsmässig tätigen Händlern oder Spenden mit Beträgen von umgerechnet mehr als CHF 10'000.- betreffen. Darüber hinaus können Bitcoin nach wie vor für Käufe im nicht-regulierten Ausland unbeschränkt Verwendung finden. In diesem Sinn bleiben Bitcoin-Transaktionen in der überwiegenden Anzahl der Fälle weiterhin zulässig. Ferner sind die Auswirkungen auf den Wert bzw. die Kaufkraft von Bitcoin gering. Daher bleiben die *Vorteile von Bitcoin* – beispielsweise die Möglichkeit, sichere, schnelle und kostengünstige Transaktionen ausführen zu können – *für die Konsumenten grundsätzlich bestehen*.

296 Das Verbot zum Ausrichten von *Spenden über CHF 10'000.- ist angesichts des hohen Freibetrags sowie der Ausweichmöglichkeiten – beispielsweise mittels vorgängigen Umtauschs – als wenig freiheitsbeschneidend zu qualifizieren*. Die Beeinträchtigung ist demgegenüber bei einer Spende, welche aus religiöser Pflicht vorgenommen wird, intensiver und stellt darüber hinaus eine Beeinträchtigung der Glaubens- und Gewissensfreiheit (Art. 15 BV) dar. Statistiken zeigen aber, dass – wie bereits erwähnt – das Spendenvolumen pro Jahr und Haushalt in der Schweiz mit ca. CHF 450.- bedeutend tiefer ausfällt und daher nur einen Bruchteil des

Maximalbetrags ausmacht.[230] Dieser Aspekt erscheint daher hinsichtlich der Bewertung der Beeinträchtigungen der Freiheit als nur untergeordnet.

Demgegenüber s*tärker ins Gewicht fällt die Beeinträchtigung der persönlichen Freiheit wegen den Auswirkungen auf die Verwendung von Bitcoin als Vorsorgekapital*. Der Annahmeobergrenze kommt im Hinblick auf den Erwerb von Immobilien aber auch bereits Fahrzeugen eine fast prohibitive Wirkung zu. Diese Konsequenz ist etwas gemildert angesichts von zugänglichen Ausweichmöglichkeiten, wie der Kauf oder Umtausch im nicht-regulierten Ausland. 297

Auf der anderen Seite fällt für die Zumutbarkeit der Annahmeobergrenze jedoch *sehr stark ins Gewicht, dass die erwähnten öffentlichen Interessen, d.h. die Bekämpfung von Terrorismusfinanzierung, Non-Proliferation von Massenvernichtungswaffen, Geldwäscherei* usw., auf internationaler Ebene unter besonderer Beobachtung stehen und die Nicht-Verhinderung solcher Delikte eine schwere Gefährdung der öffentlichen Sicherheit und Ordnung zur Folge hat. 298

Aus dem Gesagten folgt, dass die Bitcoin-Annahmeobergrenze den Individuen einen relativ grossen Freiheitsraum belässt, in dem die Benutzung von Bitcoin uneingeschränkt möglich ist. *Ausserdem stellt die Verhinderung von Geldwäscherei, Terrorismusfinanzierung etc. ein gewichtiges öffentliches Interesse dar, das selbst Mittel rechtfertigt, die auch nur den deliktischen Erfolg erschweren*. Die Annahmeobergrenze erweist sich daher im Verhältnis zur persönlichen Freiheit als eine angemessene Massnahme. 299

6. Kerngehalt

Eine Kerngehaltsverletzung der allgemeinen persönlichen Freiheit könnte vorliegen, falls s*pezifische Aspekte des Menschseins als solches durch die in Frage stehende Regulierung gefährdet* sind. 300

Die Bitcoin-Annahmeobergrenze beschlägt die persönliche Gestaltungsfreiheit von Rechtsbeziehungen zwischen Privatpersonen und insofern die Privatautonomie. Die Gestaltung von Beziehungen mithilfe des Rechts ist zwar dem Menschen eigens, indes *folgt aus einer Annahmeobergrenze keine Gefährdung des Menschseins als solches*. Ein Hinweis darauf liefern die gemachten Erwägungen zur Privatautonomie, welche zum Ergebnis führten, dass die Bitcoin-Annahmeobergrenze als einfache Beschränkung der Vertragsinhaltsfreiheit zu qualifizieren ist und nur geringfügig die Privatautonomie beeinträchtigt. Eine 301

230 Bundesamt für Statistik, Haushaltsbudgeterhebung 2012-2014 (Fn. 218).

Kerngehaltsverletzung der persönlichen Freiheit (Art. 10 Abs. 2 BV) aufgrund der Bitcoin-Annahmeobergrenze ist deshalb ausgeschlossen.

7. Fazit

302 Die Annahmeobergrenze ist ein geeignetes und erforderliches Mittel, um den genannten gewichtigen, öffentlichen Interessen Geltung zu verschaffen. Ausserdem greift sie nicht in unverhältnismässig stark in die persönliche Freiheit (Art. 10 Abs. 2 BV) ein. Ferner hat der Bund aufgrund von Art. 98 Abs. 2 i.V.m. Art. 95 BV die Kompetenz, eine Bitcoin-Annahmeobergrenze einzuführen. Es liegen also *keine Hindernisse vor, welche gegen die Einführung einer Bitcoin-Annahmeobergrenze sprechen*.

Kapitel 2: Annahmeobergrenze für Monero

303 Die bei Monero eingesetzten Verschleierungstechniken – d.h. die sogenannte Obfuskation der Monero-Blockchain – gewähren einen besseren Schutz der Privatsphäre der Benutzer im Vergleich zu Bitcoin. Gleichzeitig erhöhen sie aber auch die Attraktivität von Monero für die Verfolgung illegitimer Zwecke. Die Regulierung von Monero wird angesichts dieser unterschiedlichen Ausgangslage beurteilt, allerdings ohne auf die gemeinsamen Aspekte nochmals einzugehen. Die unter Bitcoin diskutierte Regulierungsvariante, d.h. eine Annahmeobergrenze von umgerechnet CHF 10'000.- in Bitcoin – wird bewusst nur hinsichtlich des unterschiedlichen Regulierungsobjekts angepasst. Vor dem Hintergrund der spezifischen Vorkehrungen zum Schutz der Privatsphäre erscheint die informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) von besonderem Interesse bei einer Regulierung von Monero (**II.**). Zunächst wird aber auch der Frage der Vereinbarkeit mit der Wirtschaftsfreiheit (Art. 27 BV) nachgegangen (**I.**). Abschliessend wird die Verfassungsmässigkeit der Monero-Annahmeobergrenze unter der persönlichen Freiheit (Art. 10 Abs. 2 BV) untersucht (**III.**).

I. Wirtschaftsfreiheit (Art. 27 BV)

1. Parallelen zur Bitcoin-Regulierung

Die Monero-Annahmeobergrenze ist zunächst gleich wie die Bitcoin Variante ein Gegenstand, auf den die Wirtschaftsfreiheit grundsätzlich anwendbar ist und *nicht unter die Ausnahme von Art. 100 Abs. 3 BV fällt*.[231] 304

Zweitens ist die Wirtschaftsfreiheit durch eine Monero-Obergrenze betroffen, weil sie die *Wahlfreiheit über die eingesetzten Mittel und Wege zur Erwerbsausübung einschränkt und daher eine Beeinträchtigung der ungehinderten Berufsausübungsfreiheit* darstellt. Ferner hat die Annahmeobergrenze Auswirkungen auf den Wert von Monero, zumal dadurch die Tauschmittelfunktion gestört wird, was negative Auswirkungen auf die Attraktivität der Verwendung von Monero durch Händler als Zahlungsmittel hat. 305

Drittens liegt aufgrund der Monero-Obergrenze ein *gültiger Eingriff* vor, da sie als hoheitliche Massnahme die Berufsausübungsfreiheit zielgerichtet, direkt und in rechtsförmiger sowie zwingender Weise vermindert. 306

Viertens kann sich die Monero-Obergrenze genauso auf eine *genügende Rechtsgrundlage* stützen wie die Bitcoin-Annahmeobergrenze, da eine de ferenda Norm im GwG vorliegt: 307

> Sorgfaltspflichten für Händlerinnen und Händler […] 308
>
> [1bis] Sie [Händlerinnen und Händler] dürfen anonyme virtuelle Währungen höchstens bis zu einem umgerechneten Wert von CHF 10'000.- annehmen. […]

Fünftens sprechen dieselben *öffentlichen Interessen* für eine Monero-Annahmeobergrenze wie für das Bitcoin-Korrelat, nämlich die Verhinderung von Geldwäscherei, Terrorismusfinanzierung, Korruption sowie Non-Proliferation. 309

Schlussendlich liegt auch hinsichtlich der Monero-Annahmeobergrenze und der Wirtschaftsfreiheit *keine Verletzung des Kerngehalts vor, zumal der Marktmechanismus zwischen Währungen davon unberührt* bleibt.[232] 310

---

231 Siehe zur Anwendbarkeit der Wirtschaftsfreiheit auf private Zahlungsmittel vorne Rz. 212 ff.

232 Siehe zum Marktmechanismus und Kerngehalt der Wirtschaftsfreiheit vorne Rz. 250 ff.

2. Besonderheiten bei der Monero-Regulierung

311 Die Vereinbarkeit einer Monero-Annahmeobergrenze von CHF 10'000.- mit der Wirtschaftsfreiheit (Art. 27 BV) unterscheidet sich von der Annahmeobergrenze für Bitcoin nur hinsichtlich eines zusätzlichen praktischen Interesses am Zahlungsmittel, mithin des Erfordernisses der Betroffenheit des Schutzbereichs sowie hinsichtlich der Prüfung der Zweck-Mittel-Relation.

2.1 Schutzbereich

312 Die Betroffenheit des Schutzbereichs der Wirtschaftsfreiheit könnte bei der Annahmeobergrenze für Monero zusätzlich auf den Umstand zurückzuführen sein, dass *ein anonymes Zahlungsmittel reguliert wird, welches zur Wahrung von Geschäftsgeheimnissen und weiteren vertrauenswürdigen Tatsachen dienlich sein kann*. Die Wahrung von Geschäftsgeheimnissen bzw. die freie Wahl der Mittel und Wege dazu, wird durch die umfassende Freiheit unternehmerischer Betätigung bzw. Berufsausübungsfreiheit garantiert.

313 Anonyme Monero Transaktionen sind unter Umständen von Interesse für Gewerbetreibende, insbesondere wenn es um den Schutz von Geschäftsgeheimnissen geht. Aufgrund von Transaktionsdaten, welche bei Benutzung von nicht anonymen Zahlungsmitteln anfallen, können sensible Informationen über genutzte Zulieferer, bezahlte Einkaufspreise, interne Strukturen, Kundenstamm usw. gewonnen werden. Dies kann zu Interessenskonflikten bei Banken sowie Korrespondenzbanken und weiteren Finanzintermediären führen, welche im Besitz solcher Informationen sind und diese zu ihren Gunsten nutzen könnten – etwa um Neukunden zu akquirieren. Insofern besteht die Gefahr, das sensible Informationen Konkurrenten wissentlich weitergereicht werden. Ausserdem besteht das Risiko, dass solche Daten Ziel eines Datendiebstahls oder von Angestellten veruntreut werden. *Gewerbetreibende haben daher, zumindest in bestimmten Situationen, ein hohes Interesse an der Geheimhaltung von Zahlungen selbst vor ihrer Hausbank und weiteren Finanzintermediären*. Das Verbot von Monero bei Erreichen des Grenzwerts von CHF 10'000.- bedeutet also eine Einschränkung der freien Wahl der sachlichen Mittel bei der Erwerbstätigkeit.

314 Ein schutzwürdiges Interesse an der Anonymität von Geldzahlungen haben ferner Investoren, welche ihre Vermögensanlage geheim halten möchten. Der *Erwerb von Finanzprodukten ist allerdings wegen des Umstands, dass solche Produkte auf stark regulierten Finanzmärkten gehandelt werden, die normalerweise börsenrechtlichen Transparenz- und weiteren Vorschriften unterstellt sind, nicht vergleichbar mit dem Kauf von Waren und Dienstleistungen* bei gewöhnlichen Gewerbetreibenden. Es besteht daher keine Notwendigkeit, die

Annahmeobergrenze auf den Erwerb von Finanzprodukten auf regulierten Märkten auszudehnen.

2.2 Verhältnismässigkeit

a. Eignung

Die Monero-Annahmeobergrenze muss hinsichtlich der Verhinderung von Geldwäscherei, Terrorismusfinanzierung, Korruption usw. ein taugliches Mittel darstellen, d.h. mit anderen Worten eine geeignete Massnahme im Sinne von Art. 36 Abs. 3 BV sein. 315

Eine Eignung der Annahmeobergrenze für Monero im Sinne der Zielkonformität liegt vor, weil dadurch zumindest die *Kontrollmöglichkeiten des Staates hinsichtlich möglicher Exit Points von Monero verbessert* werden.[233] 316

b. Erforderlichkeit

Als Alternative zum absoluten Verbot der Annahme bei Erreichen des Grenzwertes könnte die Pflicht der Händler treten, selbst Abklärungen hinsichtlich der Geldwäschereigefahr und den anderen Risiken vorzunehmen. Bei Monero kommt aber erschwerend hinzu, dass Transaktionen und Kontostände vor Drittpersonen grundsätzlich verborgen sind. Da die Transaktionshistorie nicht einsehbar ist, sind – im Vergleich zu Bitcoin – allfällige Geldwäscherei- und ähnliche Risiken mangels objektiver Anhaltspunkte kaum feststellbar. Händlern bliebe einzig die Möglichkeit, auf die Angaben ihrer Kunden und ggf. deren Ruf zu vertrauen. Daraus folgt jedoch, dass eine *Pflicht zur Selbstabklärung nicht gleich wirksam* ist wie eine Annahmeobergrenze. Die Abklärung geldwäschereimässiger Risiken würde ausserdem zu viel Zeit in Anspruch nehmen, um insbesondere Laufkunden angemessen bedienen zu können. 317

Vor demselben Hintergrund ist auch eine Massnahme zu sehen, welche etwa die *Pflicht zur Beauftragung einer Revisionsstelle* für die Überprüfung der Monero-Transaktionen sowie ggf. der internen Kontrollmechanismen vorsieht. Selbst besonders befähigte Stellen sind aufgrund der Obfuskation der Monero Blockchain nicht in der Lage, objektive Anhaltspunkte für Geldwäscherei oder Terrorismusfinanzierung aufgrund von Transaktionsdaten eruieren zu können. Darüber hinaus könnte eine solche Kontrolle aus praktischen Gründen nur nachträglich erfolgen und allenfalls schuldige oder immerhin verdächtige Personen ermitteln, jedoch nicht den eigentlichen Taterfolg abwenden. Mangels gleichwertiger 318

233 Siehe ausführlich zum Interesse an der Kontrolle von exit points vorne Rz. 237.

Wirksamkeit gegenüber einer absoluten Annahmeobergrenze fällt daher auch eine derartige Regulierung ausser Betracht.

319 Darüber hinaus kommen als mildere Mittel für die Verfolgung der öffentlichen Interessen die Beschränkung der Annahmeobergrenze auf B2B-Geschäfte, *eine branchenspezifische Geltung der Annahmeobergrenze sowie eine Bewilligungspflicht für die Annahme von Monero von mehr als umgerechnet CHF 10'000.- in Betracht*. Eine Freistellung von B2B-Geschäften würde jedoch die Wirkung der Regulierung schmälern, da Rechnungslegung- und Buchführungspflichten keinen gleichwertigen Ersatz für ein Annahmeverbot darstellen. Auch eine branchenspezifische Geltung der Annahmeobergrenze oder die Bewilligungspflicht für die Annahme von mehr als dem Bagatellbetrag können nur in vermindertem Masse die Abwesenheit von Geldwäschereirisiken, Terrorismusfinanzierungrisiken usw. gegenüber einem absoluten Verbot garantieren und sind daher nicht gleich wirksam.[234]

320 Als Zwischenfazit lässt sich festhalten, dass zur Monero-Annahmeobergrenze *kein milderes Mittel mit Rücksicht auf die Wirtschaftsfreiheit (Art. 27 BV) besteht*. Die Annahmeobergrenze für Monero von umgerechnet CHF 10'000.- ist daher ein erforderliches Mittel.

c. Zumutbarkeit

321 Die *Möglichkeit anonyme Geldzahlungen mit Monero durchzuführen, stellt gegenüber Bitcoin ein gesteigertes Risiko zum Missbrauch für Geldwäscherei, Terrorismusfinanzierung, Steuerhinterziehung usw. dar* und spricht besonders für die Zumutbarkeit der Annahmeobergrenze. Inkriminierte Geldwerte brauchen nicht die zweite Phase der Geldwäscherei (Verschleierung) zu durchlaufen, da Monero inhärenten Schutz vor einer Rückverfolgung bietet. Falls keine Kontrolle von Entry-Points zu Monero – beispielsweise an Automaten – stattfindet, könnte Bargeld, welches aus einer Straftat stammt, einfach in Monero getauscht werden (Platzierung) und wieder ausgegeben werden (Integration), ohne dass eine Verbindung herstellbar wäre. Die Problematik akzentuiert sich im Bereich von Kryptowährung-bezogenen Straftaten weiter: Moneros, welche direkt aus einer kriminellen Handlung stammen – z.B. aus Cybercrime-Delikten (Erpressungstrojaner) oder Erpressungen mit Monero als Lösegeld –, sind per se anonymisiert, d.h. sie haben die erste und zweite Phase von Geldwäscherei (Platzierung und Verschleierung) bereits absolviert und könnten in den „normalen" Wirtschaftskreislauf integriert werden. Dieselben Überlegungen gelten auch hinsichtlich der Terrorismusfinanzierung und der Proliferation von Massenvernichtungswaffen. Wegen der

234 Siehe dazu ausführlich vorne Rz. 238 ff.

Verschleierung der Herkunft der Vermögenswerte können allfällige Absichten von Terrorismusfinanzierung oder Proliferation nicht oder zumindest nur beschränkt erkannt werden. Freilich werden nicht-anonyme Geldmittel, wie beispielsweise Banküberweisungen, Finanzinstrumente sowie speziell geschaffene rechtliche Strukturen, zur Verschleierung von Geldflüssen regelmässig und auch mit Erfolg eingesetzt. Allerdings ist dafür im Unterschied zu Monero immer die Kollusion mit Dritten – beispielsweise Banken, Finanzdienstleister, Anwälte oder Treuhänder, Transportunternehmen usw. – nötig, was die Kosten nach oben treibt und vor allem auch die Chancen auf Aufdeckung aufgrund eines grösseren Kreises von involvierten Personen erhöht. Ausserdem bestehen im Unterschied zu Monero für die Rückverfolgung von Bargeld als anonymes Zahlungsmittel effektive und kostengünstige Mittel zur Rückverfolgung, wie etwa die Markierung von Scheinen oder eine Listung der Seriennummern.

322 Ferner ist zu berücksichtigen, dass Monero-Transaktionen von der Regulierung bis zum Erreichen der Bagatellgrenze nicht betroffen sind. Händler profitieren daher bei Geschäften unter dieser Schwelle – wie bei Bitcoin – von der Ausschaltung des *Rückbuchungsrisikos*, der *Zensurresistenz* sowie einer Bezahloption, welche *weltweite, kostengünstige und rasche Transaktionen* ermöglicht, die sie ihren Kunden zur Verfügung stellen können. Zusätzlich besteht bei Monero der Vorteil von anonymen, bargeldähnlichen Transaktionen; diese schützen die persönlichen Daten des Benutzers und verhindern, dass der – unbewusste – Erhalt von vorbelastetem Kryptogeld (Tainted Coins) die Ausgabe behindert oder sogar ein Verdacht der Geldwäscherei, Terrorismusfinanzierung usw. auf den Benutzer bzw. den Händler fallen könnte.[235] Da Händler von vielen unbekannten Personen Geldzahlungen im Austausch für Waren und Dienstleistungen erhalten, haben sie ein erhebliches Interesse an anonymen, d.h. nicht-rückverfolgbaren Transaktionen, die dieses Risiko nicht aufweisen. Eine Monero-Annahmeobergrenze von umgerechnet CHF 10'000.- bedeutet, dass die Vorteile von Monero bei Transaktionen mit Kunden (B2C) – wegen der Freistellung – nicht verloren gehen und spricht daher für die Zumutbarkeit der Massnahme.

323 Gegen die Zumutbarkeit der Monero-Annahmeobergrenze spricht demgegenüber, dass Händler ein hohes Interesse an anonymen und geheimen Geldzahlungen haben, insofern gewöhnliche, nicht-anonyme Zahlungen das Risiko tragen, dass Informationen bekannt werden, welche Händler gegenüber Konkurrenten sowie Zulieferern geheim halten möchten. Zu den möglichen Informationen mit Geheimhaltungsinteressen, die aufgrund von Finanzdaten weiteren Personen zugänglich werden, zählen insbesondere die Preissensibilität des Händlers bei eigenen Einkäufen sowie Informationen über den Kundenstamm. Ausserdem können

235 Siehe zur Problematik Tainted Coins vorne Rz. 71 ff.

Finanzdaten Geschäftsabläufe und damit Geschäftsgeheimnisse offenbaren, beispielsweise wie ein Unternehmen seine Liquidität sicherstellt oder wie es Währungsschwankungen ausgleicht. Bei Konzernen und anderen verbundenen Unternehmen lassen sich mithilfe von Finanzdaten auch interne Strukturen offenlegen. Solche *Geheimnisse liessen sich durch die Verwendung von Monero nicht schützen, zumal eine Annahmeobergrenze von CHF 10'000.- bedeutet, dass die allermeisten Transaktionen unter Gewerbetreibenden (B2B)* und weitere, wie beispielsweise Transaktionen zwischen Konzerngesellschaften oder zur Sicherstellung von Liquidität, darunter fielen und daher nicht von der Anonymität bzw. der Geheimhaltung von Monero profitieren können. Für Gewerbetreibende, welche in der Regel ein hohes Interesse an der Geheimhaltung von solchen Tatsachen haben, stellt die Monero-Annahmeobergrenze insofern eine schwere Beeinträchtigung der freien wirtschaftlichen Betätigung (Art. 27 BV) dar.

324 Darüber hinaus beeinträchtigt die Annahmeobergrenze die Tauschmittelfunktion und damit die Eignung als Zahlungsmittel von Monero. Zumal die Werthaltigkeit von Kryptogelder allein in der Erfüllung der geldmässigen Funktionen liegt, vermindert die Annahmeobergrenze den Wert und damit die Attraktivität bzw. Nützlichkeit von Monero für Händler.

325 Aus dem Gesagten folgt, dass Monero gegenüber Bitcoin ein vergleichsweises gesteigertes Risiko zum Missbrauch für Geldwäscherei, Erpressung, Terrorismusfinanzierung, Korruption sowie Kryptowährung-bezogene Straftaten aufweist. Demgegenüber haben *Gewerbetreibende aber auch ein grösseres Interesse an der Benutzung von Monero im Vergleich zu Bitcoin, weshalb sie bei gleich hoher Bagatellgrenze stärker vom Monero-Annahmeverbot als vom Bitcoin-Annahmeverbot ab umgerechnet CHF 10'000.- betroffen* sind.

326 Eine Gewichtung der sich widerstreitenden Argumente für und gegen die Zumutbarkeit einer Monero-Annahmeobergrenze führt zu folgendem Ergebnis: Die Beschränkung anonyme Zahlungen bzw. Monero-Zahlungen nur bis zu einem umgerechneten Betrag von CHF 10'000.- durchführen zu können, kommt für Gewerbetreibende einem Technologieverbot gleich, zumal B2B-Transaktionen in aller Regel die Bagatellgrenze überschreiten und daher nicht erlaubt sind. Ein Technologieverbot könnte m.E. immerhin dort gerechtfertigt sein, wo sehr bedeutende Schutzgüter zur Disposition stehen und das Verbot bzw. die Regulierung einen nahezu absoluten Schutz vor Beeinträchtigungen gewährt. Wie bereits erläutert, ist der Schutz von gewichtigen öffentlichen Interessen zumindest im Fall der Verhinderung von Terrorismusfinanzierung sowie Proliferation mit der Annahmeobergrenze beabsichtigt. Die Monero-Annahmeobergrenze deckt allerdings nur einen Teilbereich der möglichen Handlungen, welche zur Terrorismusfinanzierung dienlich sind, ab und bietet daher höchstens einen partiellen Schutz. *Die*

Vorteile der Annahmeobergrenze in Bezug auf die Wahrung der öffentlichen Interessen vermögen daher die aus dem Technologieverbot resultierenden Beeinträchtigungen nicht aufzuwiegen.

3. Fazit

Die für Gewerbetreibende wegen der Monero-Annahmeobergrenze resultierenden Beeinträchtigungen kommen einem *Technologieverbot gleich, das in Anbetracht der eingeschränkten Wirksamkeit der Annahmeobergrenze nicht gerechtfertigt ist. Im Ergebnis stellt die Monero-Annahmeobergrenze folglich eine Verletzung der Wirtschaftsfreiheit (Art. 27 BV) dar*. 327

II. Informationelle Selbstbestimmung (Art. 13 Abs. 2 BV)

Die informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV könnte von der Annahmeobergrenze für Monero betroffen sein, da eine zuvor bestehende rechtliche Freiheit, nämlich anonym – d.h. mit Monero – mehr als CHF 10'000.- zu bezahlen, aufgehoben wird. 328

1. Schutzbereich

Der Anspruch auf informationelle Selbstbestimmung kommt sämtlichen natürlichen Personen wie auch den juristischen Personen sowie den Personenvereinigungen zu. 329

Der *sachliche Schutzbereich* der informationellen Selbstbestimmung (Art. 13 Abs. 2 BV) bezieht sich auf sämtliche Nutzungshandlungen mit personenbezogenen Daten. Als personenbezogene Daten gelten grundsätzlich alle Informationen mit bestimmbarem Bezug zu einzelnen Personen bzw. Personenvereinigungen. 330

Im Bereich der *Finanzdaten* hat das Bundesgericht noch unter der alten BV und hinsichtlich der persönlichen Freiheit – mangels einer Art. 13 Abs. 2 BV entsprechenden Bestimmung – entschieden, dass blosse finanzielle Angaben nicht den gleichen Schutz wie spezifisch persönlichkeitsbezogene Daten geniessen.[236] Unter Geltung der neuen BV urteilte das Bundesgericht aber, dass immerhin Informationen über die «wirtschaftlichen Verhältnisse» einer Person zu deren 331

236 BGE 124 I 176 – Steuerdaten Minelli, nicht-publizierte Erwägung 4e., abgedruckt in: plädoyer 1999, 79-80 (79).

Privatsphäre gemäss Art. 13 BV zu zählen sind.[237] Darüber hinaus anerkannte das Bundesgericht im Google Street View Entscheid die Möglichkeit der elektronischen Datenverarbeitung zur Gewinnung von besonders schützenswerten Persönlichkeitsprofilen aus an sich harmlosen Informationen, welche lediglich dem Öffentlichkeitsprinzip zuzuordnen wären.[238]

332 Das Grundrecht der informationellen Selbstbestimmung ist ein Vorfeldrecht, d.h. es schützt die Interessen, Rechte und Belange von Individuen bereits im Vorfeld materieller Schädigungen oder konkreter Gefahren.[239] Der Schutz der informationellen Selbstbestimmung bezieht sich insbesondere auf Informationen bzw. Daten, welche aufgrund ihrer Nähe zur Persönlichkeit ein besonderes Gefahrenpotential aufweisen und auch bereits von Gesetzes wegen als besonders schützenswerte Daten gelten (Art. 3 lit. c DSG) (**1.1**). Als weiteres, verfassungsmässiges Geheimhaltungsinteresse kommt zudem der Quellenschutz in Betracht (**1.2**). Schlussendlich könnte die informationelle Selbstbestimmung auch in übrigen Situationen, d.h. bei denen keine besonders schützenswerten Daten bearbeitet werden, betroffen sein, zumal von einer Auswertung von Finanzdaten mit modernen Datenverarbeitungsmethoden, die Gefahr einer umfassenden Registrierung sowie Katalogisierung von Personen ausgeht und insofern zu chilling effects bei den Grundrechtsträgern führen könnte (**1.3**).

1.1 Situation mit besonders schützenswerten Daten (Art. 3 lit. c DSG)

a. Medizinische Behandlungen und Untersuchungen

333 Als besonders schützenswerte Daten gelten unter anderem Datensätze, welche über den Gesundheitszustand einer Person Informationen enthalten (Art. 3 lit. c DSG). Der *Begriff Gesundheitsdaten ist weit auszulegen und erfasst nicht nur die Ergebnisse einer Untersuchung, sondern bereits den Umstand, dass sich jemand einer nicht routinemässigen Untersuchung unterzogen hat.* Dies gilt für medizinisch indizierte Eingriffe bzw. Untersuchungen, aber auch für Eingriffe, die lediglich kosmetische Zwecke verfolgen.

334 Obwohl die vorgenommenen Behandlungen bzw. Untersuchungen nicht direkt aus den Transaktionsdaten lesbar sind, können aufgrund des Betrages sowie des Empfängers *zumindest gewisse Rückschlüsse hinsichtlich des Gesundheitszustands sowie weiteren Eigenschaften* einer Person gezogen werden. Der Schutz

237 BGE 137 II 431, 437 E. 2.1.2 – *UBS-FINMA*.

238 BGE 138 II 346, 359 E. 8.2 – *Google Street View*.

239 H.P. BULL, Zweifelsfragen um die informationelle Selbstbestimmung. Datenschutz als Datenaskese?, in: NJW 2006, 1617-1624 (1623).

personenbezogener Daten ist aber auch auf Informationen zu erstrecken, die nicht als sicher, sondern nur als wahrscheinlich angenommen werden und selbst auf solche, welche sich als falsch erweisen.[240] Daraus folgt, dass ein legitimes subjektives Interesse an Anonymität am Bezahlvorgang an sich besteht, mit dem der Konsum von Leistungen im Gesundheitsbereich abgegolten wird.

Die *Freigrenze von CHF 10'000.- bedeutet für Transaktionen im Bereich der medizinischen Behandlungen und Untersuchungen, dass diese rasch ausgeschöpft ist* und dementsprechend Transaktionen nicht mit Monero vorgenommen werden können. 335

Der Möglichkeit, anonym für medizinisch Behandlungen zu bezahlen, kann im Einzelfall – und für bestimmte Personengruppen – jedoch eine zentrale Bedeutung zukommen. Zu denken ist dabei vorwiegend an *Einzelunternehmer oder wichtige Teilhaber einer Unternehmung, von deren Gesundheit das Schicksal des Geschäfts abhängt.* Diese könnten ein Interesse daran haben, dass Informationen über vorgenommene Untersuchungen auf schwere Krankheiten geheim bleiben, weil bereits der Verdacht auf einen positiven Befund geschäftsschädigend sein kann. Beispielsweise könnte der Wert bzw. Aktienkurs betroffen sein oder Konkurrenten könnten dieses Wissen im Rahmen von Auftragsvergaben zu ihren Gunsten verwenden. 336

b. Ausrichten von Spenden und Mitgliederbeiträgen

Daten über ausgerichtete *Spenden und Mitgliederbeiträge* stellen geradezu besonders schützenswerte Daten (Art. 3 lit. c DSG) dar, wenn sie an eine Organisation oder an einen Verein mit politischer, weltanschaulicher, religiöser usw. Zielsetzung gehen. Weil die Empfänger von Spenden oder Mitgliederbeiträgen meist in der Öffentlichkeit auftreten, sind ihre Zielsetzungen in der Regel auch publik. Dies gilt jedoch nicht für das einzelne Mitglied oder den Spender. Allerdings darf regelmässig die Annahme zutreffen, dass der Spendengeber mehr oder weniger dieselben Ansichten vertritt, wie die Organisation bzw. Verein, an die die Spende geht. Wie bereits erwähnt, bezieht sich der Schutz der informationellen Selbstbestimmung auch auf persönliche Informationen, die falsch sind oder lediglich mit 337

240 R. MATHYS, Was bedeutet Big Data für die Qualifikation als besonders schützenswerte Personendaten? Das Beispiel der Gesundheitsdaten, in: jusletter.ch vom 21. Mai 2015, Rz. 14 ff.; G. BLECHTA, Art. 3 DSG, in: U. Maurer/G. Blechta (Hrsg.), Datenschutzgesetz, Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014, Rz. 34.

einer gewissen Wahrscheinlichkeit zutreffen. Finanzdaten über getätigte Spenden sind daher als besonders schützenswerte Daten zu qualifizieren.

338 Wie bereits erläutert, sind die durchschnittlich getätigten Spendenbeträge weit unterhalb der festgesetzten Bagatellgrenze angesiedelt. Eine Annahmeobergrenze von umgerechnet CHF 10‘000.- würde daher ausschliesslich im seltenen Fall von hohen Spendenbeiträgen an Vereinigungen mit politischen, religiösen und weltanschaulichen Motiven oder Ansichten relevant werden.

c. Daten über den Kauf von Zeitschriften und anderen Medien

339 Sodann gelten die gleichen Überlegungen für Transaktionsdaten, welche den Konsum von bestimmten Zeitschriften oder anderen Medien ausweisen. Aus der Bezahlung eines Zeitschriftenabonnements kann – analog den Finanzdaten über Spenden – geschlossen werden, dass der Überweiser in etwa dieselben Ansichten wie der Autor bzw. die Redaktion besitzt. Auch in dieser Hinsicht geben Finanzdaten Hinweise auf politische, weltanschauliche, religiöse usw. Ansichten und müssen daher als besonders schützenswerte Daten qualifiziert werden.

340 Die betragsmässig hoch angesetzt Grenze von CHF 10‘000.- bedeutet jedoch, dass kaum je ein Sachverhalt unter diesen Gesichtspunkt fällt. Da Transaktionen für den Bezug einzelner Dokumente und auch Abonnements die Grenze nicht erreichen, darf Monero als anonymes Zahlungsmittel eingesetzt werden und der Schutzbereich der informationellen Selbstbestimmung ist insofern nicht betroffen.

1.2 Quellenschutz

341 Als weiteres Geheimhaltungsinteresse kommt der Quellenschutz im Rahmen von journalistischer Tätigkeit in Betracht. Dabei besteht in der Regel ein hohes Interesse an Anonymität auf Seiten der Quelle oder des Whistleblowers. Das Redaktionsgeheimnis im Sinne von A*rt. 17 Abs. 3 BV schützt unter anderem. davor, die Identität von Quellen offenbaren zu müssen*, und ist unter diesem Aspekt eng verwandt mit dem Recht auf informationelle Selbstbestimmung. Die Erwähnung in Art. 17 BV zeugt davon, dass der Quellenschutz einen verfassungsmässigen Anspruch darstellt.

342 Die Annahmeobergrenze könnte zu einer erzwungenen Deanonymisierung der Quelle führen, falls diese wegen Überschreiten der Bagatellgrenze sowie wegen der gewerbsmässigen Tätigkeit nicht die Entschädigung in Monero erhalten kann. Aus der Höhe der Bagatellgrenze folgt jedoch, dass die *Annahmeobergrenze nicht einmal im Fall von komplexen und kostspieligen Recherchen oder verdeckten Ermittlungen* berührt ist. Ausserdem bestehen Ausweichmöglichkeiten, wie die

Konvertierung in gewöhnliche Währung – beispielsweise bei Internettauschbörsen – oder die Nutzung von Prepaid-Karten usw.

1.3 Chilling Effects

Die Datenverarbeitungen der Finanzintermediäre im Bereich der Finanzdaten könnten ferner chilling effects bei den Grundrechtsträgern aufgrund von unkontrollierten Persönlichkeitsprofilen hervorrufen. Dies ist auf den Umstand zurückzuführen, dass Geldtransaktionen ein Abbild der individuellen Handlungen sowie Unterlassungen darstellen.[241] Wie es die dissenting opinion von J. Douglas in *California Bankers Association v. Schultz* prägnant zum Ausdruck bringt, kann aus einem solchen Abbild ohne grossen Aufwand auf persönliche Neigungen und Ansichten geschlossen werden: 343

> «The records of checks -- now available to the investigators -- are highly useful. *In a sense a person is defined by the checks he writes*. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum.»[242] 344

Aus einer fortwährenden Aufzeichnung von Transaktionsdaten kann sogar ein Persönlichkeitsprofil erstellt werden. *Finanzdaten sind zur Erstellung von Persönlichkeitsprofilen besonders geeignet*, da sie hauptsächlich Angaben beinhalten, welche über einen längeren Zeitraum anfallen (sogenanntes Längsprofil).[243] Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlaubt (Art. 3 lit. d DSG), d.h. Auskunft über Gesundheitsmuster, Kaufverhalten etc. gibt oder die zur Erstellung von Kundenprofilen genutzt werden kann.[244] Die Bearbeitung von Persönlichkeitsprofilen ist jedoch besonders schutzwürdig, weil davon die Gefahr ausgeht, dass sich Individuen in der Gesellschaft nicht mehr so verhalten, wie sie es persönlich für richtig halten (chilling effects). 345

Indes stellt sich die Frage, ob eine Annahmeobergrenze für Monero für allfällige chilling effects ursächlich ist. *Chilling effects sind dort keine notwendige* 346

---

241 K. HUMMLER, Das Schweizerische Bankgeheimnis. Eine Grundrechtsfrage, in: K. Hummler/G. Schwarz (Hrsg.), Das Recht auf sich selbst. Bedrohte Privatsphäre im Spannungsfeld zwischen Sicherheit und Freiheit, Zürich 2003, 175-188 (187).

242 California Bankers Association v. Schultz, Dissenting Opinion J. Douglas, 416 U.S. 21, 1974 (Hervorhebung nicht im Originaltext).

243 Urteil der Eidgenössischen Datenschutzkommission vom 27. Jan. 2000, VPB 65.48, E. 2.b.; BLECHTA, Art. 3 DSG (Fn. 240), Rz. 68.

244 BLECHTA, Art. 3 DSG (Fn. 240), Rz. 62.

Folge, wo dem Grundrechtsträger zur Vermeidung von Datenerhebungen, welche zur Erstellung von Persönlichkeitsprofilen genutzt werden können, Ausweichmöglichkeiten zur Verfügung stehen oder wo die Erstellung von Persönlichkeitsprofilen aufgrund anderer Faktoren eingeschränkt ist.

347 Zunächst ist hervorzuheben, dass Finanzintermediäre keine gemeinsame Datenbank führen, sondern, dass jeder Finanzintermediär eigens für die Überwachung und Protokollierung der Transaktionen sorgt. Die *Erstellung eines umfassenden Bildes einer Person bzw. eines Persönlichkeitsprofils kann daher bereits durch die Verwendung mehrerer Bankkonten, Kreditkarten usw., welche von unterschiedlichen Finanzintermediären verwaltet werden, verhindert werden*. Durch die Verwendung ausländischer Bankkonten und Zahlungsmittel kann die Erstellung von Persönlichkeitsprofilen sogar noch weiter erschwert werden. Der Staat und auch Dritte müssten daher die unterschiedlichen Datenbanken zunächst zusammenführen, was allerdings in der Schweiz aufgrund des Bankgeheimnisses nicht ohne weiteres möglich ist. Sodann steht die Möglichkeit offen, Bargeld vom Konto abzuheben und dieses – bis zum geltenden Höchstbetrag für Barzahlungsgeschäfte (CHF 100'000.-) – für die anonyme Bezahlung von Schulden zu verwenden (siehe Art. 8*a* GwG). Bargeld stellt nur dort keine taugliche, anonyme Bezahlform dar, wo der Empfänger weit entfernt ist und die Übertragung bzw. Übergabe auf postalischem Weg erfolgen müsste.

348 Darüber hinaus brauchen die Ausweichmöglichkeiten zur Vermeidung von chilling-effects gar nicht genutzt zu werden, zumal wegen relativ hohen Bagatellgrenze von CHF 10'000.- die Bezahlung der allermeisten Gegenstände mit Monero nicht verunmöglicht wird. Ferner ist zu berücksichtigen, dass, zumal die Vorteile von Monero für Privatpersonen auch unter der Annahmeobergrenze grösstenteils bestehen bleiben, sie nicht zu einer massgeblichen Entwertung von Monero führt. Daher ist Monero als Instrument zur Durchsetzung der informationellen Selbstbestimmung im finanziellen Bereich in dieser Hinsicht nicht massgeblich beeinträchtigt.

349 Aus dem Gesagten folgt, dass eine Monero-Annahmeobergrenze nicht zu chilling-effects auf die Benutzung von Monero führt. Als Zwischenfazit zum Schutzbereich der informationellen Selbstbestimmung lässt sich also festhalten, dass das Monero-Annahmeverbot als Beschränkung der informationellen Selbstbestimmung aufzufassen ist, welche den Grundrechtsträgern ein a priori wirkendes Verfügungsrecht über die eigenen persönlichen Daten einräumt. Der Schutzbereich der informationellen Selbstbestimmung ist folglich betroffen.

2. Eingriff

Ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) liegt vor, zumal aus der gesetzlichen Annahmeobergrenze auch die *unmittelbare Beschränkung der Konsumenten* und anderen Grundrechtsträgern einhergeht, Monero-Zahlungen bzw. anonyme Geldzahlungen von umgerechnet über CHF 10'000.- an Gewerbetreibende auszuführen. 350

Wie weiter oben bereits erläutert, verhindert die Annahmeobergrenze für Monero anonyme Zahlungsvorgänge, an denen ein grundrechtlich geschütztes Interesse an der Geheimhaltung der Informationen aufgrund ihres engen Bezugs zur Persönlichkeit bestehen.[245] Die zukünftigen Implikationen für die Grundrechtsträger können daher schwerwiegend und – angesichts der unbegrenzt möglichen Dauer der Speicherung – dauerhaft sein. Ausserdem drohen insbesondere im Bereich der Gesundheitsdaten ernsthafte Nachteile für das Individuum. Demgegenüber ist allerdings festzuhalten, dass die Auswirkungen auf die informationelle Selbstbestimmung keinesfalls eine zwingende Konsequenz der Monero-Annahmeobergrenze darstellen, zumal taugliche Ausweichmöglichkeiten, wie beispielsweise Bargeldzahlungen, die Verwendung mehrerer Bankkonten sowie Kreditkarten etc., bestehen. Aufgrund des relativ hohen Bagatellbetrags von CHF 10'000.- fallen ferner nur wenige bis gar keine Transaktionen, welche eine einzelne Privatperson tätigt, unter das Annahmeverbot. Daher sind auch absolut betrachtet, nur eine kleine Zahl Personen davon betroffen. Es *liegt daher ein bloss leichter Eingriff in die informationelle Selbstbestimmung* (Art. 13 Abs. 2 BV) vor. 351

3. Genügende gesetzliche Grundlage

Als gesetzliche Grundlage kommt eine *de lege ferenda Bestimmung im GwG* in Betracht: 352

> Sorgfaltspflichten für Händlerinnen und Händler […] 353
>
> [1bis] Sie [Händlerinnen und Händler] dürfen anonyme virtuelle Währungen höchstens bis zu einem umgerechneten Wert von CHF 10'000.- annehmen. […]

4. Öffentliches Interesse

Die Monero-Annahmeobergrenze dient der Verhinderung von Geldwäscherei, Terrorismusfinanzierung, Korruption, Steuerhinterziehung sowie Proliferation 354

245 Siehe dazu vorne Rz. 333 ff.

von Massenvernichtungswaffen und damit dem unmittelbaren Schutz der öffentlichen Sicherheit und Ordnung als Polizeigüter.

5. Verhältnismässigkeit

5.1 Eignung

355 Eine Annahmeobergrenze stellt hinsichtlich der genannten öffentlichen Interessen *eine geeignete Massnahme dar*, da sie für deren Verwirklichung förderlich ist bzw. nicht erschwerend wirkt sowie nicht völlig wirkungslos ist.

5.2 Erforderlichkeit

356 Als milderes Mittel zum Annahmeverbot wurde weiter oben die Pflicht zur *Selbst-Vornahme der GwG-Sorgfaltspflichten für Händler* diskutiert.[246] Es stellt sich zunächst die Frage, ob diese Alternative unter der informationellen Selbstbestimmung überhaupt ein milderes Mittel darstellt. Dies ist zu verneinen, da bei einem Annahmeverbot von anonymen Geldzahlungen bzw. Monero gar keine Datenbearbeitung stattfindet, während bei der Pflicht zur Selbst-Vornahme der Sorgfaltspflichten es zu einer Datenbearbeitung durch den Händler sowie allfällig von ihm hinzugezogenen Hilfspersonen kommt.

357 Ein milderes Mittel stellt ferner die Ausnahme bestimmter Branchen oder einzelner Transaktionen von der Pflicht zur Beachtung der Annahmeobergrenze dar, bei denen regelmässig besonders schützenswerte Daten wie weiter oben beschrieben verarbeitet werden. In diesem Sinne könnten beispielsweise Geldzahlungen an medizinische Einrichtungen bzw. Behandlungen vom Monero-Annahmeverbot ausgenommen werden. Eine auch nur *branchenspezifische Ausnahme* eröffnet aber die Möglichkeit zum Missbrauch. Folglich ist diese Alternative nicht gleich wirksam wie ein vollständiges Verbot.

358 Hinsichtlich der informationellen Selbstbestimmung sind also *keine anderweitigen Mittel ersichtlich*, welche gleichermassen wie die Annahmeobergrenze den öffentlichen Interessen zum Durchbruch verhelfen, und die aber weniger stark als eine Annahmeobergrenze in grundrechtlich geschützte Gehalte eingreifen.

5.3 Zumutbarkeit

359 Die *Zumutbarkeit der Annahmeobergrenze* für Monero beurteilt sich anhand einer Abwägung zwischen dem Gewicht der Beeinträchtigung der informationellen

246 Siehe dazu vorne Rz. 317.

Selbstbestimmung auf der einen Seite sowie der durch die Annahmeobergrenze gewonnen Vorteile für die Verwirklichung der öffentlichen Interessen auf der anderen Seite.

Zunächst sind diejenigen Aspekte der Annahmeobergrenze für Bitcoin zu nennen, welche unverändert auch für die Monero Annahmeobergrenze übernommen werden können. Demnach spricht der *hohe Stellenwert, welche der Bekämpfung von Gelwäscherei, Terrorismusfinanzierung usw.* auf nationaler und internationaler Ebene zukommt, für die Zumutbarkeit der Annahmeobergrenze.[247] 360

Darüber hinaus folgt aus der *relativ hoch angesetzten Bagatellgrenze von CHF 10'000.- und dem damit verbundenen, gewährten Freiraum, dass das Gewicht der Beeinträchtigung eher gering zu qualifizieren* ist und die Massnahme zumutbarer erscheint. Aufgrund des verbleibenden Freiraums sind anonyme Monero Transaktionen in der Mehrheit der Fälle weiterhin möglich und die Individuen profitieren vom besseren Schutz der Privatsphäre bei Monero-Transaktionen sowie von den Vorteilen, welche Kryptogeld bzw. Bitcoin bieten – d.h. von einem schnellen, kostengünstigen, zensurresistenten sowie diskriminierungsfreien bzw. von persönlichen Eigenschaften unabhängigen, elektronischen Zahlungsmittel. 361

Im Unterschied zu Bitcoin folgt aus den bei *Monero eingesetzten Verschleierungstechniken zur Wahrung der Anonymität der Benutzer, dass das Risiko des Missbrauchs für illegale Zwecke substantiell grösser* ist und eine dagegen gerichtete Massnahme daher umso angezeigter ist. Falls aktuell noch für Terrorismusfinanzierung Bitcoin Monero vorgezogen wird, ist dies auf die im Vergleich zu Monero breitere Akzeptanz von Bitcoin, auf mangelndes Fachwissen oder aber einfach Gleichgültigkeit hinsichtlich der Entdeckung zurückzuführen.[248] 362

Sodann stellt sich die Frage, welches Gewicht den Beeinträchtigungen der informationellen Selbstbestimmung zukommt, die spezifisch aufgrund der Annahmeobergrenze für Monero als anonymes Zahlungsmittel drohen. Die *Frage nach dem Gewicht des Verbots einer anonymen elektronischen Geldtransaktion* im Allgemeinen ist schwierig zu beantworten, als dass die unter dem Schutzbereich diskutierten Situationen im Einzelfall Daten mit unterschiedlicher Schutzwürdigkeit beinhalten können – beispielsweise sind nicht alle Gesundheitsdaten gleich persönlichkeitsnah. Ausserdem sind die Risiken, welche sich aufgrund der Nutzung 363

247 Siehe zu den gewichtigen öffentlichen Interessen vorne Rz. 298.

248 N. POPPER, „Terrorists turn to Bitcoin to raise funds discreetly", in: NewYork Times International Edition vom 22. Aug. 2019, 1; Siehe Z. GOLDMANN/E. MARUYAMA/E. ROSENBERG/E. SARAVALLE/J. SOLOMON-STRAUSS, Terrorist use of Virtual Currencies. Containing the Potential Threat, 2017, 10 ff.

von Finanzdaten ergeben können, zahlreich und unterschiedlich, so dass eine Feststellung aller zukünftigen Implikationen für die Lebensgestaltung der Individuen nicht möglich ist.[249] Die folgenden Absätze sind daher nur eine Illustration der Schwere der möglichen Auswirkungen, welche durch die Verarbeitung von Transaktionsdaten entstehen können.

364 Das Spektrum möglicher Konsequenzen der Bearbeitung besonders schützenswerter Daten sowie ihren Auswirkungen auf den Lebensalltag der Betroffenen zeigt sich zunächst beispielhaft *im Fall von Gesundheitsdaten*. Für Konsumenten besteht die Gefahr hauptsächlich darin, dass ihnen aufgrund von solchen Daten schlechtere Konditionen beim Abschluss von einer Krankenversicherung drohen, den Ausschluss von einzelnen Leistungen oder sogar die Ablehnung bestimmter Versicherungslösungen als Ganzes riskieren. Personen, welche gleichzeitig Einzelunternehmer oder wichtige Teilhaber sind, könnten aufgrund ihrer Gesundheitsdaten zusätzlich auch geschäftlich geschädigt werden. Dabei können schwere finanzielle Verluste drohen, welche von Überschuldung bis hin zur Liquidation des Unternehmens führen könnten.

365 Schlussendlich sind im Bereich von *Spendenbeiträgen*, Folgen für die Grundrechtsträger nicht auszuschliessen, zumal mithilfe von Transaktionsdaten auf persönliche Ansichten oder Tätigkeiten im Sinne von Art. 3 lit. c Ziff. 1 DSG schliessen lässt. Die Bearbeitung von Transaktionsdaten über die Vornahme solcher Zahlungen ist also gleichzeitig eine Bearbeitung von besonders schützenswerten Personendaten. Deren unrechtmässige Bearbeitung kann schwere Grundrechtsbeeinträchtigungen hervorrufen, etwa im Falle der Bekanntgabe an eigentliche „Unrechtsregime". Konsequenzen, wie z.B. die Verweigerung der Erteilung von Visa, fortwährende Überwachung, etc., könnten auch drohen, wenn Spenden an Vereine oder Organisationen ausgerichtet werden, welche im In- oder Ausland als Gefahr für die öffentliche Sicherheit betrachtet werden.

366 Die genannten Beispiele machen deutlich, dass nicht-anonyme Geldtransaktionen im Widerspruch zur informationellen Selbstbestimmung stehen, zumal sie die Gewinnung höchstpersönlicher Daten und sogar von Persönlichkeitsprofilen zulassen, welche zum Nachteil der betroffenen Personen eingesetzt werden können. Das Gewicht der Beeinträchtigung ist jedoch deutlich reduziert angesichts des Umstands, dass der Bagatellvorbehalt von CHF 10'000.- die allermeisten Gegenstände und Dienstleistungen erfasst und diese daher anonym bezahlt werden können, d.h. kein Risiko besteht, dass Transaktionsinformationen anfallen, aus

---

249 Siehe zur Schwierigkeit zukünftige Auswirkungen von gegenwärtigen Verletzungen der informationellen Selbstbestimmung zu bestimmen BULL, Zweifelsfragen (Fn. 239), 1623.

denen höchstpersönliche Daten oder sogar Persönlichkeitsprofile gewonnen werden können.

Demgegenüber spricht für die Zumutbarkeit das besonders hohe Gewicht des 367
Interesses am Schutz von Gemeinwohlbelangen, welche insbesondere durch Terrorakte und organisierter Kriminalität ernsthaft gefährdet sind. In diesem Sinne kommt der Verhinderung von Terrorismusfinanzierung, Geldwäscherei, Verhinderung der Proliferation von Massenvernichtungswaffen sowie der Korruptionsbekämpfung ein ausserordentlich hohes Gewicht zu. Im Endeffekt übersteigen daher die öffentlichen Interessen die privaten Interessen.

Daraus folgt, dass eine Annahmeobergrenze für Monero von umgerechnet 368
CHF 10'000.- zur Verhinderung von Terrorismusfinanzierung, Geldwäscherei, Steuerhinterziehung usw. zumutbar ist.

6. Wahrung des Kerngehalts

Der Kerngehalts der informationellen Selbstbestimmung könnte in Fällen betrof- 369
fen sein, wo eine staatliche Massnahme ohne jegliche Rechtfertigung auf die Ausforschung des gesamten Bereichs persönlichkeitsrelevanter Informationen gerichtet ist oder die Erstellung von Persönlichkeitsprofile beabsichtigt ist, die die Vorhersage von individuellen Handlungen und Unterlassungen, d.h. von Verhaltensmustern, im höchstpersönlichen Bereich machen.

Ein Betroffensein des Kerngehalts der informationellen Selbstbestimmung 370
kommt vorliegend nicht in Betracht, da die Annahmeobergrenze weder auf die Ausforschung von persönlichkeitsrelevanten Informationen gerichtet ist noch Persönlichkeitsprofile über Verhaltensmuster im höchstpersönlichen Bereich zulässt.

7. Fazit

Als Fazit lässt sich festhalten, dass eine Annahmeobergrenze von umgerechnet 371
CHF 10'000.- für Monero bzw. anonyme Geldtransaktionen keine Verletzung der informationellen Selbstbestimmung (Art. 13 Abs. 2 BV) bedeutet.

III. Persönliche Freiheit (Art. 10 Abs. 2 BV)

1. Parallelen zur Bitcoin-Regulierung

1.1 Schutzbereich

372 Der Schutzbereich der persönlichen Freiheit – als subsidiäres Auffanggrundrecht – könnte von der Monero-Annahmeobergrenze dort betroffen sein, wo keine besonderen Anonymitätsansprüche der Benutzer bzw. Konsumenten bestehen.

373 Die Beeinträchtigung der persönlichen Freiheit unter der Monero-Annahmeobergrenze lassen sich in dieselben Fallgruppen wie unter Bitcoin-Variante einteilen. In diesem Sinne kann die Benutzung von Monero zunächst als Konsum eines identitätsstiftenden Produkts und damit als Grundentscheidung für den eigenen Lebensplan aufgefasst werden. Des Weiteren ist Monero von besonderer praktischer Bedeutung hinsichtlich der persönlichen Vorsorge, der Ausrichtung von Spenden – zumal Monero bei Bedarf de-anonymisiert werden kann – sowie hinsichtlich finanzieller Exklusion.[250] Nicht zuletzt ist auch die Privatautonomie bzw. die Vertragsfreiheit der Konsumenten an sich durch die Annahmeobergrenze betroffen. Allerdings führt der Bagatellvorbehalt von Art. 10 Abs. 2 BV auch hier zum Ergebnis, dass nur im Fall der persönlichen Vorsorge der Schutzbereich der persönlichen Freiheit eröffnet ist, weil in dieser Beziehung ein Betrag von CHF 10'000.- relativ bald ausgeschöpft ist.

374 Die Annahmeobergrenze hat ferner negative Auswirkungen auf den Wert von Monero. Wie bereits erwähnt, ist der Wertverlust aufgrund einer national geltenden Annahmeobergrenze jedoch nur sehr gering.[251] Ein bloss minimaler Wertverlust vermag die Bagatellgrenze von Art. 10 Abs. 2 BV nicht zu durchbrechen.

1.2 Eingriff

375 Es liegt ein Eingriff in die persönliche Freiheit vor, zumal die Annahmeobergrenze die Möglichkeiten der Verwendung von Monero-Sparguthaben zielgerichtet und bewusst verkürzt. Dieser Eingriff ist angesichts des hohen Bagatellbetrags und der Möglichkeit des Umtauschs im In- und Ausland als nur geringfügig zu qualifizieren.

---

250 Vgl. dazu die Fälle besonderer praktischer Bedeutung von Bitcoin vorne Rz. 257 ff.

251 Siehe zum Wertverlust Rz. 268.

1.3 Gesetzliche Grundlage

Als gesetzliche Grundlage kommt eine Bestimmung im GwG mit folgendem Wortlaut in Betracht: 376

> Sorgfaltspflichten für Händlerinnen und Händler […] 377
>
> [1bis] Sie [Händlerinnen und Händler] dürfen anonyme virtuelle Währungen höchstens bis zu einem umgerechneten Wert von CHF 10'000.- annehmen. […]

Diese Norm erfüllt die Anforderungen hinsichtlich der Normdichte sowie der Normstufe für einen Eingriff in die persönliche Freiheit wie die Monero-Annahmeobergrenze. 378

1.4 Öffentliches Interesse

Als öffentliche Interessen für eine Rechtfertigung des Eingriffs in die persönliche Freiheit kommt die Verhinderung von Terrorismusfinanzierung, Geldwäscherei, Steuerhinterziehung sowie die Verhinderung der Proliferation von Massenvernichtungswaffen, von Korruption usw. in Betracht. 379

1.5 Eignung der Annahmeobergrenze

Die Monero-Annahmeobergrenze ist hinsichtlich der Verwirklichung der öffentlichen Interessen eine geeignete Massnahme, da sie an einen möglichen Exit-Point von Monero ansetzt und insofern zu einer besseren Kontrolle über das Zahlungsmittel führt. 380

2. Besonderheiten der Monero-Regulierung

2.1 Erforderlichkeit

Als milderes Mittel gegenüber einem Annahmeverbot steht zunächst die Pflicht der Händler zur Diskussion, die geldwäschereimässigen Risiken selbst abzuklären, falls der Grenzwert (CHF 10'000.-) bei einer Transaktion überschritten wird. Da Monero-Transaktionen und -Adressen jedoch vor Einsichtnahme Dritter geschützt sind, könnten allfällige jedoch Risiken kaum erkannt werden. Der Käufer könnte immerhin mittels den erwähnten View Keys auf Verlangen Einsicht gewähren. Allerdings ist ein solches Prozedere mit grossen Defiziten belastet. Einerseits ist zu zeitintensiv für gewöhnliche Kaufgeschäfte und setzt – wie bereits erwähnt – ein beträchtliches Fachwissen voraus. Darüber hinaus ersetzt eine Bekanntgabe von View Keys nicht die bei Bitcoin mögliche Blockchain-Analyse. 381

Im Gegensatz zu Bitcoin können *Monero-Transaktionen nur über diejenigen Adressen bzw. Konten hinaus zurückverfolgt werden, zu denen ein View Key vorhanden ist. Damit aber steht fest, dass die Pflicht zur Selbstabklärung der Risiken einer Monero-Zahlung nicht die gleiche Wirksamkeit aufweist wie ein vollständiges Verbot der Annahme solcher Zahlungen*.

382 Darüber hinaus kommt eine Beschränkung der Annahmeobergrenze auf Personen, welche nicht im Land niedergelassen sind, in Betracht. Allerdings wäre das Risiko, dass mithilfe von „Geldeseln" dieser Regulierung ausgewichen würde, gegenüber Bitcoin – wegen der Verschleierung der Monero-Blockchain – noch grösser. Daraus folgt, dass diese Alternative nicht gleich wirksam hinsichtlich der Verhinderung von Terrorismusfinanzierung, Geldwäscherei etc. ist wie eine Annahmeobergrenze für Monero.

383 Aus dem Gesagten erschliesst sich, dass keine milderen Mittel gegenüber einer Monero-Annahmeobergrenze in Bezug auf die persönliche Freiheit existieren, welche die genannten öffentlichen Interessen gleich weitgehend förderten. Die Annahmeobergrenze von umgerechnet CHF 10'000.- für Monero ist also ein erforderliches Mittel.

2.2 Zumutbarkeit

384 Für die *Zumutbarkeit einer Monero-Annahmeobergrenze spricht, dass wegen des hoch angesetzten Bagatellbetrags die tatsächlichen Handlungsoptionen von Individuen kaum beschränkt werden*. In diesem Sinne bleibt die Möglichkeit grundsätzlich bestehen, Spenden mit Monero auszurichten. Ausserdem sind sämtliche Kaufgeschäfte über Alltagsgegenstände und weiterer Gegenstände angesichts der Höhe des Freibetrags nach wie vor möglich. Ferner können unter der diskutierten Monero-Annahmeobergrenze Zahlungen zwischen Privatpersonen in unbeschränkter Höhe nach wie vor vorgenommen werden.

385 Auf der anderen Seite *weist Monero wegen der Verschleierung der Blockchain ein erhöhtes Risiko für Terrorismusfinanzierung, Geldwäscherei etc. gegenüber Bitcoin auf*. Das Interesse an einer Annahmeobergrenze ist daher im Bereich von Monero im Vergleich zu Bitcoin gesteigert.

386 Aus dem Gesagten folgt, dass das *Gewicht der Interessen an der Annahmeobergrenze zur Verhinderung von Geldwäscherei, Terrorismusfinanzierung usw. gegenüber dem Gewicht der Interessen am unveränderten Fortbestand der persönlichen Freiheit (Art. 10 Abs. 2 BV) überwiegt*. Die Bitcoin-Annahmeobergrenze ist folglich eine zumutbare Einschränkung der persönlichen Freiheit von Konsumenten.

2.3 Kerngehalt

Die Beeinträchtigungen durch die Bitcoin-Annahmeobergrenze weisen keinen besonders engen Bezug zur ungehinderten Persönlichkeitsentfaltung der Individuen auf. *In jedem Fall sind die spezifischen Aspekte des Menschseins als solches nicht durch die diskutierte Regulierung gefährdet*. Daraus folgt, dass die Monero-Annahmeobergrenze nicht in den Kerngehalt der persönlichen Freiheit (Art. 10 Abs. 2 BV) eingreift. 387

3. Fazit

Eine Annahmeobergrenze für Monero von umgerechnet CHF 10'000.- ist *angesichts der gewichtigen öffentlichen Interessen an deren Wahrung vor dem Hintergrund der allgemeinen persönlichen Freiheit (Art. 10 Abs. 2 BV) verfassungsmässig*. 388

Kapitel 3: Meldepflicht für Kryptogeld-Wallets

Die fünfte Geldwäschereirichtlinie der EU sieht unter anderem vor, dass die Mitgliedstaaten zentrale Datenbanken einrichten müssen, welche die schnelle Identifizierung sämtlicher Bank- und Zahlungskonten einer Person erlauben (Art. 32a Abs. 1 5.AMLR). Finanzintermediäre müssen daher bei Aufnahme einer Geschäftsbeziehung oder bei der Durchführung von Transaktionen den Namen des Kunden und weitere Angaben an diese zentralen Register melden (Art. 32a Abs. 3 5.AMLR). Ferner sollen diese Informationen den für die Bekämpfung von Geldwäschereidelikten zuständigen nationalen Fachstellen «direkt, sofort und ungefiltert» zugänglich sein (Art. 32a Abs. 2 5.AMLR). Darüber hinaus sollen die Geldwäschereibekämpfungsfachstellen (FIUs) untereinander, auf Ersuchen aber auch spontan, sämtliche Informationen austauschen können, welche im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung «von Belang sein können» (Art. 32a Abs. 2 i.V.m. 53 Abs. 1 5.AMLR). Auskunftsgesuche von anderen europäischen Fachstellen können daher nur in Ausnahmefällen verweigert werden (Art. 53 Abs. 3 5.AMLR). 389

Die vorgesehene zentrale Datenbank für Bankkonten mit direktem Zugriffsrecht der Geldwäschereibekämpfungsfachstelle markiert eine Abkehr vom bisherigen Regulierungsansatz, welcher auf geteilten Datenbanken bei den jeweiligen Finanzintermediären beruht und Ermittlungen i.d.R. aufgrund von einer durch Finanzintermediäre ausgelösten Verdachtsmeldung eingeleitet wurden (Art. 23 Abs. 2 i.V.m. Art. 9 und Art. 11*a* Abs. 1 und 2 GwG) – sogenannter risikobasierter 390

Ansatz.[252] Die fünfte Geldwäschereirichtlinie sieht demgegenüber die Notwendigkeit vor, die Finanzströme in umfassender bzw. «methodischer» Weise zu überwachen, d.h. dass Auslöser für einen Verdacht auf Geldwäsche oder Terrorismusfinanzierung nebst Verdachtsmeldungen auch «eigene Analysen der zentralen Meldestellen» sein können und diese insbesondere *einen zeitnahen Zugriff auf Daten über die Inhaberschaft von Bank- und Zahlungskonten bedürfen, was eine zentralisierte Datensammlung voraussetzt* (siehe Erw. 17 ff. 5.AMLR).[253] Diese Ausweitung der Kompetenzen erfolgt vor dem Hintergrund einer Intensivierung des Vorgehens insbesondere gegen Terrorismusfinanzierung, welche neu auch die «mit geringen Kosten» verbundenen terroristischen Operationen, die aufgrund der Verwendung «neuartiger Zahlungsmethoden» schwer aufzuspüren sind, erfassen soll.[254]

391 Die Pflicht der Finanzintermediäre, die Inhaber von Bank- und Zahlungskonten zu melden, gilt vorerst nur für konventionelle Bank- und Zahlungskonten (Art. 32a 5.AMLR) und nicht für Kryptogeld-Adressen. Die *EU-Kommission ist jedoch dazu aufgerufen, die Einführung einer entsprechenden Regelung im Bereich von Kryptogeld zu prüfen und entsprechende Gesetzgebungsvorschläge bis Januar 2022* allenfalls einzureichen (Art. 65 Abs. 1 und Erw. 16 ff. 5.AMLR). Die Schweiz könnte zur Wahrung eines äquivalenten Schutzniveaus mit der EU zumindest indirekt verpflichtet sein, eine Regulierung, welche eine zentrale Datenbank für Kryptogeld vorsieht, zu übernehmen.

I. Monero und informationelle Selbstbestimmung (Art. 13 Abs. 2 BV)

392 Aufgrund der *Obfuskation der Monero Blockchain* sind Monero-Adressen, d.h. Kontostand und getätigte Transaktionen, nur für den Inhaber und nicht öffentlich einsehbar. Damit im Einzelfall dem Bedürfnis nach Publizität entsprochen werden kann, bietet Monero die Möglichkeit, einzelne Transaktionen oder ganze Adressen mittels View Keys sowie Spend Keys offen zu legen (im Folgenden gemeinsam

252 Siehe zu geldwäschereirechtlich-motivierten Verdachtsmeldungen Rz. 192 ff.

253 Europäische Kommission, Vorschlag (Fn. 82), Erw. 19.; Europäischer Datenschutzbeauftrager, Stellungnahme des EDSB zu einem Vorschlag der Kommission zur Änderung der Richtlinie (EU) 2015/849 und der Richtlinie 2009/101/EG. Zugang zu Informationen über den wirtschaftlichen Eigentümer und Implikationen für den Datenschutz, 2017, Erw. 52.

254 Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament und den Rat. Ein Aktionsplan für ein intensiveres Vorgehen gegen Terrorismusfinanzierung, COM(2016) 50 final, 4.

als View Key bezeichnet).[255] Custody Wallet-Anbieter als *Inhaber der Monero-Adresse bzw. des privaten Schlüssels, können daher verpflichtet werden, View Key und Angaben zur Identifikation von Kunden an ein zentrales Register zu übermitteln*. Diese Informationen könnte die MROS als die FIU der Schweiz nutzen, um allfällige Risiken für Terrorismusfinanzierung, Geldwäscherei oder Proliferation von Massenvernichtungswaffen festzustellen. Weil View Keys nur zur Einsicht genutzt werden können, ist mit diesem Vorgehen ausgeschlossen, dass die FIU oder Personen, welche den View Key beispielsweise gestohlen haben, Moneros veruntreuen könnten.

1. Schutzbereich

Der persönliche Schutzbereich der informationellen Selbstbestimmung umfasst nach h.L. und bundesgerichtlicher Rechtsprechung sowohl die *natürlichen Personen wie auch die juristischen Personen und die Personenvereinigungen*. 393

Zum sachlichen Schutzbereich der informationellen Selbstbestimmung zählen sämtliche möglichen *Datenbearbeitungshandlungen, welche Personendaten betreffen*. 394

Die Verpflichtung der Finanzintermediäre, die von ihnen verwalteten Monero-Adressen mit der dazugehörigen Identität des Kunden zu melden sowie passende View Keys für eine Überprüfung der Adressen durch die MROS bereit zu stellen, beinhaltet gleich mehrere Datenbearbeitungshandlungen. Im Zentrum der Betrachtung steht die *Pflicht der Finanzintermediäre zur Weitergabe von Daten über die Identität des Wallet-Inhabers und des dazugehörigen View Keys an die Geldwäschereibekämpfungsfachstelle sowie deren Datenbearbeitungen im Rahmen ihrer eigenen Analysen*. 395

Mithilfe der übermittelten View Keys hat die MROS einen umfassenden Zugriff auf die Zahlungsprofile der Benutzer von verwalteten Wallets, die von der Regulierung betroffen sind. Zahlungsprofile lassen, wie bereits erwähnt, zumindest Rückschlüsse auf vorgenommene medizinische Behandlungen und Untersuchungen und insofern auf den Gesundheitszustand zu.[256] Darüber hinaus führt die Meldepflicht für die Identität der Inhaber von verwalteten Monero-Wallets und der dazugehörigen View Keys dazu, dass die MROS Kenntnis von ausgerichteten 396

255 Siehe dazu vorne Rz. 195 und 381.

256 Siehe zur Möglichkeit der Herleitung von Daten über den Gesundheitszustand aus Zahlungsprofilen vorne Rz. 333 ff.

Spenden oder Mitgliederbeiträgen hat und damit auf politische, gewerkschaftliche, religiöse usw. Ansichten schliessen kann.

397 Die Meldepflicht hat ausserdem Auswirkungen auf die Verwendung von Monero für Mikrozahlungen bzw. Mikropayments oder Kleinbetragszahlungen. Als Mikrozahlung versteht man Zahlungen geringer Summen insbesondere für den Kauf von digitalen Produkten, wie elektronische Zeitung- bzw. Zeitschriftenartikeln oder Musikstücken. Mikrozahlungen stehen ferner für den werbefreien Besuch von Webseiten teilweise zur Verfügung. Zumal Monero bis auf zwölf Nachkommastellen teilbar ist, kostengünstig, elektronisch und schnell transferiert werden kann, eignet es sich besonders gut für Mikrozahlungen. Eine fortdauernde Aufzeichnung der besuchten Webseiten, der gekauften Zeitungs- und Zeitschriftenartikel usw. kann jedoch – wie bereits erwähnt – Hinweise auf persönliche Ansichten und Neigungen geben, die im Einzelfall als besonders schützenswerte Daten qualifiziert werden müssen (Art. 3 lit. c DSG).[257]

398 Darüber hinaus hat die Meldepflicht für Monero-Adressen Auswirkungen auf die Attraktivität von Monero als anonymes Zahlungsmittel, zumal die Anonymität, welche ein zentrales Merkmal von Monero darstellt, teilweise aufgehoben wird. Ein Attraktivitätsverlust hat zur Folge, dass weniger Benutzer das Zahlungsmittel verwenden und insofern akzeptieren werden. Dadurch wird die Universalität von Monero beeinträchtigt, was negative Auswirkungen auf dessen Wert hat. Dieser Wertverlust trifft nicht nur die Benutzer von verwalteten Wallets, sondern sämtliche Inhaber von Monero. Insofern entzieht der Staat – zumindest ansatzweise – ein Instrument zur Durchsetzung der informationellen Selbstbestimmung.

399 Der Schutzbereich der informationellen Selbstbestimmung ist folglich wegen der Meldepflicht für verwaltete Monero-Wallets eröffnet.

2. Eingriff

2.1 Vorliegen eines Eingriffs

400 Die Verpflichtung, Monero-Adressen sowie dazugehörige View Keys den FIUs zu übermitteln, trifft ausschliesslich gewerbsmässig tätige Finanzintermediäre. Die gewöhnlichen Benutzer solcher Dienstleistungen, mithin die Kunden solcher Finanzintermediäre, gehören nicht zu den Normadressaten (i.e.S.). Die staatliche Beeinträchtigung der informationellen Selbstbestimmung der Benutzer, d.h. über Datenbearbeitungen persönlicher Daten selbst entscheiden zu können, geschieht jedoch wissentlich und ist so beabsichtigt. Die *Meldepflicht von Bitcoin-Adressen*

257 Siehe zur Aussagekraft von Zahlungsprofilen vorne Rz. 343 ff.

ist damit zielgerichtet und verkürzt die informationelle Selbstbestimmung unmittelbar. Als gesetzliche Anordnung im GwG erweist sich diese Verpflichtung als rechtsförmige und ferner nicht als reine fakultative Beschränkung eines Grundrechts. Es liegt damit ein Eingriff in die informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) vor.

2.2 Intensität des Eingriffs

Es stellt sich ferner die Frage, welches Gewicht der Beeinträchtigung der informationellen Selbstbestimmung zuzumessen ist. Für einen *leichten Eingriff spricht*, dass es sich bei Daten über Transaktionen und Kontostände um reine Finanzdaten handelt, die grundsätzlich wenig Bezug zur Persönlichkeit aufweisen. Darüber hinaus folgt aus der Meldepflicht für verwaltete Monero-Wallets nur eine partielle De-Anonymisierung eines anonymen Zahlungsmittels. Nicht-verwaltete Wallets bzw. selbst gehaltene Moneros fallen nicht darunter und können daher weiterhin zur Ausführung vollständig anonymer Zahlungen verwendet werden. Wegen der Möglichkeit, Moneros selbst zu verwahren, d.h. auf Custody Wallet-Anbieter zu verzichten, kann dieser Regulierung daher – mit bloss minimen Abstrichen hinsichtlich der Benutzerfreundlichkeit und allenfalls von gewissen börsenähnlichen Dienstleistungen – einfach und effektiv ausgewichen werden. Ferner bestehen konventionelle Alternativen bzw. Ausweichmöglichkeiten, um Geldzahlungen anonym tätigen zu können, die von der Monero-Meldepflicht nicht betroffen sind. Dazu zählt unter anderem die Verwendung mehrerer ausländischer Bankkonten und Kreditkarten. 401

Für einen *schweren Eingriff* sprechen demgegenüber die folgenden Einwände. Zunächst ist die besondere Persönlichkeitsrelevanz von aufgewerteten Finanzdaten zu nennen. Wie bereits erwähnt, können aus gewöhnlichen Finanzdaten Zahlungsprofile erstellt werden, welche zumindest Rückschlüsse auf besonders schützenswerte Persönlichkeitsmerkmale, wie beispielsweise den Gesundheitszustand oder die politischen bzw. gewerkschaftlichen Ansichten, erlauben. 402

Darüber hinaus weisen die grosse Zahl betroffener Personen, die direkte Zugriffsmöglichkeit des Staates auf deren persönlichen Daten sowie die generelle Betroffenheit der Custody Wallet-Benutzer auf das Bestehen eines schweren Eingriffs hin. Weil die Pflicht zur Bekanntgabe der Identität und des View Keys an die MROS nicht an einen Verdachtsmoment gekoppelt ist, sind grundsätzlich alle Kunden, d.h. eine grosse Zahl von Personen, betroffen. Ausserdem stehen dem Staat aufgrund der v*erdachtsunabhängigen Ausgestaltung der Meldepflicht und der Speicherung in einer staatlichen, zentralisierten Datenbank die* 403

Zahlungsprofile unmittelbar zur Verfügung.[258] Dabei wiegt besonders schwer, dass – zumal der Regulierung einfach und ohne besondere Fachkenntnisse ausgewichen werden kann – die Beeinträchtigungen der Meldepflicht vor allem Personen trifft, welche kein Risiko für Geldwäscherei, Terrorismusfinanzierung usw. darstellen.

404 Ein schwerwiegender Eingriff könnte ferner durch den vorgesehenen, erleichterten Datenaustausch zwischen den europäischen FIUs begründet sein. Für die im Rahmen eines Abrufs erhaltenen Daten ausländischer FIUs gilt nämlich, dass deren Richtigkeit und Zustandekommen nur schwer überprüfbar ist, zumal die Untersuchungen der MROS und der Datenaustausch mit ausländischen FIUs heimlich erfolgen. Mangels Weisungsbefugnis von inländischen Behörden über ausländische Fachstellen kann weder deren Arbeitsweise überprüft noch weitere Abklärungen angeordnet werden. Insofern besteht eine erhöhte Gefahr, dass es zu Persönlichkeitsverletzungen oder sogar zur Erhebung einer Strafanklage durch unrichtige oder illegitim erhobene Daten führt. Darüber hinaus kann jedenfalls nicht ausgeschlossen werden, dass die Daten im Ausland für die Verfolgung eines Delikts Verwendung finden, für welches sie im Inland nicht genutzt werden dürften.[259]

405 Darüber hinaus spricht die Möglichkeit der FIU, *heimliche Untersuchungen von sich aus durchzuführen, für das Bestehen eines schweren Eingriffs auf die informationelle Selbstbestimmung*. Bei heimlich durchgeführten Eingriffen können Betroffene ihre Interessen, d.h. ihre Verfahrensrechte, bestenfalls nur nachträglich geltend machen. Es besteht daher die Gefahr, dass die Persönlichkeit der betroffenen Personen übermässig stark ausgeforscht wird. Ausserdem kann aus der Unsicherheit, Ziel einer Untersuchung zu sein bzw. aus der Ungewissheit, welche Handlungen eine heimliche Untersuchung zur Folge haben, die ferner zu einer Strafanklage führen können, ein latentes Gefühl der Überwachung entstehen. Ferner ist die MROS in das Bundesamt für Polizei integriert und kann daher nicht ganz unabhängig agieren. Individuen könnten daher vom Einsatz von Monero in

258 Siehe zur Speicherung persönlicher Daten zum Zweck sie allenfalls Strafverfolgungsbehörden zugänglich zu machen: BVerfGE 125, 260 (319 ff.) – *Vorratsdatenspeicherung*.

259 Die Gefahr besteht insbesondere aufgrund einer Zweckausweitung zur Vermeidung von Steuerhinterziehung, siehe EDSB, Stellungnahme (Fn. 253), Erw. 18.

bestimmten Fällen aber auch ganz allgemein abgeschreckt sein (chilling effects).[260]

406 Ein schwerer Eingriff könnte ferner wegen der umfassenden Sammlung von Daten über eine grosse Zahl von Personen und der davon ausgehenden Gefahr für die Persönlichkeit bei Verletzung des Grundsatzes der Zweckbindung (Art. 4 Abs. 3 DSG) oder der Datensicherheit (Art. 7 DSG) vorliegen. Personendaten dürfen nach dem Grundsatz der Zweckbindung nur für den Zweck bearbeitet werden, welcher bei der Beschaffung der Daten bzw. im Gesetz ursprünglich angegeben wurde. Entsprechend gilt, dass die hier diskutierten Daten nur für die Zwecke der Verhinderung von Terrorismusfinanzierung und Non-Proliferation von Massenvernichtungswaffen sowie zur Bekämpfung von Geldwäscherei und Korruption eingesetzt werden können, aber nicht auch für weitere, insbesondere geringfügigere Delikte. Die fortdauernde Einhaltung dieses Grundsatzes ist jedoch zweifelhaft *angesichts der Entwicklung, bestehende Datenbanken auf europäischer Ebene miteinander zu vernetzen und für andere Zwecke – beispielsweise EURODAC zur Strafverfolgung sowie SIS zur Verhinderung irregulärer Migration – zu verwenden (Art. 34 ff. SISVo)*.[261] Darüber hinaus erscheint fraglich, ob die Datensicherheit einer umfassenden Datenbank ausreichend gewährleistet werden kann. Aufgrund der Zahl und der Aussagekraft der darin gespeicherten Datensätze stellt

260 Siehe zu den Auswirkungen einer lückenlosen Überwachung von Finanzdaten auf das Individuum R. BARTONE, Abschaffungs des Bargelds? Eine Problemskizze, in: jM 2016, 285-289 (286 ff.).

261 Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28.11.2019 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006; Europäische Kommission, Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Änderung der Verordnung (EG) Nr. 767/2008, der Verordnung (EG) Nr. 810/2009, der Verordnung (EU) 2017/2226, der Verordnung (EU) 2016/399, der Verordnung (EU) 2018/XX [Interoperabilitäts-Verordnung] und der Entscheidung 2004/512/EG sowie zur Aufhebung des Beschlusses 2008/633/JI des Rates, COM/2018/302 final; S. PROGRIN-THEUERKAUF/M. ZOETEWEIJ-TURHAN/TURHAN OZAN, Interoperabilität der Informationssysteme im Migrationsbereich. Digitale Grenzkontrollen 2019, in: A. Achermann/A. Epiney/J. Künzli et al. (Hrsg.), Jahrbuch für Migrationsrecht. 2018/2019, 2020, 3-41 (35 ff.).

eine solche Datenbank ein beliebtes Ziel von Datendiebstählen für kommerzielle oder gar kriminelle Zwecke dar.[262]

407 Abschliessend lässt sich hinsichtlich der Schwere des Eingriffs festhalten, dass dieser Regulierung mit nur wenig Sachkenntnissen effektiv und nahezu vollständig ausgewichen werden kann – v.a. durch den Verzicht auf verwaltete Wallets. Der Eingriff erscheint insofern vordergründig als bloss geringfügig, zumal den Datenbearbeitungshandlungen so entgangen werden kann. Allerdings besteht insofern die durchaus plausible Gefahr, dass die tatsächlich in Geldwäscherei-, Terrorismusfinanzierung usw. involvierten Personen Kenntnis von der Regulierung haben und auf verwaltete Wallets verzichten. Gleichzeitig führt diese Regulierung aber zur Überwachung einer grossen Zahl unverdächtiger Personen, die Custody Wallet-Dienstleistungen wegen ihrer Vorteile hinsichtlich der Benutzerfreundlichkeit nutzen, und die aber keine Kenntnis der Regulierung haben. Insofern führt diese Regulierung dazu, dass unschuldige Personen Ziel von weitreichenden und umfassenden Untersuchungen werden, während sie zur Verhinderung von Geldwäscherei-, Terrorismusfinanzierung usw. keinen oder allenfalls nur beschränkten Nutzen stiftet.

408 Nach dem Gesagten erweist sich die Meldepflicht für verwaltete Monero Wallets und View Key für die Einsicht in die Transaktionshistorie als *schwerwiegende Beeinträchtigung der informationellen Selbstbestimmung* (Art. 13 Abs. 2 BV).

3. Genügende gesetzliche Grundlage

409 Als gesetzliche Grundlage kommen insbesondere de-lege ferenda Normen im GwG in Betracht, die als Teil eines formellen Gesetzes die nötige *Normstufe* aufweisen, welche die Verfassung für schwere Eingriffe voraussetzt.

410 Eingriffe in die informationelle Selbstbestimmung müssen sich auf eine genügend konkrete gesetzliche Grundlage stützen können (Art. 36 Abs. 1 BV). Als schwerwiegende Beeinträchtigung der informationellen Selbstbestimmung muss die gesetzliche Grundlage diesen Eingriff besonders präzise umschreiben. Folgende Bestimmungen erfüllen den Grundsatz der *Normdichte*:

411 Art. 8bis Meldepflicht für Adressen von Kryptowährung

[1] Der Finanzintermediär muss die von ihm im Rahmen der Sorgfaltspflichten erfassten Identitäten und die dazugehörigen Adressen von

262 C. KELLER/M. HESS, Rechtliche Anforderungen an System- und Datensicherheit und Compliance, in: R. WEBER/F. THOUVENIN (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, 2015, 181-205 (185 ff.).

> Kryptowährung an die zentrale Datenbank für Kryptowährungen melden.
>
> [2] Der Finanzintermediär muss bei anonymen Kryptowährungen (Monero) zusätzlich der Meldestelle die Möglichkeiten einräumen, Kontostand sowie getätigte Transaktionen für jede Adresse einzusehen. Dazu kann er der Meldestelle private Schlüssel zur Einsicht (View Keys) bereitstellen [...]
>
> Art. 23 Meldestelle für Geldwäscherei [...]
>
> [3bis] Sie [die Meldestelle] unterhält eine Datenbank für Adressen von Kryptowährung und der Identität der dazu Berechtigten.
>
> [3ter] Die Meldestelle kann jederzeit auf Informationen der zentralen Datenbank für Kryptowährung zugreifen und Datenbearbeitungshandlungen durchführen.
>
> [3quater] Zur Ergänzung, Berichtigung und zur Pflege der zentralen Datenbank kann die Meldestelle von entsprechenden ausländischen Datenbanken jederzeit weitere Informationen einholen. Ausserdem kann sie öffentlich zugängliche Informationen der Blockchain zugreifen und diese auch im Rahmen eigener Abklärungen verwenden [...]
>
> Art. 30 Zusammenarbeit mit ausländischen Behörden [...]
>
> [1bis] Die Meldestelle teilt Informationen der zentralen Datenbank für Kryptowährungen, welche von ausländischen Strafverfolgungsbehörden angefordert werden, und mit deren Ländern die Schweiz aufgrund gesetzlicher oder völkerrechtlicher Bestimmungen zur Zusammenarbeit verpflichtet ist, auf deren Ersuchen unverzüglich mit. Die Informationserteilung kann nur aus Gründen des ordre public verweigert werden.

Es stellt sich allerdings die Frage, ob der Bund zum Erlass dieser Vorschriften überhaupt kompetent ist. Wie bereits erwähnt, hat der Bund eine umfassende Gesetzgebungskompetenz im Bereich der Finanzdienstleistungen gemäss Art. 98 i.V.m. Art. 95 BV. Soweit *verwaltete Wallets von dieser Regulierung betroffen sind, ist eine Gesetzgebungskompetenz vorhanden, zumal die Aufbewahrung von fremden Vermögenswerten bereits als Finanzdienstleistung* zu qualifizieren ist.[263] 412

Demgegenüber ist die Kompetenz der Meldestelle, aus eigenem Anlass auf Daten der Blockchain zuzugreifen und diese für eigene Abklärungen zu verwenden (Art. 8[bis] Abs. 3[quater] GwG) problematisch, weil davon Adressen bzw. Wallets 413

263 Siehe dazu vorne Rz. 161.

betroffen sind, die nicht verwaltet, sondern von den Benutzern selbst gehalten werden. Wie bereits erwähnt, liegt in Situationen, in denen ausschliesslich *„selbstverwaltete" Wallets betroffen sind, keine Finanzdienstleistung vor, weshalb sie nicht unter die Gesetzgebungskompetenz für die – übrigen – Finanzdienstleistungen (Art. 98 Abs. 2 i.V.m. Art. 95 BV) fallen*. Der zweite Satz von Art. 8bis Abs. 3^{quater} GwG erweist sich daher mangels Kompetenzgrundlage in Bezug auf die nicht-verwalteten Wallets als verfassungswidrig.

414 Wegen dem besonderen Schutz der Monero-Blockchain vor unberechtigter Einsicht und vor Netzwerküberwachung hat diese Kompetenz in praktischer Hinsicht jedoch wenig Relevanz. Die nicht-verwalteten Adressen können mangels der Möglichkeit, einen View Key von einem Finanzintermediär heraus zu verlangen nicht überwacht werden.

415 Es liegt also eine genügende gesetzliche Grundlage für die Meldepflicht von verwalteten Monero Wallets vor.

4. Legitimes Eingriffsinteresse

416 Die *Geldwäsche EU-RL diente in ihrer ursprünglichen Konzeption allein der Verhinderung von Geldwäscherei*. Mit den Änderungen von 2005 wurde im Rahmen der zweiten Revision die Verhinderung von Terrorismusfinanzierung in ihre erklärte Zielsetzung aufgenommen. Die vierte Geldwäsche EU-RL will ferner eine bessere Vereinbarkeit mit den vorgeschlagenen Massnahmen insbesondere der FATF und erwähnt daher auch die Verhinderung der Proliferationsfinanzierung (Erw. 4 4.AMLR).

417 Die diskutierte Regulierung geht auf die vierte Revision (5.AMLR) der Geldwäsche-Richtlinie zurück. Interessanterweise wird die Verhinderung von Proliferationsfinanzierung in der revidierten Richtlinie nicht mehr erwähnt. In den Erwägungen wird aber nach wie vor gefordert, den Empfehlungen der FATF sowie die aus völkerrechtlichen Übereinkünften resultierenden Verpflichtungen zu berücksichtigen (Erw. 12 5.AMLR). Das Mandat der FATF wurde im Jahr 2008 um den Bereich der Bekämpfung der Proliferation von Massenvernichtungswaffen erweitert und die FATF hat ihre Empfehlungen in diesem Bereich zuletzt 2018 revidiert.[264] Im Rahmen der fünften Revision wurden darüber hinaus Bestimmungen aufgenommen, welche für die Verhinderung von Geldwäscherei konzipiert sind, die allerdings auch für die Verhinderung bzw. Aufdeckung von

264 FATF, FATF Guidance on Counter Proliferation Financing. The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, 2018.

Steuerhinterziehung dienlich sein können. Dazu zählen die Transparenzregister für Angaben über die wirtschaftlichen Eigentümer von Gesellschaften und juristischen Personen (Art. 30 ff. 5.AMLR).

Auf die Gefahr einer schleichenden Zweckausweitung bzw. *Verwendung personenbezogener Daten zu einem anderen Zweck, als denjenigen, der bei der Beschaffung der Daten angegeben worden ist* wurde bereits bei der Frage der Schwere des Eingriffs hingewiesen.[265] Hier sind demgegenüber allein die in der Richtlinie explizit erwähnten Eingriffsinteressen – d.h. die Verhinderung von Terrorismusfinanzierung und Geldwäscherei – massgebend. Diese Interessen dienen dem Schutz der öffentlichen Ordnung und Sicherheit und sind daher legitime Eingriffsinteressen. Die Gefahr einer zukünftigen Zweckerweiterung wird aber noch im Rahmen der Untersuchung der Verhältnismässigkeit zu berücksichtigen sein. 418

5. Verhältnismässigkeit

5.1 Eignung

Es stellt sich insbesondere die Frage, ob sich die vorgeschlagene Regulierung angesichts der einfach zugänglichen Ausweichmöglichkeit, nämlich auf Anbieter von verwalteten Wallets zu verzichten und ausschliesslich selbst die Monero zu halten, als völlig wirkungslos erweisen würde und insofern die Eignung zu verneinen wäre. Dieser Einwand rechtfertigt sich vor dem – bereits erwähnten – Hintergrund, dass kriminelle Nutzer von Monero dieser Regulierung ohne Weiteres ausweichen können und daher die Massnahmen fast ausschliesslich rechtschaffene Nutzer trifft, bei denen keine Gefahr für Terrorismusfinanzierung, Geldwäscherei usw. besteht. 419

Dagegen lässt sich allerdings einwenden, dass die Anforderungen an die Massnahme hinsichtlich der Eignung tief angesetzt sind. In diesem Sinne ist es ausreichend, wenn zumindest die Möglichkeit besteht, dass einzelne kriminelle Akteure die Ausweichmöglichkeiten nicht zu nutzen wissen und daher aufgrund dieser Regulierung Terrorismusfinanzierung oder Geldwäscherei, wenn nicht unbedingt verhindert, so zumindest aufgedeckt oder wenigstens dienliche Informationen für die Strafverfolgung gewonnen werden können. 420

Aus dem Gesagten folgt, dass die oben skizzierte de-lege ferenda Regulierung – d.h. die Bereitstellung von View Keys zuhanden der MROS, die Meldepflicht der Finanzintermediäre für Monero-Adressen bzw. Wallets und der zugehörigen Identität des Monero-Benutzers sowie des View Keys – *zu einer grundsätzlich* 421

265 Siehe zur schleichenden Zweckausweitung vorne Rz. 406.

besseren Kontrolle des Staates über Monero führen und daher die Gefahren von Terrorismusfinanzierungs- und Geldwäschereidelikten etc. kleiner sind. Ausserdem erzeugen die Meldepflicht für Monero-Wallets keine nachteiligen Wirkungen hinsichtlich der genannten öffentlichen Interessen. Der Eingriff in die informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) ist folglich geeignet.

5.2 Erforderlichkeit

422 Der *Verzicht auf die Verpflichtung der Finanzintermediäre der MROS View Keys für Monero Wallets zur Verfügung zu stellen und nur die verwendeten Adressen zu melden*, stellt ein milderes Mittel dar, zumal weniger Personendaten bekanntgegeben bzw. verarbeitet werden. Diese Alternative ist jedoch zum Zweck der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und der Proliferationsfinanzierung nicht gleich wirksam wie eine Regulierung, die zusätzlich eine Pflicht zur Bekanntgabe des View Keys umfasst. Ohne den View Key könnte die MROS wegen der Obfuskation der Monero Blockchain nämlich keine eigenen Analysen durchführen und hätte nur Kenntnis darüber, welche Personen ein verwaltetes Wallet verwenden und welcher Finanzintermediär das Wallet betreut. Diese Alternative ist mangels der Möglichkeit der Geldwäschereibekämpfungsfachstelle, selbständig Einsicht in Wallets zu nehmen und eigene Abklärungen durchzuführen, nicht gleich wirksam wie eine Pflicht der Finanzintermediäre zur Bekanntgabe von View Keys.

423 Als Mittelweg kommt darüber hinaus ein Verfahren in Betracht, bei welchem eine *Identifizierung erst dann erfolgt, wenn Anhaltspunkte für Geldwäscherei, Terrorismusfinanzierung, Korruption usw. festgestellt würden*. Realisieren liesse sich ein solches Konzept beispielsweise durch folgende Vorgaben: Zunächst müssten die Finanzintermediäre ebenfalls View Keys von den von ihnen verwalteten Monero Adressen herstellen. Die Finanzintermediäre teilten diesen Schlüssel jedoch ohne Angabe der dazugehörigen Identität einer speziell dafür geschaffenen, unabhängigen Stelle mit.[266] Diese Stelle könnte mit deren Hilfe Transaktionen und Kontostände einsehen und mithilfe einer automatisierten Analyse verdächtige Adressen eruieren. Eine Deanonymisierung würde aber erst stattfinden, wenn durch die Analyse Anhaltspunkte für das Bestehen von Geldwäscherei, Terrorismusfinanzierung usw. festgestellt würden. Durch den Einsatz von Smart Contracts könnte das Verfahren zur Deanonymisierung derart ausgestaltet werden, dass die automatisierte Feststellung der erwähnten Risiken automatisch die Berechtigung bildet, Daten für die Identifizierung abzurufen. Diese Alternative stellt hinsichtlich der informationellen Selbstbestimmung eine mildere Massnahme dar, da sie

266 Die MROS ist demgegenüber in das Bundesamt für Polizei integriert und kann daher nicht vollständig unabhängig agieren siehe vorne Rz. 405.

grundsätzlich getrennte Datensammlungen vorsieht, die nur im Falle der Feststellung von Risiken miteinander verknüpft werden.

Dieses Konzept müsste allerdings die gleiche Wirksamkeit hinsichtlich der Verfolgung der öffentlichen Interessen aufweisen wie die Verpflichtung, die View Keys sowie die Identität der MROS bekannt zu geben. Allein mithilfe der View Keys liessen sich beispielsweise Adressen eruieren, welche sich wegen der grossen Anzahl an Transaktionen oder aufgrund der involvierten Beträge verdächtig erscheinen. *Schwierigkeiten ergeben sich jedoch daraus, dass, insbesondere für eine Untersuchung zur Eruierung von Risiken hinsichtlich Geldwäscherei und der Proliferation von Massenvernichtungswaffen, Angaben über die Identität der Vertragsparteien und teilweise auch über die wirtschaftlichen Eigentümer notwendig sind*. Eine dahingehende Untersuchung kann daher nicht sinnvollerweise durchgeführt werden, ohne dass die Identität der Vertragspartner geklärt ist. Weil Monero zusätzlich vor Netzwerkaufklärung geschützt ist, können Transaktionen auch nicht mit bestimmten IP-Adressen in Verbindung gebracht werden. Dadurch entfällt auch die Möglichkeit, Anhaltspunkte aufgrund des Abgleichs von Transaktionen mit bestimmten Herkunftsländern zu gewinnen. Diese Alternative ist folglich nicht gleich wirksam, wie wenn der Geldwäschereibekämpfungfachstelle für verwaltete Monero-Wallets sowohl der View Key wie auch Angaben über die Identität für Abklärungen zur Verfügung stehen. 424

In eine ähnliche Richtung ginge der Ansatz, die *View Keys dezentral abzuspeichern und den Zugriff der MROS von der Voraussetzung einer Verdachtsmeldung eines Finanzintermediärs abhängig zu machen*. Diese Alternative bietet den Vorteil, dass für die nach einer Verdachtsmeldung erforderlichen Abklärungen keine weiteren Interaktionen mit dem Finanzintermediär notwendig wären, sondern dass der Geldwäschereibekämpfungsfachstelle mit der Verdachtsmeldung das dafür benötigte Instrument unmittelbar zur Verfügung stünde. Auch unter dieser Variante liessen sich diese Vorgaben durch den Einsatz von Smart Contracts realisieren. Gleichzeitig wäre diese Massnahme hinsichtlich der informationellen Selbstbestimmung ein milderes Mittel, da die staatlichen Stellen nur nach erfolgter Verdachtsmeldung Zugriff auf Informationen über getätigte Transaktionen sowie Kontostand erhielten. 425

Es ist allerdings fraglich, ob dieser Ansatz die gleiche Wirksamkeit hinsichtlich der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung, etc. aufweist, wie die anlasslose Pflicht zur Datenbekanntgabe für Finanzintermediäre. Obwohl die Unterlassung einer gebotenen Meldung mit Strafe bedroht ist (Art. 305ter StGB), gibt es immer wieder Fälle, bei denen überhaupt keine Meldungen erstattet 426

wurden oder diese erst viel später vorgenommen wurden.[267] Als Grund dafür kommt die grundsätzlich gewinnorientierte Tätigkeit privater Akteure in Betracht, welche durch kostenverursachende Abklärungen und Vorkehrungen zur Vermeidung von Geldwäschereirisiken und ähnliches beeinträchtigt wird. Denkbar ist weiterhin auch, dass Verdachtsmeldungen, welche Personen mit langjähriger Kundenbeziehung betreffen, nur mit Zurückhaltung erfolgen. Darüber hinaus ist die Wirksamkeit dieser Massnahme gegenüber einer Massnahme, welche der MROS einen direkten Zugriff auf die Datenbank für die View Keys erlaubt, vermindert, zumal die MROS ohne sie keine eigenen Analysen und Ermittlungen durchführen könnte. Folglich ist die Beschränkung auf Verdachtsmeldungen für die Einleitung von Geldwäschereiuntersuchungen mit Rücksicht auf die Verfolgung der öffentlichen Interessen nicht gleich wirksam wie ein umfassenderes Instrumentarium, das eigene Abklärungen der Fachstelle zulässt.

427 Es liegen also *keine milderen Mittel vor, welche ein gleichwertiges Schutzniveau gewähren wie eine Meldepflicht für Monero-Custody Wallets sowie dazugehörige View Keys*. Der Eingriff ist also erforderlich.

5.3 Zumutbarkeit

428 Die Pflicht zur Meldung der Monero-Adressen sowie zur Einreichung von View Keys ist zumutbar, wenn aufgrund einer umfassenden Güterabwägung das Interesse des Staates an der Verfolgung der *öffentlichen Interessen (Verhinderung von Terrorismusfinanzierung und Geldwäscherei sowie Verhinderung von Korruption und Non-Proliferation von Massenvernichtungswaffen) gleich oder höher zu gewichten ist als das private Interesse* an einer ungehinderten Ausübung der informationellen Selbstbestimmung.

429 Für die Zumutbarkeit spricht zunächst die besondere Bedeutung der Bekämpfung obengenannter Delikte. Wie bereits erwähnt, gehen mit solchen Aktivitäten eine *starke Gefährdung der öffentlichen Sicherheit* einher. Ausserdem erfährt die Bekämpfung solcher Formen von Kriminalität international grosse Aufmerksamkeit, zumal mithilfe von grenzüberschreitenden Vermögensverschiebungen die Strafverfolgung und die Rückverfolgbarkeit von Vermögenswerten entschieden erschwert wird. Schlussendlich hat sich die Schweiz sich aufgrund der Ratifizierung verschiedener völkerrechtlichen Vereinbarungen im Bereich der Bekämpfung von Terrorismusfinanzierung, Geldwäscherei usw. verpflichtet,

267 TheEconomist vom 8. Sep. 2018, „Stubborn stains", 59 f.

Massnahmen und Empfehlungen internationaler Institutionen – insbesondere diejenigen der FATF – zu befolgen.[268]

Darüber hinaus spricht für die Zumutbarkeit der Massnahme, dass sie nur *einen Teilbereich des Umgangs mit Kryptogeld betrifft*. Kryptogeld kann auch von Privatpersonen selbst gehalten werden, ohne dass Finanzintermediäre oder Banken benötigt werden. Wird der für die Verfügung über das Kryptogeld notwendige private Schlüssel also nicht einem unterstellten Anbieter übertragen, besteht keine Pflicht zur Meldung an ein zentrales Register und das Kryptogeld-Guthaben bleibt insofern geheim. 430

Falls demgegenüber auf ein Custody Wallet nicht verzichtet werden möchte, bieten *Multi-Signature-Keys die Möglichkeit, weit entfernte und unbekannte Dienstleistungsanbieter – beispielsweise im nicht-regulierten Ausland – zu nutzen*.[269] Custody Wallets haben die Vorteile, dass die Verfügung über Monero grundsätzlich einfacher und geräteunabhängig erfolgen kann, und die Verantwortung für die sichere Aufbewahrung des zur Verfügung notwendigen privaten Schlüssels nicht dem Benutzer obliegt. Als nachteilig erweisen sich Custody Wallets insofern, als dass der Finanzdienstleister als Inhaber des privaten Schlüssels im Custody Wallet gehaltenes Kryptogeld veruntreuen könnte. An diesem Punkt setzen die bereits erwähnten Multi-Signature Keys an, welche das Mittel bieten, den privaten Schlüssel in mehrere Teile zu spalten, und die Verfügung von Moneros von der Zustimmung der Mehrheit der Teile abhängig macht. Bei korrekter Implementierung von multisig-Schlüsseln kann ausgeschlossen werden, dass der Dienstleistungsanbieter alleinige Verfügungsmacht erhält und die Moneros veruntreuen könnte. Im *Vergleich zu Finanzdienstleister und Banken im konventionellen Bereich ist das Vertrauen in solche Anbieter daher von untergeordneter Bedeutung*. Es besteht insofern auch unter der diskutierten Regulierung die Möglichkeit, sichere und nicht-überwachte Custody Wallets ohne Gefahr der Veruntreuung verwenden zu können, nämlich durch Ausweichen auf nicht-regulierte, ausländische Anbieter. 431

Ferner hat die Pflicht zur Bekanntgabe der Identität und des View Keys nicht zur Folge, dass die *Vorteile von Custody Wallets mit Rücksicht auf die informationelle Selbstbestimmung selbst bei einem von der Regulierung betroffenem Anbieter vollständig getilgt werden*. Monero-Custody Wallets sind nach wie vor nützlich, um der Erstellung von Zahlungsprofilen und der Bearbeitung besonders schützenswerter Daten durch Private oder Drittstaaten zu begegnen. Auch die verbliebenen Vorteile für die übrige persönliche Lebensgestaltung sprechen für die 432

268 Siehe zur Bedeutung im internationalen Kontext vorne Rz. 100 ff.

269 Zu Multi-Signature Keys siehe vorne Rz. 88.

Zumutbarkeit der Massnahme. Die Regulierung hat gerade keinen Einfluss auf die Funktion von Monero als Anlagemittel oder als Ausweichmittel gegen währungspolitische Massnahmen oder gegen inflationäre Tendenzen der staatlichen Währung.

433 Auf der anderen Seite bestehen unterschiedliche Einwände gegen die Zumutbarkeit und damit gegen eine Vereinbarkeit der vorgeschlagenen Regulierung mit der informationellen Selbstbestimmung. *Im Vordergrund steht zunächst der Umfang und die Detailschärfe der Gesamtheit der der MROS zur Verfügung stehender Daten über einzelne Personen*. Der Umfang einer solchen Datensammlung über eine bestimmte Person variiert dabei offensichtlich nach der Häufigkeit der Bezahlung mit einem Wallet, das von der Regulierung erfasst ist. Je mehr ein Benutzer ein Custody Wallet zur Bezahlung von Waren und Dienstleistungen verwendet, desto grösser wird seine Datenspur und entsprechend erhöht sich die Wahrscheinlichkeit, dass daraus persönlichkeitsnahe und damit besonders schützenswerte Daten gewonnen werden können. Wie bereits erwähnt, können aus Zahlungsprofilen insbesondere auf Angaben über den Gesundheitszustand oder über die politischen sowie gewerkschaftlichen Ansichten und Tätigkeiten einer Person geschlossen werden.[270]

434 Die Meldepflicht für Monero Adressen und View Key hat insbesondere Auswirkungen auf die Verwendung von Monero zur Bezahlung von Kleinstbeträgen bzw. Mikropayments. Kryptogelder eignen sich gut für die Bezahlung von Kleinstbeträgen, wie die Bezahlung von einzelnen Artikeln oder den werbefreien Besuch von Webseiten usw., zumal sie sehr kleine Einheiten zulassen und kostengünstige Transaktionen bieten. Eine fortdauernde Aufzeichnung der Bezüge von Artikeln, besuchten Webseiten etc. einer Person lässt jedoch zumindest Rückschlüsse auf die politischen, gewerkschaftlichen und religiösen Ansichten dieser Person zu.[271] Solche Daten gelten aber als besonders schützenswerte Daten (Art. 3 lit. c DSG). Die Meldepflicht führt daher zu einer nicht gerechtfertigten Bearbeitung von besonders schützenswerten Daten der Benutzer von verwalteten Wallets. Demgegenüber sind Personen, welche kein verwaltetes Wallet zur Bezahlung von Kleinstbeträgen benutzen, nicht von diesen Konsequenzen betroffen.

435 Darüber hinaus spricht die grosse Zahl der von der Regulierung betroffenen Personen, welche aber nicht in Terrorismusfinanzierung, Geldwäscherei usw. involviert sind und auch nie Anlass für einen Verdacht gaben, für die Unzumutbarkeit des Eingriffs in die informationelle Selbstbestimmung. Für diese Personen

270 Siehe dazu vorne Rz. 333 ff.

271 Siehe zur Möglichkeit auf politische Ansichten etc. aufgrund von Transaktionsdaten zu schliessen vorne Rz. 344 ff. und 396.

wirkt der Eingriff besonders intensiv, zumal *geldwäschereirechtliche Regulierungen nicht allgemein bekannt sind, und sie von der Annahme ausgehen könnten, dass die Benutzung von Monero ihre Privatsphäre schütze, was aber gerade durch die diskutierte Massnahme zumindest teilweise negiert wird*.

Das Interesse an der Verwendung von Monero als Anlagemittel und als Ausweichmittel gegen währungspolitische Massnahmen sind eigentlich der allgemeinen persönlichen Freiheit (Art. 10 Abs. 2 BV) zuzuordnen. Als mögliche Beeinträchtigung der persönlichen Freiheit bleibt nach Abzug der hier bereits diskutierten Folgen, jedoch nur das – ungewisse – Risiko einer Strafverfolgung mit entsprechender Strafe übrig. 436

437 Gegen die Zumutbarkeit ist in dieser Hinsicht ferner zu erwähnen, dass angesichts des Fallenlassens einer betragsmässigen Bagatellgrenze und der angestrebten, «methodischen» Überwachung sowie der neu vorgesehener Möglichkeit der Geldwäschereibekämpfungsfachstellen, eigenständig Untersuchungen einzuleiten, zumindest der Eindruck entstehen kann, dass jeder ein potentielles Ziel von solchen Massnahmen darstellt.[272] Diese Wahrnehmung wird dadurch bestärkt, dass die *Abklärungen der MROS grundsätzlich heimlich erfolgen, sie eine staatliche Behörde darstellt und ausserdem Informationen mit weiteren Behörden, darunter auch Strafverfolgungsbehörden und ausländischen Behörden, teilen kann (Art. 35 Abs. 2 GwG). Ferner ist die MROS nicht unabhängig von dem Bundesamt für Polizei und es besteht daher die Gefahr einer Einflussnahme. Insofern besteht das Risiko der Entstehung eines nachhaltig-wirkenden Abschreckungseffekts (chilling effect)* hinsichtlich der Benutzung von Monero, insbesondere in bestimmten Situationen – beispielsweise bei Kontakten oder Reisen in Regionen mit erhöhtem Risiko für Terrorismus oder Terrorismusfinanzierung.

Ausserdem ist fraglich, welche Methoden im Rahmen der Überwachung zur Anwendung kommen sollen in Anbetracht der Zielsetzung, selbst die mit bloss geringen Kosten verbundenen terroristischen Operationen und Geldwäschereidelikte rechtzeitig zu identifizieren.[273] Es besteht eine grosse Wahrscheinlichkeit, dass zur Erfüllung dieses Ziels *angesichts der grossen Zahl von Monero Adressen Filter eingesetzt werden, welche an verpönte Merkmale anknüpfen und daher zu einer diskriminierende Behandlung führen* (Art. 8 Abs. 2 BV). Beispielsweise erscheint es plausibel, dass ein Filter zur Anwendung kommt, welche auf den Namen abstellte und insofern eine Diskriminierung aufgrund der Herkunft vorliegt. 438

272 BARTONE, Abschaffung (Fn. 260), 286.

273 Siehe Europäische Kommission, Mitteilung (Fn. 254), 4; Europäische Kommission, Vorschlag (Fn. 82), Erw. 19.

439 Als weiteren Einwand gegen die Zumutbarkeit des Eingriffs auf die informationelle Selbstbestimmung spricht das Missbrauchsrisiko der umfassenden Datenbank. Wie bereits erläutert, lässt sich mit dem View Key die genaue Transaktionshistorie sowie Kontostand einer Monero Adresse einsehen. Eine Datenbank von vielen Benutzern mit den Schlüsseln für die Einsicht in deren Zahlungsprofile ist daher ein *lohnendes Ziel für Datendiebstahl oder Veruntreuung*. Es geht daher von dieser Datenbank und insofern von dieser Regulierung ein grosses Risiko hinsichtlich der Privatsphäre der Benutzer von Monero aus.

440 Schlussendlich haben die diskutierten Konsequenzen der Regulierung *Auswirkungen auf den Wert von Monero als Mittel zur individuellen Durchsetzung der Ansprüche aus Art. 13 Abs. 2 BV.* Die Meldepflicht für Identität sowie View Key hebt die Anonymität von verwalteten Monero Wallets gegenüber dem Staat auf und bedeutet insofern eine Beeinträchtigung der Funktion von Monero. Zumal der Wert von Kryptogeld massgeblich von der Erfüllung seiner Funktionen bzw. von der Erwartung des Publikums in die Erfüllung dieser Funktionen abhängt, bewirkt die erzwungene Deanonymisierung einen entsprechenden – jedoch kaum quantifizierbaren – Wertverlust von Monero an sich.

441 Gesamthaft zeigt die Analyse der Argumente für und gegen die Zumutbarkeit, dass die informationelle Selbstbestimmung wesentlich durch die diskutierte Regulierung zurückgedrängt wird. Die Meldepflicht für verwaltete Monero-Wallets und der dazugehörigen View Keys gewährt dem Staat den Zugriff auf Informationen über sämtliche getätigten und erhaltenen Zahlungen und führt daher zu einer umfassenden Überwachung von verwalteten Monero-Wallets. Demgegenüber führt diese Überwachung jedoch nur zu einem sehr lückenhaften Schutz vor Terrorismusfinanzierung, Geldwäscherei und Proliferationsfinanzierung zumal der Regulierung mit nur wenig Kenntnissen bzw. mit dem Verzicht auf solche Wallets erfolgreich ausgewichen werden kann. Dieser Umstand beeinträchtigt die grundsätzliche Eignung der Massnahmen zur Verhinderung von Terrorismusfinanzierung, Geldwäscherei usw. in einem Ausmass, das die Zumutbarkeit der Massnahme fraglich erscheinen lässt. Kriminelle Akteure – insbesondere in den diskutierten Bereichen – werden mit grösster Wahrscheinlichkeit das zum Ausweichen nötige Wissen haben oder zumindest schnell erwerben. Diese R*egulierung wird daher über einzelne unvorsichtige Täter hinaus kaum einen Beitrag zur Verhinderung von schweren Verbrechen leisten können*. Sie greift gleichzeitig jedoch stark in Schutzgehalte der informationellen Selbstbestimmung ein.

442 Nach dem Gesagten überwiegt das private *Interesse an der ungehinderten Ausübung der informationellen Selbstbestimmung dem Interesse des Staates an einer Regulierung, welche eine Meldepflicht für verwaltete Monero-Wallets und für die dazugehörigen View Keys zur Bekämpfung von Terrorismusfinanzierung,*

Geldwäscherei usw. vorsieht. Die Zumutbarkeit der Massnahme ist damit nicht gegeben.

6. Kerngehalt

Eine Betroffenheit des Kerngehalts der informationellen Selbstbestimmung könnte dort vorliegen, wo *vollständig und ohne jegliche Rechtfertigung den gesamten Bereich persönlichkeitsrelevanter Informationen ausgeforscht* wird oder der Eingriff die systematische Bearbeitung höchstpersönlicher Daten einer grossen Zahl Personen zur Erstellung von Persönlichkeitsprofilen für die Vorhersage von Verhaltensmustern gerichtet ist.[274] 443

Angesichts der zahlreichen Alternativen und Ausweichmöglichkeiten hat die *Monero-Annahmeobergrenze nicht die Wirkung in der Art einer lückenlosen Ausforschung sämtlicher persönlichkeitsrelevanter Informationen*. Darüber hinaus findet keine systematische Bearbeitung höchstpersönlicher Daten einer grossen Zahl Personen statt. Höchstpersönliche Daten können zwar allenfalls durch Analysetechniken gewonnen werden. Deren Bearbeitung ist jedoch nicht vorgesehen. Daraus folgt, dass der Kerngehalt von der Meldepflicht für Monero-Adressen nicht betroffen ist. 444

7. Fazit

Aufgrund fehlender Zumutbarkeit ist die Meldepflicht für Monero-Adressen und gleichzeitiger Meldepflicht für View Keys nicht verhältnismässig (Art. 36 Abs. 3 BV). Folglich ist die Beschränkung der informationellen Selbstbestimmung wegen dieser Regulierung grundrechtswidrig. Darüber hinaus besteht keine verfassungsmässige Kompetenz für die Überwachung von nicht-verwalteten Wallets. 445

Wie bereits erwähnt, stellt das Interesse an der Benutzung von Monero als Anlagemittel und als Ausweichmittel gegen währungspolitische Massnahmen Aspekte der allgemeinen persönlichen Freiheit (Art. 10 Abs. 2 BV) dar, welche gegen die Gefahr einer Strafverfolgung aufzuwiegen wären. Da die Erhebung einer Strafanklage stark vom jeweiligen Einzelfall abhängt, die übrigen Konsequenzen der Annahmeobergrenze bereits abgehandelt wurden sowie die Verfassungswidrigkeit der Monero-Annahmeobergrenze unter der informationellen Selbstbestimmung feststeht, wird auf eine gesonderte Untersuchung der persönlichen Freiheit hinsichtlich dieses Aspekts verzichtet. Dasselbe gilt in Bezug auf die Meldepflicht für verwaltete Bitcoin Wallets. 446

---

274 Siehe zur Ausforschung von persönlichen Meinungen und Überzeugungen (sogenanntes *forum internum*) und dem Schutz des Kerngehalts, SCHEFER, Kerngehalte (Fn. 199), S. 456 f.

II. Bitcoin und informationelle Selbstbestimmung (Art. 13 Abs. 2 BV)

447 Im Unterschied zu Monero ist die Bitcoin-Blockchain einsehbar, d.h. Informationen über die getätigten und erhaltenen Transaktionen sowie über den Kontostand sind grundsätzlich für jede Adresse bzw. Wallet öffentlich zugänglich. Damit *entfällt bei Bitcoin die Notwendigkeit, Finanzintermediäre zur Herausgabe von View Keys zuhanden der MROS zu verpflichten*.

1. Schutzbereich

448 Die Pflicht der Finanzintermediäre zur Weitergabe von Daten über die Identität der Inhaber von Bitcoin-Zahlungsadressen für die Speicherung in einer zentralen Datenbank stellen Bearbeitungshandlungen von Personendaten dar.

449 Wegen der Offenheit der Bitcoin-Blockchain kann die Geldwäschereibekämpfungsfachstelle ohne Weiteres auf die Informationen über die getätigten und erhaltenen Zahlungen zugreifen. Für die von unterstellten Finanzintermediären verwalteten Wallets stehen ihr ausserdem Informationen über die Identität des jeweiligen Inhabers zur Verfügung. Aus diesen Zahlungsprofilen lassen sich – wie bereits mehrfach erwähnt – zumindest Rückschlüsse auf persönliche Ansichten und Neigungen ziehen und bilden daher besonders schützenswerte Daten.[275]

450 Darüber hinaus beeinträchtigt die vorgeschlagene Massnahme den Wert von Bitcoin, zumal die Meldepflicht für verwaltete Bitcoin-Wallets die Attraktivität der Verwendung von Bitcoin reduziert. Als pseudonymes, dezentrales Zahlungsmittel schützt Bitcoin zumindest teilweise die Privatsphäre. Die Meldepflicht ist daher auch in dieser Beziehung als Beeinträchtigung der informationellen Selbstbestimmung zu werten.

451 Der persönliche Schutzbereich der informationellen Selbstbestimmung umfasst nach h.L. und Rechtsprechung des Bundesgerichts allein die natürlichen Personen. Juristische Personen können sich jedoch auf entsprechende Garantien der Wirtschaftsfreiheit (Art. 27 BV) berufen.

---

275 Für die Möglichkeit, aus Zahlungsprofilen besonders schützenswerte Daten abzuleiten, siehe vorne Rz. 333 ff. und 397.

2. Eingriff

Aufgrund der Meldepflicht für Bitcoin Wallets und für die dazugehörige Identität liegt ein direkter staatlicher Eingriff in die informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) vor, da die gesetzliche *Verpflichtung der Finanzintermediäre zur Meldung der Bitcoin-Adresse und der dazugehörigen Identität sowie deren anschliessender Speicherung in einer staatlichen Datenbank bewusst und gewollt die Verfügungsfreiheit über die eigenen, persönlichen Daten verkürzt*. 452

Es stellt sich die Frage, welches Gewicht der Beeinträchtigung der informationellen Selbstbestimmung beizumessen ist. Für einen leichten Eingriff spricht, dass die Speicherung der Zahlungsadressen sowie der dazugehörigen Identität keine Bearbeitung besonders schutzwürdiger Daten darstellt. Diese Daten sind an sich als gewöhnliche Finanzdaten zu werten. Darüber hinaus bestehen *unterschiedlich geeignete Ausweichmöglichkeiten, welche die Intensität des Eingriffs vermindern*: Personen können einerseits selbst ihre Bitcoins halten, d.h. auf Custody Wallet-Anbieter verzichten, welche zur Datenbekanntgabe verpflichtet wären. Andererseits besteht der Ausweg, Anbieter von Custody Wallets zu nutzen, die in Ländern niedergelassen sind, welche keine entsprechende Regulierung kennen. Der Einsatz von *multisig*-Schlüsseln kompensiert dabei den Nachteil des Risikos von Veruntreuung durch entfernte und persönlich unbekannte Dienstleistungsanbieter. 453

Auf der anderen Seite spricht für einen schweren Eingriff der Umstand, dass diese Daten in Kombination mit den öffentlich zugänglichen Daten auf der Blockchain, Rückschlüsse auf die Geschäftspartner oder sogar auf einzelne gekaufte Gegenstände oder bezogene Dienstleitungen zulassen, welche sich im Einzelfall als besonders schutzwürdige Daten erweisen können.[276] Darüber hinaus ist eine sehr grosse Anzahl Personen davon betroffen, unabhängig von ihrem tatsächlichen Risiko für Geldwäscherei oder Terrorismusfinanzierung. Ferner ist die vorgesehene Möglichkeit der MROS, nach eigenem Dafürhalten heimliche Untersuchungen einzuleiten, die zur Erhebung einer Strafanklage führen können, als schwerwiegenden Beeinträchtigung der informationellen Selbstbestimmung zu werten. Dies lässt sich auch darauf zurückführen, dass die MROS nicht unabhänig vom Bundesamt für Polizei ist und Daten an Strafverfolgungsbehörden weitergeben kann. Auf das *Bestehen eines schweren Eingriffs deutet ferner der Umstand hin, dass die Geldwäschereibekämpfungsfachstellen mit dem direkten Zugriff auf das nationale Register und der vereinfachten Möglichkeit, Daten aus europäischen Register abzurufen, Einblick in umfassende Zahlungsprofile geniessen*, ohne besondere 454

276 Zur Gefahrenlage nicht-anonymer Zahlungen für Händler bzw. Geschäftsleute siehe vorne Rz. 323.

Voraussetzungen beachten zu müssen. Schlussendlich spricht auch für einen schweren Eingriff, dass personenbezogene Daten eher an ausländische – d.h. europäische – Behörden weitergegeben werden, wo die Kontrolle über die eigenen Daten schwieriger ist und darüber hinaus die Gefahr vergrössert, dass Zahlungsprofile zur Verfolgung auch anderer Delikte – insbesondere Steuerhinterziehung – Verwendung finden.[277]

455 Aus dem Gesagten folgt, dass die Verpflichtung zur Meldung an zentrale Register ein staatlicher Eingriff darstellt, und dass dieser Eingriff eine *schwerwiegende Einschränkung der informationellen Selbstbestimmung* (Art. 13 Abs. 2 BV) bedeutet.

3. Genügende gesetzliche Grundlage

456 Als schwerwiegende Beeinträchtigung der informationellen Selbstbestimmung setzt die Meldepflicht für verwaltete Bitcoin Wallets eine formell-gesetzliche Bestimmung voraus, aus deren Wortlaut sich der Eingriff in klarer und unzweideutiger Weise ergibt.

457 Der zukünftige Erlass eines die Richtlinie umsetzenden formellen Gesetzes wird für den weiteren Gang der Untersuchung vorausgesetzt. Die gesetzlichen Grundlagen für die Regulierung von Bitcoin könnten *de lege ferenda* mit folgendem Wortlaut in das bestehende GwG eingefügt werden:

458

> Art. 8bis Meldepflicht für Adressen von Kryptowährung
>
> [1] Der Finanzintermediär muss die von ihm im Rahmen der Sorgfaltspflichten erfassten Identitäten und die dazugehörigen Adressen von Kryptowährung an die zentrale Datenbank für Kryptowährungen melden. [...]
>
> Art. 23 Meldestelle für Geldwäscherei [...]
>
> [3bis] Sie [die Meldestelle] unterhält eine Datenbank für Adressen von Kryptowährung und der Identität der dazu Berechtigten.
>
> [3ter] Die Meldestelle kann jederzeit auf Informationen der zentralen Datenbank für Kryptowährung zugreifen und Datenbearbeitungshandlungen durchführen.
>
> [3quater] Zur Ergänzung, Berichtigung und zur Pflege der zentralen Datenbank kann die Meldestelle von entsprechenden ausländischen Datenbanken jederzeit weitere Informationen einholen. Ausserdem

277 EDSB, Stellungnahme (Fn. 253), Erw. 15 ff.

> kann sie öffentlich zugängliche Informationen der Blockchain zugreifen und diese auch im Rahmen eigener Abklärungen verwenden [...]
>
> Art. 30 Zusammenarbeit mit ausländischen Behörden [...]
>
> [1bis] Die Meldestelle teilt Informationen der zentralen Datenbank für Kryptowährungen, welche von ausländischen Strafverfolgungsbehörden angefordert werden, und mit deren Ländern die Schweiz aufgrund gesetzlicher oder völkerrechtlicher Bestimmung zur Zusammenarbeit verpflichtet ist, auf deren Ersuchen unverzüglich mit. Die Informationserteilung kann nur aus Gründen des ordre public verweigert werden.

Diese Bestimmungen sind *genügend präzise formuliert und weisen eine Norm-* 459
stufe auf, welche den Anforderungen für einen schweren Eingriff entspricht.[278]

Soweit die gesetzlichen Grundlagen eine Überwachung von nicht-verwalteten 460
Wallets vorsehen (siehe Art. 8[bis] Abs. 3[quater] GwG), stellt sich allerdings die Frage, ob der Bund überhaupt kompetent ist, eine derartige Regelung zu erlassen. Zumal bei vom Benutzer selbst gehaltenen Bitcoins keine Finanzdienstleistung im Sinne von Art. 98 Abs. 2 BV betroffen ist – und auch die übrigen Kompetenznormen nicht in Betracht kommen –, besteht keine Verfassungsgrundlage für diese Bestimmung. Im Unterschied zu Monero hat diese Konsequenz praktische Relevanz, da die Bitcoin-Blockchain nicht vor Einsicht und Netzwerküberwachung geschützt ist und daher im Sinne einer effektiven Bekämpfung von Terrorismusfinanzierung usw. dieser Anspruch an die Behörden gestellt werden könnte.

Nach dem Gesagten besteht für die Meldepflicht für verwaltete Bitcoin-Wal- 461
lets eine genügende gesetzliche Grundlage, zu deren Erlass der Bund kompetent ist. Demgegenüber besteht für die Überwachung von rein privaten Wallets bzw. selbst gehaltenen Bitcoins keine Verfassungsgrundlage.

4. Legitimes Eingriffsinteresse

Die bereits erwähnten öffentlichen Interessen – d.h. die *Verhinderung von Geld-* 462
wäschereidelikten, Terrorismusfinanzierung und Bestechungsdelikten sowie das Interesse an der Nonproliferation von Massenvernichtungswaffen – können auch

278 Für mögliche Kriterien, welche für einen schweren Eingriff sprechen würden, siehe vorne Rz. 284

für die Meldepflicht von Bitcoin-Adressen sowie deren Inhaber-Identitäten angeführt werden.[279]

5. Verhältnismässigkeit

5.1 Eignung

463 Eine zentrale Datenbank für Kryptogeld-Adressen und deren Inhaber sowie die darauf bezogenen, umfassenden Datenbearbeitungsrechte der Meldestelle stellen *geeignete Massnahmen dar, weil sie hinsichtlich der Verwirklichung der genannten öffentlichen Interessen förderlich wirken*.

464 Die Voraussetzung der Eignung stellt keine hohen Anforderungen an die Massnahme. In diesem Sinne ist es ausreichend, wenn auch nur ein kleiner Mehrwert aufgrund der Massnahmen im Hinblick auf die Verwirklichung der öffentlichen Interessen zu erwarten ist. Wie bereits weiter oben bei Monero erwähnt, *ist zumindest nicht ausgeschlossen, dass einzelne Fälle unvorsichtiger Täter eruiert oder zumindest dienliche Information für weitere Untersuchungen gewonnen werden können*.[280] Der Eingriff ist daher geeignet.

5.2 Erforderlichkeit

465 Ein *milderes Mittel stellt zunächst der Verzicht auf die Pflicht der Finanzintermediäre, der MROS Daten über die Identität ihrer Kunden und den von ihnen verwendeten Bitcoin-Adressen zu übermitteln*. Diese Variante liefe auf geteilte, von den jeweiligen Finanzintermediären geführte Datenbanken hinaus, wie es die geltende Geldwäschereigesetzgebung vorsieht. Geteilte Datenbanken sind im Hinblick auf die informationelle Selbstbestimmung gegenüber zentralisierten Datensammlungen von Vorteil, da sie für sich genommen ein weniger umfassendes Bild einer Person abgeben. Die MROS könnte jedoch unter dieser Alternative selbst mittels Blockchainanalysen verdächtige Adressen bzw. Transaktionen ermitteln und von sich aus Untersuchungen einleiten. Daher wären aufgrund der Offenheit der Bitcoin Blockchain verdächtige Adressen, beispielsweise wegen der hohen Frequenz von Transaktionen oder mithilfe der Lokalisierung von IP-Adressen, eher identifizierbar. Allerdings könnten die eigenen Untersuchungen der Geldwäschereibekämpfungsfachstelle nicht gleich effektiv durchgeführt werden. Einerseits müssten zusätzliche Abklärungen unternommen werden, um sämtliche Custody Wallets einer Person zu identifizieren. Andererseits sind Abklärungen von

279 Ausführlich zu den legitimen Eingriffsinteressen siehe vorne Rz. 231 ff.

280 Siehe zu den tiefen Anforderungen an der Eignung einer Massnahme und den daraus ergebenden Konsequenzen vorne Rz. 420 f.

allfälligen Risiken für Geldwäscherei oder Proliferation ohne Informationen über die Inhaberschaft zumindest nicht gleich effektiv, wie wenn solche Informationen den Behörden zur Verfügung stünden. Diese Alternative ist also nicht gleich wirksam.

Die eben erwähnten Nachteile liessen sich zumindest teilweise dadurch kompensieren, dass die *Finanzintermediäre immerhin die von ihnen verwalteten Bitcoin-Adressen der MROS melden müssten*. Dadurch stünden der MROS immerhin diejenigen Informationen zur Verfügung, um den Finanzintermediär zu bestimmen, welcher das Wallet verwaltet und daher Informationen zur Identifikation des Inhabers beisteuern könnte. Ferner würde dadurch im Vergleich zur Regulierung des konventionellen Zahlungsverkehrs annähernd „gleich lange Spiesse" im Bereich von Bitcoin geschaffen, zumal aus den Transaktionsdaten, d.h. aus den Zahlungsadressen, die verantwortlichen Finanzintermediäre – soweit es sich um Custody Wallet-Anbieter oder Tauschbörsen handelte – durch die Fachstelle schnell eruieren liessen. Darüber hinaus wären die von der MROS durchzuführenden Blockchainanalysen oder Netzwerküberwachungen zur Abklärung allfälliger Risiken für Geldwäscherei, Terrorismusfinanzierung usw. a priori ohne konkreten Personenbezug und insofern ohne Einfluss auf die informationelle Selbstbestimmung. Allerdings stellt bereits die Speicherung von Personendaten durch Private zum Zweck, sie allenfalls später staatlichen Behörden zugänglich zu machen, eine dem Staat zurechenbare Bearbeitung von Personendaten dar.[281] Gleichwohl würde diese Alternative weniger stark in die informationelle Selbstbestimmung eingreifen und insofern ein milderes Mittel darstellen, zumal Personendaten nur in Verdachtsfällen an die Geldwäschereibekämpfungsfachstelle weitergeleitet würden und sie andernfalls keinen Personenbezug zu den Daten auf der Blockchain herstellen könnte. 466

Allerdings weist die Beschränkung auf eine Meldepflicht der verwalteten Bitcoin Custody Wallets *nicht die gleiche Wirksamkeit auf wie die uneingeschränkte Pflicht der Finanzintermediäre, Bitcoin-Adresse und Identität der MROS bekanntzugeben, zumal die Effektivität der Untersuchungen mangels Kenntnis der Identität der Inhaber von verdächtigen Wallets beeinträchtigt wäre*. Ausserdem bieten – wie bereits erwähnt – Abklärungen von Finanzintermediären aufgrund der engen Beziehung zwischen Kunde und Aufsicht nicht die gleiche Gewähr für das Fernbleiben von geldwäschereimässigen und anderen Risiken wie eine Untersuchung durch eine unabhängige Fachstelle.[282] Die Beschränkung der Meldepflicht der 467

281 EuGH, Urteil vom 08.04.14, Rs. C-293/12 & C-594/12, EU:C:2014:238, Rn. 29 – *EU-Vorratsdatenspeicherung I*; BGE 144 I 126, 133 E. 4.2 – *Vorratsdatenspeicherung*.

282 Siehe zur fehlenden adäquaten Wirksamkeit vorne Rz. 426.

Finanzintermediäre auf die von Kunden genutzten Wallets ist also nicht gleich wirksam wie eine Pflicht zur Bekanntgabe der Adressen inklusive der Identität der Inhaber.

468 Darüber hinaus *stellt der Verzicht auf die Kompetenzen, Daten von ausländischen Datenbanken abzurufen und mit diesen zu teilen, mildere Mittel dar, insofern die Palette der möglichen Datenbearbeitungshandlungen eingeschränkt* ist. Allerdings hätte die Weigerung, Daten mit ausländischen Meldestellen zu teilen, mit grösster Wahrscheinlichkeit zur Folge, dass auch diese keine Daten mehr bekannt geben würden. Dadurch sind die Reichweite sowie die Effizienz von Untersuchungen der Geldwäschereibekämpfungsfachstellen beeinträchtigt und die Wirksamkeit des Massnahmenpakets gegenüber einer Regulierung, welche diese Kompetenzen vollumfänglich gewährte, reduziert.

469 Es liegen also *keine milderen Mittel vor, welche die öffentlichen Interessen – d.h. Verhinderung von Terrorismusfinanzierung, Geldwäscherei und Nonproliferation – gleich gut zu verwirklichen vermögen* wie eine zentralisierte Datenbank mit Bitcoin-Adressen und der dazugehörigen Identitäten mit umfassenden Bearbeitungsrechten der MROS. Die Meldepflicht für verwaltete Bitcoin-Adressen und der dazugehörigen Identität ist also erforderlich.

5.3 Zumutbarkeit

470 Zunächst kann auch für das zentrale Register für Kryptogeld-Adressen das *besondere Gewicht der verfolgten öffentlichen Interessen angeführt werden*. Die Bekämpfung von Terrorismusfinanzierung, Geldwäscherei usw. stellen gewichtige öffentliche Anliegen dar, zu der sich die Schweiz ausserdem international verpflichtete.[283]

471 Überdies *spricht für die Zumutbarkeit der Massnahme, dass davon nur ein Teilbereich des Umgangs mit Kryptogeld betroffen* ist. Kryptogeld kann auch von Privatpersonen selbst gehalten werden, ohne dass Finanzintermediäre oder Banken benötigt werden. Ausserdem kann auf nicht-regulierte, ausländische Custody Wallets-Anbieter ausgewichen werden. Der Einsatz von Multi-Signature-Keys verringert dabei das Risiko der Vermögensveruntreuung durch persönlich unbekannte und weit entfernte Anbieter. Wird der für die Verfügung über das Kryptogeld notwendige private (kryptografische) Schlüssel also nicht einem unterstellten

283 Siehe zu den Auswirkungen internationaler Vorgaben im Geldwäschereibereich vorne Rz. 231 ff.

Anbieter übertragen, besteht keine Pflicht zur Meldung an ein zentrales Register und die Bitcoin-Adresse bleibt damit geheim.

Ferner beschränkt sich die Pflicht der Finanzintermediäre auf die Meldung der Bitcoin-Adressen und *verlangt insbesondere nicht, sämtliche getätigten sowie erhaltenen Transaktionen zu melden*. Dies spricht für die Zumutbarkeit der Massnahme, zumal Transaktionsdaten Rückschlüsse auf besonders persönlichkeitsnahe Eigenschaften und Verhaltensweisen geben können, während dies aufgrund von Daten über die Inhaberschaft von Bitcoin-Adressen allein nicht möglich ist. 472

Dagegen lässt sich aber sogleich einwenden, dass *bei Bitcoin und anderen pseudonymen Währungen die Blockchain und sämtliche darin aufgezeichneten Transaktionen öffentlich einsehbar* sind. Der Staat kann also ohne Weiteres die Informationen der Blockchain mit den Daten über die Inhaberschaft der Bitcoin-Adressen abgleichen und erhält damit ein umfassendes Logbuch über die getätigten sowie erhaltenen Zahlungen eines Custody Wallets, d.h. Angaben über Betrag, Empfänger, Zeitpunkt der Zahlung sowie entsprechende Informationen über Zahlungseingänge. Die Meldepflicht von Bitcoin-Adressen ermöglicht daher dem Staat in Kombination mit den öffentlich zugänglichen Bitcoin-Blockchaindaten die Erstellung von Zahlungsprofilen. Anhand von Zahlungsprofilen lassen sich sogar Rückschlüsse auf den Gesundheitszustand einer Person und deren politische sowie religiösen Ansichten ziehen.[284] Ein entsprechendes Risiko besteht insbesondere hinsichtlich von Zahlungen über Kleinstbeträgen bzw. Mikrozahlungen. Wie bereits erwähnt, sind Mikrozahlungen insbesondere von Interesse für den Kauf einzelner Artikel aus Zeitungen oder Zeitschriften oder für den werbefreien Besuch von Webseiten. Eine Zusammenstellung sämtlicher getätigten Mikrozahlungen einer Person lässt daher im Einzelfall Rückschlüsse auf persönliche politische, gewerkschaftliche oder religiöse Ansichten und Neigungen zu, welche aufgrund ihres engen Bezugs zur Persönlichkeit als besonders schützenswerte Daten gelten. 473

Darüber hinaus besteht an einer *Datensammlung, welche eine Identifikation einer grossen Zahl Bitcoin-Adressen zulässt, und die zusammen mit öffentlich zugänglichen Informationen sogar besonders persönlichkeitsnahe Momente der von Bitcoin-Nutzer offenbart, ein erhöhtes Risiko des Missbrauchs*. Die Einrichtung und der Betrieb einer solchen Datenbank wäre daher besonders rechtfertigungsbedürftig. Einerseits besteht in Anbetracht von Praxisbeispielen eine gewisse 474

284 Siehe zur Möglichkeit, anhand von Zahlungsprofilen auf besonders schützenswerte Daten zu schliessen, vorne Rz. 396 f.; R.W. RAHN, The Case for Financial Privacy, in: K. HUMMER/L.D. BRANDEIS (Hrsg.), Das Recht auf sich selbst. Bedrohte Privatsphäre im Spannungsfeld zwischen Sicherheit und Freiheit, 2003, 167-175 (168 ff.).

Wahrscheinlichkeit, dass der Staat zukünftig die Datenbank für weitere Zwecke einsetzt – beispielsweise zur Bekämpfung von Steuerhinterziehung und andere, leichtere Formen von Kriminalität –, als diese ursprünglich konzipiert war.[285] Andererseits könnten die Daten, auch wegen ihres hohen monetären Werts, durch Dritte gestohlen oder von korrupten Beamten verkauft und auch für illegitime Zwecke wie beispielsweise Erpressung verwendet werden. Die Meldepflicht für Bitcoin-Custody Wallets hat daher Auswirkungen auf den Grundsatz der Datensicherheit und der Zweckbindung von Daten (Art. 7 und Art. 4 Abs. 3 DSG).

475 *Gegen die Zumutbarkeit spricht ausserdem die Möglichkeit einer übermässigen Ausforschung persönlicher Lebenssachverhalte einer grossen Zahl unschuldiger Personen*. Diese Gefährdung geht hauptsächlich von der neu geschaffenen Möglichkeit der Geldwäschereibekämpfungsfachstellen aus, selbst und ohne Vorliegen einer vorgängigen Verdachtsmeldung eines Finanzintermediärs, Untersuchungen wegen Geldwäscherei oder Terrorismusfinanzierung einzuleiten. Im Unterschied zur obfuskierten Monero-Blockchain können auch die „selbstverwalteten" bzw. privaten Wallets überwacht werden und ihnen im Einzelfall eine Identität zugeordnet werden – beispielsweise mithilfe von Clustering sowie der Kontrolle von Exit Points. Wie bereits erwähnt, besteht für eine Überwachung von privaten Wallets keine Verfassungsgrundlage. Für eine effektive Bekämpfung von schweren Delikten wie Terrorismusfinanzierung könnte jedoch – gerade im Nachgang an einen verübten Terroranschlag – dieser Anspruch an die Behörden gestellt werden.

476 Ferner sind die Nachteile für die informationelle Selbstbestimmung zu berücksichtigen, die sich daraus ergeben können, dass die *MROS Informationen ins Ausland bekanntgibt und von dort erhält*. Die Bekanntgabe von Daten ins Ausland hat zur Folge, dass die tatsächlichen Kontroll- und Beschwerdemöglichkeiten des Berechtigten eingeschränkt sind und die Geheimhaltung der Daten zusätzlich erschwert ist. Darüber hinaus besteht ein erhöhtes Risiko für die zuvor geschilderte Gefahr, dass die Daten für weitere Zwecke als ursprünglich angegeben bzw. zur Bekämpfung leichterer Formen von Kriminalität verwendet werden. Ausserdem kann bei Informationen, welche vom Ausland eingeholt werden, die Rechtmässigkeit und die genauen Umstände der Erhebung kaum überprüft werden. Dadurch besteht das Risiko, dass die Grundsätze der Datensicherheit und der Zweckbindung von Datenbanken verletzt werden.

---

285 Siehe zur Gefahr der – schleichenden – Zweckausweitung vorne Rz. 406; siehe dazu ferner J. BÜLTE, Das neue deutsche Geldwäschegesetz 2017, in: ZWF 2018, 49-54 (53 f.).

Als problematisch erweist sich darüber hinaus die grundsätzliche Offenheit gegenüber der zum Einsatz kommenden Mitteln. Es besteht insofern die Gefahr, dass im *Hinblick auf eine wirkungsvolle Bekämpfung von Geldwäscherei, Terrorismusfinanzierung usw. intensive und permanente Überwachungsmethoden wie beispielsweise Blockchainanalysen oder sogar Netzwerkaufklärung eingesetzt* werden. Dieser Aspekt ist besonders problematisch angesichts des Umstands, dass die Anforderungen an die jeweiligen Instrumente zur Bekämpfung der genannten Delikte unterschiedlich sind. Die methodische Überwachung ist nur dort von grossem Interesse, wo eine schnelle Reaktion direkt dem Schutz gewichtiger Rechtsgüter dient – beispielsweise bei Terrorismusfinanzierung bzw. der Verhinderung von Terroranschlägen. Demgegenüber ist die zeitliche Dringlichkeit und damit eine verdachtsunabhängige, methodische Überwachung bei Geldwäscherei von untergeordneter Bedeutung.[286] 477

Im Rahmen einer umfassenden Überwachung des Bitcoin-Netzwerks mittels Blockchainanalysen sind beispielsweise Filter denkbar, welche besonders oft genutzte Adressen oder Adressen, mit betragsmässig ungewöhnlich hohen Zu- oder Abgängen, aussondern. Ausserdem können weiterreichende Mittel zum Einsatz kommen, wie die zuvor erwähnte Netzwerkaufklärung, bei welcher ein Mitschnitt des Bitcoin-Netzwerks und der darin versandten Datenpakete erfolgt, und diese mit den auf der Blockchain publizierten Transaktionen abgeglichen werden. Mithilfe von Netzwerkaufklärung liesse sich also eine Zuordnung zwischen einzelnen Transaktionen und der jeweilig verwendeten IP-Adresse des Absenders bzw. des Geräts vornehmen. Anhand der IP-Adresse lässt sich im Einzelfall auf die Identität des Internetbenutzers schliessen, weshalb sie Personendaten darstellen.[287] Schweizerische Internetanbieter müssen dem Überwachungsdienst für den Post- und Fernmeldeverkehr alle Angaben für eine Identifikation liefern, wenn auch nur der Verdacht besteht, dass eine Straftat über das Internet begangen worden ist (Art. 22 BÜPF). IP-Adressen sind ausserdem aufschlussreich hinsichtlich der geografischen Herkunft des Internetbenutzers und können unter anderem für die Aufdeckung von Terrorismusfinanzierungsrisiken dienlich sein. *Netzwerkaufklärungen und permanente Blockchain-Kontrolle mittels Filter stellen intensive Überwachungsmethoden dar und können beim Individuum den Eindruck hinterlassen, dass der Staat gegenüber den Benutzern von Bitcoin ein grundsätzliches Misstrauen hegt*.[288] Dieses Empfinden wird dadurch bestärkt, dass Untersuchungen der MROS heimlich durchgeführt werden (Art. 10a GwG) und die Ergebnisse dieser Untersuchung von Strafverfolgungsbehörden verwendet werden können. Die 478

286 EDSB, Stellungnahme (Fn. 253), Erw. 51.

287 Siehe zu IP-Adressen als persönliches Datum BGE 136 II 508, 516 E. 3.5 – *IP-Adresse*; EuGH, Urteil vom 19.10.16, C-582/14, EU:C:2016:779, Rn. 39 ff. – *Breyer*.

288 BARTONE, Abschaffung (Fn. 260), 286 ff.

methodische Überwachung sowie die Gefahr, dass deren Ergebnisse im Rahmen eines Strafverfahrens gegen einem verwendet werden können führt daher zu einer abschreckenden Wirkung (chilling-effect) hinsichtlich der Benutzung von Bitcoin.[289] Dafür spricht auch der Umstand, dass die MROS keine unabhängige Stellung gegenüber dem Bundesamt für Polizei hat. Wegen der Offenheit der Bitcoin-Blockchain bzw. der Möglichkeit sämtliche Wallets einzusehen erstreckt sich die abschreckende Wirkung grundsätzlich auf alle, potentiellen Benutzer von Bitcoin. Vor dem Hintergrund der grossen Zahl an Bitcoin Adressen müssen jedoch Filter eingesetzt werden, um verdächtige Bitcoin Wallets zu identifizieren.

479 In dieser Hinsicht besteht die Gefahr einer diskriminierenden Behandlung aufgrund der für die methodische Überwachung eingesetzten Filter bzw. der dazu zur Anwendung kommenden Kriterien. Zumal eine ausschliessliche Anknüpfung an den Betrag im Hinblick auf die Zielsetzung, terroristische Operationen mit geringen finanziellen Mitteln aufzudecken, nicht zielführend ist, müssen andere Kriterien gefunden werden, um Wallets mit Risiken für Terrorismusfinanzierung, Geldwäscherei usw. zu identifizieren. Wie bereits erwähnt, besteht mangels anderweitig geeigneter Alternativen die Gefahr*, dass im Rahmen einer wirkungsvollen Bekämpfung insbesondere eine Anknüpfung an den Namen erfolgt und insofern eine diskriminierende Behandlung aufgrund der Herkunft* vorliegt.[290]

480 Schlussendlich führt eine Abwägung der genannten Argumente zu folgenden Überlegungen. Zunächst ist die Möglichkeit der Nutzung der erwähnten Ausweichmöglichkeit – d.h. der Verzicht auf verwaltete Wallets oder das Ausweichen auf ausländische, nicht-regulierte Anbieter – hinsichtlich der Zumutbarkeit der Regulierung nur leicht zu gewichten, zumal das Ausweichen auf fremde Rechtsordnungen faktisch erzwungen wird und dem Konzept der Grundrechte als Raum der Freiheitsverwirklichung und damit der Verfassung zuwiderläuft. Ausserdem bietet diese Alternative keine Gewähr für eine fortdauernde, uneingeschränkte Benutzung von verwalteten Wallets. Für die Verhältnismässigkeit der Massnahme stärker ins Gewicht fällt aber die Tatsache, dass für die Inhaber von nicht-verwalteten Wallets das Risiko einer Identifizierung oder auch nur Einsicht in das Wallet bzw. Zahlungsprofil – angesichts deren grossen – klein ist und insofern keine Personendaten betroffen sind. *Besonders stark für die Zumutbarkeit der Massnahme spricht aber die internationale Aufmerksamkeit und die Bedeutung für die Staatengemeinschaft*, welche der Bekämpfung von Terrorismusfinanzierung, Geldwäscherei und Non-Proliferation von Massenvernichtungswaffen zukommen.

---

289 Vgl. dazu der Entscheid des BGer über die vorsorgliche (Rand-) Datenspeicherung im Fernmeldeverkehr: BGE 144 I 126, 135 ff. E. 5.2 ff.– *Vorratsdatenspeicherung*.

290 Siehe dazu vorne Rz. 460.

Auf der anderen Seite fällt g*egen die Zumutbarkeit schwer ins Gewicht, dass aufgrund der aktualisierten Zielsetzung, terroristische Operationen mit geringen finanziellen Aufwendungen identifizieren zu können, umfassende und einschneidende Überwachungsmethoden* eingesetzt werden, die auch Personen treffen, bei welchen überhaupt keine Verbindung zu schweren Straftaten bestehen. Verschärfend wirkt ausserdem der Umstand, dass der Staat einen umfassenden Zugriff auf die Gesamtheit der Daten in den Zahlungsprofilen hat und damit Kenntnis von besonders schützenswerten Personendaten erhält. Mit dem Einsatz von Algorithmen zur Erkennung von allfälligen Risiken lässt sich sogar die grosse Zahl der vorhandenen Bitcoin Wallets bzw. Adressen automatisch überwachen. In diesem Sinne sind sämtliche Benutzer von Bitcoin ein potentielles Ziel von heimlichen Untersuchungsmassnahmen und gegebenenfalls sogar einer Strafuntersuchung, was zu chilling effects hinsichtlich der Benutzung von Bitcoin führt und als besonders intensive Beeinträchtigung zu werten ist. Umso schwerer wiegt dabei, dass die Wirksamkeit der Massnahme angesichts der einfach zugänglichen Ausweichmöglichkeiten gleichzeitig drastisch reduziert ist und daher mit grossen Defiziten belastet ist. Die eingangs erwähnten Auswirkungen auf den Wert und damit auf die Eignung von Bitcoin als Zahlungsmittel fallen hingegen nur noch sehr leicht gegen die Zumutbarkeit ins Gewicht. 481

Insgesamt zeigt sich, dass die *Argumente, welche gegen die Zumutbarkeit einer zentralen Datenbank für Bitcoin-Adressen sowie umfassenden Bearbeitungsrechten der Geldwäschereibekämpfungsfachstelle sprechen, deutlich überwiege*n. Die erwähnten, teilweise weitgehenden, Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) können insbesondere angesichts der beschränkten Wirksamkeit nicht gerechtfertigt werden. Eine Regulierung, welche der MROS die Kompetenz gewährt, ohne Verdachtsmomente Untersuchungen einzuleiten sowie Finanzintermediäre verpflichtet, Identitätsangaben zu Bitcoin-Custody Wallets bekanntzugeben, ist folglich nicht zumutbar. 482

6. Kerngehalt

Eine Eingriff in den Kerngehalt der informationellen Selbstbestimmung (Art. 13 Abs. 2 BV) kommt vorliegend nicht in Betracht, weil weder die Datensammlung über die *Identität der Nutzer von verwalteten Bitcoin-Wallets noch die auf der öffentlich einsehbaren Bitcoin-Blockchain gespeicherten Daten noch die Kombination dieser Datensammlungen eine Ausforschung des gesamten persönlichkeitsrelevanten Lebensbereichs* zulassen.[291] 483

[291] Zur Ausforschung von persönlichen Ansichten und den Auswirkungen ihrerseits auf die informationelle Selbstbestimmung mit weiteren Referenzen siehe oben Rz. 443

7. Fazit

484 Die Pflicht zur Bekanntgabe der Identität der Benutzer von verwalteten Bitcoin-Wallets sowie die umfassenden Rechte der FIU eigene Recherchen sowie Untersuchungen durchzuführen und zu diesem Zweck die Blockchain methodisch zu überwachen stellt eine nicht zumutbare Einschränkung der informationellen Selbstbestimmung dar. Darüber hinaus besteht hinsichtlich von Nutzern selbst gehaltene Moneros, d.h. nicht-verwalteten Wallets, keine verfassungsmässige Kompetenzgrundlage für deren Überwachung. Auch in dieser Hinsicht erweist sich der Eingriff daher als verfassungswidrig.

Schlussbetrachtung

Kryptogelder stellen private Zahlungsmittel dar, welche sich durch eine dezentrale Registerführung der Transaktionen auszeichnen – sogenannte Blockchain oder Distributed Ledger Technology. Der Einsatz von Kryptographie ermöglicht die Sicherstellung der Integrität des Systems trotz eines grundsätzlich offenen sowie möglicherweise anonymen Kreises von Personen, welche Zahlungen mit Kryptogeld verarbeiten (*Dezentralität*). Diese Personen – auch als *Miner* bezeichnet – können Transaktionen aber weder verhindern noch eine De-Anonymisierung vornehmen. Aufgrund dieser Konzeption stellt Kryptogeld eine *bargeldähnliche Institution* dar bzw. ein Peer-to-Peer Zahlungssystem. Die traditionellen Regulierungsansätze beruhen demgegenüber auf der Prämisse, dass es für die Ausführung elektronischer Transaktionen Finanzintermediäre bedarf, die aufgrund ihrer Rolle als Bindeglied zwischen Sender und Empfänger, einzelne Finanzflüsse kennen und sogar verhindern können. Insofern lassen sich die *traditionellen Regulierungsansätze nicht unbesonnen auf Kryptogeld übertragen*, vielmehr ist eine differenzierte Betrachtung der Nutzen und Risiken einer Regulierung von Kryptogeld angezeigt.

Als mögliche Regulierung wurde zunächst eine *Annahmeobergrenze für Bitcoin* zur Diskussion gestellt. Die Bitcoin-Annahmeobergrenze setzt an einem sogenannten Exit Point für Kryptogeld an, zumal im Kaufvorgang ein Umtausch von immateriellen Bitcoin-Vermögenswerten gegen andere, in der Regel materielle Vermögenswerte stattfindet. Die Kontrolle von Exit Points soll verhindern, dass durch den Umtausch die Herkunft der Vermögenswerte verschleiert werden kann und damit deren Rückverfolgbarkeit sicherstellen (Paper Trail). Die Annahmeobergrenze orientiert sich an den in- und ausländischen Vorschriften für den Umgang mit Bargeld, welches ähnlich wie Bitcoin keine Identifikation verlangt, sondern grundsätzlich den Inhaber an der Werteinheit berechtigt. Im *Unterschied zu Bargeld kann Kryptogeld allerdings schnell und sicher, weltweit elektronisch transferiert* werden, weshalb sich für Bitcoin eine tiefere Grenze von CHF 10‘000.- anbietet. Aufgrund der Höhe der Bagatellgrenze kann die überwiegende Mehrheit der Geschäfte mit Konsumenten weiterhin mit Kryptogeld abgewickelt und von den Vorteilen von Kryptogeld profitiert werden. Demgegenüber profitieren B2B-Transaktionen nicht von der Ausnahme für Bagatellfälle. Allerdings sind die Vorteile von Bitcoin-Zahlungen zwischen Händlern eher gering, und es kommen Nachteile, wie die *Offenheit der Bitcoin-Blockchain* hinzu, die Geschäftsgeheimnisse und andere vertrauenswürdige Informationen offenbaren könnte. Angesichts der gewichtigen öffentlichen Interessen am Eingriff – d.h. die Verhinderung von Terrorismusfinanzierung, Geldwäscherei usw. – ist daher eine Kontrolle mittels Annahmeobergrenze *unter der Wirtschaftsfreiheit (Art. 27 BV)* gerechtfertigt. Es konnte jedoch gezeigt werden, dass Beschränkungen eines privaten Zahlungsmittels, welche zum alleinigen Zweck des Schutzes der staatlichen

Währung erfolgen, im Widerspruch zur institutionellen Garantie der Wirtschaftsfreiheit stehen, und weil sie keine Grundlage in der Verfassung haben, unzulässig sind.

Im Unterschied zu Gewerbetreibenden werden *Privatpersonen bzw. Konsumenten durch die Bitcoin-Annahmeobergrenze* nicht unmittelbar verpflichtet, dennoch sind sie in den unterschiedlichsten Situationen davon betroffen. Wie die Untersuchung gezeigt hat, profitieren Konsumenten aber vom Grundrechtsschutz hinsichtlich geldwäschereirechtlich-motivierten Regulierungen, die nur Finanzintermediäre und Banken direkt verpflichten. Der *allgemeinen persönlichen Freiheit gemäss Art. 10 Abs. 2 BV* kommt für den Schutz von sämtlichen Personen, welche keiner gewerblichen Tätigkeit nachgehen, eine entscheidende Bedeutung zu, da sie als inhaltlich offene Garantie Schutz vor Einschränkungen auch eines abstrakten Phänomens, wie es (Krypto-) Geld auszeichnet, bietet. Die Interessen an gewöhnlichen, d.h. nicht-anonymen Zahlungsvorgängen wären andernfalls – abgesehen von nur wenig praxisrelevanten Spezialtatbeständen, wie bei einer Spende aus religiösen Motiven (Art. 15 BV) – ungenügend geschützt. Bitcoins sind zwar grundsätzlich Gegenstand der Eigentumsgarantie, blosse Beschränkungen der Verfügungsfreiheit über das Eigentum, die nicht die Schwere einer Enteignung erreichen, wie es sich im Fall der Bitcoin-Annahmeobergrenze verhalten würde, fallen allerdings nicht unter die Eigentumsfreiheit.

Darüber hinaus wurde eine Annahmeobergrenze für *Monero*, welches *stellvertretend für weitere anonyme dezentrale Zahlungsmittel* steht, thematisiert. Eine Regulierung möglicher Exit Points, wie durch eine Annahmeobergrenze, kommt bei Monero gegenüber Bitcoin eine grössere Bedeutung zu, zumal sämtliche Monero-Transaktionen vor Kenntnisnahme Dritter geschützt sind und daher die Rückverfolgbarkeit von Vermögenswerten innerhalb von Monero ausgeschlossen ist. Demgegenüber bestehen an Monero massgebende *wirtschaftliche und persönliche Interessen von Gewerbetreibenden, die zur Wirtschaftsfreiheit (Art. 27 BV)* zu zählen sind. Dazu gehört insbesondere der Schutz von Betriebsgeheimnissen, welche durch nicht-anonyme Zahlungen gefährdet sind. Eine Bagatellgrenze von CHF 10'000.- bedeutet für Gewerbetreibende, dass Transaktionen mit anderen Gewerbetreibenden (B2C) in der Regel vom Annahmeverbot betroffen sind, und es insofern eine prohibitive Wirkung hat, was einem Technologieverbot gleichkommt. In Anbetracht der beschränkten Effektivität der Annahmeobergrenze lässt sich diese Konsequenz nicht rechtfertigen. Darüber hinaus sollte ein Monero-Annahmeverbot vor dem Hintergrund gesehen werden, dass eine Reihe von *konventionellen, d.h. nicht auf Kryptogeld basierenden Mitteln für Geldwäscherei, Terrorismusfinanzierung, Steuerhinterziehung etc. zur Verfügung stehen* und mit Erfolg genutzt werden. Die Monero-Annahmeobergrenze erscheint daher als nicht

gerechtfertigte Ungleichbehandlung eines Zahlungsmittels, das mehr den Interessen der Benutzer dient, als denjenigen von Banken und Fiskus.

Auf der anderen Seite wurde untersucht, ob *Interessen von Privatpersonen bzw. Konsumenten an anonymen Geldzahlungen* bestehen und inwieweit diese durch eine *Monero-Annahmeobergrenze* beeinträchtigt sind. Auch Privatpersonen haben einen Anspruch aus der *informationellen Selbstbestimmung* (Art. 13 Abs. 2 BV) auf die Geheimhaltung von Zahlungsvorgängen, insbesondere gegenüber solchen, die Aufschluss über den Gesundheitszustand geben oder politische und religiöse Ansichten wiederspiegeln. Solche Informationen sind zu den besonders schützenswerten Daten zu zählen, weil sie ernsthafte Nachteile für die Betroffenen bei deren Bekanntheit nach sich ziehen könnten und insofern die ungestörte Persönlichkeitsentfaltung zumindest beeinträchtigen. Demgegenüber zeigte die Untersuchung, dass chilling effects keine notwendigen Folgen einer Monero-Annahmeobergrenze von CHF 10'000.- sind. Darüber hinaus reduziert die Annahmeobergrenze – angesichts des hohen Freibetrags – mögliche Nutzungshandlungen von Konsumenten mit Monero nur wenig. Daher erweist sich im Ergebnis das Monero-Annahmeverbot als verfassungsmässige Beschränkung der informationellen Selbstbestimmung. Zu einem anderen Resultat müsste man wohl gelangen, falls die Bagatellgrenze deutlich nach unten gesenkt oder konventionelle Ausweichmöglichkeiten – wie die Verwendung mehrerer, insbesondere ausländischer, Bankkonten und Kreditkarten – nicht mehr zugänglich wären.

Ferner wurde die *Monero-Annahmeobergrenze* auf ihre Auswirkungen hinsichtlich der *persönlichen Freiheit der Konsumenten* untersucht. Im Zentrum der Betrachtung stehen – nach Abzug der unter die Wirtschaftsfreiheit sowie unter die informationelle Selbstbestimmung fallenden Aspekte – die Auswirkungen auf die persönliche Vorsorge. Zu erwähnen sind jedoch ferner – wie bei den übrigen Konstellation auch – die negativen Konsequenzen einer Annahmeobergrenze auf den Wert und damit auf die zukünftige Nützlichkeit von Kryptogeld. Die Annahmeobergrenze beschneidet die Funktion als Zahlungsmittel von Kryptogeld. Die *Werthaltigkeit von Kryptogeld liegt mangels eines Stoff- oder abgeleiteten Werts allein in der Erfüllung der geldmässigen Funktionen*. Wegen der geringen Auswirkungen auf den Wert von Monero, durchbricht die Annahmeobergrenze in dieser Hinsicht jedoch nicht den Bagatellvorbehalt von Art. 10 Abs. 2 BV. Das Beispiel vermag jedoch zur Illustration der Gefahr dienen, dass der Staat durch eine Reihe einzelner Eingriffe, die für sich gesehen unter den Bagatellvorbehalt fallen und daher mir Rücksicht auf die persönliche Freiheit unbeachtlich wären, den Wert und damit die Nützlichkeit von Kryptogeld gesamthaft soweit reduzieren kann, dass das Interesse der Individuen am Gegenstand komplett entfällt. Insofern erhellen sich die Defizite einer nur auf elementare Erscheinungen der Persönlichkeitsentfaltung gerichteter persönlichen Freiheit.

In einem vorletzten Schritt wurde die Verfassungsmässigkeit einer Regulierung geprüft, welche *Finanzintermediäre, die verwaltete Wallets anbieten*, verpflichtet, die *Identität ihrer Kunden*, sowie, im Fall von Monero, sogenannte *View Keys für die Einsichtnahme in die ansonsten verborgenen Wallets*, d.h. Transaktionen und Kontostände, den Geldwäschereibekämpfungsfachstellen (FIU) zur Verfügung zu stellen. Diese Regulierung markiert ausserdem eine Abkehr vom vormals geltenden risikobasierten Ansatz, weil die Geldwäschereifachstellen nunmehr aus eigenem Anlass Untersuchungen einleiten können und insbesondere nicht vom Vorliegen einer Verdachtsmeldung abhängig sind. In der Kombination mit der umfassenden Datensammlung sowie der Datenbearbeitungsrechte erweist sich diese Beeinträchtigung der *informationellen Selbstbestimmung* (Art. 13 Abs. 2 BV) als schweren Eingriff, da der Staat Zugang zu Zahlungsprofilen von Individuen erhält und diese für heimliche Untersuchungen, die zu einer strafrechtlichen Anklage führen können, verwenden darf. Allerdings kann der *Regulierung durch den Verzicht auf die Nutzung von verwalteten Wallets oder durch die Wahl von nicht-regulierten Anbieter leicht ausgewichen* werden, was ihren Nutzen stark beeinträchtigt. Im Ergebnis überwiegt daher das Gewicht der Interessen an der informationellen Selbstbestimmung gegenüber dem staatlichen Interesse an einer Meldepflicht. Die gemachten Erwägungen weisen ausserdem auf die grundsätzliche Problematik hin, dass eine mit dem konventionellen Zahlungssystem auch nur annähernd vergleichbare Kontrolle von Monero sogar mit weitreichenden Eingriffen in grundrechtlich geschützte Sphären angesichts der praktischen Hürden (Dezentralität und Obfuskation) nicht möglich ist.

Schliesslich war die *Meldepflicht von verwalteten Bitcoin-Wallets* an FIUs Gegenstand der Untersuchung. Im Unterschied zu Monero wird kein View Key benötigt, um auf die aggregierten Daten der Blockchain und insofern auf Zahlungsprofile zugreifen zu können. Weil Bitcoin nicht vor Überwachung der Transaktionen und des Netzwerks geschützt ist, können nicht nur die verwalteten Wallets, sondern grundsätzlich alle Adressen auf Anzeichen für Geldwäscherei, Terrorismusfinanzierung usw. überprüft werden. Zumal die Erstellung neuer Zahlungsadressen praktisch unbegrenzt möglich ist und überhaupt keiner Interaktionen bedarf, können nur geringe Beträge zwischen Bitcoin-Wallets verschoben werden, die für sich gesehen unter das Radar der FIU fallen. In diesem Sinne könnte es angezeigt sein, Bitcoin umfassend mittels Filter zu überwachen, was aber die Gefahren von diskriminierenden Behandlungen sowie von chilling effects auf die Benutzung von Bitcoin schaffen. Mangels geeigneter Alternativen für die Eruierung verdächtiger Transaktionen bzw. Wallets könnte eine effektive Bekämpfung nämlich dazu führen, dass Transaktionen anhand der verwendeten IP-Adressen mit bestimmten Ländern oder Regionen abgeglichen werden oder dort, wo diese Informationen vorhanden sind, auf den Namen bzw. Herkunft

abgestellt wird, um das Risiko für Geldwäscherei etc. zu bestimmen. Diese Regulierung, welche eine umfassende Deanonymisierung von verwalteten Bitcoin-Wallets gegenüber dem Staat bezweckt und auch Benutzer von nicht-verwalteten Wallets betrifft, insofern sie alle Ziel einer heimlichen Untersuchung sein können, ist daher als schwere Beeinträchtigung der informationellen Selbstbestimmung zu werten, welche angesichts des beschränkten Nutzens nicht gerechtfertigt ist. Darüber hinaus besteht keine Kompetenzgrundlage in der Verfassung für die Überwachung nicht-verwalteter Wallets.

Die dargestellten Ergebnisse rechtfertigen die Aussage, dass eine Regulierung von Kryptogeld als privates, dezentrales Zahlungsmittel einerseits aufgrund der Gefährdung der öffentlichen Sicherheit durch schwere Delikte angezeigt ist, andererseits angesichts der breiten Palette an Vorteilen sowie den grundsätzlichen Einwänden nicht beliebig weit gehen darf und gewisse Regulierungen – d.h. die Überwachung nicht-verwalteter Wallets – mangels verfassungsmässiger Kompetenzgrundlage sogar gänzlich unterlassen werden müssen. In jedem Fall muss vermieden werden, dass unter dem *Vorwand der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und anderer gewichtigen Interessen ein für Regierungen, Zentral- und Geschäftsbanken unliebsames Geld dem Publikum entzogen wird*.

Zum Ende gilt es, das eingangs im ersten Teil genannte Zitat in Erinnerung zu rufen, d.h. dass sich kaum «ein stärkerer Eingriff in die wirtschaftliche Freiheit, wie ein Verbot an die Verkäufer, ihre Waren gegen ein anderes als das vom Staat bezeichnete Gut abzulassen, […] ausdenken [lässt]». In diesem Zusammenhang kann auch das Sprichwort «Geld stinkt nicht» (lat.: [*Pecunia*] *Non olet*) nicht unerwähnt bleiben, also dass das *Augenmerk vermehrt auf die direkte Bekämpfung der genannten Delikte gerichtet werden sollte*. Eine umfassende, methodische Überwachung von Kryptogeld, wie es die Meldepflicht anstrebt, ist m.E. abzulehnen, zumal der Nutzen in keinem Verhältnis zu den Beeinträchtigungen steht. Eine überbordende Regulierung hat nicht nur Auswirkungen auf individuelle Grundrechtspositionen, sondern gefährdet auch den technologischen Fortschritt und damit die Weiterentwicklung des Finanzplatzes Schweiz. *Darüber hinaus sind zum gegenwärtigen Zeitpunkt keine effektiven und zugleich grundrechtskonforme Lösungen ersichtlich*. Die Regulierung von Kryptogeld sollte sich deshalb auf die Verhinderung von exzessiven Missbrauchsfällen konzentrieren, wozu eine Annahmeobergrenze dienlich sein kann, und ansonsten die Öffentlichkeit von den vielen Vorteilen, welche Kryptogeld bietet, profitieren lassen. Im Hinblick auf eine bessere Kontrolle von Geldwäscherei, Terrorismusfinanzierung, Steuerhinterziehung usw. könnten daher auch neue Ansätze, wie beispielweise Unexplained Wealth Orders bzw. die erleichterte Einziehung von «Vermögen unklarer Herkunft», in Betracht gezogen werden.