Zürcher Hochschule für Angewandte Wissenschaft

School of Management and Law

Modul

Masterarbeit

«Bekämpfung der Geldwäscherei auf der Blockchain»

Betreuungsperson:

Dr. Annette Althaus Stämpfli

Manuel Peduto

Matrikelnummer:

16562829

ZHAW Winterthur, Frühlingssemester 2023

Abgabetermin: 31. Mai 2023

Management-Summary

Kryptowährungen haben zweifellos eine Revolution in der Finanzwelt ausgelöst, indem sie innovative Technologien wie Blockchain nutzen, um digitale Transaktionen zu ermöglichen. Während viele Menschen die Vorteile dieser neuen Form des Geldes schätzen, existiert auch eine dunkle Seite: die Gefahr von Kryptowährungen, zur Geldwäscherei missbraucht zu werden.

Diese Arbeit untersucht im Rahmen einer qualitativ - empirischen Sekundäranalyse Kryptowährungen, ihre Funktionsweise und die Herausforderungen in Bezug auf Geldwäscherei. Dabei werden auch verschiedene Regulierungsansätze analysiert, indem die Geldwäschereigesetzgebungen in Deutschland, der Schweiz und dem Vereinigten Königreich im Hinblick auf ihre Handhabung von Kryptowährungen untersucht werden. Im Anschluss werden die gewonnenen Erkenntnisse kritisch mit den Meinungen von Experten aus verschiedenen relevanten Bereichen abgeglichen, um eine umfassendere Bewertung vornehmen zu können.

Es wird dargelegt, dass Kryptowährungen aufgrund ihrer inhärenten Eigenschaften wie Anonymität und Dezentralisierung einzigartige und neuartige Herausforderungen für Regulierungsbehörden darstellen. Dies hat weitreichende Auswirkungen auf den Kampf gegen Geldwäsche, da die traditionellen Methoden und Ansätze zur Identifizierung und Verfolgung von Geldwäscheaktivitäten oft bei Transaktionen mit Kryptowährungen an ihre Grenzen stossen. Das Versäumnis, diese neuen Herausforderungen angemessen zu adressieren, könnte es Kriminellen ermöglichen, die Lücken im gegenwärtigen regulatorischen Rahmen auszunutzen und Geldwäscheaktivitäten durchzuführen.

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	anderer Auffassung
AG	Aktiengesellschaft
AML	Anti-Geldwäsche-Gesetze
AMLD	Anti-Money Laundering Directive
ATM	Automated Teller Machine
BaFin	Bundesanstalt für Finanzdienstleistungen
BankG	Bundesgesetz vom 8. November 1934 über die Banken und Sparkassen (Bankengesetz; SR 952.0)
BBI	Bundesblatt (www.admin.ch > Bundesrecht > Bundesblatt)
BT	Besonderen Teil des Strafgesetzbuches
CDD	Customer Due Diligence
CDD	Customer Due Diligence
CEO	Chief Executive Officer
CFTC	Commodity Futures Trading Commission
CHF	Schweizer Franken
DAO	Decentralized Autonomous Organization
DeFi	Dezentrale Finanzprotokolle
DGwG	Deutsches Geldwäschegesetz
DLT	Distributed Ledger Technology
DStGB	Deutsches Strafgesetzbuch
DStPO	Deutsche Strafprozessordnung
EU	Europäische Union
EUR	Euro
FAQ	Frequently Asked Questions
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FDP	Freie Demokratische Partei
FDR	Franklin D. Roosevelt
FEDPOL	Bundesamt für Polizei
FinCEN	Financial Crimes Enforcement Network
FINMA	Eidgenössische Finanzmarktaufsicht
FIU	Financial Intelligence Unit
G7	Gruppe der Sieben

GDAX	Coinbase Digital Asset Exchange
GmeR	Geschäftsbeziehung mit erhöhten Risiken
GWG	Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz; SR 955.0)
GWV	Verordnung vom 11. November 2015 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereiverordnung; SR 955.01)
GWV-FINMA	Verordnung vom 3. Juni 2015 der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor (Geldwäschereiverordnung-FINMA; SR 955.033.0)
HSLU	Hochschule Luzern
ICO	Initial Coin Offering
Inc.	Incorporated
KGB	Komitet Gossudarstwennoi Besopasnosti (sowjetischer Geheimdienst)
KGGT	Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung
KWG	Kreditwesengesetz
KYC	Know-Your-Customer
M&A	Mergers & Acquisitions
mbH	mit beschränkter Haftung
MiCA	Markets in Crypto-Assets
MROS	Meldestelle für Geldwäscherei
NRA	National Risk Assessment
NZZ	Neue Zürcher Zeitung
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
P2P	Peer-to-Peer
PSC	People with significant control
SAR	Suspicious Activity Reporting
SDX	SIX Digital Exchange

SEC	US Securities and Exchange Commission
SEPA	Single Euro Payments Area
SIX	Swiss Infrastructure and Exchange
SOCA	Serious Organised Crime Agency
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFR	Transfer of Funds and certain Crypto-Assets
UK	United Kingdom
UNO	United Nations Organization
USB	Universal Serial Bus
USD	US Dollar
VASP	Virtual Asset Service Provider
VW-HSG	Institut für Versicherungswirtschaft Universität St. Gallen
WZG	Bundesgesetz über die Währung und die Zahlungsmittel vom 22. Dezember 1999 (SR 941.10)

Literaturverzeichnis

ACKERMANN JÜRG-BEAT, Geldwäscherei – Money Laundering – Eine vergleichende Darstellung des Rechts der Erscheinungsformen in den USA und der Schweiz, Diss., Universität Zürich, 1992 (zit. Ackermann, Diss.).

ALLISON IAN, Crypto 'Gray' Markets Could Be Unintended Consequence of FATF Travel Rule, coindesk.com 21. Mai 2020, <https://www.coindesk.com/policy/2020/05/21/crypto-gray-markets-could-be-unintended-consequence-of-fatf-travel-rule/>, besucht am 13. April 2023 (zit. Sunrise Problem).

ALLISON IAN, Crypto Firms Establish Messaging Standard to Deal With FATF Travel Rule, coindesk.com 7. Mai 2020, <https://www.coindesk.com/policy/2020/05/07/crypto-firms-establish-messaging-standard-to-deal-with-fatf-travel-rule/>, besucht am 15. Mai 2023 (zit. Messaging Standard).

ALOOSH ARASH/LI JIASUN, Direct Evidence of Bitcoin Wash Trading, Mont-Saint-Aignan/ Fairfax, 2022.

AMRIT KUMAR/ FISCHER CLÉMENT/TOPLE SHRUTI/SAXENA PRATEEK, A Traceability Analysis of Monero's Blockchain in: Computer Security – ESORICS 2017, Vol. 10493, Cham 2017.

ANDROULAKI ELLI/ KARAME GHASSAN / ROESCHLIN MARC/SCHERER TOBIAS/ CAPKUN, Evaluating User Privacy in Bitcoin, in: Financial Cryptography and Data Security, Financial Cryptography and Data Security, 17th International Conference, FC 2013, Okinawa 2013, S. 34-51.

ANG CARMEN, Comparing Bitcoin's Market Cap to Other Cryptocurrencies, Visual Capitalist 13. Januar 2021, <https://www.visualcapitalist.com/bitcoin-market-cap-compared-to-crypto/>, besucht am 11. Dezember 2022.

BASE DETLEV MICHAEL, Kommentar zu Art. 1 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar, Bern 2017.

BASLER ANDRÉ, HSLU, Market Manipulation and Insider Trading in Switzerland – an overview* (Part I), HSLU 2018, <https://hub.hslu.ch/economiccrime/market-

manipulation-and-insider-trading-in-switzerland-an-overview-part-i/>, besucht am 28. Januar 2023.

BECKER GARY S., Crime and Punishment: An Economic Approach, Journal of Political Economy 1968, Vol. 76, No. 2, S. 169-217.

BERENTSEN ALEKSANDER/SCHÄR FABIAN, Bitcoin, Blockchain und Kryptoassets, Eine umfassende Einführung, Basel 2017.

BERNASCONI PAOLO, Finanzunterwelt – Gegen Wirtschaftskriminalität und organsiertes Verbrechen, Zürich 1988.

BILLE MARTIN/ SPINDLER GERALD, Rechtsprobleme von Bitcoins als virtuelle Währung, Zeitschrift für Wirtschafts- und Bankrecht 2014, S.1357 ff.

Bitcoin, <https://bitcoin.org/de/>, besucht am 11. Dezember 2022 (zit. Homepage).

Bitfinexed, Wash Trading Bitcoin Part II: Who and why is someone wash trading on Bitfinex?, Medium 2017, <://bitfinexed.medium.com/wash-trading-bitcoin-part-ii-who-and-why-is-someone-wash-trading-on-bitfinex-e1c7b5e0b3bb>, besucht am 29. Januar 2023 (zit. Bitfinexed).

Bitrates, Fungibility, TERMINOLOGY, bitrates.com, <https://www.bitrates.com/guides/terminology/fungibility>, besucht am 15. April 2023.

BRENIG CHRISTIAN/ACCORSI, RAFAEL/MÜLLER GÜNTER, Economic Analysis of Cryptocurrency Backed Money Laundering, Freiburg 2015.

BRUNONE MATTEO/MOLO GIOVANNI, Kryptowährungen im Visier der staatlichen Kontrolle, Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht 2022, S. 299-308.

Bundesanstalt für Finanzdienstleistungsaufsicht, Geldwäscherechtliche Hinweise für Institute, die das Kryptoverwahrgeschäft erbringen, als Neu-Verpflichtete nach dem Geldwäschegesetz (GwG), 14. Mai 2020, besucht am 15. April 2023 <https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Auslegungsentscheidung/A/ae_200512_krypto_gw.html;jsessionid=78A870D1CCED92E30342D88E33701500.2_cid501?nn=13733456>, besucht am 15. April 2023 (zit. BaFIN-Geldwäscherechtliche Hinweise).

Bundesanstalt für Finanzdienstleistungsaufsicht, Pressemitteilung, BaFin setzt Verbot binärer Optionen für Kleinanleger in Deutschland fort, 1. Juli 2019 <https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Pressemitteilung/2019/pm_190601_Verbot_binaere_Optionen.html>, besucht am 15. April 2023 (zit. BaFin-Pressemittelung 2019).

CFTC, Fall Nr. 8369-21, CFTC Orders Coinbase Inc. to Pay $6.5 Million for False, Misleading, or Inaccurate Reporting and Wash Trading, 19. März 2021,<https://www.cftc.gov/PressRoom/PressReleases/8369-21#:~:text=The%20order%20requires%20Coinbase%20to,or%20CFTC%20regulations%2C%20as%20charged>, besuch am 6. Februar 2023 (zit. CFTC Coinbase).

CHATTERJEE POULOMI, Public vs private blockchains: How do they differ, What are public blockchains?, Analyticsindiamag 16. Februar 2022, <https://analyticsindiamag.com/public-vs-private-blockchains-how-do-they-differ/>, besucht am 28. Januar 2023 (zit. What are public blockchains?).

Companies House, People with significant control (PSC) discrepancy reporting service, <https://www.lawscot.org.uk/media/372665/companies-house-psc-discrepancy-reporting-information-apr-2022.pdf>, besucht am 15. April 2023 (zit. PSC).

Comply Advantage, Neudefinition der Geldwäsche in Deutschland: § 261 und seine Auswirkungen, complyadvantage.com 29. März 2022, <https://complyadvantage.com/de/insights/neudefinition-der-geldwaesche-in-deutschland-sektion-261-und-seine-auswirkungen/#:~:text=Der%20Straftatbestand%20der%20Geldw%C3%A4sche%20nach,%3A%20Geldw%C3%A4schegesetz)%20grundlegend%20neu%20geregelt.>, besucht am 15. April 2023 (zit. Neudefinition der Geldwäsche in Deutschland).

CONG LIN WILLIAM/ LI XI/ TANG KE/YANG YANG, Crypto Wash Trading, National Bureau of Economic Research, Working Paper Series, Working Paper 30783, 2022.

Cryptopeida Staff, Digital Assets: Cryptocurrencies vs. Tokens, What Is a Digital Asset?, Gemini 28. Juni 2022,

<https://www.gemini.com/cryptopedia/cryptocurrencies-vs-tokens-difference>, besucht am 28. Januar 2023 (zit. What Is a Digital Asset?).

DE NIKHILESH, FinCEN's Proposed Crypto Wallet Rule Might Hit DeFi, coindesk.com 23. Dezember 2020, <https://www.coindesk.com/policy/2020/12/23/fincens-proposed-crypto-wallet-rule-might-hit-defi/>, besucht am 13. April 2023 (zit. FinCEN's Wallet Rule).

DORIT RON/SHAMIR ADI, Quantitative Analysis of the Full Bitcoin Transaction Graph, in: Financial Cryptography and Data Security, 17th International Conference, FC 2013, Okinawa 2013.

DRZALIC JANA JOHANNA/MOLO GIOVANNI, Können Kryptowährungen compliant sein?, Aktuelle Juristische Praxis 2019, S. 40-57.

EDMONDS TIM, Money Laundering Law, House of Commons Library, Briefing Paper, N. 2592, 14. February 2018.

EGLOFF PASCAL/TURNES ERNESTO, Blockchain für die Praxis, Kryptowährungen, Smart Contracts, ICOs und Tokens, St. Gallen 2019.

Egmont Group of Financial Intelligence Units, <https://egmontgroup.org/>, besucht am 7. Februar 2023 (zit. Egmont Group FIU).

Europäisches Parlament, Crypto assets: deal on new rules to stop illicit flows in the EU, Pressemitteilung vom 29. Juni 2022, <https://www.europarl.europa.eu/news/en/press-room/20220627IPR33919/crypto-assets-deal-on-new-rules-to-stop-illicit-flows-in-the-eu>, besucht am 13. Mai 2023 (zit. Pressemitteilung TFR-Entwurf).

Europäisches Parlament, Crypto-assets: green light to new rules for tracing transfers in the EU, Pressemitteilung vom 20. April 2023, <https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu>, besucht am 18. Mai 2023 (zit. Pressemitteilung TFR-Entscheid).

FATF, "Black and grey" lists, FATF 2023, <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>, besucht am 6. Februar 2023 (zit. FATF, Black and grey lists).

FCA, FCA establishes Temporary Registration Regime for cryptoasset businesses, fca.org.uk 16. Dezember 2020, <https://www.fca.org.uk/news/press-releases/fca-establishes-temporary-registration-regime-cryptoasset-businesses>, besucht am 15. April 2023 (zit. Register).

FCA, FCA Warning List of unauthorised firms, fca.org.uk 3. April 2004, <https://www.fca.org.uk/consumers/warning-list-unauthorised-firms>, besucht am 15. April 2023 (zit. Warnung).

FCA, Money Laundering Regulations, fca.org.uk 23. Dezember 2019, <https://www.fca.org.uk/firms/financial-crime/money-laundering-regulations>, besucht am 24. April 2023 (zit. Money Laundering Regulations)

Federal Reserve Bank of St. Louis, Functions of Money – The Economic Lowdown Podcast Series, <https://www.stlouisfed.org/education/economic-lowdown-podcast-series>, besucht am 14. Januar 2023.

FEDPOL, Geldwäscherei, Meldestelle für Geldwäscherei (MROS), <https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei.html>, besucht am 7. Februar 2023 (zit. MROS).

FERWERDA JORAS, The Effectiveness of Anti-Money Laundering Policy: A Cost-Benefit Perspective in: King/ C.,Walker/C., Gurulé, J. (Hrsg.), The Palgrave Handbook of Criminal and Terrorism Financing Law, Cham 2018.

FinCEN, FinCEN Extends Comment Period for Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions, Office of Strategic Communications, 703-905-3770, 14. Januar 2021, <https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering>, besucht am 13. April 2023 (zit. Extends Comment Period).

FinCEN, What We Do,<https://www.fincen.gov/what-we-do>, besucht am 7. Februar 2023 (zit. What we do).

FINLEY KLINT, A $50 Million Hack Just Showed That the DAO Was All Too Human, Wired 18. Juni 2016, <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/>, besucht am 28. Januar 2023 (zit. DAO).

FINMA, Aufsichtsmitteilung: Konsequente Geldwäschereibekämpfung im Blockchain-Bereich vom 26. August 2019, <https://www.finma.ch/de/news/2019/08/20190826-mm-kryptogwg/> (zit. Medienbericht der FINMA-Aufsichtsmitteilung 2019), besucht am 6. Februar 2023.

FINMA, Entwicklungen im Bereich Fintech, aus dem Jahresbericht 2018, <https://www.finma.ch/de/dokumentation/dossier/dossier-fintech/entwicklungen-im-bereich-fintech/>, besucht am 15. April 2023 (zit. FINMA-Entwicklung 2018).

FRANKENFIELD JAKE, Difficulty Bomb: Ethereum's Increasing Difficulty in Mining, investopedia.com April 2022, <https://www.investopedia.com/terms/d/difficulty-bomb.asp> besucht am 15. April 2023.

Generalzolldirektion, Financial Intelligence Unit, Fachliche Informationen, zoll.de, <https://www.zoll.de/DE/FIU/Fachliche-Informationen/fachliche-informationen_node.html>, besucht am 15. April 2023 (zit. Zoll FIU).

GOSCHENKO SERGIO, Marathon Mines First OFAC Compliant Bitcoin Block, Bitcoin.com 2021, <https://news.bitcoin.com/marathon-mines-first-ofac-compliant-bitcoin-block/>, besucht am 6. Februar 2023.

GRECO SERGIO/KRAMER STEFAN, Das Schweizerische Bankgeschäft, Teil 7: Zahlungsverkehr und Zahlungsmittel, Zürich 2021, S. 713-734.

GRIFFIN JOHN M./SHAMAS AMIN, Is Bitcoin Really Untethered?, The Journal of Finance, 2020, Volume 75, S. 1775-2321.

GRUHNWALD SYLKE/ HOSTETTLER OTTO/ STARK ALEXANDRA, «LAUNDROMAT», Geldwäsche: Die Schweiz als Drehscheibe, Beobachter 2017,<https://www.beobachter.ch/wirtschaft/geldwasche-die-schweiz-als-drehscheibe-39588>, besucht am 29. Januar 2023.

HARDING LUKE, Deutsche Bank faces action over $20bn Russian money-laundering scheme, The Guardian 2019, <https://www.theguardian.com/business/2019/apr/17/deutsche-bank-faces-action-over-20bn-russian-money-laundering-scheme>, besucht am 29. Januar 2023.

HARKIN CHRISTIE, Bitcoin Miner Marathon Will No Longer Censor Transactions, CEO Says, coindesk.com 31. Mai 2021, <https://www.coindesk.com/tech/2021/05/31/bitcoin-miner-marathon-will-no-longer-censor-transactions-ceo-says/>, besucht am 6. Februar 2023.

HAWKINS FIONA, Stämpflis Handkommentar, Geldwäschereigesetz (GwG), GwG 2a, Art. 2a / I. - II., 1. Auflage, Bern 2017.

HEGER MARTIN, Kommentar zu DStGB, § 261 DStGB, 30. Auflage, Berlin 2023.

History.com, FDR takes United States off gold standard, History.com 24. November 2009, <https://www.history.com/this-day-in-history/fdr-takes-united-states-off-gold-standard>, besucht am 14. Januar 2023 (zit. Gold Standard).

IKEMEYER RAPHAEL/KRIMPHOVE DIETER, Geldwäsche: Tatbestände, Aufgriffsmöglichkeiten, Indizien im Zahlungs- und Kapitalmarkt, Compliance Berater 2022, 432-435.

JEFFRIES ADRIANNE, Inside the bizarre upside-down bankruptcy of Mt. Gox, theverge.com/ 22. März 2018, <https://www.theverge.com/2018/3/22/17151430/bankruptcy-mt-gox-liabilities-bitcoin>, besucht am 15. April 2023.

KAISER PHILIPPE J.A./MÜLLER LUKAS/REUTLINGER MILENA, Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union, Zeitschrift für Europarecht, 20. Jahrgang, Nr. 3 Mai 2018, S. 80-102.

KAKUSCHKE NICK, Grundlagen der Kryptografie und symmetrischer Verschlüsselung, ccecosystems.news 27. März 2023, <https://ccecosystems.news/grundlagen-der-kryptografie-und-symmetrischer-verschluesselung/>, besucht am 15. April 2023.

Kanton Zug, Kryptowährungen Bezahlung Steuern, <https://www.zg.ch/behoerden/finanzdirektion/steuerverwaltung/zahlen-mit-kryptowaehrungen>, besucht am 15. April 2023 (zit. Kryptowährungen Bezahlung Steuern).

KIELY JOE, Understanding the EU's 6AMLD and the risk to your business, cointelegraph 18. Oktober 2022, <https://cointelegraph.com/news/understanding-the-eu-s-6amld-and-the-risk-to-your-business>, besucht am 6. Februar 2023.

KÖLLING MARTIN, Die Geschichte des Bitcoin,Eine Pleite führte zum globalen Durchbruch, Handelsblatt 30. Juli 2017, <https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/die-geschichte-des-bitcoin-eine-pleite-fuehrte-zum-globalen-durchbruch/20104424-all.html>, besucht am 11. Dezember 2022.

LANDERER NINO, Pauschale Kritik an Kryptowährungen ist deplatziert, NZZ Nr. 248 24.10.2022, S. 25.

LEVI MICHAEL/REUTER PETER, Money Laundering, Crime and Justice, Vol. 34, Nr. 1 2006, S. 289-375.

MAEDER RUEDI, EU gibt sich mit MiCA einen Rechtsrahmen für den Kryptomarkt, moneytoday.ch 24. April 2023, <https://www.moneytoday.ch/news/eu-gibt-sich-mit-mica-einen-rechtsrahmen-fuer-den-kryptomarkt#:~:text=EU%2DParlament%20und%20Rat%20haben,Verordnung%202024%20in%20Kraft%20treten.> besucht am 18. Mai 2023 (zit. MiCA).

MANTEL BRIAN/MCHUGH TIMOTHY, Competition and Innovation in the Consumer e-Payments Market? Considering the Demand, Supply, and Public Policy Issues, Federal Reserve Bank of Chicago Publicy Working Paper, Chigaco 2001.

MASCIANDARO DONATO, Money Laundering: the Economics of Regulation, European Journal of Law and Economics 1999, 7 (3), S. 225 – 240.

MEIKLEJOHN SARAH/ POMAROLE MARJORI/ JORDAN GRANT/ LEVCHENKO KIRILL/ MCCOY DAMON/VOELKER GEOFFREY M./ SAVAGE STEFAN, A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, Communications of the ACM, Vol. 59, A. 4, 2016, S. 86–93.

MONNERAT LUCIEN, «Krypto-Banken», Eine Übersicht der Lizenzpflichten nach dem Bankengesetz bei Entgegennahme von Kryptozahlungsmitteln für Kundenkonti mit besonderer Beurteilung der FinTech-Bewilligung nach Art. 1b BankG, Zürich 2022.

MONNERAT LUCIEN, Einleitung - I. Gegenstand der Kryptowährungen, «Krypto-Banken», IMPULSE - Impulse zur praxisorientierten Rechtswissenschaft, Zürich 2022.

MOSER MALTE et al., An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, S. 143–63.

MÜLLER CHRISTOF, Geldwäscherei – Motive, Formen, Abwehr: eine betriebswirtschaftliche Analyse, Diss., Uiversität St. Gallen, 1992.

MÜLLER LUKAS/ONG MALIK, Aktuelles zum Recht der Kryptowährungen, Aktuelle Juristische Praxis 2020, S. 198-212.

NEUHEUSER, Münchener Kommentar zum DStGB, § 261 DStGB, 4. Auflage, München 2021.

NJUGUNA BRIAN, Police Search of South Korean Coinbit Crypto Exchange Finds 99% Trade Volume Manipulation, Blockchain.News 2020,< https://blockchain.news/news/police-south-korean-coinbit-crypto-exchange-99-trade-volume-manipulation>, besucht am 30. Januar 2023.

Nova, Ancient Worlds, The History of Money, PBS 26. Oktober 1996, <https://www.pbs.org/wgbh/nova/article/history-money/>, besucht am 14. Januar 2023.

PALMER DANIEL, South Korean Crypto Exchange Coinbit Raided Over Allegations of Wash Trading: Report, CoinDesk 2020, <https://www.coindesk.com/markets/2020/08/26/south-korean-crypto-exchange-coinbit-raided-over-allegations-of-wash-trading-report/>, besucht am 29. Januar 2023.

PETRY HEIKO, Währung oder nicht? Eine Einordnung und Definition von Bitcoin, I. VW-HSG Trendmonitor 2017, 2 ff.

PIETH MARK, Strafrecht BT, Basel 2014 (zit. Pieth, BT).

POST KOLLEN, An 'OFAC-compliant' bitcoin miner revives debate about transaction censorship, theblock.co 8. Mai 2021, <https://www.theblock.co/post/104263/an-ofac-compliant-bitcoin-miner-revives-debate-about-transaction-censorship>, besucht am 6. Februar 2023.

REIFF NATHAN, Bitcoin vs. Ethereum: What's the Difference?, Investopedia 4. Oktober 2022, <https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp>, besucht am 14. Januar 2023.

REVOREDO TATIANA, MiCA und TFR: Ein ausführlicher Blick auf die Krypto-Regulierung der EU, cointelegraph.com 17. Juli 2022, <https://de.cointelegraph.com/news/mica-and-TFR-the-eu-moves-to-regulate-the-crypto-asset-market>, besucht am 13. Mai 2023 (zit. MiCA und TFR).

River Financial, Understanding Bitcoin Fungibility, river.com, <https://river.com/learn/bitcoin-fungibility/>, besucht am 15. April 2023 (zit. Bitcoin Fungibility).

SATW, Digital Assets und Kryptowährungen Cybersecurity – Herausforderungen für die politische Schweiz, September 2020.

SCHERP DIRK/ WROCKLAGE FELIX, Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche tritt in Kraft, Compliance Berater 202, S. 186-190.

SCHMIDT NIKLAS, Kryptowährungen und Blockchains Technologie, Praxis, Recht, Steuern, Wien 2019.

SCHOLL A., Die Befragung. UVK Verlagsgesellschaft mbH: Konstanz 2018.

Square, Inc., Square, Inc.'s Federal Comment Letter Regarding FinCEN's Proposed Rulemaking on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, squareup.com 4. Januar 2021, <https://squareup.com/gb/en/press/fincen-letter>, besucht am 13. April 2023 (zit. Federal Comment Letter).

TOMIC IVAN/MAUCHLE YVES, Neue Regulerung von Kryptowerten in der EU mit TFR und MiCA – ein Modell für die Schweiz?, e.foresight und Baker McKenzie, 21.11.2022.

TRECHSEL STEFAN/PIETH MARK, Kommentar zu Art. 305bis StGB, in: Trechsel Stefan/Pieth Mark (Hrsg.), Schweizerisches Strafgesetzbuch Praxiskommentar, 3. Aufl., Zürich 2018.

TROST ANDREA, Kaufpreiszahlungen in Kryptowährungen im M&A-Bereich / AML- und GwG-Themen, Anwaltsrevue: Das Praxismagazin des schweizerischen Anwaltsverbandes 2022, S. 206-208.

U.S. Department of the Treasury, Office of Foreign Assets Control - Sanctions Programs and Information, <https://home.treasury.gov/policy-issues/office-of-

foreign-assets-control-sanctions-programs-and-information>, besucht am 6. Februar 2023 (zit. U.S. Department of the Treasury, OFAC).

WARREN JONATHAN, Why is the UK so successful in fintech?, ftadviser.com 30. Januar 2023, <https://www.ftadviser.com/investments/2023/01/30/why-is-the-uk-so-successful-in-fintech/#:~:text=Setting%20aside%20the%20fintech%20scene,be%20a%20global%20financial%20centre>, besucht am 13. April 2023 (zit. UK's fintech).

WHITAKER BILL, SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments, Cbsnews.com 4. Juli 2021, <https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-07-04/>, besucht am 13. April 2023 (zit. Solar Winds).

WRONKA CHRITOPH, Anti-money laundering regimes: a comparison between Germany, Switzerland and the UK with a focus on the crypto business, Journal of Money Laundering Control, Vol. 25 No. 3, 2022 S. 656-670.

YERMACK DAVID, Is Bitcoin a Real Currency? An Economic Appraisal, in: David Lee Kuo Chen (Hrsg.), Handbook of Digital Currency, Singapur 2015, 31 ff.

ZÜND ANDRE, Geldwäscherei: Motive – Formen – Abwehr, Schweizer Treuhänder 1990.

Materialienverzeichnis

Bericht der International Bank for Reconstruction and Development / the World Bank, Distributed Ledger Technology (DLT) und Blockchain, FinTech Note – Nr. 1 vom 01. Januar 2017 (zit. World Bank, DLT).

Bericht des Bundesrates zu rechtlichen Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz Eine Auslegeordnung mit Fokus auf dem Finanzsektor vom 14. Dezember 2018 (zit. DLT-Auslegeordnung).

Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.36687) und Weibel (13.4070) vom 25. Juni 2014 (zit. Bericht des Bundesrates zu virtuellen Währungen).

Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierung in der Schweiz – Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), Juni 2015 (zit. NRA-Bericht).

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17. Juni 1996, BBI III1101 (zit. Botschaft GwG 1996).

Deutscher Bundestag, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Frank Schäffler, Christian Dürr, Dr. Florian Toncar, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/10417, Europäische Gesetzesinitiativen zu Kryptoassets. 24. Juni 2019 (zit. Europäische Gesetzesinitiativen zu Kryptoassets).

Eidgenössisches Finanzdepartement, Faktenblatt, Blockchain und Crypto-Assets im Finanzsektor: Vorreiterrolle der Schweiz auf internationaler Ebene vom 21. Januar 2022 (zit. Faktenblatt Krypto).

Europäisches Parlament, Provisional Agreement Resulting from Interinstitutional Negotiations, Proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) (COM (2021)0442 – C9-0341/2021 – 2021/0241(COD)) vom 5. Oktober 2022 (zit. TFR-Entwurf).

FATF, 12-Month Review of the revised FATF Standards on Virtual Assets and Virtual Asset Services Providers, Juni 2021 (zit. FATF-12-Month Review).

FATF, Aktualisierter Leitfaden für einen risikobasierten Ansatz für virtuelle Vermögenswerte und Anbieter von virtuellen Vermögensdienstleistungen vom 28. Oktober 2021 (zit. FATF aktualisierter Leitfaden für virtuelle Vermögenswerte).

FATF, Ergebnisse der FATF-Plenartagung vom 16. – 21. Juni 2019 (zit. FATF-Ergebnisse 2019).

FATF, Massnahmen zur Bekämpfung der Geldwäscherei und der Finanzierung von Terrorismus und Proliferation in der Schweiz, Evaluationsbericht der Schweiz 2016, (zit. FATF-Bericht über die Schweiz).

FATF, Nachfolgebericht über die Schweiz von Januar 2020 (zit. FATF-Ergebnisse 2020).

FEDPOL, Meldestelle für Geldwäscherei (MROS), Jahresbericht 2020 vom Mai 2021(zit. MROS).

His Majesty's Treasury, UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: in title heading: Response to the consultation and call for evidence, April 2022 (zit. UK regulatory approach).

National Crime Agency, UK Financial Intelligence Unit Suspicious Activity Reports Annual Report 2020 (zit. SARs Annual Report 2020).

1 Einleitung

Der Sammelbegriff *Kryptowerte*, auch *Krypto-Assets* genannt, steht für digitale Vermögenswerte, die grösstenteils auf einer dezentral organisierten Blockchain abgebildet werden. Unter diesem Sammelbegriff werden nicht nur Kryptowährungen, sondern auch andere digitale Token subsumiert, welche in der Lage sind, Rechte (z. B. Aktien)[1] oder Realwerte (z. B. Uhren)[2] abzubilden. Satoshi Nakamotos Konzept[3] einer reinen Peer-to-Peer-Version von elektronischem Geld basierte auf der Idee, Online-Zahlungen direkt von einer Partei zur anderen zu senden – ohne Umweg über ein Finanzinstitut.[4] Was lediglich als Idee für eine digitale Finanzwelt begann, rückt mittlerweile sogar bei institutionellen Anlegerinnen und Anlegern immer mehr in den Fokus als alternative Anlagemöglichkeit. Dieses Interesse kommt zu der meist starken Unterstützung durch Privatanleger/-innen hinzu. Mit diesem rasanten Wachstum kommt es zu diversen komplexen operativen und regulatorischen Herausforderungen, welche die Krypto- und Digital-Asset-Märkte durch die zunehmende Geschwindigkeit des technologischen Fortschritts weiter verschärfen,[5] z. B. in folgenden Bereichen: dezentralisierte Finanzen (DeFi), Tokenisierung, Blockchain und Distributed-Ledger-Technologie (DLT).

[1] Die Schweizer Börse hat hierzu eine vollständig integrierte Handelsplattform für digitale Vermögenswerte entwickelt. Die neue Börse trägt den Namen SIX Digital Exchange (SDX) und basiert auf der Technologie des Distributed Ledgers; siehe https://www.sdx.com/ aufgerufen am 21. November 2022.

[2] So hat das Schweizer Familienunternehmen Bucherer, einer der weltweit grössten Retailer für luxuriöse Uhren und Schmuck, das Zürcher Startup Adresa AG übernommen. Die Adresta AG hat einen fälschungssicheren Eigentums- und Echtheitsnachweis für Uhren entwickelt; siehe https://www.itreseller.ch/Artikel/97071/Bucherer_uebernimmt_Adresta.html aufgerufen am 21. November 2022.

[3] KÖLLING (Bitcoins Geschichte), Satoshi Nakamoto ist der Schöpfer von Bitcoin. Auch wenn die Identität der Person, die sich hinter dem Pseudonym Satoshi Nakamoto verbirgt, immer noch unbekannt ist, wird allgemein anerkannt, dass das Papier eine direkte Reaktion auf das zentralisierte, fehlerhafte Finanzsystem war, das zu der Krise führte.

[4] Bitcoin, Video, Was ist Bitcoin?, (Homepage).

[5] MONNERAT, S. 3.

1.1 Forschungsziel und Aufbau der Arbeit

Das Ziel dieser Masterarbeit ist es, die zentralen Compliance-Grundlagen bei Krypto-Investitionen greifbar zu machen, da bezüglich der *Aufsicht* und *Geldwäsche* im Zusammenhang mit Kryptowährungen weltweit Klärungsbedarf besteht.

Dazu wird die Arbeit in folgende Kapitel unterteilt:

Im ersten Teil der vorliegenden Masterarbeit werden Kryptowährungen im Allgemeinen, ihre Funktionsweise und die Herausforderungen thematisiert, die in Bezug auf Geldwäscherei bestehen. Die Erkenntnisse werden im zweiten Teil auf unterschiedliche Regulierungsansätze angewendet. Dazu werden die Geldwäschereigesetzgebungen in Deutschland, der Schweiz und dem Vereinigten Königreich in Bezug auf ihre Handhabung im Umgang mit Kryptowährungen untersucht. Abschliessend werden die Erkenntnisse, welche zur Beantwortung der nachfolgenden Forschungsfragen benötigt werden, mit den Meinungen verschiedener Personen mit Expertise kritisch beurteilt. Die daraus resultierenden Empfehlungen werden schliesslich im Hinblick auf ihre praktische Umsetzungsmöglichkeit geprüft.

1.2 Forschungsfragen

Vor dem Hintergrund der beschriebenen Ausgangslage und des Forschungsziels soll in dieser Masterarbeit eine praktische Anleitung zu den operativen Compliance-Grundlagen für Krypto-Assets erarbeitet werden.

Dazu wird folgenden Forschungsfragen nachgegangen:

- *Besitzen Kryptowährungen ein höheres Geldwäscherei-Risiko und worin liegen die Gründe dafür?*

- *Genügen die aktuellen gesetzlichen Grundlagen oder benötigt es Anpassungen?*

- *Wie lassen sich die Risiken im Zusammenhang mit Kryptowährungen aus der Geldwäscherei-Prävention mitigieren?*

1.3 Abgrenzungen

In dieser Masterarbeit sollen Kryptowährungen im Allgemeinen untersucht werden – einschliesslich ihrer Funktionsweise und der Herausforderungen im Zusammenhang mit Geldwäsche. Es wird auch der Frage nachgegangen, wie die Gesetzgebung das System durch die Kontrolle von Geldwäsche und die Förderung der Stabilität des Staates schützt und wie in den Gesetzen die neue revolutionäre Form der digitalen Währung vernachlässigt wurde.

Da jedoch ein Mangel an konkreten Statistiken über den Missbrauch von Kryptowährungsguthaben besteht, werden in dieser Arbeit die regulatorische und rechtliche Debatte über Kryptowährungen und blockchainbasierte Produkte fokussiert. Die Forschung bezieht sich insbesondere auf die Gesetze zur Geldwäschereibekämpfung (Anti money laundering, AML), welche die Verbindung zu neuen Währungsgeschäften herstellen, und deren Wirksamkeit bei der Kontrolle oder Unterstützung. Die Fallstudien dienen als Modelle, um die Grenzen der Staaten und ihre Auswirkungen auf ihre Gesetze zu untersuchen.

Es ist zu beachten, dass diese Masterarbeit keine Überprüfung im technischen Sinn darstellt und dass die Informationen über Algorithmen und Berechnungen nicht kritisch überprüft wurden. Ausserdem werden die Initial Coin Offering- (ICO) und Steuerthematiken nicht berücksichtigt, da dies den Rahmen dieser Arbeit überschreiten würde. Aufgrund der vielfältigen Erscheinungsformen einzelner Kryptowährungen beschränkt sich diese Arbeit auf das Grundprinzip, auf welchem Kryptowährungen basieren, und es wird nicht auf einzelne Währungen eingegangen.

1.4 Forschungsansatz und Methodik

Um die Forschungsfragen beantworten und das Forschungsziel erreichen zu können, werden verschiedene Vorgehensweisen angewendet. Als primäre Untersuchungsform dient in dieser Masterarbeit die Sekundäranalyse. Im Sinne dieser Untersuchungsform wird eine rechtsdogmatische Analyse durchgeführt, welche primär die Auswertung von Primärquellen wie Gesetzgebung und Materialien (Botschaften, erläuternde Dokumente etc.) sowie die Auswertung von in Sekundärquellen publizierter wissenschaftlicher Fachliteratur und Fachartikel umfasst. Zur Sekundäranalyse gehört neben der rechtsdogmatischen auch die rechtspolitische Analyse, um aktuelle Meinungen mit einbeziehen zu können. Des Weiteren sollen zwei Experteninterviews Aufschluss über den Status quo der Bankinstitute geben. Experteninterviews zählen als strukturiertere Variante des Leitfadeninterviews zu den qualitativen Forschungsmethoden. Im Fokus steht hierbei weniger die befragte Person. Vielmehr wird auf die Betrachtungs- und Vorgehensweise der Expertinnen und Experten im Zusammenhang mit deren Fachgebiet abgezielt. Schliesslich sollen durch das Zusammenführen der extrahierten Informationen der verschiedenen Methoden die Forschungsfragen beantwortet werden bzw. das Forschungsziel soll in einer anschaulichen Darstellung im interdisziplinären Kontext erreicht werden.

2 Krypto-Assets

In den folgenden Abschnitten werden die modernen operativen Mechanismen hinter Krypto-Technologien analysiert.

2.1 Krypto-Assets

Für Kryptowerte bzw. Krypto-Assets, welche oft als *Kryptos* abgekürzt werden, existiert in der Literatur noch keine allgemeingültige Definition.[6] Hierfür eine Definition zu finden, gestaltet sich insofern als Herausforderung, als sich das gesamte Krypto-Ökosystem rasant weiterentwickelt.[7] Diese Entwicklung betrifft diverse Bereiche. Neue Technologien führten zu Fortschritten hinsichtlich der zugrunde liegenden Fähigkeiten, der Art und Weise, wie solche Währungen jeweils gespeichert und gehandelt werden, sowie in Bezug auf technische Anwendungsmöglichkeiten. Aus Sicht der Kapitalmärkte ist der Gegenwert, der in Kryptowährungen investiert wurde, in den letzten Jahren exponentiell angestiegen, was zu zahlreichen Fortschritten bezüglich der Art und Weise geführt hat, wie Kryptowährungen gewinnbringend eingesetzt werden können – u. a. wurden vermehrt Plattformen für das profitable Verleihen von Kryptowährungen gegründet.[8] Die Mehrheit der Menschen assoziiert den Begriff *Kryptowährung* mit *Bitcoin*, zumal dieser neuartigen Währung aufgrund der grössten Gesamtkapitalisierung im Markt der Kryptowährungen die meiste mediale Aufmerksamkeit zufliesst. Jüngsten Schätzungen zufolge hat Bitcoin eine Kapitalisierung von etwa 650 Milliarden USD, was etwa 67 % der Gesamtkapitalisierung der Kryptowerte weltweit ausmacht.[9] Folglich bildet der Bitcoin eine der bedeutendsten Kryptowährungen und dennoch handelt es nur um eine Kryptowährung im Krypto-Ökosystem, welches sich ständig weiterentwickelt, wächst und neue Optionen hervorbringt. Aber was genau ist eine Kryptowährung?

Als Kryptowährung werden in dieser Masterarbeit jegliche Formen von Währungen bezeichnet, welche nur digital existieren und in der Regel nicht durch zentrale Ausgabe- oder Regulierungsbehörden herausgegeben, sondern durch ein dezentrales System verwaltet werden, um Transaktionen aufzuzeichnen und die Ausgaben neuer Einheiten

[6] MONNERAT, S. 4f.

[7] BRUNONE /MOLO, S. 300; MONNERAT, S. 4.

[8] BRUNONE /MOLO, S. 300.

[9] ANG, The Briefing; BRUNONE /MOLO, S. 299.

zu verwalten.[10] Die Technologie basiert hierbei meist auf Kryptografie, um Fälschungen und betrügerische Transaktionen zu verhindern.[11] Die nachfolgend verwendete Definition in Anlehnung jener des Bundesrates besagt, dass Kryptwährungen nur digital existieren und folglich nichts sind, was in der realen Welt physisch gehaltet oder angefasst werden kann. Das Gegenstück zu Kryptowährungen bilden demnach nichtdigitale Vermögenswerte wie Papiergeld oder physische Münzen.

2.2 Traditionelle Definition von Geld

Historisch betrachtet existierten vor Kryptowährungen zwei grosse Kategorien von **Geldmittel**: zum einen ***repräsentatives Geld***, welches als Zertifikat diente, um den Gegenwert in einen tatsächlichen, physischen Rohstoff eintauschen zu können. Beispielhaft sind Papiergeld oder Münzen zu nennen – beides kann bei einer Zentralbank gegen Gold eingetauscht werden. Damit stellte das Geld oder die Münze einen repräsentativen Platzhalter für den Besitz von Gold dar. Die Vereinigten Staaten hielten z. B. lange Zeit an einem Goldstandard fest. Im Juni 1933 wurde der Goldstandard jedoch aufgrund der durch die Weltwirtschaftskrise verursachten Goldhortung aufgegeben.[12] Die Übergangsära endete schliesslich im August 1971, als die Vereinigten Staaten ihre Währung nicht mehr in Gold umtauschten.

Geld, welches nicht mehr durch eine Ware gedeckt ist, bildet die zweite grosse Kategorie, die als ***Fiat-Geld*** bekannt ist. Sie wird auch als *Fiat-Währung* oder einfach *Fiat* bezeichnet. Diese Art von Geld erhält ihren Wert dadurch, dass sie durch eine Regierung des Landes, welche es herausgibt, zu einem sog. «gesetzlichen Zahlungsmittel» deklariert wurde.[13]

Aus rechtlicher Sicht sind die Regierungen verpflichtet, alle Schulden zu begleichen, welche durch die Ausgabe ihrer Fiat-Gelder entstehen.[14] Da hinter Fiat-Geldern – im

[10] BRUNONE /MOLO, S. 301; EGLOFF /TURNES, S. 28.

[11] BRUNONE /MOLO, S. 301; vgl. hierzu die Definition im Bericht des Bundesrates zu virtuellen Währungen, S. 7-8.

[12] History.com, 1933, FDR takes United States off gold standard (Gold standard).

[13] Federal Reserve Bank of St. Louis, Functions of Money.

[14] Art. 99 Abs. 1 und 2 BV.

Gegensatz zum repräsentativen Geld – kein physischer Gegenwert besteht, liegt der Wert lediglich im Vertrauen gegenüber der Regierung. Fiat-Gelder wurden in der Vergangenheit traditionell schlicht als *Geld* bezeichnet. In der modernen Wirtschaftswissenschaft wird zwischen *Geld als gesetzlichem Zahlungsmittel* und *Geld im weiteren Sinne* unterschieden, wobei drei Hauptfunktionen erfüllt sein müssen:[15]

- **Tauschmittel** – das Konzept, dass Geld zum Tausch von Waren oder Dienstleistungen verwendet werden kann

- **Rechnungseinheit** – dies bezieht sich auf das Konzept, dass es einen gemeinsamen Wertmassstab für Geld gibt

- **Wertaufbewahrungsmittel** – der Gedanke, dass Geld im Allgemeinen seinen Wert beibehält

Bevor es das Papiergeld gab, wurde ein Tauschsystem angewendet, bei welchem Ware oder Dienstleistungen untereinander ausgetauscht wurden. In der Zeitperiode zwischen dem Tauschsystem und der Entwicklung hin zu Metallmünzen und Papiergeld existierten Zwischenformen solcher Tauschgeschäfte, z. B. Salz, Vieh oder zeremonielle Gegenstände.[16] Mit der Entwicklung hin zum Fiat-Geld veränderte sich die Wahrnehmung der Art und Weise, wie sich Reichtum langfristig erwirtschaften und übertragen lässt. In der heutigen Zeit, in der Kryptowährungen zunehmend beliebter werden und immer mehr Investitionen sowohl von Privatanlegern als auch von institutionellen Anlegern getätigt werden, hat sich die Wahrnehmung, was eine Währung ausmacht und wie Werte gespeichert und abgewickelt werden, erneut verändert. Insbesondere steigt dadurch, dass die Akzeptanz gegenüber Kryptowährungen als Zahlungsmittel zunimmt,[17] auch die Anzahl von Händlern, welche sie als Zahlungsmittel akzeptieren.[18] Trotz der steigenden Akzeptanz und der damit verbundenen anwachsenden Netzwerkeffekte können Kryptowährungen (noch) nicht als ein allgemein akzeptiertes

[15] Bericht des Bundesrates zu virtuellen Währungen, S. 7; YERMACK S. 32; BERENTSEN/SCHÄR, S. 11; PETRY, S. 15; KAISER/MÜLLER/REUTLINGER, S. 86 f.

[16] Nova, In the Beginning: Barter.

[17] BRUNONE /MOLO, S. 301; MÜLLER/ONG, S. 207; YERMACK, S. 32.

[18] BRUNONE /MOLO, S. 299; YERMACK, S. 32.

und etabliertes Zahlungsmittel angesehen werden.[19] Dies könnte daran liegen, dass die aktuell bekannteste und am meisten verbreitete Kryptowährung *Bitcoin* im Vergleich zu anderen Optionen wie Ethereum bei Transaktionen einen höheren Energieverbrauch aufweist und darüber hinaus langsamer und teurer ist.[20] Anders als bei gesetzlichen Zahlungsmittel besteht bei Kryptowährungen keine Verpflichtung zur Annahme als Zahlungsmittel.[21]

2.3 Allgemeine Eigenschaften von Krypto-Assets

Ausgehend von den obigen Ausführungen über die traditionellen Merkmale von Geldmittel werden nachfolgend die allgemeinen Eigenschaften von Kryptowährungen dargelegt. Kryptowährungen basieren weder auf physischen Eigenschaften wie Gold und Silber noch auf dem Vertrauen in zentrale Behörden wie bei Fiat-Geldern, sondern auf rein mathematischen Eigenschaften.[22] Ansonsten ähneln sich viele Eigenschaften, darunter folgende:

- **Transportierbarkeit/Portabilität** – Kryptowährungen lassen sich leicht lagern, bewegen oder übertragen.

- **Teilbarkei**t – Kryptowährungen lassen sich aufteilen. Zum Beispiel ist ein Bitcoin in bis zu acht Dezimalstellen teilbar.

- **Langlebigkeit** – Im Gegensatz zu Fiat-Münzen, Papiergeld oder physischen Edelmetalle sind Kryptowährungen physisch unzerstörbar.

[19] BRUNONE /MOLO, S. 301; LANDERER. S. 25; PETRY, S. 15; TROST, S. 206.

[20] Reiff, Bitcoin vs. Ethereum: An Overview.

[21] Art. 3 WZG; Kanton Zug, Kryptowährungen Bezahlung Steuern, seit Februar 2021 können jedoch natürliche und juristische Personen, welche in Zug ansässig sind, ihre Steuerrechnung mit ausgewählten Kryptowährungen bezahlen (Kryptowährungen Bezahlung Steuern); BRUNONE /MOLO, S. 301.

[22] Bitcoin, FAQ (Homepage).

- **Fungibilität** – Fungible Vermögenswerte sind untereinander zum gleichen Kurs austauschbar.[23] Im Krypto-Kontext bedeutet dies, dass ein Bitcoin genau den gleichen Wert wie ein anderer Bitcoin hat.[24]

- **Knappheit** – Kryptowährungen, welche ein begrenztes Angebot aufweisen, werden als *knapp* bezeichnet. Eine solche Knappheit spiegelt sich in verschiedenen Varianten wider. Bitcoin hat zum Beispiel ein endliches Angebot von 21 Millionen Münzen,[25] wohingegen bei Ethereum mittels komplizierter Berechnungen sog. *Schwierigkeitsbomben* die Geschwindigkeit reduziert wird, mit der neue Münzen geschürft werden, um eine Knappheit zu erzeugen.[26] Schwierigkeitsbomben sind ein Mechanismus, der in der Ethereum-Blockchain implementiert wurde, um die Schwierigkeit beim Mining von Ether (ETH) zu erhöhen und die Blockzeit zu verlangsamen. Die Idee hinter der Schwierigkeitsbombe ist, dass sie das Mining von Ether erschweren soll, indem sie die Schwierigkeit der kryptografischen Rätsel erhöht, die Miner lösen müssen, um einen neuen Block zur Blockchain hinzuzufügen.

- **Erkennbarkeit** – Wie bereits ausgeführt, werden die Eigenschaften eines Wertaufbewahrungsmittels, Tauschmittels und einer Rechnungseinheit benötigt, damit etwas als Geld anerkannt wird. Kryptowährungen mit einer grossen Kapitalisierung wie Bitcoin und Ethereum besitzen diesen Eigenschaften, zumal sie für Investitionszwecke und Transaktionen genutzt werden.

---

[23] Bitrates, Fungibility, Terminology.

[24] A. A. River Financial, Jurisdictional Bitcoin Premiums (Bitcoin Fungibility), welche argumentieren, dass Bitcoin an dezentralen Börsen z. T. verschiedene Preise aufweisen und folglich nicht wirklich fungibel sind. Ihrer Begrünung ist jedoch entgegenzuhalten, dass die Preise von Münzen mit grosser Marktkapitalisierung wie Bitcoin sowohl an zentralen als auch an dezentralen Börsen immer einheitlicher werden.

[25] Bitcoin, FAQ (Homepage).

[26] FRANKENFIELD, Understanding the Difficulty.

- **Zweckdienlichkeit** – Um dauerhaft zu existieren, muss eine Kryptowährung eine vorhersehbare Verwendung für Zwecke wie den Kauf von Waren, Dienstleistungen oder die Erleichterung von Transaktionen aufweisen.

2.4 Abgrenzung von digitalen Vermögenswerten und digitalen Token

Kryptowährungen bilden eine Untergruppe der digitalen Vermögenswerte. Der Begriff *digitale Vermögenswerte* muss nicht zwingend bedeuten, dass man in sie investieren kann. Digitale Vermögenswerte können i. w. S. als alles definiert werden, dass digital gespeichert werden kann. Daher gehören Bilder, Fotos und Dateien zu den digitalen Vermögenswerten, welche als auch *inhaltsbezogene digitale Vermögenswerte* bezeichnet werden. Dabei gilt zu beachten, dass digitale Vermögenswerte oft mit dem Begriff *Krypto-Vermögenswerte* verwechselt werden. Der Unterschied zwischen diesen beiden Vermögenswerten besteht jedoch darin, dass Krypto-Vermögenswerte eine Art von digitalen Vermögenswerten bilden, welche sich jedoch durch die Verwendung der Kryptografie unterscheiden.[27]

Der Definition der Kryptografie zufolge werden Nachrichten mittels eines Geheimcodes oder einer Chiffre verschlüsselt und entschlüsselt.[28] Die Verschlüsselung bildet dabei eine Unterform der Kryptografie, bei welcher Informationen in andere Formate umgewandelt werden, sodass die ursprüngliche Form unlesbar wird. Erst durch die Entschlüsselung wird die Verschlüsslung rückgängig gemacht, sodass die Daten in ihr ursprüngliches, lesbares Format zurückversetzt werden. Durch die Verschlüsselung wird sichergestellt, dass Dritte nicht mitlesen oder gar auf die Daten zugreifen können. Heutzutage wird der Prozess der Ver- und Entschlüsselung mithilfe von Computern durchgeführt. Dazu werden komplexe kryptografische Algorithmen benötigt.

Kryptowährungen und Krypto-Token bilden die gängigste Form der digitalen Vermögenswerte. Im Unterschied zu Krypto-Token besitzen Kryptowährungen eigene Blockchains.[29] Krypto-Token bauen hingegen auf bereits existierenden Blockchains

[27] SATW, S. 1.

[28] KAKUSCHKE, Was ist Kryptografie?.

[29] What Is a Digital Asset?; World Bank, DLT, S. 8 f.

auf.[30] Eine Blockchain stellt im Grunde ein Hauptbuch dar, in welchem sämtliche Transaktionen aufgezeichnet werden. Die einzelnen Transaktionen werden jeweils in Blöcken gespeichert, welche alle miteinander verbunden sind. Dabei bestehen einerseits öffentliche Blockchains, wie jene bei Bitcoin und Ethereum, und andererseits private Blockchains.[31]

Mithilfe von Blockchains lässt sich unwiderlegbar beweisen, dass Transaktionen erfolgt sind. Dieses Prinzip wird auch als *Nichtabstreitbarkeit* bezeichnet und basiert auf einem kryptografischen Beweis im Hauptbuch. Das Entscheidende bei Blockchains ist folglich, dass die Datenblöcke im Allgemeinen unveränderbar sind.[32] In vereinzelten Fällen haben jedoch schon Angriffe auf öffentliche Blockchains stattgefunden, bei welchen Anpassungen an den Transaktionsblöcken vorgenommen wurden, wodurch es zu finanziellen Verlusten kam, u. a. beim Hack des ethereumbasierten Smart Contracts *DAO* im Juni 2016. Die Hacker/-innen konnten in der Codierung eine Schwachstelle ausfindig machen, welche zu einem Abfluss von Geldern führte. Der Verlust wird auf über 50 Millionen USD geschätzt.[33]

Es gilt zu beachten, dass Blockchains nicht mit verteilten Ledgern gleichzusetzen sind. Blockchains bilden eine Art von verteilen Ledgern. In der umfangreicheren Kategorie der DLT werden Knoten-Netzwerke (d. h. unabhängige Computer) verwendet, welche zum Zwecke der Dokumentation synchron sämtliche Transaktionen in einem entsprechenden elektronischen Hauptbuch abspeichern.[34] Der Vorteil besteht darin, dass die in den Ledgern gespeicherten Informationen dezentral über verschiedene Knoten repliziert werden. Bei einem Hackerangriff müssen folglich alle Knoten angegriffen werden, da anderenfalls der Konsens des Netzwerks nicht gewährleistet ist.[35]

[30] What Is a Digital Asset?; World Bank, DLT, S. 8 f.

[31] EGLOFF /TURNES, S. 28; CHATTERJEE, What are public blockchains?.

[32] What Is a Digital Asset?; World Bank, DLT, S. 8 f.

[33] FINLEY, A Never-Ending ATM (DAO).

[34] EGLOFF /TURNES, S. 28; Terminologie der World Bank, DLT, S. 2.

[35] Egloff /Turnes, S. 36 f.

2.5 Verwahrung von Kryptowährungen

Eine der genannten Software-Anwendungen wird im Allgemeinen als *Wallet* bezeichnet und ist unerlässlich für das Senden und Empfangen von Kryptowährungen. Die Kryptowährungen selbst werden auf der Blockchain gespeichert, während Wallets die privaten und öffentlichen Schlüssel sowie die Wallet-Adressen der anwendenden Person speichern.[36] Es gibt verschiedene Arten von Wallets, die alle eine «Schlüsselfunktion» erfüllen.[37] Während Hot Wallets mit dem Internet verbunden sind, sind Cold Wallets nicht mit dem Internet verbunden. In der Regel werden Kryptowährungen in Hot Wallets aufbewahrt, die als Dienstleistung von Wallet-Providern angeboten werden. Als Cold Wallets gelten Hardware-Wallets, bei denen es sich um physische Geräte wie USB-Sticks handelt, sowie Paper-Wallets, bei denen die Schlüssel und Adressen auf Papier ausgedruckt werden. Hot Wallets umfassen Online-Wallets, Exchange-Wallets, Desktop-Wallets und Mobile Wallets. Jeder Typ hat Vor- und Nachteile und birgt potenzielle Risiken wie Hacking, Viren, Verlust oder Zerstörung.[38]

2.6 Zentrales und dezentrales Netzwerk

Kryptowährungen basieren auf einem dezentralen Netzwerk, das auch verteiltes Netzwerk genannt wird. Im traditionellen Finanzsystem hingegen herrscht ein zentrales oder «intermediäres» System vor, bei dem eine zentrale Partei als Intermediär für Transaktionen fungiert.[39] Zum Beispiel kann nur *Bankenbuchgeld* gesendet und empfangen werden, wenn die Zwischenpartei dazu autorisiert wurde und diese Anweisung ausführt.

In einem verteilten (Peer-to-Peer-)Transaktionssystem können Transaktionen jedoch ohne die Notwendigkeit von Drittparteien (z. B. kontoführende Banken) durchgeführt werden. Das System erhält seinen Namen dadurch, dass die Teilnehmer/-innen gleichberechtigt und direkt miteinander kommunizieren, was zu einer verbesserten

[36] SCHMIDT, S. 78 f.

[37] EGLOFF /TURNES, S. 87 f.

[38] EGLOFF /TURNES, S. 89 ff.; SCHMIDT, S. 79 ff.

[39] EGLOFF /TURNES, S. 28.

Resilienz gegenüber Angriffen und Ausfällen führt.[40] Jede/r Teilnehmer/-in ist aufgrund der Gleichberechtigung ersetzbar, sodass bei Ausfall andere Netzwerkteilnehmer/-innen einspringen können, um verlorene Daten wiederherzustellen und die Kommunikation auf alternativen Pfaden aufrechtzuerhalten. Im Falle eines Manipulationsversuchs können die anderen Teilnehmer/-innen die Attacke durch den Konsensmechanismus verhindern, weshalb dieses System als manipulationssicher bezeichnet werden kann.

[40] EGLOFF /TURNES, S. 36 f.

3 Geldwäscherei

In den folgenden Abschnitten wird die Geldwäscherei auf Grundlage von wissenschaftlichen Erkenntnissen analysiert. Anschliessend werden die Herausforderungen dargelegt, welche mit Kryptowährungen in Bezug auf Geldwäscherei einhergehen. Dazu werden die allgemeine Struktur des Geldwäscherei-Prozesses und die vorherrschenden Kontrollmechanismen vorgestellt.

3.1 Geldwäscherei und Kontrollen

Für Krimielle ist es oft schwierig, über jene Vermögenswerte frei zu verfügen, welche durch illegale Handlungen erwirtschaftet wurden. Einer der Hauptgründe könnte darin liegen, dass die Ausgabe hoher Beträge für teure Anschaffungen entweder auf einmal oder in kleineren Beträgen über eine längere Zeitspanne hinweg stattzufinden hat, was die Aufmerksamkeit der Strafverfolgungsbehörden auf sich ziehen kann. Folglich hat die Ausgabe solcher illegal erwirtschafteter Vermögenswerte möglichst unauffällig zu erfolgen.

Der Erfolg der Geldwäscherei ist demnach davon abhängig, ob die Informationsasymmetrie zwischen den geldwaschenden Personen und den Ermittlungsbehörden aufrechtgehalten werden kann. Die Geldwäscherei weist im Grunde zwei Merkmale auf: Illegalität und Verschleierung.[41] Das Bundesgericht beschreibt die Geldwäscherei in juristischer Hinsicht als eine Aktivität mit dem Ziel, Vermögenswerte aus kriminellen Machenschaften in den legalen Wirtschaftskreislauf einspeisen zu können. Durch den Vorgang der Geldwäsche soll gegenüber Dritten der Eindruck erweckt werden, dass die Vermögenswerte legal erwirtschaftet wurden. Die illegale Abstammung wird verschleiert, damit die Vermögenswerte nicht durch Behörden eingezogen werden und die Urheberin bzw. der Urheber selbst darüber verfügen kann.[42] Der wirtschaftliche Aspekt der Geldwäscherei besteht darin, die potenzielle Kaufkraft deliktisch erworbener Vermögenswerte in wirkliche Kaufkraft umzumünzen – zumal ungewaschene Vermögenswerte nicht direkt investiert oder angespart werden können, da anderenfalls

[41] MASCIANDARO, S. 226.

[42] BASSE, Art. 1 GwG N 4 ff.

die Einziehung durch den Staat droht.[43] Die Erzeugung oder Aufrechthaltung von Informationsasymmetrien bildet den Geldwäscherei-Prozess, welcher durch den Einsatz von Geldwäscherei-Instrumenten erfolgt. Auf der anderen Seite dienen die Verhinderung, Aufdeckung und Untersuchung von Geldwäscherei durch die Ermittlungsbehörden als Geldwäscherei-Kontrollen, welche die Verringerung der Informationsasymmetrien zum Ziel haben. Je wirkungsvoller diese greifen, desto schwieriger ist es, den Geldwäscherei-Prozess erfolgreich durchzuführen oder aufrechtzuhalten – zumal sich das Risiko der Strafverfolgung erhöht.[44]

3.1.1 Geldwäscherei-Prozess

Gemäss den obigen Ausführungen handelt es sich bei Geldwäscherei um einen Vorgang, der diverse Handlungen oder Phasen beinhaltet. Um verstehen zu können, wie Geldwäscherei funktioniert, wurden Modelle[45] entwickelt, welche den Prozess der Geldwäscherei beschreiben. Zu den beiden bekanntesten Modellen zählen das Zielmodell, welches durch den Bundesrat in der Botschaft zum Geldwäschereigesetz (GwG) angewendet wurde,[46] sowie das Drei-Phasen-Modell, welches oftmals in der Lehrmeinung wiedergegeben wird.[47] Obwohl viele Möglichkeiten bestehen, Geldwäscherei zu betreiben, können immer wieder ähnliche Phasen festgestellt werden.[48] Während der ersten Phase findet die Einspeisung (das sog. *Placement*) statt. Dabei werden die Vermögenswerte, meist in Form von Bargeld, geografisch verschoben, in andere physische Werte oder in Buchgeld umgetauscht oder mit Geldern legitimer Herkunft vermischt. Während der zweiten Phase findet eine Verschleierung (das sog. *Layering*) statt. Dabei wird versucht, die Herkunft der Vermögenswerte unkenntlich zu machen, indem diese physisch oder virtuell vom Tatort des Verbrechens entfernt werden. Dies erfolgt in der Praxis oft durch mehrfache, unmittelbar aufeinanderfolgende Überweisungen, wobei die Vermögenswerte z. T. mittels Offshore-Gesellschaften,

[43] MASCIANDARO, S. 226.

[44] BECKER, S. 179.

[45] Diese werden unter anderem im Zwei-Phasen-Modell (BERNASCONI, S. 30), im Drei-Phasen-Modell (TRECHSEL/PIETH, Art. 305bis StGB N4), im Zyklusmodell (ZÜND, S. 403 ff.) und im Zielmodell (ACKERMANN, Diss., S. 10 ff.) veranschaulicht.

[46] Botschaft GwG 1996, BBI 1996 II 1104.

[47] So u. a. MÜLLER, S.113; PIETH, BT, S. 297; TRECHSEL/PIETH, Art. 305bis StGB N4.

[48] MÜLLER, S. 99.

Stiftungen oder Handelsgesellschaften in unterschiedliche Strukturen aufgeteilt und untereinander transferiert werden, um die Rückverfolgbarkeit zu erschweren. Während der dritten Phase findet die Integration statt. Diese Phase dient der Verwässerung und der Wiedereinführung der Vermögenswerte in den regulären Wirtschaftskreislauf. Dies erfolgt beispielsweise durch den Erwerb von Immobilien oder Gesellschaften aller Art.[49]

Es gilt zu beachten, dass es sich bei dem oben beschriebenen Modell um ein theoretisches Modell handelt, weshalb es nicht zu starr verstanden werden sollte. Die einzelnen Phasen müssen in der Praxis nicht unbedingt chronologisch ablaufen, sondern können übersprungen oder wiederholt werden. Ferner können in jeder Phase verschiedene Techniken angewendet werden. Die Geldwäscherei ist dann beendet, wenn die Urheberin bzw. der Urheber über die Vermögenswerte frei verfügen kann, ohne staatliche Eingriffe wie eine Einziehung durch Behörden befürchten zu müssen.

Ein Praxisbeispiel wie Geldwäscherei betreiben werden kann ist das sog. *Wash-Trading*, bei dem es sich um eine Art des Scheingeschäfts handelt. Dabei wickelt ein Händler eine Vielzahl von Transaktionen für den Kauf und anschliessenden Verkauf desselben Finanzinstruments zu einem identischen oder ähnlichen Preis ab – sofern mehrere Konten verwendet werden –, wodurch der Preis des betreffenden Finanzinstruments ansteigt.[50] Dadurch kann der Händler aufgrund des falschen Anscheins einer überholten Nachfrage im Handelsvolumen seine Anteile mit einem Gewinn abstossen.

Dadurch, dass sowohl die kaufende als auch die verkaufende Person zwei Kopien des scheinbar gleichen Geschäftes erhält, wird das Vorgehen auch als «Mirror-Trading» bezeichnet.[51] Bei einem von 2010 bis 2015 bekannten Geldwäsche-System des *Russian Laundromat* (russische Waschmaschine) wurde Wash-Trades im grossen Umfang eingesetzt. Beim *Russian Laundromat*-Schema wurde über eine Vielzahl von Scheinfirmen kriminell erlangtes Geld in den russischen Finanzmarkt eingeschleust. Danach wurden litauische und moldawische Banken missbraucht, um über 20 Milliarden USD aus Russland zu schleusen.[52] Während dieses Vorgangs erwarben KGB-

[49] NRA-Bericht, S. 11.

[50] BASLER, Market Manipulation.

[51] IKEMEYER/KRIMPHOVE, S. 433.

[52] GRUHNWALD/HOSTETTLER/STARK, Der «Russian Laundromat».

nahestehende Personen über die Moskauer Niederlassung der Deutschen Bank Finanztitel, welche wiederum über die Londoner Niederlassung mittels einer Art *Wash-Trade-Vereinbarung* verkauft wurden.[53]

Das Verfahren zum Waschen traditioneller Fiat-Währungen scheint mittlerweile auch bei Kryptowährungen angewendet zu werden. Teilweise besteht die Befürchtung, dass das Wash-Trading bei Bitcoins im grossen Stil angewendet wird, um einerseits den Kurspreis zu manipulieren und andererseits lauter und unlauter erworbenes Geld zu vermischen, um Vermögen über unterschiedliche Krypto-Handelsplätze zu waschen.[54] In der Forschung scheint die These eines gross angelegten Wash-Trading bei Kryptowährungen, einschliesslich Bitcoin, gestützt zu werden.[55] Hierbei gilt einerseits zu beachten, dass sich bei dieser Forschung vorwiegend um einen indirekten Beweis handelt, welcher aus Börsen- und Marktaktivitäten abgeleitet wurde. Andererseits wird durch einen Forschungsartikel, der im Journal of Fiance veröffentlicht wurde suggeriert, dass Marktmanipulationen via Wash-Trading nicht nur Bitcoin, sondern auch andere Kryptowährungen wie Tether betreffen.[56] Die Ergebnisse dieses Forschungsartikel deutet darauf hin, dass Tether in der Vergangenheit zur Manipulation des Bitcoin-Kurses missbraucht wurde. Es gilt jedoch zu beachten, dass die Analyse nicht endgültig beweisen kann, dass eine Manipulation erfolgt ist.

In der Forschung wird folglich zunehmend die Erarbeitung direkter Beweise von Daten auf individueller Ebene fokussiert. So wurden in einer aktuellen Studie die entwendeten Daten eines Hackerangriffes auf die japanische Kryptobörse, Mt. Gox, analysiert, welche in Vergangenheit als grösste Handelsplattform für Kryptowährungen galt.[57] Insbesondere weil es sich hierbei um reale Kundendaten und deren getätigten Transaktionen handelte,

[53] HARDING, Exclusive: in confidential internal report seen by the Guardian, bank says scandal has hurt global brand.

[54] Bitfinexed. The Wash Trading could also be money laundering (Bitfinexed).

[55] CONG/ LI/TANG/YANG, S. 33.

[56] GRIFFIN/SHAMAS, S. 1961.

[57] ALOOSH /LI, S. 9 ff.

konnten die Strafverfolgungsbehörden bei mehr als 5 Millionen USD einen illegalen Ursprung nachweisen und diese Summe beschlagnahmen.[58]

Inwiefern das Wash-Trading zu den Kryptowährungsmärkten zum Zwecke der Marktmanipulation sowie Geldwäsche durchgedrungen ist, verdeutlichen die nachfolgenden beiden Beispiele aus der jüngsten Vergangenheit:

- Im Dezember 2020 wurden die Führungskräfte einer der grössten digitalen Währungsbörse in Südkorea, Coinbit, der Marktmanipulation beschuldigt.[59] Diese sollen 99 % des gesamten Transaktionsvolumens der Kryowährungen mittels Wash-Trading manipuliert haben, wodurch sie über 84 Millionen USD illegal erwirtschaftet haben sollen.[60]

- Im März 2021 wurde gegen Coinbase, Inc. aufgrund falscher, irreführender oder ungenauer Berichterstattung sowie Wash-Trading bei der von Coinbase betriebenen Plattform *GDAX* eine Verfügung seitens der US Commodity Futures Trading Commission (CFTC) erlassen.[61] Das Verfahren wurde schliesslich gegen eine Zahlung in der Höhe von 6.5 Millionen USD eingestellt.[62]

3.1.2 Geldwäscherei-Kontrollen

Wie bereits Kapitel 3.1 angedeutet, hat die Wirksamkeit der Geldwäscherei-Kontrollen Auswirkungen auf die Wahrscheinlichkeit, entdeckt zu werden, was wiederum ein erhöhtes Risiko für Kriminelle darstellt. Mit zunehmendem Risiko steigen auch die Kosten, den Gelwäscherei-Prozess trotzdem durchzuführen, was sich wiederum negativ auf die ökonomischen Anreize auswirkt.[63] Zu beachten gilt, dass diese Anreize oft nur schwer zu beziffern sind.[64] Sind jedoch gar keine Kontrollmechanismen implementiert

[58] JEFFRIES, Mt. Gox.

[59] PALMER, Update.

[60] NJUGUNA, Foul play detected.

[61] CFTC, Fall Nr. 8369-21 (zit. CFTC Coinbase).

[62] CFTC, Fall Nr. 8369-21 (zit. CFTC Coinbase).

[63] MASCIANDARO, S. 228 f; FERWERD, S. 338.

[64] So z. B. FERWERD, S. 334, welche auf das fehlende empirische Daten verweist; LEVI /REUTER, S. 315.

oder können diese leicht umgangen werden, liegen positive ökonomische Anreize zur Nutzung von Geldwäscherei-Instrumenten vor.

Um die wirtschaftlichen Anreize von Kryptowährungen als Geldwäscherei-Instrument feststellen zu können, muss das Instrument als solches mit der Wirksamkeit der existierenden Geldwäscherei-Kontrollen verglichen werden. In der Regel sind in gesetzlichen Bestimmungen Massnahmen zur Bekämpfung von Geldwäscherei vorgesehen, welche auf den Empfehlungen der Financial Action Task Force (FATF) basieren.[65]

Die Kontrollen in der Schweiz basieren auf den sog. *Sorgfaltspflichten*. Bei diesen handelt es sich um die der Geldwäschereigesetzgebung inhärenten Pflichten, die von allen Finanzintermediären einzuhalten sind, also von jenen natürlichen und juristischen Personen, die dem GwG unterstellt sind. Diese auf die Vermeidung der Gelwäscherei ausgerichteten Pflichten können in allgemeine/formelle[66] und besondere/materielle[67] Sorgfaltspflichten unterteilt werden. Erstere regeln die Identifizierung der Vertragspartei und die Feststellung der wirtschaftlich berechtigten Person sowie die erneute Identifizierung. Der Identifizierungsvorgang wird in der Praxis auch als *Know Your Customer* (KYC) oder *Customer Due Diligence* (CDD) bezeichnet. Diese Begriffe werden oft synonym verwendet, um den Prozess zu beschreiben, bei dem ein Finanzinstitut die Identität seiner Kunden überprüft und deren Risikoprofil bewertet, um die Einhaltung von Anti-Geldwäsche (AML)- und Know-Your-Customer (KYC)-Bestimmungen sicherzustellen. Zu den besonderen/materiellen Sorgfaltspflichten zählen die Risikoeinschätzung einer Geschäftsbeziehung, inkl. Der Errichtung von Kriterien für Geschäftsbeziehungen und Transaktionen mit erhöhten Risiken und deren risikoadäquate Behandlung, sowie die Abklärung mittels *Suspicious Activity Reporting* (SAR) der wirtschaftlichen Hintergründe und des Zwecks einer Transaktion, wenn sie ungewöhnlich erscheint, mit erhöhten Risiken behaftet ist oder Anhaltspunkte für Gelwäscherei vorliegen.

[65] Kapitel 4.1.1.

[66] Art. 3 – 5 GwG.

[67] HAWKINS, Stämpflis Handkommentar, Art. 2a GwG N 5.

3.2 Anreize zur Geldwäscherei

Das Konzept zur Analyse des Geldwäscherei-Prozesses und der Geldwäscherei-Kontrollen in den obigen Abschnitten basiert darauf, mit welchen wirtschaftlichen Anreizen Krimielle zur Geldwäscherei verleitet werden. Die Anreize werden durch kontextuelle und transaktionsbezogene Eigenschaften des Geldwäscherei-Prozesses gesteuert, welche sich jeweils wiederum in direkte oder indirekte Auswirkungen auf den Geldwäscherei-Prozess aufteilen lassen.[68] Die direkten Auswirkungen beeinflussen die Effizienz und Effektivität des Geldwäscherei-Prozesses, indem sie die Prozesse z. B. günstiger, zeiteffizienter oder robuster gestalten. Die indirekten Auswirkungen beeinflussen die Wirksamkeit der jeweiligen Geldwäscherei-Kontrollen – zumal sie einen Einfluss darauf haben, mit welcher Wahrscheinlichkeit der Geldwäscherei-Prozess aufgedeckt wird.

3.2.1 Zusammenhängende Faktoren

Nachfolgend werden die Risiken von Kryptowährungen, als Geldwäscherei-Instrument missbraucht zu werden, dargelegt. Dazu werden die stärksten Anreize analysiert, welche Personen dazu verleiten, Kryptowährungen als solche zu verwenden.[69] Hierzu wird u. a. auf das zweite Kapitel verweisen, in dem die erforderlichen Eigenschaften erläutert werden. Wenn Kryptowährungen im Vergleich zu üblichen Geldwäscherei-Instrumenten mittels Fiat-Währung als vorteilhafter wahrgenommen, liegen positive wirtschaftliche Anreize vor, was den ganzheitlichen Geldwäscherei-Prozess erleichtert.[70] Es wird angemerkt, dass die nachfolgende Auflistung nicht abschliessend ist.

3.2.1.1 Anonymität

In Bezug auf Kryptowährungen wird immer wieder die Anonymität kritisiert, welche sie im Hinblick auf ihre Verwendung bieten.[71] Fraglich ist jedoch, wie Kryptowährungen Anonymität bieten. Bei herkömmlichen Zahlungsvorgängen steht ein Finanzinstitut als

[68] BRENIG/ACCORSI/MÜLLER, S. 6.

[69] Bericht des Bundesrates zu virtuellen Währungen, S. 19 f.; BRUNONE /MOLO, S. 300; NRA-Bericht, S. 10 f.; DLT-Auslegeordnung, S. 144 f.

[70] MANTEL/MCHUGH, S. 23 f.

[71] BRUNONE /MOLO, S. 300; NRA-Bericht, S. 21 f; TOMIC/MAUCHLE, S. 3.

Vermittler zwischen den Parteien und überträgt das Geld vom Konto der auftraggebenden Person auf das Konto des bzw. der Begünstigten. Ein Zahlungsvorgang wird über zentrale Stellen wie Banken und Zahlungsdienstleister abgewickelt, die alle der Geldwäschereigesetzgebung unterliegen.[72] Demnach besteht ein dichtes Netz von zentralen Kontrollmechanismen. Bei Kryptowährungen wie Bitcoin (die auf einer öffentlichen, erlaubnisfreien Blockchain basieren) existiert aufgrund des dezentralen Charakters des Protokolls (in der Regel) kein Finanzinstitut als Vermittler zwischen den beteiligten Parteien; der Zahlungsvorgang wird durch das Blockchain-Protokoll selbst (d. h. durch automatisierte Konsensmechanismen) ermöglicht und das Protokoll wird von seinen Nutzerinnen und Nutzern betrieben – und nicht von einer regulierten zentralen Stelle. Mithilfe der Blockchain-Technologie können Vermögenswerte innerhalb von Sekunden und ohne vorherige Identifizierung der beteiligten Personen weltweit übertragen werden – alles, was dazu benötigt wird, ist eine Wallet, d. h. eine Software, die dank zahlreicher Internetanwendungen einfach und kostenlos eingerichtet werden kann. Die Einrichtung einer solchen elektronischen Wallet erfolgt in der Regel anonym und ohne Identifizierung. In der Theorie besitzen Nutzer/-innen eine Adresse, bei welcher die Identität der Person, welche die Adresse verwendet, nicht veröffentlicht wird. In Bezug auf die Praxis konnten Forscher/-innen jedoch nachweisen, dass der Grad der Anonymität bei Bitcoin, dem mit Abstand dominantesten Akteur im Krypto-Bereich,[73] nicht so stark ist wie angenommen.[74] Die Daten legen nahe, dass Bitcoin kein attraktives System für grosse Beträge illegaler Aktivitäten wie Geldwäsche darstellt. Dies könnte u. a. daran liegen, dass öffentliche Blockchain-Ledger[75] mithilfe von neuen Technologielösungen[76] durchleuchtet werden können. Bei letzterem handelt es sich im Wesentlichen um Datenanalysetools, welche die in unterschiedlichen Quellen gesammelten Daten miteinander kombinieren und mittels Algorithmen in einen Kontext zu Risikokriterien setzen und bewerten.[77] Bei den Anbietern solcher Lösungen handelt es

[72] DLT-Auslegeordnung, S. 145 ff; EGLOFF /TURNES, S. 28.

[73] Kapitel 2.1.

[74] BRUNONE /MOLO, S. 303; DORIT/SHAMIR, S. 12 f.;
ANDROULAKI/KARAME/ROESCHLIN/SCHERER/CAPKUN, S. 46 f.;
MEIKLEJOHN/POMAROLE/JORDAN/LEVCHENKO/MCCOY /VOELKER/ SAVAGE, S. 93.

[75] BILLE/SPINDLER, S. 1359; BRUNONE /MOLO, S. 303; TOMIC/MAUCHLE, S. 3.

[76] Kapitel 2.4.

[77] TOMIC/MAUCHLE, S. 3.

sich um hochspezialisierte Unternehmen mit mehrheitlich forensischem Hintergrund. Der Einsatz solcher Technologien ermöglicht bei pseudonymen Blockchains, auf denen u. a. Bitcoin und Ethereum basieren, Einblicke in Transaktionsketten – was bei Bargeld nicht möglich ist –, da jede Transaktion erfasst und gespeichert wird und mit zunehmender Transaktionshistorie Muster und Verbindungen erkennbar werden.[78]

Der pseudonyme Charakter von Kryptowährungen hat also einen indirekten Effekt, der für geldwaschende Personen negative Anreize schafft – zumal die öffentliche Aufzeichnung die Rückverfolgung einer jeden Transaktion ermöglicht, die jemals stattgefunden hat. Sofern die Strafverfolgungsbehörden eine Person mit einem Pseudonym in Verbindung bringen, ist es möglich, sämtliche verdächtige Aktivitäten in der Transaktionshistorie nachzuverfolgen bzw. aufzuarbeiten.[79] Im Zuge dessen haben sich sowohl Kryptowährungen (z. B. Monero, Verge, Dash) als auch Blockchain-Dienstleistungen (z. B. Mixer oder Tumbler) entwickelt, die der Verschleierung und Anonymisierung von Transaktionen dienen und deren Zweck mitunter die Geldwäscherei darstellt.[80] Mixer und Tumblers sind Anonymisierungsdienste für Kryptowährungen. Wie der Name bereits vermuten lässt, werden Kryptowährungen in diesen Diensten so gemischt, dass ihre Herkunftsadresse nicht mehr zurückverfolgt werden kann. Wer Coins an einen solchen Dienst überweist, erhält eine zeitverzögerte Rückerstattung des gleichen Betrags abzüglich einer Servicegebühr, deren Herkunft nicht zurückverfolgbar ist. Bei einigen Kryptowährungen wie Dash, Verge und Monero sind solche Mischdienste bereits automatisch im Protokoll enthalten. Auch in der wissenschaftlichen Literatur werden solche Anonymisierungsdienstleistungen zunehmend behandelt. Es konnte aufgezeigt werden, dass die Mischdienste nicht immer wie gewünscht funktionieren.[81] Untersuchungen zu Monero haben ergeben, dass die Herkunft der Vermögenswerte in 88 % der Fälle rekonstruiert werden konnte.[82] Es gilt zu beachten, dass ein Fehler in der Datenerfassung solcher Dienstleistungen oder Währungen im Laufe der Zeit die Identität vergangener Transaktionen offenlegen kann. In Anbetracht dieser Risiken, die sich für

[78] Brunone /Molo, S. 303

[79] BRUNONE /MOLO, S. 303; DLT-Auslegeordnung, S. 26 f.; TOMIC/MAUCHLE, S. 3.

[80] DLT-Auslegeordnung, S. 27.

[81] MOSER et al., S. 144.

[82] AMRIT / FISCHER /TOPLE /SAXENA, S. 14.

die geldwaschenden Personen ergeben, sind bei den erläuterten Mischdiensten indirekte Effekte mit negativen Anreizen festzustellen.

3.2.1.2 Dezentralität

Aufgrund des dezentralen Charakters von Blockchain-Protokollen ist keine zentrale Stelle für die Verarbeitung von Transaktionen erforderlich.[83] Die gesetzlichen Vorschriften zur Geldwäschereibekämpfung sind in der Regel auf zentrale Stellen ausgerichtet, also auf Finanzinstitute und nicht auf Einzelpersonen oder Softwareentwickler/-innen.[84] Das Konzept der Dezentralisierung verhindert die Ausübung staatlicher Kontrollen, welche der Staat über die klassischen Finanzinstitute ausübt, weshalb die Befürchtung bestand, dass Kryptowährungen die Bestrebungen der Geldwäschereibekämpfung aushebeln könnten.[85] Dies verbesserte sich zwar mit der FATF-Erklärung zu virtuellen Vermögenswerten und zugehörigen Anbietern im Jahr 2019.[86] Die Problematik von P2P-Transaktionen, also dezentralen Transaktionen zwischen Wallets ohne Einbezug von VASP,[87] wurde auf FATF-Ebene noch nicht gelöst.[88] Im Gegensatz dazu sind die Schweiz und auch die EU P2P-Transaktionen angegangen.[89] Obwohl die Schweiz und Europa als einzige Jurisdiktionen weltweit einen möglichen Lösungsansatz für die Dezentralität erarbeitet haben, können die geldwaschenden Personen von der sog. Sunrise-Problematik profitieren, die nachfolgend erläutert wird.

Mit dem Sunrise-Problem wird die Herausforderung bezeichnet, dass die globale Umsetzung der Geldwäschereibekämpfung in den einzelnen Ländern unterschiedlich schnell in Kraft tritt.[90] Solange allein die Schweiz und Europa eine mögliche Lösung

---

[83] Kapitel 2.1.

[84] Kapitel 3.1.2.

[85] BRUNONE/MOLO, S. 307 f.;TOMIC/MAUCHLE, S. 3.

[86] Kapitel 4.1.1.4.

[87] Kapitel 4.1.1.3.

[88] BRUNONE/MOLO, S. 307 f.

[89] Kapitel 4.1.1.5; 4.1.3.

[90] ALLISON, Sunrise Problem; BRUNONE /MOLO, S. 308.

bereithalten, können Kriminelle die Schweiz und Europa virtuell meiden[91] und aus solchen Ländern operieren, in denen keine angemessenen Vorschriften existieren. Ferner gilt zu beachten, dass einige Länder noch nicht einmal die zuvor erwähnte FATF-Erklärung zu virtuellen Vermögenswerten und zugehörigen Anbietern umgesetzt haben. In der zweiten zwölfmonatigen Überprüfung der Umsetzung ihrer überarbeiteten Standards zu virtuellen Vermögenswerten und VASP fasst die FATF zusammen, dass 58 von 128 berichtenden Ländern die überarbeiteten FATF-Standards umgesetzt haben, wobei 52 von ihnen die VASP regulieren und 6 von ihnen den Betrieb von VASP verbieten. Die anderen 70 Länder haben die überarbeiteten Standards noch nicht in nationales Recht umgesetzt.[92] Allerdings ist zu erwarten, dass die meisten Länder am Ende die überarbeiteten FATF-Standards umsetzen werden.

Weiter gilt bei einem dezentralen System zu beachten, dass unrechtmässig erworbene Kryptowährungen auf der Blockchain nur dann beschlagnahmt werden können, wenn die Private Keys der Wallet bekannt sind.[93] Sofern die Kryptowährungen auf einer Custodial Wallet liegen, könnte der Anbieter Vermögenswerte sperren und den Strafverfolgungsbehörden aushändigen; dies wird jedoch nur dann der Fall sein, wenn die Anbieter in der Schweiz ansässig sind, was aufgrund der oben beschriebenen Sunrise-Thematik jedoch nur selten vorkommt.

Die Dezentralität wirkt sich demnach indirekt auf die Durchführung des Geldwäscherei-Prozesses aus und schafft starke positive Anreize dafür, Kryptowährungen als Geldwäscherei-Instrument zu verwenden.

3.2.2 Zwischenergebnis

Die obigen Ausführungen geben einen Überblick über die zentralen Ergebnisse. Es wurde untersucht, ob sich Kontext- oder Transaktionsfaktoren jeweils direkt oder indirekt auf den Geldwäscherei-Prozess auswirken und demzufolge entweder positive oder negative

[91] Dank dem Internet könnten geldwaschende Personen von überall agieren, ohne physisch präsent sein zu müssen.

[92] FATF-12-Month Review, S. 8 f.

[93] BRUNONE /MOLO, S. 303f.; DRZALIC /MOLO, S. 34; NRA-Bericht, S.35.

Anreize dafür schaffen, Kryptowährungen im Vergleich zu herkömmlichen Finanzinstrumenten und -dienstleistungen als Gelwäscherei-Instrument zu missbrauchen.

Zusammenfassend lässt sich feststellen, dass sich die beiden Faktoren ausgleichen. Dies impliziert jedoch, dass die Abhängigkeiten zwischen den beiden Faktoren und deren Bedeutungen noch nicht berücksichtigt wurden. Die Anonymität wurde als ein Faktor identifiziert, welcher indirekt negative Anreize setzt. Die Dezentralität bildet hingegen einen Faktor, welcher positive Anreize dafür schafft, Kryptowährungen im Vergleich zu herkömmlichen Finanzinstrumenten und -dienstleistungen als Geldwäscherei-Instrument zu missbrauchen. Der Vergleich verdeutlicht, dass Kryptowährungen aufgrund ihrer Dezentralität eine Triebkraft für die Geldwäscherei sein können – unbekannt ist allerdings, in welchem Ausmass der Faktor die Geldwäscherei erleichtert. Die Anonymität, welche Kryptowährungen zugeschrieben wird, scheint sich nicht zu bewahrheiten – zumal es im Gegensatz zu Bargeld-Transaktionen möglich ist, sämtliche verdächtige Aktivitäten in der Transaktionshistorie nachzuverfolgen bzw. aufzuarbeiten. Auch die erläuterten Mischdienste scheinen nicht so zuverlässig zu sein wie angenommen oder befürchtet.

4 Geldwäschereibekämpfung

Geldwäsche ist ein ernstes Problem, das sowohl staatliche als auch private Institutionen weltweit beschäftigt. Insbesondere im Finanzsektor sind Massnahmen erforderlich, um die Bekämpfung der Geldwäsche zu unterstützen. In diesem Kapitel werden einige dieser Institutionen und Instrumente vorgestellt, darunter die Financial Action Task Force (FATF), die Anti-Geldwäsche-Richtlinien Nr. 5 und Nr. 6, die TFR-Regulierung, die Sanktionen und das Mining des US-Office of Foreign Assets Control und das Financial Crimes Enforcement Network. Darüber hinaus wird auf die Kontroverse um nicht gehostete Wallets eingegangen.

4.1 Bedeutsame Behörden und Instrumente

Neben staatlichen Institutionen existieren auch private Institutionen, die sich mit der Bekämpfung der Geldwäscherei befassen. Dabei handelt es sich vorwiegend um Selbstregulierungsmassnahmen im Bereich des Finanzsektors. Nachfolgend wird aufgezeigt, welche internationalen Instrumente und Organisationen zur Bekämpfung der Geldwäscherei bestehen, die sich explizit auf Kryptowährungen beziehen.

4.1.1 Financial Action Task Force

Bei der FATF handelt es sich um eine supranationale Organisation. Sie wurde auf Initiative der G7 gegründet und besteht aus 36 Mitgliedsstaaten sowie 2 Organisationen, der EU-Kommission und dem Kooperationsrat der Golfstaaten. Der Standort der FATF befindet sich am Sitz der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (engl. Organisation for Economic Co-operation and Development, OECD) in Paris. Zu den FATF-Kernaufgaben gehört die Verfassung internationaler Standards zur Bekämpfung der Geldwäscherei sowie der Terrorismus- und Proliferationsfinanzierung. Ferner überwacht sie deren effektive Umsetzung durch gesetzgeberische, regulatorische und operative Massnahmen anhand gegenseitiger Länderprüfungen, sog. *Mutual Evaluations*. Darüber hinaus befasst sich die Taskforce mit der Ausarbeitung von Richtlinien, zu denen die «40 Empfehlungen zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung» gehören, welche 1990 verfasst und in den folgenden Jahren mehrmals revidiert wurden. Institutionen wie die Weltbank, der Internationale Währungsfonds sowie der Sicherheitsrat der UNO haben die Empfehlungen der FATF als internationale Standards zur Bekämpfung von Geldwäscherei anerkannt. Trotz der

fehlenden rechtlichen Verbindlichkeit haben sich bereits über 180 Länder dazu verpflichtet, die Empfehlungen zu ratifizieren – vorwiegend aufgrund von Konventionen wie den Europaratsabkommen von 1990 und 2005.[94]

Die Umsetzung der Empfehlungen wird regelmässig durch internationale Assessments überprüft und beurteilt. Sofern die Umsetzung eines Lands bei der Bewertung als ungenügend bewertet wird oder das Land als ein solches angesehen wird, das ein Umfeld für die Geldwäscherei und Terrorismusfinanzierung fördert, kann es auf die Graue Liste gesetzt werden, welche die FATF als *Rechtordnung mit strategischen Mängeln* bezeichnet. Aktuell gehören Albanien, Barbados, Burkina Faso, Kambodscha, die Kaimaninseln, die Demokratische Republik Kongo, Gibraltar, Haiti, Jamaika, Jordanien, Mali, Marokko, Mosambik, Panama, Philippinen, der Senegal, der Südsudan, Syrien, Tansania, die Türkei, Uganda, die Vereinigten Arabischen Emirate sowie der Jemen der Grauen Liste an.[95] Länder auf der Grauen Liste müssen in Zusammenarbeit mit der FATF konkrete Verbesserungsmassnahmen umsetzen. Diese Massnahmen sollen die Mängel beheben und die Bekämpfung der Geldwäscherei und Terrorismusfinanzierung verbessern.

Ein negatives Assessment-Ergebnis kann dazu führen, dass der betreffende Staat als *non-cooperative* deklariert und auf der sog. *Schwarzen Liste* aufgeführt wird, sodass er den sog. *Hochrisiko-Jurisdiktionen* mit Aufruf zur Handlung unterfällt. Dies kann die Reputation des entsprechenden nationalen Finanzplatzes negativ beeinflussen, was sich wiederum negativ auf die Bereitschaft anderer Länder und globaler Organisationen auswirkt, in diesen Ländern Geschäfte zu betreiben.[96] Aktuell gehören die Demokratische Volksrepublik Korea, der Iran und Myanmar der Schwarzen Liste an.[97]

4.1.1.1 Empfehlungen der Financial Action Task Force

Die FATF veröffentlichte 1990 ihre ersten 40 Empfehlungen zur Bekämpfung der Geldwäscherei in einem internationalen Kontext. Die Empfehlungen mussten über die Jahre immer wieder überarbeitet werden – auch aufgrund des dezentralen Charakters von

[94] TRECHSEL/PIETH, Art. 305bis StGB, N5a.

[95] FATF, Black and grey lists.

[96] TRECHSEL/PIETH, Art. 305bis StGB, N5a.

[97] FATF, Black and grey lists.

Blockchain-Protokollen. Wie im vorherigen Kapitel erläutert, ist auf der Blockchain keine zentrale Stelle für die Verarbeitung von Transaktionen erforderlich. Durch die dezentrale Ausgestaltung wird der Grad der Anonymität durch das Protokoll selbst definiert.

In den damaligen Geldwäscherei-Vorschriften sowie den FATF-Empfehlungen waren Sorgfaltspflichten jedoch nur für zentrale Stellen und nicht für Einzelpersonen oder Softwareentwickler/-innen vorgeschrieben. Die Geldwäschereibestimmungen waren bis 2019 demnach nicht auf den Blockchain-Bereich anwendbar,[98] solange kein zentraler Dienstleister beteiligt war, welcher als Finanzinstitut im Sinne der FATF oder als Finanzintermediär im Sinne der Schweizer GwG-Vorschriften galt. Dies betraf vor allem Kryptobörsen und Custodial-Wallets-Anbieter. Selbst wenn die Geldwäschereivorschriften anwendbar waren, enthielten die Anforderungen für Finanzinstitute keine Regeln zur Identifizierung der Gegenpartei bei blockchainbasierten Transaktionen, die über eine Wallet-Adresse übertragen wurden.[99] Dies änderte sich im Juni 2019, als die FATF eine öffentliche Erklärung zu virtuellen Vermögenswerten und zugehörigen Anbietern herausgab und eine Auslegeordnung veröffentlichte, in der klargestellt wurde, dass VASP und andere an Aktivitäten mit virtuellen Vermögenswerten beteiligte Einrichtungen alle in den FATF-Empfehlungen beschriebenen Präventivmassnahmen (Nr. 10–21) anwenden müssen.[100] Damit wurde die Anforderung an die Länder formalisiert, für VASP dieselben Präventivmassnahmen wie für Finanzinstitute zu ergreifen – einschliesslich der Sorgfaltspflicht gegenüber der Kundschaft, Aufzeichnungen aufzubewahren und verdächtige Transaktionen zu melden sowie Informationen über den bzw. die Auftraggeber/-in und den bzw. die Begünstigte/-n gemäss 16. Empfehlung einzuholen, aufzubewahren und sicher zu übermitteln, wenn sie virtuelle Vermögenswerte transferieren.[101]

4.1.1.2 Financial Action Task Force – Travel Rule und deren Ausprägungen

Die FATF-Empfehlung Nr. 16 zur Bekämpfung der Geldwäscherei wird als *Travel Rule* bezeichnet. Sie regelt den Informationsaustausch bei elektronischen Überweisungen und

[98] TOMIC/MAUCHLE, S. 3.

[99] TOMIC/MAUCHLE, S. 3.

[100] FATF-Ergebnisse 2019.

[101] TOMIC/MAUCHLE, S. 3.

stellt sicher, dass grundlegende Informationen über die auftraggebende und die begünstigte Person von Überweisungen bei Bedarf verfügbar sind für:

a) die zuständigen Strafverfolgungs- und/oder Staatsanwaltschaftsbehörden, um sie bei der Aufdeckung, Ermittlung und Verfolgung von Terroristinnen und Terroristen oder anderen Straftäterinnen und Straftätern sowie beim Aufspüren deliktischer Vermögenswerte zu unterstützen;

b) die Finanzfahndungsstellen, um verdächtige oder ungewöhnliche Aktivitäten zu analysieren und bei Bedarf zu verbreiten; und

c) auftraggebende, zwischengeschaltete und begünstigte Finanzinstitute, um die Identifizierung und Meldung verdächtiger Transaktionen zu erleichtern und die Anforderungen an die Ergreifung von Sicherstellungsmassnahmen sowie die Einhaltung des Verbots von Transaktionen mit benannten Personen und Einrichtungen umzusetzen.

Die Empfehlung Nr. 16 verlangt von den Finanzinstituten, dass bei einer Transaktion die dazugehörigen Kundeninformationen (auftraggebende und begünstigte Person) untereinander ausgetauscht werden müssen. Die FATF hat die Travel Rule entwickelt, um zu verhindern, dass Kriminelle ungehinderten Zugang zu telegrafischen Überweisungen haben, um ihre Gelder zu bewegen.

Die Travel Rule für Überweisungen in staatlich ausgegebenen Währungen, den sog. Fiat-Währungen, wurde erstmals auf zwischenstaatlicher Ebene mit den FATF-Empfehlungen von 2012 eingeführt. In den USA war jedoch bereits ein ähnliches Konzept in Kraft, das Banken und Gelddienstleister aufforderte, bei Zahlungen Informationen über die auftraggebende Person zu übermitteln. Während sich die US-Vorschriften auf die Angaben zur auftraggebenden Person konzentrierten, verlangte die mit der 16. FATF-Empfehlung eingeführte Regel, dass sowohl Angaben zur auftraggebenden als auch zur begünstigten Person übermittelt werden.

In der Schweiz wurde die 16. FATF-Empfehlung in Art. 10 Abs. 1 GwV-FINMA umgesetzt, wodurch ausdrücklich verlangt wird, dass die Finanzintermediäre sicherstellen, dass sie ihrer Pflicht zur Aufzeichnung und Übermittlung der erforderlichen

Informationen über die auftraggebende und die begünstigte Person nachkommen.[102] Im Bericht der FATF über die gegenseitige Begutachtung für das Jahr 2016 wurde die Schweiz als nur teilweise konform mit der 16. Empfehlung eingestuft, da die Finanzintermediäre nicht verpflichtet sind, Massnahmen zur Kontrolle der Qualität der in den Überweisungsaufträgen enthaltenen Informationen zu ergreifen.[103] Nachdem die FINMA ihre GwV-FINMA im Jahr 2018 revidiert hatte (in Kraft getreten am 1. Januar 2020), wurde die Schweiz erneut als weitgehend konform mit der 16. Empfehlung eingestuft.[104] Die Auswirkungen der 16. Empfehlung bzw. des Art. 10 Abs. 1 GwV-FINMA auf die Finanzinstitute waren aus technischer Sicht gering, da die Branche bereits Messaging-Standards für inländische und grenzüberschreitende Zahlungen entwickelt hatte (z.B. ISO20022, SWIFT und SEPA).[105]

4.1.1.3 Virtual Asset Service Provider

Die FATF verwendet den Begriff *Virtual Asset Service Provider (VASP)*, um sich auf Unternehmen zu beziehen, die den FATF-Empfehlungen unterliegen. Ein VASP kann jedes Unternehmen sein, das im Ökosystem virtueller Vermögenswerte als Vermittler auftritt. Durch die Verwendung einer weit gefassten, auf Aktivitäten basierenden Definition wollte die FATF Flexibilität in einem sich schnell entwickelnden Bereich schaffen.

Im FATF-Glossar wird VASP wie folgt definiert: «jede natürliche oder juristische Person, die nicht anderweitig unter die Empfehlungen fällt und als Unternehmen eine oder mehrere der folgenden Aktivitäten oder Operationen für oder im Namen einer anderen natürlichen oder juristischen Person durchführt:

a) Austausch zwischen virtuellen Vermögenswerten und Fiat-Währungen;

b) Austausch zwischen einer oder mehreren Formen von virtuellen Vermögenswerten;

c) Übertragung von virtuellen Vermögenswerten;

---

[102] TOMIC/MAUCHLE, S. 4.

[103] FATF-Bericht über die Schweiz, S. 3 f.

[104] FATF-Ergebnisse 2020, S. 4.

[105] GRECO /KRAMER, Rz. 2637 ff.

d) Verwahrung und/oder Verwaltung von virtuellen Vermögenswerten oder von Instrumenten, die die Kontrolle über virtuelle Vermögenswerte ermöglichen; und

e) Beteiligung an und Erbringung von Finanzdienstleistungen im Zusammenhang mit dem Angebot und/oder dem Verkauf eines virtuellen Vermögenswerts durch einen Emittenten.[106]»

Auch wenn von der FATF Beispiele und weitere Einzelheiten zu den Aktivitäten genannt werden, die unter die obige Definition fallen, wird immer noch Raum für Interpretationen gelassen. Anbieter wie Börsen (Krypto/Krypto oder Fiat/Krypto), Broker für virtuelle Vermögenswerte, Stablecoin-Emittenten, Depot- und fortgeschrittene Handelsdienstleistungen, Bitcoin-Geldautomaten und Initial-Coin-Offering-Unternehmen unterfallen dieser Definition und können als VASP betrachtet werden. Dezentrale (Peer-to-Peer-)Börsen, d. h. Plattformen und Anbieter, die die Möglichkeit bieten, virtuelle Vermögenswerte direkt zwischen Einzelpersonen zu übertragen und bei denen jede Funktion von der Blockchain selbst bereitgestellt wird, können in einigen Fällen als VASP definiert werden – insbesondere, wenn die Kundschaft für den Betrieb der Softwaregebühren zahlen muss. Das Gleiche gilt für dezentrale Finanzprotokolle (DeFI). Die FATF stellt klar, dass nur Plattformen, die eine sehr begrenzte Funktionalität bieten, die hinter dem Austausch, der Übertragung, der Verwahrung, der Verwaltung, der Kontrolle und der Erbringung von Finanzdienstleistungen im Zusammenhang mit der Emission zurückbleibt, im Allgemeinen keine VASP sind. Dazu können beispielsweise Websites gehören, die lediglich ein Forum für Käufer/-innen und Verkäufer/-innen bieten, um sich zu identifizieren und miteinander zu kommunizieren, ohne dass sie, auch nur teilweise, die in der Definition von VASP enthaltenen Dienstleistungen anbieten.[107]

Reine Peer-to-Peer-Transaktionen zwischen Einzelpersonen ohne Nutzung oder Beteiligung eines VASP (z. B. Überweisungen von virtuellen Vermögenswerten zwischen zwei nicht gehosteten Geldbörsen, deren Nutzer/-innen in eigenem Namen handeln) sowie Softwareentwickler/-innen fallen nicht unter die Definition von VASP.[108]

[106] FATF, aktualisierter Leitfaden für virtuelle Vermögenswerte, S. 24.

[107] FATF aktualisierter Leitfaden für virtuelle Vermögenswerte, S. 35.

[108] TOMIC/MAUCHLE, S. 3.

4.1.1.4 Travel Rule für Kryptowährungen

Die Travel Rule verpflichtet die VASP, die erforderlichen und korrekten Informationen über die auftraggebende und die begünstigte Person einzuholen, aufzubewahren und zu übermitteln und diese Informationen zusammen mit einer inländischen oder grenzüberschreitenden Transaktion mit virtuellen Vermögenswerten über dem Schwellenwert von 1'000 USD/EUR zu übermitteln. Die Informationen müssen gemeinsam mit den virtuellen Vermögenswerten sicher an den empfangenden VASP übermittelt werden.

Ein Vermittler unterliegt den Verpflichtungen, wenn er als VASP gemäss der Definition der FATF qualifiziert ist. Transaktionen ohne Beteiligung eines VASP unterliegen daher nicht den Verpflichtungen der Travel Rule.

Gemäss Abs. 181 ff. des aktualisierten Leitfadens für einen risikobasierten Ansatz für virtuelle Vermögenswerte und VASP sollten die Informationen, die allen qualifizierten Überweisungen beiliegen, immer die folgenden Angaben enthalten:

a) **den vollständigen Namen der auftraggebenden Person**, der von dem auftraggebenden VASP überprüft wurde. Der begünstigte VASP muss den Namen der auftraggebenden Person nicht auf seine Richtigkeit hin überprüfen, sollte ihn aber zum Zwecke der Überwachung verdächtiger Transaktionen und der Sanktionsprüfung überprüfen;

b) **die Kontonummer der auftraggebenden Person**, wenn ein solches Konto für die Abwicklung der Transaktion verwendet wird. Im Zusammenhang mit virtuellen Vermögenswerten könnte dies die Adresse der Wallet bzw. der öffentliche Schlüssel sein;

c) **die physische (geografische) Adresse der auftraggebenden Person** oder die nationale Identitätsnummer oder die Kundenidentifikationsnummer (d. h. keine Transaktionsnummer), die die auftraggebende Person gegenüber dem auftraggebenden VASP eindeutig identifiziert, oder Geburtsdatum und -ort. Für die Übermittlung der geografischen Adresse der auftraggebenden Person bedeutet dies die Adresse, die von der VASP der auftraggebenden Person im Rahmen ihres KYC-Verfahrens auf ihre Richtigkeit überprüft wurde;

d) **den Namen der begünstigten Person** (d. h. den Namen der Person, die die auftraggebende Person als Empfänger/-in des Transfers virtueller Vermögenswerte angibt). Dieser Name muss von dem auftraggebenden VASP nicht auf seine Richtigkeit hin überprüft werden, sollte aber zum Zweck der Überwachung verdächtiger Transaktionen und der Sanktionsprüfung überprüft werden. Der begünstigte VASP muss den Namen der empfangenden Person in Bezug auf die Richtigkeit überprüfen, sodass der begünstigte VASP bestätigen kann, ob der Name und die Kontonummer der empfangenden Person, die er vom auftraggebenden VASP erhält, mit den überprüften Kundendaten des begünstigten VASP übereinstimmen; und

e) **die Kontonummer der begünstigten Person**, wenn ein solches Konto für die Abwicklung der Transaktion verwendet wird. Im Zusammenhang mit virtuellen Vermögenswerten könnte dies – ebenso wie bei der auftraggebenden Person – die Adresse der Wallet bzw. der öffentliche Schlüssel sein.

4.1.1.5 Anforderungen der neuen Travel Rule in der Schweiz

In der Schweiz ist die Travel Rule der FATF in der GwV-FINMA umgesetzt und verlangt ausdrücklich, dass Finanzintermediäre, die Zahlungsaufträge mit anderen Finanzintermediären abwickeln, sicherstellen, dass Finanzintermediäre ihrer Pflicht zur Aufzeichnung und Übermittlung von Informationen über die auftraggebende und die begünstigte Person bei Transaktionen über einem Schwellenwert von CHF 1'000 nachkommen – konkret soll sie den Namen, die Kontonummer und die Adresse der auftraggebenden Person sowie den Namen und die Kontonummer der begünstigten Person offenlegen.[109]

Am 26. August 2019 veröffentlichte die FINMA als Reaktion auf die öffentliche Stellungnahme der FATF vom 21. Juni 2019 eine Wegleitung und stellte klar, dass aufgrund des technologieneutralen und prinzipienbasierten Charakters der Verordnung Art. 10 Abs. 1 GwV-FINMA bereits auf jene Finanzintermediäre anwendbar ist, die auf Blockchain-Technologie basierende Dienstleistungen anbieten, und daher keine

[109] Art. 10 Abs. 1 GwV-FINMA; Tomic/Mauchle, S. 3.

zusätzliche Umsetzung erforderlich ist.[110] Die Schweiz hat die GwV-Vorschriften schon immer auf VASP angewandt, die als Finanzintermediäre zu qualifizieren sind.

Ein VASP in der Schweiz unterliegt den Bestimmungen des schweizerischen GwG und dessen Verordnungen, wenn er professionelle Dienstleistungen[111] anbietet, die als Finanzintermediation im Sinne von Art. 2 Abs. 2 GwG zu qualifizieren sind. Der Bundesrat hat bereits 2018 klargestellt, dass die folgenden Blockchain-Dienstleistungen Finanzintermediationstätigkeiten darstellen:

- Anbieter von Custodial Wallets;
- zentrale Handelsplattformen (mit Zugang zu privaten Schlüsseln);
- dezentralisierte Handelsplattformen (ohne Zugang zu privaten Schlüsseln), die die technische Kontrolle haben oder anderweitig Kundentransaktionen erleichtern (z. B. durch Bestätigen, Genehmigen oder Sperren von Aufträgen über Smart Contracts);
- Wechselstuben (professioneller Kauf und Verkauf von Kryptowährungen);
- Krypto-Fonds;
- Ausgabe von Zahlungstokens oder hybriden Zahlungstokens (die sowohl Zahlungs- als auch andere Vermögens- oder Nutzenfunktionen bieten).[112]

Nach der Definition der FATF gelten VASP in der Schweiz daher als Finanzintermediäre und sind somit dem GwG unterstellt.

Da das GwG grundsätzlich technologieneutral ist, gilt es bereits für Transaktionen mit virtuellen Vermögenswerten. Der Bundesrat hat bereits im Juni 2014 festgestellt, dass es

---

[110] Medienbericht der FINMA-Aufsichtsmitteilung 2019; TOMIC/MAUCHLE, S. 4.

[111] Gemäss Art. 7 Abs. 1 GwV gelten Dienstleistungen als gewerbsmässig erbracht, wenn die VASP: a) dadurch einen Bruttoumsatz von mehr als 50'000 Franken pro Kalenderjahr erzielt; b) mit mehr als 20 Vertragspartnern pro Geschäftsbeziehungen mit mehr als 20 Vertragspartnern pro Kalenderjahr eingeht, die sich nicht auf eine einmalige Tätigkeit beschränken; c) eine unbeschränkte Verfügungsgewalt über fremde Vermögenswerte von mehr als 5 Millionen Franken hat oder d) Transaktionen mit einem Gesamtvolumen von mehr als 2 Millionen Franken pro Jahr tätigt.

[112] Bericht des Bundesrates bezüglich DLT, S. 137 ff.

möglich ist, Kryptowährungen als Zahlungsmittel für reale Waren und Dienstleistungen zu verwenden und an Kryptobörsen zu handeln. Damit erfüllen Kryptowährungen wesentliche Funktionen von Geld und gelten unter der Schweizer Geldwäschereigesetzgebung als Vermögenswerte. Kryptowährungen können somit auch als Instrument oder Mittel zur Geldwäsche oder Terrorismusfinanzierung verwendet werden.[113]

Im Gegensatz zu den FATF-Standards ist in Art. 10 GwV-FINMA keine Ausnahme für Zahlungen mit unregulierten Wallet-Anbietern vorgesehen, da gemäss FINMA «eine solche Ausnahme unbeaufsichtigte Dienstleister begünstigen und dazu führen würde, dass beaufsichtigte Anbieter die Ausführung problematischer Zahlungen nicht verhindern könnten».[114] Solange also ein von der FINMA beaufsichtigtes Institut nicht in der Lage ist, die Bestimmungen von Art. 10 Abs. 1 GwV-FINMA zu erfüllen, d. h. die im Zahlungsverkehr erforderlichen Informationen zu senden und zu empfangen, sind solche Transaktionen von und zu externen Wallets nur zulässig, wenn diese einem eigenen Kunden bzw. einer eigenen Kundin des Instituts gehören und dessen bzw. deren Eigentum an dem externen Wallet mit geeigneten technischen Mitteln nachgewiesen wurde. Bei einer Überweisung von oder zu einer externen Wallet, die einer oder einem Dritten gehört, muss das Institut die Identität des bzw. der Dritten überprüfen, die Identität der wirtschaftlich berechtigten Person feststellen und das Eigentum des bzw. der Dritten nachweisen.[115] Die FINMA stellt in ihrer Aufsichtsmitteilung 02/2019 klar, dass die Informationen nicht zwingend über die Blockchain laufen bzw. übertragen werden müssen. Die Übermittlung kann über andere Kommunikationskanäle erfolgen.

4.1.2 Anti-Geldwäsche-Richtlinie Nr. 5 und Nr. 6

Aufbauend auf den FATF-Empfehlungen hat das Europäische Parlament im April 2018 die Richtlinien (5AMLD oder AMLD5) zur Konkretisierung der FATF-Empfehlungen erlassen. Die Richtlinien decken die Aspekte der Geldwäschereibekämpfung ab.

[113] Bericht des Bundesrates bezüglich DLT, S. 137 ff.

[114] FINMA-Aufsichtsmitteilung 2019, S. 3; Tomic/Mauchle, S. 3.

[115] FINMA-Aufsichtsmitteilung 2019, S. 3.

Im Zusammenhang mit Kryptowährungen und digitalen Vermögenswerten sind folgende Artikel der 5AMLD massgebend:

- Art. 10–24 (Sorgfaltspflicht gegenüber der Kundschaft)
- Art. 33–35 (Meldung verdächtiger Transaktionen)
- Art. 40 (Aufbewahrung von Aufzeichnungen)
- Art. 45 und 46 (interne Kontrollen)

Im Weiteren ist für Kryptowährungen und digitale Vermögenswerte Folgendes relevant:

- Onboarding von Depotbanken und VASP[116] gemäss dem Anwendungsbereich der Richtlinie
- erhöhte Aufsichtsanforderungen in Bezug auf politisch exponierte Personen (PEP)
- Anforderungen an Anbieter von virtuellen Währungen und Verwahrer/-innen zur Durchführung von Abklärungen sowohl bei Bestands- als auch bei Neukundschaft

Nach der Richtline 5 erliess das Europäische Parlament die sechste Geldwäscherichtlinie (6AMLD), welche am 3. Dezember 2020 in Kraft trat und bis zum 3. Juni 2021 umgesetzt werden musste.[117] Die neue Richtline baut auf ihrem Vorgänger auf und fokussiert die Harmonisierung-Definitionen. Darin heisst es: «*Die Verwendung virtueller Währungen birgt neue Risiken und Herausforderungen im Hinblick auf die Bekämpfung der Geldwäsche. Die Mitgliedstaaten sollten sicherstellen, dass diesen Risiken angemessen begegnet wird.»*[118]

4.1.3 Transfer-of-Funds-and-certain-Crypto-Assets-Regulation

Am 29. Juni 2022 wurde der vorläufige Text der *Transfer-of-Funds-and-certain-Crypto-Assets-Regulation* (TFR) durch das EU-Parlament, den EU-Rat und die EU-Kommission angenommen.[119] Die TFR wurde schliesslich am 20. April 2023 durch das EU-Parlament offiziell als Teil des Markets-in-Crypto-Assets(MiCA)-Regulierungspakets

[116] Kapitel 4.1.1.4.

[117] KIELY, Why is it changing?.

[118] EU - Richtlinie 2018/1673.

[119] Europäisches Parlament (Pressemitteilung TFR-Entwurf).

angenommen.[120] Diese Regelung wurde eingeführt, um die Travel Rule der FATF umzusetzen und ihre Anwendung auf Kryptotransaktionen in Europa auszuweiten.[121] Die MiCA und demnach auch die TRF werden voraussichtlich 2024 in Kraft treten.[122]

Mit der TFR werden neue Vorschriften für Transaktionen von Kryptodienstleistern wie Kryptobörsen, ungehosteten Wallets und selbstgehosteten Wallets eingeführt.[123] Insbesondere gelten folgende Bestimmungen im Zusammenhang mit Transaktionen von Kryptodienstleistern:

- Jede Kryptotransaktion muss, unabhängig von ihrem Wert, der auftraggebenden und der empfangenden Person zugeordnet werden können.[124]

- Kryptodienstleister müssen umfangreiche Informationen über die auftraggebende und die begünstigte Person einer Transaktion erfassen, darunter die Namen, Adressen, nationale Identifikationsnummern, Wallet-Adressen, Bankdaten und den Wohnsitz.[125]

- Unternehmen, die Kryptodienstleistungen innerhalb der EU anbieten, sind verpflichtet, die geltenden Geldwäschebestimmungen einzuhalten.[126]

- Die Vorschriften gelten auch für Transaktionen mit ungehosteten Wallets, wenn diese mit gehosteten Wallets interagieren, die von Kryptodienstleistern verwaltet werden.[127] Ein ungehostetes Wallet ist ein Wallet, das von der anwendenden Person selbst verwaltet wird. Wenn ein Kunde bzw. eine Kundin mehr als 1.000

[120] Europäisches Parlament (Pressemitteilung TFR-Entscheid).

[121] Europäisches Parlament (Pressemitteilung TFR-Entwurf); (TFR-Entwurf), S. 3; (Pressemitteilung TFR-Entscheid).

[122] MAEDER (MiCA).

[123] Europäisches Parlament (Pressemitteilung TFR-Entwurf); (TFR-Entwurf), S. 3; (Pressemitteilung TFR-Entscheid); REVOREDO, die Hauptpunkte der Transfer of Funds Regulation (MiCA und TFR).

[124] Europäisches Parlament (TFR-Entwurf), S. 25.

[125] Europäisches Parlament (TFR-Entwurf), S. 31.

[126] Europäisches Parlament (TFR-Entwurf), S. 24.

[127] Europäisches Parlament (TFR-Entwurf), S. 14.

Euro an ein eigenes ungehostetes Wallet sendet oder von diesem empfängt, muss der Kryptodienstleister überprüfen, ob das ungehostete Wallet tatsächlich im Besitz oder unter der Kontrolle des Kunden bzw. der Kundin steht.[128]

- Die erweiterten Bestimmungen gelten auch dann, wenn EU-ansässige Kryptodienstleister mit Marktteilnehmenden ausserhalb der EU zusammenarbeiten.[129]

4.1.3.1 Herausforderungen einer einheitlichen Anwendung der Travel Rule

Die einheitliche Anwendung der Travel Rule im Europäischen Wirtschaftsraum und in der Schweiz hat zu Kritik seitens betroffener Dienstleister und Intermediäre bzw. Intermediärinnen geführt.[130] Die Praxis steht vor erheblichen und kostspieligen Herausforderungen – zumal die Travel Rule besagt, dass Kryptodienstleister die Identität von Privatpersonen überprüfen müssen, insbesondere im Falle von eigenverwahrten Wallets, auch bekannt als ungehostete Wallets. Die Identifizierung und Überprüfung jedes einzelnen privaten Wallets erweist sich als sehr aufwendig und zeitintensiv.

Als Reaktion auf diese Anforderungen besteht die Möglichkeit, dass Dienstleister die Geschäftsentscheidung treffen, generell keine Transaktionen mehr mit ungehosteten Wallets anzubieten. Dies würde faktisch dazu führen, dass nur noch zugelassene Kryptoverwahrer/-innen genutzt werden können. Diese Entwicklung steht im Widerspruch zum dezentralen Vorgehen in Bezug auf Kryptowährungen und würde ein zusätzliches Drittparteirisiko bedeuten. Eine solche Einschränkung könnte zu einer erheblichen Zentralisierung des Kryptomarktes führen, was wiederum die technische Innovation der Blockchain-Technologie und ihre dezentralen Transaktionen ohne die zwingende Einbindung von Dienstleistern beeinträchtigen würde.[131]

[128] Europäisches Parlament (TFR-Entwurf), S. 15.

[129] Europäisches Parlament (TFR-Entwurf), S. 34.

[130] REVOREDO, Abschliessende Überlegungen (MiCA und ToFR); Tomic/Mauchle, S. 6.

[131] REVOREDO, Abschliessende Überlegungen (MiCA und ToFR); Tomic/Mauchle, S. 6.

4.1.3.2 Standardisiertes Travel-Rule-Protokoll

Die Travel Rule kann ihr volles Potenzial zur Geldwäschebekämpfung nur dann entfalten, wenn ein Messaging-Standard auf globaler Ebene etabliert würde.[132]

Als die Travel Rule für Fiat-Zahlungen eingeführt wurde,[133] war der technische Einfluss auf Finanzinstitute gering, da die Branche bereits Messaging-Standards für inländische und grenzüberschreitende Zahlungen entwickelt hatte (z. B. ISO20022, Society for Worldwide Interbank Financial Telecommunication [SWIFT] und Single Euro Payments Area [SEPA]).[134]

Durch die Nutzung dieser Messaging-Standards waren Finanzinstitute gut vorbereitet, um Informationen im Rahmen der Travel Rule effizient auszutauschen.[135] Die vorhandenen Standards ermöglichten es den Institutionen, die erforderlichen Daten in einer standardisierten und strukturierten Form zu übermitteln. Dadurch konnten sie die Anforderungen der Travel Rule erfüllen, ohne grössere technische Anpassungen vornehmen zu müssen.[136]

Die Nutzung dieser bereits etablierten Standards bot den Finanzinstituten den Vorteil, dass sie auf bewährte und erprobte Systeme zurückgreifen konnten. Dadurch wurde die Implementierung der Travel Rule in Bezug auf Fiat-Zahlungen erleichtert und der Betriebsablauf der Institutionen nur geringfügig beeinträchtigt. Die bestehenden Messaging-Standards hatten sich als zuverlässig und effektiv erwiesen, um Zahlungen auf nationaler und internationaler Ebene abzuwickeln.[137]

Insofern verlief der technische Übergang zur Einhaltung der Travel Rule in Bezug auf Fiat-Zahlungen vergleichsweise reibungslos. Finanzinstitute konnten auf ihren bereits vorhandenen Infrastrukturen und Systemen aufbauen, um die erforderlichen Informationen auszutauschen und die Anforderungen der Regelung zu erfüllen. Dies trug

---

[132] ALLISON (Messaging Standard); BRUNONE /MOLO, S. 306.

[133] Kapitel 4.1.1.2.

[134] GRECO /KRAMER, Rz. 2637 ff.

[135] GRECO /KRAMER, Rz. 2637 ff.

[136] BRUNONE /MOLO, S. 306.

[137] GRECO /KRAMER, Rz. 2637 ff.

massgeblich dazu bei, dass der Betrieb der Finanzinstitute weitgehend stabil blieb und unnötige technische Herausforderungen vermieden werden konnten.

Weder die FATF noch nationale Behörden wie die FINMA empfiehlt die Verwendung eines spezifischen Messaging-Standards der Travel Rule für virtuelle Vermögenswerte.[138] Daher arbeiten verschiedene Organisationen an SWIFT-ähnlichen Protokollen der zweiten Ebene, um Transaktionsinformationen gemäss der Travel Rule zu übermitteln (z. B. Travel Rule Protocol [TRP], OpenVASP, 21 Analytics usw.). Es ist noch nicht absehbar, welches Protokoll sich global durchsetzen wird. Daher müssen VASP derzeit zur Einhaltung der Vorschriften die relevanten Informationen auf herkömmliche Weise wie sichere E-Mails austauschen. Diese Methode ist kostspielig, da VASP mit jedem Gegenpartei-VASP bilaterale Vereinbarungen treffen und klären müssen, wann, welche und wie Informationen übermittelt werden sollen.[139] Das Fehlen globaler Messaging-Standards der Travel Rule lässt weiterhin viel Raum für nicht konforme VASP, da sie sich immer auf die fehlende Standardisierung berufen können – insbesondere in Ländern, die nicht vorgeben, wie VASP mit (unregulierten) VASP in Rechtsgebieten interagieren sollen, in denen die Travel Rule noch nicht umgesetzt wurde.

4.1.4 Sanktionen und Mining des US-Office of Foreign Assets Control

Bei der Bekämpfung von Geldwäscherei sind Sanktionen elementar – vor allem die Liste des US-Office of Foreign Assets Control (OFAC), welche regelmässig Listen von Personen und Unternehmen veröffentlicht, die aus diversen Gründen wie nationalen Sicherheitsbedenken oder einer Verbindung zum Drogenhandel und Terrorismus mit Sanktionen belegt sind.[140] Bereits im Bereich des Krypto-Ökosystems waren Sanktionen von zentraler Bedeutung. Im Mai 2021 gab das US-Mining-Unternehmen *Marathon Digital Holding* bekannt, dass es den ersten Bitcoin-Block geschürft habe, welcher vollkommen OFAC-konform sei – zumal sämtliche Transaktionen von sanktionierten Subjekten gemäss der OFAC-Sanktionsliste ausgeschlossen wurden.[141] Das Vorhaben wurde jedoch in der Krypto-Szene stark kritisiert – insbesondere weil es nach Ansicht der

[138] ALLISON (Messaging Standard); BRUNONE /MOLO, S. 305.

[139] ALLISON (Messaging Standard).

[140] U.S. Department of the Treasury, OFAC.

[141] GOSCHENKO, A Looming Fungibility Problem.

Kritiker/-innen eine Zensur darstellt, welche mit dem Gedankengut der Dezentralisierung von Bitcoin nicht vereinbar sei.[142] Kurz darauf wurde das OFAC-konforme Mining durch das Unternehmen eingestellt.[143]

4.1.5 Financial Crimes Enforcement Network

Das Financial Crimes Enforcement Network (FinCEN) ist Teil des US-Finanzministerium und soll das Finanzsystem vor illegaler Nutzung schützen. Der Ablauf ist dabei folgender: Das FinCEN erhält Daten über Finanztransaktionen. Diese Daten werden anschliessend für Strafverfolgungszwecke analysiert und mit einem globalen Netzwerk von Parteiorganisationen in anderen Ländern geteilt, um die Integrität des Finanzsystems in der Bekämpfung der Geldwäschebemühungen von Kriminellen zu fördern.[144]

Das FinCEN fungiert in diesem Netzwerk als Finanical Intelligence Unit (FIU) für die USA. Grundsätzlich können auch private Unternehmen die Funktion als FIU wahrnehmen. In der Regel wird jedoch in einem staatlichen Kontext eine zentralisierte nationale Behörde als FIU ernannt. In der Schweiz nimmt die Meldestelle für Geldwäscherei (MROS) im Bundesamt für Polizei (fedpol) die Funktion als FIU wahr.[145] Ein FIU sammelt, analysiert und gibt behördlich offengelegte Finanzinformationen im Zusammenhang mit mutmasslichen Erträgen aus Straften an andere FIU weiter, um die Geldwäscherei und Terrorismusfinanzierung in einem internationalen Kontext anzugehen.[146] Weltweit existieren über 100 staatliche FIU, einschliesslich FinCEN und MROS, welche alle der «Egmont-Gruppe» angehören.[147]

[142] POST, Controversy.

[143] HARKIN, Tech.

[144] FinCEN, Office of Strategic Communications, 703-905-3770 (Extends Comment Period).

[145] FEDPOL, Geldwäscherei (MROS).

[146] FinCEN (What we do).

[147] Egmont Group of Financial Intelligence Units, (Egmont Group FIU).

4.1.5.1 Kontroverse für nicht gehostete Wallets

Die FinCEN präsentierte Anfang Dezember 2020 eine neue Empfehlung im Zusammenhang mit der Geldwäschereibekämpfung, um die BSA-Anforderungen um spezifische Kryptowährungs-Meldepflichten für Finanzinstitute zu ergänzen.

Dabei wurden Meldepflichten für jene Wallets eingeführt, welche durch Finanzinstitute gehostet wurden und mit einer einzelnen Transaktion oder mit diversen Transaktionen einen Gesamtwert von mehr als 10'000 USD überschritten.

Der Vorschlag wurde in der Krypto-Community jedoch stark kritisiert – darunter von Jack Dorsey, dem CEO von Square Inc., und Brian Armstrong, dem CEO und Mitgründer von Coinbase.[148] Dabei wurden die nachfolgenden Einwände hervorgebracht:

- Finanzinstitute gaben Datenschutzbedenken kund – zumal die neuen Daten für den Report grösstenteils Daten von Hacks von privaten sowie staatlichen Einrichtungen beinhalten würden, einschliesslich der Daten des gross angelegten SolarWinds-Hacks, der 18 000 Netzwerke angriff, wobei das US-Finanzministerium selbst ein Opfer war.[149]

- Der Ansatz, von Finanzinstituten zu verlangen, Daten von Personen und Einrichtungen zu sammeln, die nicht einmal zur Kundschaft der meldepflichtigen Finanzinstitute zählen, scheint weniger effizient als z. B. die Wallet-Adressen über die Blockchain nach illegalen Aktivitäten zu durchsuchen.

- Durch die neue FinCEN-Empfehlung würden Einzelpersonen massiv eingeschränkt, wenn sie Krypto-Vermögenswerte zwischen Finanzinstituten transferieren. Dies hätte zur Folge, dass zukünftig regulierte Einrichtungen für Kryptowährungen gemieden und mehr Transaktionen über nicht regulierte Einrichtungen getätigt würden.

[148] Square, Inc. (Federal Comment Letter).

[149] WHITAKER (Solar Winds).

- Durch die vagen Ausformulierungen von Schlüsselbegriffen würde Unklarheit herrschen – u. a. fehle die Definition, was genau unter einer *nicht gehosteten Wallet* zu verstehen ist.

Im Weiteren wurden dahingehend Bedenken geäussert, dass sich die neuen Empfehlungen negativ auf den DeFi-Bereich auswirken könnten – zumal viele solcher Projekte Smart Contracts verwenden, um Treuhandgelder automatisch zu speichern. Ferner verwenden DeFi-Smart-Contract-Plattformen, im Unterschied zu herkömmlichen Unternehmen, keine physischen Adressen. Durch die Empfehlungen sei die Existenz von DeFi-Plattformen im Allgemeinen gefährdet.[150] All dies führe dazu, dass bei der FinCeN über 7500 Beschwerden eingingen und die Frist zur Einreichung von Beschwerden verlängert werden musste. In der Zwischenzeit wurden die Empfehlungen nochmals überarbeitet.[151]

[150] DE NIKHILESH (FinCEN's Wallet Rule)

[151] FinCEN (Extends Comment Period).

4.2 Gesetzlicher Rahmen für Kryptowährungen und Meldewesen

Nachfolgend werden die Geldwäschereibestimmungen von Deutschland, der Schweiz und dem Vereinigten Königreich in Bezug auf ihre Handhabung im Umgang mit Kryptowährungen verglichen, da in den drei Staaten eine unterschiedliche Haltung zu erkennen ist.

4.2.1 Vereinigtes Königreich

Die Geldwäschebekämpfungsvorschriften des Vereinigten Königreichs beruhen primär auf dem Proceeds of Crime Act (PoCA 2002) und den Money Laundering Regulations (MLR 2003).[152]

Mit dem PoCA wird der Tatbestand der Geldwäscherei in Abschnitt 340(11)(a) als das Verbergen von kriminellen Vermögenswerten (Art. 327) und das Eingehen von Vereinbarungen zum illegalen Geldtransfer (Art. 328) sowie der Erwerb, die Verwendung und der Besitz solcher Vermögenswerte (Art. 329) unter Strafe gestellt. Die Tätigkeit, Planung oder Anstiftung zur Begehung von Straftaten nach Art. 327, 328 und 329 fallen unter die Definition der Geldwäscherei. Der Abschnitt 340(11) stellt u. a. auch die Erleichterung, Beratung, Beschaffung und Unterstützung der oder zur Geldwäscherei unter Strafe. Das PoCA sieht im Falle einer Verurteilung zur Geldwäscherei eine Freiheitsstrafe von 14 Jahren oder eine Geldstrafe vor.

Finanzinstitute, welche es versäumen, verdächtige Aktivitäten oder Geldwäscheaktivitäten zu melden, machen sich gemäss Abschnitt 340(11) strafbar. Mitarbeiter/-innen, die offensichtlich Kenntnis von der Geldwäscherei hatten und schweigen, können nach Abschnitt 330 belangt werden und riskieren gemäss Abschnitt 334 eine Freiheitsstrafe von 5 Jahren oder eine Geldstrafe. Das englische System zur Bekämpfung der Geldwäscherei zielt demnach nicht nur auf die Kontrolle der Täter/-innen, sondern auch jener ab, die von der Straftat wissen, sie verheimlichen oder ihre Sorgfaltspflichten nach Abschnitt 7 des MLR 2003 vernachlässigen. Darunter fällt auch das Versäumnis, eine Verdachtsmeldung abzusetzen, wenn gemäss dem KYC-Prinzip konkrete Hinweise dafür vorliegen, dass die Kundschaft in

[152] EDMONDS, S. 8 f.

Geldwäschereihandlungen verwickelt ist. Diese Verdachtsmeldungen muss das Finanzinstitut an die SOCA übermitteln. Die SOCA bildet das britische FIU, welche die SAR-Meldungen koordiniert, sammelt und analysiert und den Strafermittlungsbehörden weiterleitet.[153]

Die Financial Conduct Authority (FCA) ist im Vereinigten Königreich seit Januar 2020 damit beauftragt, die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu überwachen, den Vorgaben der FATF zu entsprechen sowie die fünfte EU-Geldwäschereirichtline umzusetzen.[154] Zeitgleich wurde die Vorschrift Nr. 33 der britischen Gesetzgebung zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung aus dem Jahre 2017 überarbeitet und dem Vorgehen der FCA angepasst.[155] Zu den bedeutsamsten Änderungen zählen:

- Die Ergänzung neuer Hochrisikokriterien zur Beurteilung der Notwendigkeit einer verstärkten Sorgfaltspflicht für die Kundschaft. Neuerdings gelten Transkationen zwischen Parteien in Hochrisikoländern sowie Geschäftsbeziehungen, welche auf dem Korrespondenzweg ohne besondere Schutzmassnahmen wie ein elektronisches Identifizierungsverfahren eröffnet wurden, als Hochrisikoindizien.

- Der Schwellenwert für monatliche Zahlungstransaktionen ohne allfällige Identifizierungspflichten wurde von 250 auf 150 EUR reduziert.

- Neuerdings müssen Widersprüchlichkeiten zwischen den Kundeninformationen, die dem Finanzinstitut über die wirtschaftliche Eigentümerschaft vorliegen, und jenen Informationen aus dem Register der Personen mit signifikanten Kontrollmöglichkeiten, dem Companie House Register, welches durch die britische Regierungsbehörde geführt wird, umgehend der FCA gemeldet werden.[156]

[153] Kapitel 4.1.4.

[154] FCA (Money Laundering Regulations).

[155] FCA (Money Laundering Regulations).

[156] Companies House (PSC).

Die neuen Vorschriften der FCA gelten einerseits für traditionelle Finanzinstitute und andererseits für Unternehmen mit Bezug zu Kryptowährungen, einschliesslich Kryptobörsen sowie Unternehmen, welche Krypto-Vermögenswerte ihrer Kundschaft schützen. Ferner mussten sich sämtliche bestehenden Unternehmen mit Bezug zu Kryptowährungen bis zum 10. Januar 2021 bei der FCA registrieren. Unternehmen, die eine solche Tätigkeit nach dem 10. Januar 2021 aufgenommen haben, mussten bereits zum Zeitpunkt der Geschäftstätigkeit bei der FCA angemeldet und registriert sein.

Wegen des kurzen Zeitraums zur Umsetzung der Vorschriften, welcher die Unternehmen zum Teil in ihrer Geschäftstätigkeit blockierte, führte die britische FCA im Dezember 2020 ein temporäres Registrierungssystem ein, damit bereits bestehende Unternehmen mit Bezug zu Kryptowährungen, welche die Registrierung bei der FCA bereits beantragt hatten, ihre Geschäftstätigkeit fortsetzen konnten, während der Antrag geprüft wurde.[157]

Um Druck auf die Kryptounternehmen auszuüben, damit sich diese bei der FCA anmelden und die neuen Vorschriften zur Bekämpfung der Geldwäscherei auch einhalten, hat die FCA eine Liste mit über 100 nicht registrierten Unternehmen publiziert, welche Dienstleistungen im Krypto-Asset-Bereich ausüben, die nicht bei der FCA registriert sind.[158]

4.2.2 Schweiz

In der Schweiz bilden das Strafgesetzbuch (StGB), das GwG sowie die entsprechende Verordnung (GwV) die Grundlage für das Geldwäschereibekämpfungsdispositiv. In Art. 305 StGB ist festgelegt, dass Geldwäscherei ein Vergehen oder eine Handlung darstellt, welche die Rechtsordnung stört bzw. die Rechtsordnung untergräbt. Folglich handelt es sich um ein Gemeindelikt, welches durch jeden Menschen begangen werden kann. Die finanzmarktrechtliche Ordnung wird durch das GwG sichergestellt, indem die Geldwäschereibekämpfung im Sinne von Art. 305 StGB mittels Auferlegung der notwendigen Sorgfaltspflichten für Finanzintermediäre angegangen wird. Aus den Sorgfaltspflichten kann das KYC-Prinzip bezüglich der Identifizierung der Vertragspartei

[157] FCA (Register).

[158] FCA (Warnung).

und der wirtschaftlich Berechtigten abgeleitet werden.[159] Die Finanzintermediäre sind meldepflichtig, wenn der Verdacht besteht, dass eine Straftat vorliegt oder eine Person verdächtigt wird, in irgendeiner Weise mit dem Verbrechen oder Vergehen nach Art. 305 StGB in Verbindung zu stehen. Ein solcher Verdacht muss der MROS[160] gemeldet werden, wobei die Konten der verdächtigen Person für fünf Tage gesperrt bleiben, bis die MROS über die Weiterleitung der Meldung an die Staatsanwaltschaft entscheidet.[161] Sofern die Voraussetzungen für eine Meldepflicht unklar sind, darf der Finanzintermediär trotzdem eine Meldung erstatten, ohne dass das Bankkundengeheimnis verletzt wird.[162] Die strafrechtlichen Konsequenzen sind in Art. 305 StGB und Art. 37 GwG aufgeführt.

Im Unterschied zur britischen Geldwäschereigesetzgebung ist das Schweizer Gesetz klarer ausformuliert – zumal in England drei Grunddelikte unter Strafe gestellt sind, während das GwG einen engeren Anwendungsbereich aufweist.[163] Ein weiterer Unterschied liegt darin, dass in der Schweiz Täter/-innen von Geldwäschereidelikten unabhängig von der Vortat bestraft werden können. Ebenso wie das Vereinigte Königreich sieht die Schweiz vor, dass eine im Ausland begangene Straftat in gleicher Weise strafbar ist wie im Herkunftsland – sofern das Land gleiche Bestimmungen für die Bestrafung nach Art. 305 StGB aufweist. In beiden Ländern wird die Geldwäscherei unterschiedlich streng bestraft. Während sie im Vereinigten Königreich eine Strafe von bis zu 14 Jahren Haftstrafe nach sich ziehen kann, wird sie in der Schweiz nach Art. 305 StGB nur mit bis zu drei Jahren Freiheitsstrafe sowie Geldbusse bestraft wird, wobei schwerwiegende Umstände die Haftstrafe um zwei Jahre erhöhen können.

Im Gegensatz zum Vereinigten Königreich werden in der Schweiz nicht diejenigen bestraft, welche es versäumen, eine Meldung abzusetzen, sondern diejenigen, die ihre Kundschaft nicht korrekt identifizieren. Im Falle der Missachtung der Identifizierungspflichten droht eine Freiheitsstrafe von bis zu einem Jahr oder eine

[159] Identifizierung der Vertragspartei (Art. 3–5 GwG), Abklärungspflichten (Art. 6 GwG) und Dokumentationspflichten (Art. 7 GwG).

[160] Kapitel 4.1.4.

[161] Meldepflichten (Art. 9 GwG) und Vermögenssperren (Art. 10 GwG).

[162] Melderecht (Art. 305ter StGB).

[163] WRONKA, S. 665.

Geldstrafe. Die Unterlassung einer Meldung bildet keine Straftat, solange dies nicht absichtlich erfolgt. Im Vergleich zum Vereinigten Königreich setzt die Schweiz weitaus weniger Verdachtsmeldungen ab, weist aber dennoch eine höhere Einziehungsquote auf.[164] Im vereinigten Königreich wurden im Jahr 2020 insgesamt 573'085 Verdachtsmeldungen von Geldwäsche und Terrorismusfinanzierung registriert.[165] In der Schweiz wurden im gleichen Jahr lediglich 5'334 Meldungen von Verdachtsfällen von Geldwäsche, Terrorismusfinanzierung und Sanktionsverstössen abgesetzt.[166] Der britische Ansatz, mehr auf die Quantität als auf die Qualität zu fokussieren, scheint demnach eine gewisse Ineffizienz aufzuweisen, wenn man berücksichtigt, dass jede Verdachtsmeldung Zeit und Geld kostet. Ferner droht die Gefahr, dass die zuständigen Behörden die Verdachtsmeldungen nicht effizient und rechtzeitig bearbeiten können.

Vor dem Hintergrund, dass der Schweizer Gesetzgeber der Blockchain-Technologie ein positives Potenzial für die Finanzindustrie zuschreibt, besteht eine positive Einstellung gegenüber Kryptowährungen.[167] In Bezug auf die Geldwäschereibekämpfung hat die Schweiz die gesetzlichen Bestimmungen so angepasst, dass Kryptowährungen und andere digitale Vermögenswerte in den gleichen Geltungsbereich des GwG fallen.[168] Dadurch werden Unternehmen, die mit Kryptowährungen handeln oder Dienstleitungen im Kontext mit digitalen Vermögenswerte anbieten, verpflichtet, die gleichen Sorgfaltspflichten zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung einzuhalten wie traditionelle Finanzinstitute. In diesem Zusammenhang wurden diverse Richtlinien und Standards in Bezug auf Kryptowährungen seitens FINMA für den Schweizer Finanzmarkt entwickelt. Auch die Bestimmungen bezüglich der Anwendung der Travel Rule gem. Art. 10 GwV-FINMA wurden konkretisiert.[169] Die neue konkretisierte Travel Rule nimmt sich der Problematik der Dezentralität von Blockchain-Transaktionen an.[170] Die FINMA hat darüber hinaus die Lizenzierung von

[164] WRONKA, S. 668.

[165] National Crime Agency (SARs Annual Report 2020), S. 4.

[166] FEDPOL (MROS), S. 16.

[167] Faktenblatt Krypto, S. 2; LANDERER. S. 25.

[168] DRZALIC /MOLO, S. 49; BRUNONE /MOLO S. 304.

[169] Kapitel 4.1.1.5.

[170] Kapitel 3.2.1.2.

Kryptounternehmen eingeführt, die bestimmten Voraussetzungen erfüllen müssen, um in der Schweiz tätig sein zu dürfen.[171]

4.2.3 Deutschland

In Deutschland bilden das Strafgesetzbuch (DStGB), die Strafprozessordnung (DStPO) sowie das Geldwäschegesetz (DGwG) die Grundlagen für das Geldwäschereibekämpfungsdispositiv. Der Straftatbestand der Geldwäsche ist in Deutschland in § 261 DStGB geregelt und soll verhindern, dass illegale Einkünfte in den legalen Wirtschaftskreislauf eingeschleust werden, deren Herkunft verschleiert wird und der Anschein erweckt wird, dass sie auf legale Weise erworben wurden.[172] Die Vortat wird jedoch gem. § 261 Abs. 1 DStGB eingeschränkt. Gemäss Abs. 2 wird auch der Besitz oder die Verwendung von Vermögenswerten, die aus einer rechtswidrigen Tat stammen, unter Strafe gestellt.Vor 2021 musste die Geldwäscherei auf einer von mehreren Katalogvortaten basieren,[173] wobei es sich hauptsächlich um schwere Vergehen handelt, welche von Banden oder auf kommerzieller Basis begangen werden mussten.[174] Dank der überarbeiteten Fassung von § 261 DStGB ist der Bezug zu einer bestimmten Straftat nicht mehr erforderlich; nun reicht es aus, wenn die Geldwäscherei aus einer «rechtswidrigen Handlung» herrührt, um den Straftatbestand der Geldwäscherei zu erfüllen.[175] Ebenso wie in der Schweiz und dem Vereinigten Königreich wird eine im Ausland begangene Straftat gleich geahndet, wenn das Land über gleiche Gesetze verfügt.

Anders als in Grossbritannien und in der Schweiz wird in Deutschland die Vortat bei der Strafbarkeit der Geldwäscherei nicht mitbestraft.[176] Das bedeutet, dass es in Deutschland grundsätzlich ausreicht, wenn die Täterin bzw. der Täter weiss oder zumindest damit rechnet, dass die Vermögenswerte aus einer rechtswidrigen Tat stammen, um sich der Geldwäscherei strafbar zu machen.[177] Den Grund für die Aufteilung bildet das Trennungsprinzip, welches besagt, dass jede Tat für sich alleine betrachtet und geahndet

[171] FINMA-Entwicklung 2018.

[172] NEUHEUSER, Münchener Kommentar, Rn. 35, 36 zu § 261 DStGB

[173] Scherp/Wrocklage, S. 188.

[174] Comply Advantage (Neudefinition der Geldwäsche in Deutschland).

[175] Comply Advantage (Neudefinition der Geldwäsche in Deutschland).

[176] WRONKA, S. 667.

[177] HEGER MARTIN, Kommentar zu DStGB Rn. 104 zu, § 261 DStGB.

wird. Folglich wird jede Straftat, einschliesslich der Geldwäscherei, unabhängig von der Vortat beurteilt, um zu verhindern, dass eine doppelte Bestrafung für die Vortat und die Geldwäschereihandlung erfolgt. Das Trennungsprinzip trägt ferner dazu bei, dass sich Täter/-innen durch die Geldwäscherei nicht der Strafverfolgung entziehen können, wenn eine Vortat unaufgeklärt bleibt oder verjährt.

Auch in Deutschland wird die Geldwäscherei milder bestraft als in Grossbritannien – zumal das Strafmass je nach Schwere zwischen drei Monaten und fünf Jahre Freiheitsstrafe, variieren kann. Ähnlich wie in der Schweiz kann in schweren Fällen die Haftstrafe verlängert werden. Die deutsche Geldwäschereigesetzgebung unterscheidet sich insofern von der Schweizer und der britischen, als ein fahrlässig begangenes Verbrechen oder eine Straftat ein Strafmass von bis zu zwei Jahren nach sich zieht.

In den allgemeinen Sorgfaltspflichten nach § 10 DGwG ist u. a. vorgesehen, dass die Vertragsparteien nach § 11 identifiziert und die an den eingebrachten Vermögenswerten wirtschaftlich Berechtigten festgestellt und ebenfalls identifiziert werden. Neben der Identifizierungspflicht besteht nach § 42 DGwG bei dem Verdacht von Geldwäscherei oder der Terrorismusfinanzierung eine Meldepflicht. Die Meldung hat bei der deutschen FIU,[178] der Generalzolldirektion, einzugehen.[179] Natürliche Personen, welche die Sorgfaltspflichten missachten, können mit einer Busse von bis zu 150'000 EUR (§ 56 Abs. 1 S. 2 DGwG) und in schwerwiegenden Fällen sogar von bis zu 1'000'000 EUR (Abs. 3) bestraft werden. Die Finanzinstituten drohen jedoch höhere Geldbussen von bis zu 5'000'000 EUR oder 10 Prozent des Gesamtumsatzes. Ebenso wie in der Schweiz liegt in Deutschland der Fokus des Geldwäschereibekämpfungsdispositivs auf der Identifizierungspflicht, wohingegen im Vereinigten Königreich die Meldepflicht im Vordergrund steht.[180] So stieg die Anzahl britischer Verdachtsmeldungen von 2019 auf 2020 um 19%.[181] Der Grund könnte darin liegen, dass die englischen Compliance-Mitarbeiter/-innen im Gegensatz zu Deutschland und der Schweiz mehr Verdachtsmeldungen absetzen, um eine Strafverfolgung zu vermeiden. Aufgrund des oben erläuterten Trennungsprinzips führen Verdachtsmeldungen in Deutschland nicht zur

[178] Kapitel 4.1.4.

[179] Generalzolldirektion (FIU).

[180] WRONKA, S. 667.

[181] National Crime Agency (SARs Annual Report 2020), S. 4.

direkten Verfolgung der Vortat. Demnach kann die Einziehungsquote der Verdachtsmeldungen von Deutschland mit jener des Vereinigten Königreichs und der Schweiz verglichen werden.

Hinsichtlich der Anpassung der Gesetzesbestimmung in Bezug auf Kryptowährungen wurden im Jahr 2020 in Deutschland die im Jahr 2018 in Kraft getretenen EU-Richtlinien[182] implementiert, wodurch neue regulatorische Anforderungen für Anbieter von Kryptowährungen vorgesehen waren und eine Zulassungsregelung für Kryptobörsen eingeführt wurde. Zusammenfassend lässt sich sagen, dass die Gesetzesbestimmungen in Bezug auf Kryptowährungen verlangen, dass die dem DGwG unterstellten Finanzinstitute die regulatorischen Anforderungen erfüllen, einschliesslich der Sorgfaltspflichten.[183]

4.2.3.1 Umgang mit Kryptowährungen

Das Vereinigte Königreich ist ein weltweit führendes Zentrum für *FinTech*, d. h. die Nutzung von Technologien zur Erleichterung der Finanztechnologie.[184] Diese Stellung möchte das Vereinigte Königreich auch in Zukunft verteidigen.[185] Um dies zu reichen, wurde der Gesetzgeber damit beauftragt, die gesetzliche Grundlage zu überarbeiten.[186] Unter anderem wurden Bestimmungen erlassen, um die oben erläuterte Problematik und die damit verbundenen Gefahren der Anonymität zu reduzieren.[187]

Die Schweiz wird oft als «Crypto Valley» bezeichnet, zumal sich dort zahlreiche Blockchain- und Kryptounternehmen angesiedelt haben.[188] Der Begriff wurde aufgrund der hohen Konzentration solcher Unternehmen im Kanton Zug populär.[189] Seit Februar 2021 können natürliche und juristische Personen, welche in Zug ansässig sind, ihre

[182] Kapitel 4.1.2.

[183] Bundesanstalt für Finanzdienstleistungsaufsicht (Geldwäscherechtliche Hinweise).

[184] WARREN (UK's fintech).

[185] UK regulatory approach, S. 2 f.

[186] UK regulatory approach, S. 34 ff.

[187] Kapitel 3.2.1.1.

[188] Faktenblatt Krypto, S. 2; LANDERER. S. 25; MÜLLER/ONG, S. 212.

[189] Gem. Cryptovalley Directory bestehen per Ende Oktober 2022 insgesamt 453 Unternehmen mit Sitz in der Schweiz, welche im Bereich Blockchain fungieren; siehe https://cryptovalley.directory/company-directory, aufgerufen am 21. November 2022.

Steuerrechnung mit ausgewählten Kryptowährungen bezahlen.[190] Zu den bekanntesten Blockchain- und Kryptounternehmen mit Sitz in der Schweiz zählt Ethereum. Für diese Akutere ist es somit elementar, dass klare gesetzliche Rahmenbedingungen vorliegen.[191] Die Schweiz wurde bereits im Jahr 2016 als ein krypto-freundliches Land angesehen, da es Unternehmen im Bereich der Kryptowährungen erlaubt ist, legal in der Schweiz zu agieren, solange sie sich an die Vorschriften zur Geldwäscheprävention halten und über die erforderlichen Lizenzen verfügen. Dies hat dazu beigetragen, dass sich die Schweiz zu einem wichtigen Standort für Kryptounternehmen entwickelt hat. Die Schweiz hat eine liberale und innovative Haltung gegenüber neuen Technologien wie Blockchain und Kryptowährungen eingenommen und verfolgt das Ziel, ein günstiges Umfeld für diese Unternehmen zu schaffen. Unternehmen wie Ethereum profitieren von dieser Haltung und können ihre Geschäftsaktivitäten in einem Umfeld betreiben, das Rechtssicherheit und Flexibilität bietet, um Innovationen voranzutreiben. Durch die Einhaltung der regulatorischen Vorgaben können sie ihre Reputation als vertrauenswürdige und seriöse Akteure in der Branche stärken.

Deutschland wird im Vergleich zu den anderen beiden Ländern nicht als Vorreiter angesehen, wenn es darum geht, das regulatorische Umfeld in Bezug auf Kryptowährungen anzupassen. Dennoch existiert in Deutschlang eine Gesetzgebung für virtuelle Währungen, welche eine Genehmigung durch die Bundesanstalt für Finanzdienstleistungen (BaFin) voraussetzt. Die BaFin verlangt von Kryptounternehmen die Einhaltung der Geldwäschereibestimmungen, um Geldwäscherei und andere illegale Aktivitäten zu verhindern.

4.2.3.2 Vergleich der Krypto-Regulierungsansätze

In Bezug auf die Haltung gegenüber Kryptowährungen und den dahinter steckendenden DLT-Technologien weisen die drei Länder unterschiedliche Regulierungsansätze auf. Der britische Gesetzgeber hat früh eine positive Einstellung eingenommen, indem er bereits im Jahr 2018 eine Arbeitsgruppe einrichtete, um die Auswirkungen von Kryptowährungen und deren Technologie auf die Wirtschaft und die Gesellschaft zu untersuchen. Die Arbeitsgruppe hat in ihrem Bericht an die britische Regierung

[190] Kanton Zug (Kryptowährungen Bezahlung Steuern); MÜLLER/ONG, S. 212.

[191] Faktenblatt Krypto, S. 2; LANDERER. S. 25.

empfohlen, Kryptowährungen und die darin enthaltene DLT zu unterstützen, um deren Potenzial voll auszuschöpfen, Innovation zu fördern und ihre Vorreiterrolle im FinTech-Bereich zu festigen. In Anbetracht dieser Empfehlung hat die britische Regierung im Jahr 2020 neue Vorschriften erlassen, in denen die Finanzinstitute mit Bezug zu Kryptowährungen verpflichtet werden, die gleichen Bestimmungen bezüglich der Geldwäschereibekämpfung einzuhalten wie herkömmliche Finanzinstitute. Das bedeutet, dass Finanzinstitute mit Bezug zu Kryptowährungen die Kundschaft identifizieren und verdächtige Transaktionen melden müssen. Ferner wurde die FCA zum Aufsichtsorgan für Unternehmen mit Bezug zu Kryptowährungen ernannt, einschliesslich Kryptobörsen sowie Unternehmen, welche Krypto-Vermögenswerte ihrer Kundschaft schützen. Die FCA forderte schliesslich, dass sich all diese ihnen neu unterstehenden Institute bei ihnen registrieren. Die oben erläuterten Herausforderungen in Bezug auf den Registrierungsprozess verdeutlichen die Wechselwirkungen zwischen dem Krypto-Ökosystem und den Finanzaufsichtsbehörden, um die praktischen Aspekte der Einhaltung von Vorschriften mit dem Ziel der staatlichen Aufsicht in Einklang zu bringen.

Insgesamt zeigt auch die Schweizer Gesetzgebung eine positive Haltung mit einem regulatorischen Rahmen, der den Unternehmen in diesem Bereich im Allgemeinen wohlgesonnen ist.[192] So wurde Zug in den letzten Jahren zu einem bedeutenden Zentrum für Kryptowährung- und DLT-Unternehmen, so dass die Stadt als *Crypto Valley* bezeichnet wird. Die Einführung eines klaren regulatorischen Rahmens, welcher die Entwicklung solcher Unternehmen förderte, war dafür ein entscheidender Faktor – zumal sich die Schweiz bereits früh als innovationsfreundliches Land positionierte und spezifische regulatorische Massnahmen ergriff, um den Sektor zu fördern und zu kontrollieren. Seit 2018 erarbeitete die FINMA spezifische Leitlinien für Initial-Coin-Offerings (ICO), welche die Ansiedlung in Zug erst ermöglichten. Mithilfe der ICO finanzieren sich nämlich Kryptounternehmen durch die erstmalige Herausgabe ihrer Kryptowährungen. In den Leitlinien wird insbesondere die Einhaltung der Anti-Geldwäscherei-Bestimmungen betont. Zusammenfassend lässt sich sagen, dass der regulatorische Rahmen einen relevanten Faktor für die Entwicklung von Zug als *Crypto Valley* bildete. Durch die Bereitstellung klarer Regeln und Anforderungen schafft die

[192] LANDERER. S. 25; MÜLLER/ONG, S. 212.

FINMA ein sicheres Umfeld für Investorinnen und Investoren und fördert die Entwicklung von Unternehmen im Krypto-Ökosystem.

Deutschland weist hingegen eine gewisse Zurückhaltung gegenüber Kryptowährungen und DLT-Technologien auf – zumal es im Gegensatz zu den anderen beiden Ländern keine Top-FinTech-Positionierung oder kein Crypto Valley besitzt, die bzw. das es verteidigen muss. Folgende Entscheidungen können sinnbildlich für die defensive Haltung gegenüber Kryptowährungen herangezogen werden: Im Jahr 2019 wurden in Deutschland die Verkäufe von binären Optionen auf Kryptowährungen verboten.[193] Binäre Optionen auf Kryptowährungen sind Finanzinstrumente, die es Anlegern ermöglichen, auf den Preis von Kryptowährungen zu spekulieren. Bei binären Optionen geht es um Wetten darauf, ob der Preis eines Vermögenswerts (in diesem Fall Kryptowährungen wie Bitcoin oder Ethereum) innerhalb eines bestimmten Zeitraums steigen oder fallen wird. Im Wesentlichen setzt der Anleger auf die Kursentwicklung des zugrunde liegenden Vermögenswerts. Begründet wurde das Verbot damit, dass binäre Optionen ein spekulatives Finanzinstrument seien und die Anleger/-innen einem hohen Risiko aussetzen würden. In Kombination mit der hohen Volatilität von Kryptowährungen wurden binäre Optionen auf Kryptowährungen als besonders riskant eingestuft. Im gleichen Jahr wurde der Betrieb von Bitcoin-Automaten in Deutschland untersagt. Ferner wurde der Betrieb von Automaten verboten, an welchen Kryptowährungen gekauft werden konnten.[194] Zur Begründung wurde angeführt, dass diese Automaten gegen das Kreditwesengesetz (KWG) verstossen, da sie Zahlungsdienste ohne eine entsprechende Erlaubnis anbieten – insbesondere vor dem Hintergrund, dass Kryptowährungen in der Vergangenheit als Finanzinstrumente eingestuft wurden, was bestimmte Regulierungsanforderungen zur Folge hatte. Im Falle der Bitcoin-Automaten war z. B. eine Erlaubnis nach dem KWG zu beantragen und es mussten strenge Vorschriften eingehalten werden. Diese Einstufung zeigt, dass die BaFin Kryptowährungen nicht als eigenständige Anlageklasse betrachtet, sondern sie in das bestehende Regulierungssystem einordnet.

[193] Bundesanstalt für Finanzdienstleistungsaufsicht, (Pressemittelung 2019).

[194] Europäische Gesetzesinitiativen zu Kryptoassets, S. 1.

Alle drei Länder haben spezifische regulatorische Massnahmen ergriffen, um die Risiken im Zusammenhang mit Kryptowährungen und der DLT-Technologie im Hinblick auf Geldwäsche zu minimieren und den Sektor besser zu kontrollieren. Da diese Regulierungen in allen drei Ländern im Grunde auf den Empfehlungen der FATF basieren,[195] entsteht der Eindruck, dass die Mindestanforderungen in Bezug auf die Bekämpfung von Geldwäsche berücksichtigt werden. Es ist jedoch zu erkennen, dass jedes dieser Länder einen unterschiedlichen Ansatz mit unterschiedlichen Schwerpunkten und Regulierungsansätzen verfolgt.

5 Empirischer Teil

Um die Forschungsfragen der vorliegenden Arbeit zu beantworten, wurden zwei Ansätze verfolgt: eine gründliche Literaturrecherche und Experteninterviews. In den kommenden Abschnitten werden die verschiedenen methodischen Schritte der Literaturrecherche erläutert, bevor die durchgeführten Recherchen und deren Relevanz für die Forschungsarbeit dargestellt werden.

5.1 Methodik

Der Leitfaden für das Experteninterview wurde auf Basis der sozialwissenschaftlichen Befragungsmethode erstellt. Dabei werden konkrete Fragen formuliert und die interviewende Person gibt die Struktur des Interviews vor. Diese Art der Fragestellung ermöglicht es der befragten Person, offene Antworten zu geben. Das Leitfadeninterview stellt somit eine Kombination aus einer offenen Fragestellung und einem standardisierten Fragebogen dar.[196]

Die Gewichtung der Standardisierung kann in einem Leitfadeninterview je nach Bedarf variieren. Die Anzahl der Fragen hängt von der Dauer des Interviews ab, wobei Interviews, die länger als eine Stunde dauern, vermieden werden sollten. In der Regel besteht das Interview aus fünf Fragen, die durch Detailfragen ergänzt werden. Die Einbeziehung dieser Detailfragen kann je nach Möglichkeit standardisiert gemäss einer bestimmten Reihenfolge oder spontan erfolgen. Eine zu starke Standardisierung wird von

[195] Kapitel 4.1.1.

[196] SCHOLL, die Befragung, S. 61.

Personen mit Expertise oft abgelehnt, da ihr Wissen dadurch nicht angemessen abgerufen werden kann.

Ein erfolgreiches Experteninterview erfordert sowohl fachspezifische Fragen als auch sachbezogene Aussagen. Daher ist die Auswahl der Personen mit Expertise, die sich durch ihre Funktion, Position und Verantwortung als Personen mit Expertise auszeichnen, von entscheidender Bedeutung. Sie können Teil der Zielgruppe sein, die in der Forschung untersucht wird, oder Aussagen über andere Zielgruppen treffen. Massgeblich ist, dass sich die Personen mit Expertise offen und ehrlich zu den gestellten Fragen äussern und den Fokus auf dem relevanten Thema halten.[197]

5.2 Erstellung des Leitfadens

Für die Erstellung des Leitfadens können die Fragen anhand folgender Fragetypen formuliert werden:[198]

- Unterscheidung zwischen Schlüsselfragen und Eventualfragen: Schlüsselfragen sind für die Beantwortung der Forschungsfragen essenziell. Eventualfragen dienen dazu, bestimmte Aspekte zu erfahren, welche die interviewte Person nicht von selbst erwähnt.
- Einleitungsfragen
- Folgefragen
- Nachhaken
- Spezifizierungsfragen
- direkte und indirekte Fragen
- Strukturierungsfragen
- Schweigen
- Interpretationsfragen

Im Rahmen des Interviews ist die interviewende Person dafür verantwortlich, das Gespräch zu führen und passende Rückfragen zu stellen, um zu gewährleisten, dass die

[197] SCHOLL, die Befragung, S. 69.

[198] SCHOLL, die Befragung, S. 69f.

Antworten der befragten Person direkt interpretiert werden können. Um sicherzustellen, dass keine Aussagen vergessen oder verloren gehen, wird das Interview aufgezeichnet, was die Grundlage für die spätere Transkription bildet. Die Rohtexte werden anschliessend qualitativ analysiert. Hier zeigt sich der Vorteil des Leitfadeninterviews, da die vorrangige themenspezifische Auseinandersetzung mit den Fragen die nachfolgende Analyse erleichtert, indem die einzelnen Kategorien bereits vorliegen.[199]

5.3 Methodische Umsetzung

Die methodische Umsetzung basiert auf den erläuterten theoretischen Grundlagen. Als essenziell wird dabei die Wahl der Personen mit Expertise angesehen. Für die Beantwortung der Forschungsfragen wurden Personen gewählt, welche sich im Bereich des behandelten Themas engagieren und eine bestimmte verantwortungsvolle Aufgabe in einem Unternehmen wahrnehmen. Vorliegend fiel die Wahl auf Nicolas Kilchenmann, einen Experten aus dem RegTech-Bereich, welcher u. a. Dienstleistungen im Bereich *Krypto-Consulting* erbringt, wenn Banken mit Fragen zu regulatorischen Umsetzungen an ihn herantreten. Der zweite Experte, Marc Baumann, ist als Compliance Officer tätig. Sein Schwerpunkt liegt u. a. auf der Risikoanalyse von Krypto-Transaktionen. In der Vorbereitungsphase des Interviews wurde ein Leitfaden erstellt, dessen theoretische Grundlagen bereits erläutert wurden. Der Schwerpunkt des Leitfadens wurde auf die folgenden beiden Themenfelder gelegt: [200]

- Kryptowährungen und ihre Anreize zur Geldwäscherei
- Regulierungsansätze

Zu den jeweiligen Themengebieten wurden zwei bis drei Fragen gestellt. Ziel war es, dass die Experten von ihren eigenen Erfahrungen berichten und im Kontext der genannten Themenfelder Empfehlungen abgeben können. Die beiden Interviews wurden im Raum Zürich persönlich durchgeführt. Zur Orientierung der Experten wurden die Erkenntnisse der Literaturrecherche mündlich zusammengefasst. Die Transkripte sind im Anhang wörtlich niedergeschrieben.

[199] SCHOLL, die Befragung, S. 79f.

[200] Kapitel 9.

6 Ergebnisse

Die Ergebnisse der Experteninterviews werden in den folgenden Abschnitten ausgewertet. Die Analyse bezieht sich auf die in Kapitel 5.1.2 erwähnten Themenfelder.

6.1 Kryptowährungen und ihre Anreize zur Geldwäscherei

Beide Interviews befassen sich als erstes mit den Auswirkungen der Anonymität von Kryptowährungen auf die Geldwäsche und welche konkreten Massnahmen ergriffen werden können, um diese negativen Auswirkungen zu reduzieren.

Marc Baumann glaubt, dass Kryptowährungen eine innovative und revolutionäre Technologie sind, die das Potenzial hat, das traditionelle Finanzsystem zu transformieren und zu verbessern. Allerdings kann die Anonymität von Kryptowährungen auch von Kriminellen ausgenutzt werden, um Geldwäsche, Steuerhinterziehung und andere illegale Aktivitäten durchzuführen. Um diese Problematik anzugehen, schlägt Marc Baumann verschiedene Massnahmen vor. Eine Möglichkeit besteht darin, Kryptobörsen zu regulieren, um die Anonymität von Kryptowährungen einzudämmen. Die meisten Kryptobörsen verlangen bereits eine Identitätsprüfung, bevor ein Benutzer ein Konto eröffnen kann. Durch die Einführung strengerer Regulierungsmassnahmen wie KYC und Anti-Money-Laundering (AML) können Benutzer gezwungen werden, ihre Identität offenzulegen, was es den Strafverfolgungsbehörden erleichtert, verdächtige Transaktionen zu identifizieren und zu überwachen. Eine weitere seitens Marc Baumann empfohlene Massnahme besteht darin, Blockchain-Analyse-Tools zu verwenden, um Transaktionen auf der Blockchain zu verfolgen und zu analysieren. Diese Tools können dazu beitragen, verdächtige Transaktionen zu identifizieren und Kriminelle aufzudecken. Eine enge Zusammenarbeit zwischen Regierungen und Kryptowährungsunternehmen kann ebenfalls dazu beitragen, die Anonymität von Kryptowährungen zu verringern. Die Regierungen können beispielsweise Anforderungen an die Kryptowährungsunternehmen stellen, um ihnen bei der Identifizierung von verdächtigen Transaktionen zu helfen. Umgekehrt können Kryptowährungsunternehmen den Regierungen Informationen über verdächtige Transaktionen bereitstellen, um bei der Strafverfolgung zu helfen. Schliesslich betont Marc Baumann, dass eine bessere öffentliche Aufklärung über Kryptowährungen und ihre potenziellen Risiken dazu beitragen kann, die Anonymität von Kryptowährungen zu verringern. Es ist wichtig, dass die Kryptowährungsbranche mit

den Regierungen und Strafverfolgungsbehörden zusammenarbeitet, um sicherzustellen, dass Kryptowährungen nicht für illegale Aktivitäten genutzt werden.

Nicolas Kilchenmann ist auch der Auffassung, dass ass die Anonymität eine wichtige Rolle bei der Geldwäscherei spielt, da die Geldwäscher ihre Identität und die Herkunft des Geldes verbergen müssen, um ihre illegalen Einkünfte oder Vermögenswerte in den legalen Finanz- und Wirtschaftskreislauf einzuführen und ihre Herkunft zu verschleiern. Die Anonymität erleichtert es den Geldwäschern, ihre Identität zu verbergen und somit die Entdeckung zu vermeiden. Auch ohne Kryptowährungen können sie bereits heute Bankkonten unter falschen Namen eröffnen oder Mittelsmänner einschalten, um das Geld zu waschen. Die Anonymität von Kryptowährungen kann jedoch auch dazu beitragen, dass das Geld nicht mit illegalen Aktivitäten in Verbindung gebracht wird, da es schwerer zu verfolgen ist. Die Anonymität war also schon immer ein Anreiz, Geldwäsche zu betreiben. Gemäss Nicolas Kilchenmann bestehen bereits Massnahmen, die die auf die Bekämpfung der Anonymität bei der Geldwäsche abzielen, wie zum Beispiel die Sorgfaltspflichten nach dem GWG. Diese Pflichten zielen darauf ab, die Identität von Kunden und wirtschaftlichen Eigentümern offenzulegen und verdächtige Aktivitäten zu erkennen und zu melden. Nach Nicolas Kilchenmanns Auffassung stellt sich daher die Frage, wie diese Sorgfaltspflichten auch auf Kryptowährungen angewendet werden können. Zumal in der Schweiz die Regulierungen zur Bekämpfung der Geldwäsche prinzipienbasiert und technologieneutral ausgestaltet sind, gelten die Sorgfaltspflichten auch bei Geschäftsbeziehungen mit Kryptowährungen. Wenn eine Finanzmarkttätigkeit in den Anwendungsbereich des GWG fällt, müssen die Finanzintermediäre die Sorgfaltspflichten einhalten. Diese Verpflichtung gilt in Bezug auf sämtliche Geschäftsbeziehungen und Transaktionen, unabhängig von der Herkunft der Vermögenswerte der Vertragspartei. Die Einhaltung und Umsetzung der formellen Sorgfaltspflichten in Bezug auf Kryptowährungen gestaltet sich bei einer Bank nicht grundlegend anders als bei herkömmlichen Dienstleistungen des Bankgeschäfts. Bei der Aufnahme jeder Geschäftsbeziehung muss die Vertragspartei mittels beweiskräftigen Dokuments identifiziert und die wirtschaftlich berechtigte Person festgestellt werden. Nach Nicolas Kilchenmann Auffassung können Bei Krypto-Transaktionen können jedoch lediglich pseudonyme Wallet-Adressen, welche von der Blockchain beliebig generiert werden, entnommen werden. Bitcoin und Ether verknüpfen nicht automatisch die pseudonyme Wallet-Adresse mit rückverfolgbaren Identitäten im herkömmlichen

Sinn. Die auf der Blockchain enthaltenen Informationen sind demnach nicht mit dem Informationsgehalt herkömmlicher FIAT-Währungs-Transaktionen vergleichbar. Nicolas Kilchenmann empfiehlt hierbei die Entwicklung von neuartigen Überwachungs- und Analyseformen sowie Instrumenten, welche die blockchainspezifischen Transaktionsanalysen abzielen und vor allem die Zu- und Abflüsse der Wallet-Adressen genauestens durchleuchten. Durch eine solche Transaktionsanalyse könne die Transaktionsgeschichte rekonstruiert und die Herkunft der Kryptowährungen bis zu deren Ursprung zurückverfolgt werden. Es gibt jedoch Kryptowährungen und Blockchain-Dienstleistungen, welche der Verschleierung und Anonymisierung der Transaktionsketten und Geldwäsche dienen. In der Theorie können solche Anonymisierungsdienstleistungen mittels komplexer forensischer und hochkomplexer Berechnungen rekonstruiert werden. Allerdings fehlt den meisten Banken das nötige Know-how, um solche Tools effektiv einzusetzen. Gemäss Nicolas Kilchenmann genügt es in der Praxis bereits, wenn eine Bank die Wallet-Adresse ihrer Kunden mit handelsüblichen Transaktionsanalyse-Tools wie z.B. Elliptic verwendet, um die vom Kunden erhaltenen KYC-Informationen zu plausibilisieren. Sobald jedoch Verbindungen zum Darknet, Mixer oder Tumbler auf den Wallet-Adressen des Kunden gefunden werden, sollte die Geschäftsbeziehung als eine Geschäftsbeziehung mit erhöhten Risiken betrachtet werden. Der Kunde muss dann die Gründe dafür darlegen, dass die Vermögenswerte nicht aus kriminellen Machenschaften stammen. Sollten die Ausführungen für die Bank nicht nachvollziehbar und plausibel erscheinen, liegt bereits ein Verdacht auf Geldwäsche vor, und die Bank sollte die Absetzung einer MROS-Meldung prüfen. Nicolas Kilchenmann fasst folglich zusammen, dass die Blockchain nicht nur das Ziel der Anonymisierung verfolgt und damit Geldwäsche begünstigt, sondern den Banken auch dabei hilft, Kundeninformationen bis ins letzte Detail zu prüfen.

Bei der zweiten Frage des Interviews geht es darum, wie sich das Ausmass der Dezentralität von Kryptowährungen im Vergleich zu herkömmlichen Finanzinstrumenten und -dienstleistungen auf die Geldwäsche auswirkt und wie man dies quantifizieren kann.

Marc Baumann erklärt, dass es schwierig ist, das Ausmass zu quantifizieren, da es keine zuverlässigen Daten gibt. Allerdings argumentiert er, dass Dezentralität nicht zwangsläufig mit einer höheren Wahrscheinlichkeit von Geldwäsche einhergeht. Die

Pseudonymität von Kryptowährungen könnte es Kriminellen erleichtern, Gelder zu waschen und anonyme Transaktionen durchzuführen. Ausserdem kann die dezentrale Natur von Kryptowährungen Geldwäscheaktivitäten erschweren zu überwachen und zu regulieren. Marc Baumann betont jedoch, dass traditionelle Finanzinstrumente und -dienstleistungen ebenfalls für Geldwäsche genutzt werden können und dass es keine klaren Beweise dafür gibt, dass Kryptowährungen im Vergleich dazu ein grösseres Risiko darstellen. Es gibt auch positive Entwicklungen im Krypto-Bereich, wie die Implementierung von KYC- und AML-Verfahren und die Zusammenarbeit mit Regulierungsbehörden, die auf die Eindämmung von Geldwäscheaktivitäten abzielen. Insgesamt bleibt gemäss Marc Baumann die Frage nach dem Ausmass, in dem die Dezentralität von Kryptowährungen die Geldwäsche begünstigt, umstritten und erfordert weitere Untersuchungen und Daten, um eine genaue Quantifizierung zu ermöglichen.

Nicolas Kilchenmann stellt zunächst fest, dass die aktuelle Datengrundlage keine klare Antwort auf diese Frage zulässt. Obwohl im Bericht der KGGT aus dem Jahr 2018, der dem Bundesrat im Dezember desselben Jahres vorgelegt wurde, kaum Fälle von Geldwäsche durch Kryptowährungen bekannt waren, wurden die Geldwäscherisiken durch dezentrale Technologien als erheblich bezeichnet. Nicolas Kilchenmann betont, dass Politiker den Markt für dezentralisierte Finanzprodukte genauer beobachten müssen, um die damit verbundenen Mechanismen und Risiken besser zu verstehen. Mit einer besseren Datengrundlage könnten die entstehenden Risiken gemildert werden, um einen sicheren Markt für dezentralisierte Finanzprodukte zu unterstützen. Dazu sei ein besseres Verständnis der dezentralen Marktmechanismen erforderlich, um zu beurteilen, ob regulatorische Lücken bestehen, neue Regulierungsansätze erforderlich sind oder ob bereits bestehende Rahmenregelungen effizient angepasst werden müssen, um ähnlichen AML-Regulierungen zu entsprechen. Nicolas Kilchenmann betont auch die Notwendigkeit von mehr und vor allem qualitativ hochwertigeren Daten für DeFi- und Krypto-Märkte, um die Märkte und ihre Auswirkungen auf die Geldwäschereibekämpfung besser analysieren und mögliche Eingriffe prüfen zu können. Darüber hinaus könnten Politiker die Erkenntnisse aus DeFi für den Einsatz von DLT im traditionellen Finanzwesen nutzen. Es bleibe jedoch abzuwarten, ob dezentrale Strukturen nur ein kurzlebiges Phänomen sind und ob dezentrale Dienstleistungen einen Mehrwert für Nutzer, das Finanzsystem und die Wirtschaft erbringen. Nicolas Kilchenmann weist darauf hin, dass die Überwachung und Einhaltung der Vorschriften

für dezentrale Netzwerke in der Praxis nicht so einfach ist. Die Anbieter solcher dezentralen Dienstleistungen und Kryptowährungen sind weltweit tätig und haben in der Regel keinen bestimmten geografischen Standort oder eine bestimmte Gerichtsbarkeit. Dies stellt eine Herausforderung für die Durchsetzung dar. Dezentrale Systeme haben eine höhere Schnelligkeit und Leichtigkeit, mit der Anbieter als Reaktion auf regulatorische Anpassungen ihren Standort wechseln können. Nicolas Kilchenmann fordert daher eine effizientere politische Zusammenarbeit und Diskussion, um die Herausforderungen im Zusammenhang mit grenzüberschreitenden Aspekten zu bewältigen und Probleme der Aufsichtsarbitrage zu reduzieren. Eine weitere Zusammenarbeit zwischen allen dezentralen Finanzakteuren, einschliesslich Politikern, wäre wünschenswert. Hier könnten Politiker eine aktive Rolle bei der Schaffung eines kooperativen Umfelds spielen und Entwickler sollten in die Diskussion über die angemessene Aufsicht über solche Systeme einbezogen werden. Nicolas Kilchenmann betont, dass die Codierung von dezentralen Systemen in die Diskussion einbezogen werden muss, um angemessene Aufsichtsmassnahmen zu entwickeln, die auf die unterschiedlichen Anreize und Ansichten der Gemeinschaften eingehen.

6.2 Regulierungsansätze

In der ersten Frage des zweiten Interviewteils handelt es sich jeweils um die Auswirkungen der regulatorischen Massnahmen zur Bekämpfung von Geldwäsche im Zusammenhang mit Kryptowährungen und den Möglichkeiten, ihre Wirksamkeit zu verbessern.

Marc Baumann erklärt, dass Kryptowährungen dezentralisiert und anonym sind, was es schwierig macht, sie zu kontrollieren und sie daher zu einem bevorzugten Instrument für Geldwäsche macht. Eine der Auswirkungen dieser Massnahmen war eine Einschränkung der Nutzung von Mischdiensten, die es den Benutzern ermöglichen, ihre Kryptowährungen zu mischen, um ihre Identität zu verbergen und ihre Transaktionen unkenntlich zu machen. Diese Dienste wurden oft von Kriminellen genutzt, um ihre illegalen Aktivitäten zu verschleiern. Die regulatorischen Massnahmen haben dazu geführt, dass viele dieser Mischdienste geschlossen wurden oder ihre Dienste einschränken mussten, um den Anforderungen der Geldwäschebekämpfung gerecht zu werden. Um die Wirksamkeit der regulatorischen Massnahmen zu verbessern, schlägt

Baumann vor, die Zusammenarbeit zwischen Regulierungsbehörden und Kryptobörsen zu stärken. Kryptobörsen könnten verpflichtet werden, ihre Kunden besser zu überprüfen und verdächtige Transaktionen an die Behörden zu melden. Eine weitere Möglichkeit, die Wirksamkeit der Massnahmen zu verbessern, besteht darin, die Verwendung von Kryptowährungen für illegale Aktivitäten stärker zu sanktionieren. Dies könnte beispielsweise durch die Erhöhung von Strafen oder die Verfolgung von Straftaten im Zusammenhang mit Kryptowährungen als schwerwiegende Verbrechen erfolgen. Insgesamt sind die regulatorischen Massnahmen gegen Geldwäsche im Zusammenhang mit Kryptowährungen ein wichtiger Schritt, um die Nutzung von Kryptowährungen für illegale Aktivitäten zu reduzieren und das Vertrauen in den Kryptowährungsmarkt zu stärken. Es könnten weitere Massnahmen ergriffen werden, um ihre Wirksamkeit zu verbessern, jedoch sollten diese Massnahmen sorgfältig abgewogen werden, um die Integrität des Kryptowährungsmarkts zu erhalten.

Gemäss Nicolas Kilchenmann haben die aktuellen regulatorischen Massnahmen gegen Geldwäsche in Bezug auf Kryptowährungen nur begrenzte Auswirkungen auf die Nutzung von Mischdiensten, da es heutzutage auch ohne solche Dienste möglich ist, die Spur von Kryptowährungen zu verwischen. Um die Wirksamkeit bei der Bekämpfung von Geldwäsche im Zusammenhang mit Kryptowährungen zu erhöhen, müssen bestehende Regulierungen konsequent durchgesetzt und technologische Lösungen wie die Transaktionsanalyse verbessert werden. Ein Blockchain-Analysetool kann Muster von Transaktionen erkennen, die typisch für Mixer sind, und Transaktionen mit einem höheren Risiko kennzeichnen, um sie genauer zu untersuchen.

Als zweite Frage wurden die Experten gefragt, wie die unterschiedlichen Regulierungsansätze in Grossbritannien, der Schweiz und Deutschland die Entwicklung von Kryptowährungen und DLT-Technologien in diesen Ländern beeinflusst haben.

Marc Baumann betont, dass er persönlich zwischen Ländern unterscheidet, die Kryptowährungen befürworten und Ländern, die dies nicht tun. Er erklärte, dass die Schweiz und Grossbritannien zu den Ländern gehören, die Kryptowährungen befürworten, während die Regierung Deutschlands eine eher restriktive Haltung gegenüber Kryptowährungen und DLT-Technologien einnimmt. Laut Baumann haben die Regulierungsansätze der Länder einen Einfluss darauf, wo sich Unternehmen im

Krypto-Space ansiedeln. Marc Baumann merkte an, dass die meisten Unternehmen im Krypto-Space in der Schweiz ansässig sind, insbesondere in Zug und bald auch in Lugano. In Grossbritannien gibt es weniger Unternehmen, aber diese seien qualitativ hochwertig und vor allem innovativ. In Deutschland hingegen kennt Baumann kaum Unternehmen im Krypto-Space, und das innovative deutsche Startup, Wirecard, existiert heute nicht mehr. Baumann argumentierte, dass ohne klare regulatorische Rahmenbedingungen diese Unternehmen Schwierigkeiten haben könnten, ihre Geschäftsmodelle zu skalieren und auszubauen. Dies könnte dazu führen, dass Investoren und Nutzer das Vertrauen in die Branche verlieren, was sich wiederum auf die Marktkapitalisierung und die Preise von Kryptowährungen auswirken kann. Er betont auch, dass technologiefreundliche Regulierungsansätze dazu führen können, dass innovative Unternehmen in einem Land ansässig werden, wo die gesetzlichen Grundlagen für ihr Geschäftsmodell passen und es ihnen erlauben, in einem solchen Gebiet tätig zu sein. Nur wenn Länder Kryptowährungen und DLT-Technologien gestatten oder positive Anreize schaffen, könne sichergestellt werden, dass sich die Technologie weiterentwickelt. Wenn sich die Technologie weiterentwickelt, entstehen nicht nur neue Protokolle für Kryptowährungen, sondern auch neue Unternehmen, die sich mit der Technologie befassen, wie z. B. RegTech-Unternehmen, die es ermöglichen, AML-Vorschriften einfacher und effizienter einzuhalten. Dadurch profitiert auch die Geldwäschereibekämpfung.

Gemäss Nicolas Kilchenmann haben die unterschiedlichen Regulierungsansätze in Grossbritannien, der Schweiz und Deutschland die Entwicklung von Kryptowährungen und DLT-Technologien in diesen Ländern beeinflusst. Während einige Länder wie China und Indien restriktive Massnahmen gegen Kryptowährungen ergriffen haben, hat Deutschland eine strengere Regulierung eingeführt, während Grossbritannien und die Schweiz sich auf die Förderung von Innovationen konzentrieren. Trotz dieser Unterschiede haben alle drei Länder Interesse an der Entwicklung von Krypto- und Blockchain-Unternehmen und bemühen sich, ein günstiges Umfeld dafür zu schaffen.

Als letztes wurden die Experten gefragt, welche konkreten regulatorischen Massnahmen die Schweizer FINMA ergriffen hat, um die Entwicklung von Kryptowährungs- und DLT-Unternehmen in Zug zu fördern und zu kontrollieren?

Marc Baumann führt als Beispiel auf, dass die FINMA in den letzten Jahren verschiedene regulatorische Massnahmen ergriffen hat, um die Entwicklung von Kryptowährungs- und DLT-Unternehmen in Zug zu fördern und zu kontrollieren. Diese Massnahmen umfassen die Schaffung klarer Regulierungsrahmen, um es Unternehmen zu ermöglichen, ihre Geschäfte legal zu betreiben. Im Jahr 2018 hat die FINMA beispielsweise Richtlinien für ICOs veröffentlicht, die es Unternehmen ermöglichen, ihre Token-Verkäufe zu regulieren und zu kontrollieren. Darüber hinaus hat die FINMA im Jahr 2019 die Bankenregulierung für Kryptounternehmen aktualisiert und klare Anforderungen für die Einhaltung von Geldwäsche- und Terrorismusfinanzierungsbestimmungen festgelegt. Auch ein spezielles Bewilligungsverfahren für Kryptounternehmen wurde eingeführt, um sicherzustellen, dass Unternehmen die Anforderungen der FINMA erfüllen und die gesetzlichen Bestimmungen einhalten. Die FINMA überwacht auch Krypto-Vermögensverwalter, die sich bei der FINMA registrieren lassen und ihre Geschäftspraktiken offenlegen müssen, um sicherzustellen, dass sie ihre Geschäfte in Übereinstimmung mit den geltenden Gesetzen und Vorschriften betreiben. Er beont jedoch, dass die Zusammenarbeit mit anderen Aufsichtsbehörden zur Bekämpfung von Geldwäsche im Zusammenhang mit Kryptowährungen und DLT-Unternehmen von entscheidender Bedeutung ist. Im Jahr 2019 hat die FINMA beispielsweise eine Zusammenarbeit mit der US-amerikanischen Securities and Exchange Commission (SEC) angekündigt, um den Informationsaustausch zu erleichtern und die Zusammenarbeit zu verbessern. Seiner Meinung nach hat die FINMA klare Regulierungsrahmen geschaffen, um die Entwicklung von Kryptowährungs- und DLT-Unternehmen in Zug zu fördern und zu kontrollieren.

Nach Nicolas Kilchenmanns Meinung hat die Schweizer FINMA verschiedene regulatorische Massnahmen ergriffen, um die Entwicklung von Krypto- und DLT-Unternehmen in Zug zu fördern und zu kontrollieren. Dazu gehören klare Richtlinien für Initial Coin Offerings (ICOs), eine Registrierungspflicht für ICO-Emittenten sowie die Veröffentlichung von Aufsichtsmitteilungen und Merkblättern, die den Unternehmen helfen, die regulatorischen Anforderungen zu verstehen und einzuhalten. Diese Massnahmen sollen den Unternehmen Rechtssicherheit geben und sicherstellen, dass sie den Schweizer Finanzmarktgesetzen entsprechen.

7 Zusammenfassung und Diskussion

Mit der vorliegenden Masterarbeit wird das Ziel verfolgt, die zentralen Compliance-Grundlagen bei Krypto-Investitionen begreifbar zu machen, da bezüglich der Aufsicht und Geldwäsche im Zusammenhang mit Kryptowährungen weltweit Klärungsbedarf besteht. Diese Masterarbeit soll allfälligen Compliance-Mitarbeiterinnen und -Mitarbeitern die modernen operativen Mechanismen hinter Krypto-Technologien aufzeigen, sodass die Herausforderungen bezüglich der Struktur des Prozesses und der Kontrollmechanismen nachvollzogen werden können, welche mit Kryptowährungen in Bezug auf Geldwäscherei einhergehen. Ferner sollten Personen, die in der Bekämpfung von Geldwäsche tätig sind, wie Compliance-Mitarbeiter/-innen, Kenntnisse über die AML-Gesetzgebungen anderer Länder erhalten – insbesondere in Bezug auf Kryptowährungen und dezentrale Systeme. In der heutigen Zeit ist es nicht mehr ausreichend, allein die Gesetzgebung des eigenen Landes zu kennen, da Vermögenswerte und folglich auch Kryptowährungen innerhalb kürzester Zeit überall auf der Welt transferiert werden können. Daher ist es von zentraler Bedeutung, dass Personen, die in der Geldwäschereibekämpfung tätig sind, über ein umfassendes Verständnis der verschiedenen internationalen AML-Regulierungen verfügen, um mögliche Geldwäscheaktiven bestmöglich identifizieren und verhindern zu können.

Mit dieser Masterarbeit soll der Horizont jener Personen erweitert werden, die in die Bekämpfung von Geldwäscherei und in die Verhinderung von illegalen Aktivtäten im Zusammenhang mit Kryptowährungen involviert sind. Dazu wurde untersucht, welche AML-Regulierungen von Kryptowährungen in der Schweiz, Deutschland und dem Vereinigten Königreich bestehen. Durch den Rechtsvergleich wurden die Unterschiede und Gemeinsamkeiten in der Handhabung von AML-Regulatoren in Bezug auf Kryptowährungen aufgedeckt. Das Ergebnis dieser Arbeit wird es der Leserschaft erleichtern, die AML-Regulierungen im Zusammenhang mit Kryptowährungen sowie die rechtlichen Anforderungen in Bezug auf die Geldwäschereibekämpfung zu verstehen.

In Kapitel 2 wurden grundlegende Erkenntnisse über die Entstehung von Kryptowährungen und deren technischen Aspekte vermittelt. Kryptowährungen gewinnen zunehmend an Beliebtheit und sowohl Privatanlegenden als auch institutionelle Anleger tätigen immer mehr Investitionen mit Kryptowährungen. Dadurch, dass die Akzeptanz gegenüber Kryptowährungen als Zahlungsmittel zunimmt, steigt insbesondere

auch die Anzahl von Händlern, welche Kryptowährungen als Zahlungsmittel akzeptieren. Trotz der steigenden Akzeptanz und der damit verbundenen anwachsenden Netzwerkeffekte können Kryptowährungen (noch) nicht als ein allgemein akzeptiertes und etabliertes Zahlungsmittel angesehen werden. Anders als bei gesetzlichen Zahlungsmitteln besteht bei Kryptowährungen keine Verpflichtung zur Annahme als Zahlungsmittel. Kryptowährungen basieren weder auf physischen Eigenschaften wie Gold und Silber noch auf dem Vertrauen in zentrale Behörden wie bei Fiat-Geldern, sondern auf rein mathematischen Eigenschaften. Dank der Blockchains, auf welchen die jeweiligen Kryptowährungen basieren, werden die Transaktionen im Allgemeinen unveränderbar in einem Hauptbuch aufgezeichnet. Es konnte jedoch gezeigt werden, dass in vereinzelten Fällen schon Angriffe auf öffentliche Blockchains erfolgt sind, bei welchen Anpassungen an den Transaktionsblöcken vorgenommen wurden, wodurch es zu finanziellen Verlusten kam. Es wurde dargelegt, dass zwischen Blockchains und verteilten Ledgern ein Unterschied besteht. Blockchains bilden jedoch eine Art von verteilten Ledgern, indem Knoten-Netzwerke zu Dokumentationszwecken synchron sämtliche Transaktionen abspeichern und somit repliziert werden können. Die technische Verwahrung von Kryptowährungen erfolgt mittels Wallets, welche unerlässlich für das Senden und Empfangen von Kryptowährungen sind. Die Kryptowährungen selbst werden auf der Blockchain gespeichert, während Wallets sowohl die privaten und öffentlichen Schlüssel als auch die Wallet-Adressen der anwendenden Person speichern. Dabei existieren in der Praxis verschiedene Arten von Wallets. Ferner wurde dargelegt, dass Kryptowährungen auf einem dezentralen Netzwerk (auch verteilten Netzwerk genannt) basieren, das sich insofern von einem traditionellen Finanzsystem unterscheidet, als keine zentrale Partei als Intermediär für Transaktionen fungiert.

In Kapitel 3 wurde die Geldwäscherei auf Grundlage von wissenschaftlichen Erkenntnissen analysiert, um anschliessend die Herausforderungen darzulegen, welche mit Kryptowährungen in Bezug auf die Geldwäscherei einhergehen. Hierzu wurden die allgemeine Struktur des Geldwäscherei-Prozesses und die vorherrschenden Kontrollmechanismen auf die allgemeinen Eigenschaften von Kryptowährungen angewendet. Um den Geldwäscherei-Prozess mithilfe der Verwendung von Kryptowährungen zu verdeutlichen, wurde in der vorliegenden Masterarbeit das Beispiel des Wash-Tradings diskutiert, da es eine Methode der Geldwäscherei darstellt. Mithilfe der Arbeit konnte nämlich aufgezeigt werden, dass die Befürchtung besteht, dass Wash-

Trading bei Kryptowährungen – einschliesslich Bitcoin – angewendet wird, um den Kurspreis zu manipulieren und Geldwäsche zu betreiben.

Anschliessend wurde die Wirksamkeit von Geldwäscherei-Kontrollen und deren Auswirkungen in Bezug auf die ökonomischen Anreize zur Nutzung von Geldwäscherei-Instrumenten analysiert, um die wirtschaftlichen Anreize von Kryptowährungen als Geldwäscherei-Instrument festzustellen. Dabei wurden die Anreize mit der Wirksamkeit der existierenden Geldwäscherei-Kontrollen verglichen, die auf den Empfehlungen der FATF basieren. Es wurde untersucht, ob sich Kontext- oder Transaktionsfaktoren jeweils direkt oder indirekt auf den Geldwäscherei-Prozess auswirken und demzufolge entweder positive oder negative Anreize dafür schaffen, Kryptowährungen im Vergleich zu herkömmlichen Finanzinstrumenten und -dienstleistungen als Gelwäscherei-Instrument zu missbrauchen.

Dabei wurde die Anonymität als ein Faktor identifiziert, welcher im Gegensatz zu herkömmlichen Finanzinstrumenten und -dienstleistungen mögliche Anreize für Geldwäscherei schafft. Diese Feststellung wurde durch die beiden Experteninterviews bestätigt. Beide Experten sind der Auffassung, dass die Anonymität von Kryptowährungen im Zusammenhang mit Geldwäsche und anderen illegalen Aktivitäten Relevanz hat. Wie in dieser Arbeit dargelegt, sind Kryptowährungen jedoch nicht vollständig anonym, da jede Transaktion in einem öffentlichen Hauptbuch der Blockchain aufgezeichnet wird, das für jede/n einsehbar ist. Jede Transaktion ist mit einer eindeutigen Adresse und einem Zeitstempel verbunden, was es ermöglicht, diese Informationen in Verbindung mit anderen Daten zu verwenden, um Benutzer/-innen zu identifizieren. Die Tatsache, dass die Blockchain insofern eine nachträgliche Identifizierung ermöglicht, stellt demnach einen indirekten negativen Anreiz dafür dar, Kryptowährungen als Geldwäscherei-Instrument zu verwenden. Im Rahmen der Experteninterviews wurden auch andere Methoden dargelegt, mit denen Benutzer/-innen von Kryptowährungen identifiziert werden können. Zum Beispiel können Kryptobörsen verpflichtet sein, KYC- und AML-Verfahren durchzuführen, um die Identität der Benutzer/-innen zu überprüfen und sicherzustellen, dass keine illegalen Aktivitäten stattfinden. Ferner wurde festgestellt, dass bereits Massnahmen zur Bekämpfung der Anonymität im Zusammenhang mit Geldwäsche bestehen, wie die Sorgfaltspflichten nach dem GWG, die auch auf Kryptowährungen angewendet werden können. Die

Einhaltung und Umsetzung dieser Verpflichtungen gestalteten sich bei einer Kryptowährungen nicht grundlegend anders als bei herkömmlichen Dienstleistungen des Bankgeschäfts.

Die Dezentralität bildet hingegen einen Faktor, welcher im Vergleich zu herkömmlichen Finanzinstrumenten und -dienstleistungen positive Anreize dafür schafft, Kryptowährungen als Geldwäscherei-Instrument zu missbrauchen. Diese Arbeit verdeutlicht, dass Kryptowährungen aufgrund ihrer Dezentralität eine Triebkraft für die Geldwäscherei darstellen können – unbekannt ist allerdings, in welchem Ausmass dieser Faktor die Geldwäscherei erleichtert. Die Anonymität, welche Kryptowährungen zugeschrieben wird, scheint sich nicht zu bewahrheiten – zumal es im Gegensatz zu Bargeld-Transaktionen möglich ist, sämtliche verdächtige Aktivitäten in der Transaktionshistorie nachzuverfolgen bzw. aufzuarbeiten. Auch die erläuterten Mischdienste scheinen nicht so zuverlässig zu sein wie angenommen oder befürchtet. Die Experten konnten diese Erkenntnis zwar bestätigen, weisen jedoch darauf hin, dass die Auswirkungen der Dezentralität auf die Geldwäschereibekämpfung nicht eindeutig sind, sondern dass weitere Forschung und Daten erforderlich sind. Einerseits wurde darauf hingewiesen, dass traditionelle Finanzinstrumente und -dienstleistungen ebenfalls für Geldwäsche genutzt werden können und nicht eindeutig bewiesen ist, dass Kryptowährungen im Vergleich zu diesen ein grösseres Risiko darstellen. Andererseits bestehen die Herausforderung der Regulierung von dezentralen Systemen und die Notwendigkeit einer besseren Datengrundlage, um die Auswirkungen auf die Geldwäschereibekämpfung besser zu verstehen.

Im Kapitel 4 wurden Institutionen und Instrumente vorgestellt, die bei der Bekämpfung der Geldwäsche hilfreich sein können. Dazu gehören die FATF, die Anti-Geldwäsche-Richtlinien Nr. 5 und Nr. 6, die TFR, die Sanktionen und das Mining des OFAC sowie das FinCEN. Ausserdem wurde auf die Kontroverse um nicht gehostete Wallets eingegangen. Es gibt sowohl staatliche als auch private Institutionen, die sich mit der Bekämpfung der Geldwäsche befassen. Im Finanzsektor sind solche Institutionen vor allem Selbstregulierungsmassnahmen. Es wurden einige internationale Institutionen und Organisationen vorgestellt, die sich explizit auf Kryptowährungen beziehen.

Die FATF definiert den Begriff *Virtual Asset Service Provider* (VASP) als jedes Unternehmen, das im Ökosystem virtueller Vermögenswerte als Vermittler auftritt. Die Definition basiert auf Aktivitäten wie dem Austausch von virtuellen Vermögenswerten und Fiat-Währungen, der Übertragung von virtuellen Vermögenswerten, der Verwahrung und/oder Verwaltung von virtuellen Vermögenswerten und von Instrumenten, die die Kontrolle über virtuelle Vermögenswerte ermöglichen, sowie der Beteiligung an und Erbringung von Finanzdienstleistungen im Zusammenhang mit dem Angebot und/oder dem Verkauf eines virtuellen Vermögenswerts durch einen Emittenten bzw. eine Emittentin. Die Travel Rule verpflichtet VASP, die erforderlichen und korrekten Informationen über die auftraggebende und die begünstigte Person einzuholen, aufzubewahren und zu übermitteln und diese Informationen zusammen mit einer inländischen oder grenzüberschreitenden Transaktion mit virtuellen Vermögenswerten über dem Schwellenwert von 1'000 USD/EUR zu übermitteln. Reine Peer-to-Peer-Transaktionen ohne Beteiligung eines VASP unterliegen nicht den FATF-Verpflichtungen.

Die Travel Rule wurde in der Schweiz in der GwV-FINMA und in Europa mit der TFR-Regulierung umgesetzt. Finanzintermediäre, die Zahlungen mit anderen Finanzintermediären abwickeln, müssen sicherstellen, dass sie Informationen über die auftraggebende und die begünstigte Person bei Transaktionen über CHF 1'000 bzw. EUR 1'000 aufzeichnen und übermitteln. Die Geldwäschereibekämpfungsbestimmungen in Europa und der Schweiz gelten demnach auch für VASP, die als Finanzintermediäre agieren, darunter Anbieter von Wallets, Handelsplattformen und Krypto-Fonds. Im Gegensatz zu den FATF-Standards besteht in der Schweiz und in Europa keine Ausnahme für Zahlungen mit unregulierten Wallet-Anbietern. Die Bemühungen der Schweiz und von ganz Europa bergen jedoch das Risiko, durch die Sunrise-Problematik untergaben zu werden – zumal Kriminelle die Schweiz und Europa virtuell meiden und aus solchen Ländern operieren, in denen keine angemessenen Vorschriften existieren. Ferner gilt zu beachten, dass einige Länder noch nicht einmal die zuvor erwähnte FATF-Erklärung zu virtuellen Vermögenswerten und zugehörigen Anbietern umgesetzt haben. Ferner lässt sich erkennen, dass die einheitliche Anwendung der Travel Rule im Europäischen Wirtschaftsraum und in der Schweiz aufgrund des erheblichen Mehraufwands und der Kosten bei betroffenen Dienstleistern und Intermediären auf Kritik stösst. Die potenziellen Auswirkungen könnten zu einer Einschränkung des Zugangs zu Krypto-

Transaktionen über unhosted Wallets führen und den Markt zentralisieren, was wiederum die technische Innovation der Blockchain-Technologie beeinträchtigen könnte. Es bleibt abzuwarten, ob die Einhaltung dieser Regelungen den europäischen Anbietern die Möglichkeit bietet, sich differenzieren und Vertrauen aufbauen zu können.

Damit die Travel Rule ihr volles Potenzial zur Bekämpfung von Geldwäsche entfalten kann, ist die Etablierung eines globalen Messaging-Standards von zentraler Bedeutung. Weder die FATF noch nationale Behörden wie FINMA empfehlen die Verwendung eines spezifischen Messaging-Standards für virtuelle Vermögenswerte im Rahmen der Travel Rule. Aus diesem Grund arbeiten verschiedene Organisationen an Protokollen, die ähnlich wie SWIFT funktionieren, um Transaktionsinformationen gemäss der Travel Rule zu übermitteln. Es ist jedoch noch unklar, welches Protokoll sich letztlich auf globaler Ebene durchsetzen wird. Aktuell müssen VASP zur Einhaltung der Vorschriften die relevanten Informationen auf traditionelle Weise austauschen, beispielsweise über sichere E-Mails. Diese Methode ist jedoch kostspielig, da VASP mit jedem VASP der Gegenpartei bilaterale Vereinbarungen treffen und klären müssen, wann, welche und wie Informationen übermittelt werden sollen. Das Fehlen globaler Messaging-Standards der Travel Rule bietet weiterhin Raum für nicht konforme VASP, da sie sich auf die mangelnde Standardisierung berufen können – insbesondere in Ländern, die nicht vorgeben, wie VASP mit unregulierten VASP in Rechtsgebieten interagieren sollen, in denen die Travel Rule noch nicht umgesetzt wurde.

Anschliessend wurde ein Rechtsvergleich der gesetzlichen Bestimmungen zur Geldwäscheprävention zwischen Deutschland, der Schweiz und dem Vereinigten Königreich vorgenommen.

Die Geldwäschebekämpfungsvorschriften in Grossbritannien basieren auf dem Proceeds of Crime Act (PoCA 2002) und den Money Laundering Regulations (MLR 2003). In der Schweiz sind sie im GwG geregelt. In Deutschland gibt es verschiedene Gesetze wie das DStGB, die DStPO und das DGwG. Im Gegensatz zu Grossbritannien und der Schweiz wird in Deutschland die Vortat nicht mitbestraft. Die Identifizierungspflicht steht in Deutschland und der Schweiz im Fokus, während in Grossbritannien die Meldepflicht im Vordergrund steht. Basierend auf dieser Grundlage wurde die politische Haltung in Bezug auf Kryptowährungen verglichen. Der Vergleich hat zeigt, dass sich die Haltungen von

Grossbritannien, der Schweiz und Deutschland zu Kryptowährungen und DLT-Technologien unterscheiden. Grossbritannien hat bereits 2018 eine positive Einstellung gegenüber Kryptowährungen und DLT-Technologien eingenommen und neue Vorschriften erlassen, durch die Finanzinstitute, die in diesem Bereich tätig sind, den gleichen Anti-Geldwäsche-Regeln wie traditionelle Finanzinstitute unterworfen sind. Die Schweiz hat ebenfalls einen klaren regulatorischen Rahmen geschaffen, der den Unternehmen in diesem Bereich wohlgesonnen ist und durch den die Stadt Zug als *Crypto Valley* bekannt wurde. Deutschland zeigt jedoch eine defensive Haltung gegenüber Kryptowährungen und hat den Verkauf von binären Optionen auf Kryptowährungen sowie den Betrieb von Bitcoin-Automaten verboten. Im Gegensatz zu Grossbritannien und der Schweiz gibt es in Deutschland weder eine Top-FinTech-Positionierung noch ein Crypto Valley.

Die unterschiedlichen Regulierungsansätze haben einen direkten Einfluss auf die Attraktivität eines Landes für Dienstleistungen mit Bezug zu Kryptowährungen. Ein Land mit klaren und konsistenten Vorschriften schafft Vertrauen und Sicherheit für Unternehmen. Die eindeutigen Regeln ermöglichen es den Unternehmen, ihre Aktivitäten entsprechend zu planen und Risiken besser einzuschätzen. Im Gegensatz dazu können durch einen Mangel an Klarheit oder widersprüchliche Vorschriften Unsicherheiten entstehen, was die Attraktivität eines Landes mindern kann, Dienstleistungen in Bezug auf Kryptowährungen im jeweiligen Land anzubieten. Ein flexibler und offener Regulierungsansatz kann die Attraktivität eines Landes für Kryptounternehmen hingegen steigern. Wenn ein Land ein förderliches Umfeld schafft, das Innovationen und neue Geschäftsmodelle im Kryptosektor unterstützt, zieht es Unternehmen an, die nach einem experimentellen und dynamischen Umfeld suchen. Die Verfügbarkeit von Unterstützungsstrukturen wie Inkubatoren, technologische Forschungseinrichtungen, regulatorische Sandboxes und FinTech-Hubs kann ein Land für Kryptounternehmen attraktiver machen. Diese Infrastrukturen bieten den Unternehmen die Möglichkeit, neue Technologien und Geschäftsmodelle zu entwickeln und fördern gleichzeitig den Austausch und die Zusammenarbeit in der Branche.

Zusammenfassend kann gesagt werden, dass die Attraktivität eines Landes für Dienstleistungen mit Bezug zu Kryptowährungen massgeblich von der Klarheit und Konsistenz der Vorschriften, der Offenheit für Innovation und der Verfügbarkeit von

innovationsfördernder Infrastruktur beeinflusst wird. Länder, die diese Aspekte berücksichtigen und einen geeigneten Regulierungsansatz verfolgen, haben gute Chancen, Kryptounternehmen anzuziehen und zu fördern.

Aufgrund des jungen Alters der Literatur zum Thema *Blockchain* gibt es zum Zeitpunkt der Erstellung dieser Arbeit weniger wissenschaftliche Veröffentlichungen als unerforschte Internetartikel, in denen dieses Thema behandelt wird. Inhaltlich stimmen diese Berichte momentan weitgehend überein und thematisieren hauptsächlich die Funktionsweise der Blockchain-Technologie sowie ihre Auswirkungen auf das Geldwäschereirisiko. Ganzheitliche ökonomische, gesetzliche und gesellschaftliche Betrachtungen sind bislang erst ansatzweise verbreitet, was die Analyse erschwert hat, da neue relevante Kriterien möglicherweise nicht berücksichtigt wurden.

Eine weitere Limitation dieser Masterarbeit ist, dass der Mangel an verfügbaren Datenbanken und Informationen zu den nationalen Geldwäschereibestimmungen in Deutschland, der Schweiz und dem Vereinigten Königreich möglicherweise die Gültigkeit und Zuverlässigkeit der Ergebnisse dieser Masterarbeit beeinträchtigt hat. Insbesondere kann die Begrenzung der verfügbaren Daten dazu führen, dass bedeutsame Unterschiede zwischen den verschiedenen nationalen Rechtsvorschriften nicht vollständig erfasst wurden, was zu ungenauen oder sogar irreführenden Ergebnissen führen kann. Darüber hinaus könnte der Mangel an Datenbanken auch bedeuten, dass relevante Themen, die in diesen Bestimmungen behandelt werden, möglicherweise nicht vollständig berücksichtigt wurden. Aus diesen Gründen sollte in zukünftigen Studien versucht werden, diese Einschränkungen zu überwinden und den Zugang zu umfassenden Datenbanken und Informationen zu verbessern, um ein vollständigeres Bild der nationalen Geldwäschereibestimmungen zu erhalten.

Zudem liegt aufgrund der Beschränkung auf zwei Experten keine repräsentative Stichprobe vor und durch weitere Befragungen hätten andere Sichtweisen aufgezeigt werden können. Obwohl mehrere *Personen mit Expertise* angefragt wurden, fiel die Rückmeldung negativ aus. Zukünftige Studien sollten daher eine grössere Anzahl von Personen mit Expertise einbeziehen und diese bestenfalls in anonymisierter Form befragen, um eine grössere Teilnahmebereitschaft zu erreichen.

Zukünftige Forschungen in Bezug auf Kryptowährungen und die damit verbundenen Geldwäschereirisiken sollten aus einer internationalen Perspektive angegangen werden, um das Problem der Geldwäsche im Zusammenhang mit Kryptowährungen besser verstehen und effektiver bekämpfen zu können. Da Kryptowährungen zur Dezentralität neigen, stellen nationale Regulierungsversuche oft eine Herausforderung dar. Aus diesem Grund sollte die Forschung den Schwerpunkt auf eine internationale Zusammenarbeit und internationale Standards legen, um einheitliche Vorschriften und Praktiken zur Bekämpfung der Geldwäsche im Zusammenhang mit Kryptowährungen zu etablieren.

Ein massgeblicher Forschungsansatz sollte darin bestehen, die technischen Mechanismen und Merkmale von Kryptowährungen genauer zu untersuchen, um zu verstehen, wie sie von kriminellen Personen genutzt werden und wie diese Aktivitäten verhindert werden können. Dies könnte dazu beitragen, geeignetere Vorschriften und Praktiken zur Bekämpfung der Geldwäsche zu entwickeln und die Implementierung effektiverer Technologien und Verfahren zu fördern.

Ein weiterer wesentlicher Forschungsansatz wäre die Analyse der Rolle von Intermediären wie Kryptobörsen und Wallet-Providern bei der Bekämpfung der Geldwäsche. Es ist von zentraler Bedeutung, ihre rechtlichen Verpflichtungen zu verstehen und zu klären, wie sie effektiv dazu beitragen können, die Geldwäsche zu verhindern. Schliesslich sollten zukünftige Forschungen auch die Entwicklung von Technologien zur Erkennung und Verhinderung von Geldwäsche im Zusammenhang mit Kryptowährungen beinhalten. Künstliche Intelligenz, maschinelles Lernen und andere datengetriebene Ansätze könnten dazu beitragen, verdächtige Transaktionen zu identifizieren und die Einhaltung von Vorschriften sicherzustellen. Insgesamt gilt, dass zukünftige Forschungsansätze in Bezug auf Kryptowährungen und Geldwäsche sowohl technologische als auch regulatorische Aspekte berücksichtigen und auf eine internationale Zusammenarbeit sowie internationale Standards hinzielen sollten. Nur so kann die Bekämpfung der Geldwäsche im Zusammenhang mit Kryptowährungen gelingen.

8 Fazit

Angesichts der vorliegenden Masterarbeit lässt sich feststellen, dass Kryptowährungen im Vergleich zu herkömmlichen Finanzinstrumenten und -dienstleistungen ein erhöhtes Risiko der Geldwäsche bergen. Einer der Hauptgründe dafür ist die Anonymität, die durch den Einsatz von Kryptowährungen ermöglicht wird. Durch die Nutzung von Kryptowährungen können Transaktionen ohne direkte Verknüpfung zu realen Identitäten durchgeführt werden, was kriminellen Personen die Verschleierung illegaler Aktivitäten erleichtert.

Die Anonymität bei Kryptowährungen basiert auf dem Prinzip, dass Transaktionen in einem öffentlichen Hauptbuch, der sogenannten Blockchain, aufgezeichnet werden. Obwohl diese Transaktionen öffentlich einsehbar sind, sind sie nicht direkt mit realen Identitäten verbunden. Stattdessen sind sie mit eindeutigen Wallet-Adressen und Zeitstempeln versehen. Diese Anonymität ermöglicht es kriminellen Personen theoretisch, Transaktionen durchzuführen, ohne leicht identifiziert zu werden. Es ist jedoch zu beachten, dass Kryptowährungen nicht vollständig anonym sind. Da alle Transaktionen in der Blockchain aufgezeichnet werden, können die Informationen aus dem öffentlichen Hauptbuch in Verbindung mit Daten von Transaktionsüberwachungs-Tools verwendet werden, um Benutzer/-innen nachträglich zu identifizieren. Obwohl also die Transaktionen an sich anonym erscheinen mögen, können forensische Analysen dazu führen, dass die Identität der beteiligten Parteien aufgedeckt wird. Darüber hinaus sind bereits Massnahmen zur Reduzierung der Anonymität im Zusammenhang mit Geldwäsche mittels herkömmlicher Finanzinstrumente in Kraft getreten, beispielsweise die Sorgfaltspflichten GWG. Diese Sorgfaltspflichten legen Finanzinstituten und Dienstleistern im herkömmlichen Bankgeschäft Verpflichtungen auf, um Geldwäscheaktivitäten zu bekämpfen und verdächtige Transaktionen zu melden. Diese Verpflichtungen können auch auf Kryptowährungen angewendet werden. Die Einhaltung und Umsetzung dieser Verpflichtungen gestalten sich bei Kryptowährungen nicht grundlegend anders als bei herkömmlichen Bankdienstleistungen. Kryptowährungsdienstleister müssen beispielsweise die Identität ihrer Kundschaft überprüfen, verdächtige Aktivitäten überwachen und gegebenenfalls Berichte über solche Aktivitäten erstatten. Des Weiteren zielt die von der FATF ausgearbeitete *Travel Rule* darauf ab, die Anonymität bei Transaktionen zwischen Kryptowährungen zu reduzieren. In der Zwischenzeit wurde die Travel Rule in der Schweiz umgesetzt und soll ab 2024

auch in ganz Europa auf die dezentralen Eigenschaften von Kryptowährungen angewendet werden.

Die Dezentralität stellt neben der Anonymität ein weiteres Risiko für Geldwäsche dar, da Kryptowährungen auf dezentralen Netzwerken basieren und somit keine zentralen Behörden die Transaktionen überwachen oder genehmigen. Dies kann es erschweren, Geldwäscheaktivitäten zu identifizieren und zu unterbinden. Im traditionellen Bankensystem gibt es strenge Überwachungs- und Meldepflichten, die bei verdächtigen Transaktionen greifen. Bei Kryptowährungen kann die Überwachung komplexer sein – insbesondere, wenn Geldwäsche über verschiedene Wallet-Adressen oder Kryptobörsen hinweg stattfindet. Darüber hinaus besteht das Risiko, dass das dezentrale Design von Kryptowährungen die nationalen Regulierungsbemühungen untergraben kann, da es Kriminellen ermöglicht, aus Ländern zu operieren, in denen keine angemessenen Vorschriften existieren. Es bleibt daher abzuwarten, ob eine internationale Harmonisierung der Regulierungsbemühungen das Problem der Dezentralität lösen wird. Zu beachten ist, dass die Regulierungsbemühungen zu einem erheblichen Mehraufwand führen könnten, der den Markt einschränken und wiederum die technische Innovation beeinträchtigen könnte. Dieser Befürchtung kann jedoch durch die Erkenntnisse aus dem Rechtsvergleich entgegengewirkt werden, aus denen hervorging, dass klare und konsistente Vorschriften die Attraktivität von Dienstleistungen im Zusammenhang mit Kryptowährungen steigern können.

In der vorliegenden Masterarbeit wurde zudem der regulatorische Rahmen für Krypto-Assets in Deutschland, dem Vereinigten Königreich und der Schweiz ausführlich untersucht, wobei insbesondere die AML-Gesetze dieser drei Länder betrachtet wurden. Die Erkenntnisse legen nahe, dass eine Weiterentwicklung dieser Gesetze notwendig ist, um Verstösse, die im Kontext von Kryptowährungen auftreten, wirksam adressieren zu können.

Ein zentrales Ergebnis der Arbeit ist die Erkenntnis, dass die aktuellen FATF-Empfehlungen, die EU-Gesetze – einschliesslich der EU-Richtlinien, die speziell auf digitale Währungen und ihre Regulierung fokussieren – bei genauer Betrachtung nicht ausreichen, um die vielschichtigen und komplexen Herausforderungen, die Kryptowährungen im Kontext der Geldwäsche mit sich bringen, effektiv zu bewältigen.

Die vorliegende Masterarbeit hat aufgezeigt, dass Kryptowährungen aufgrund ihrer inhärenten Eigenschaften wie Anonymität und Dezentralisierung einzigartige und neuartige Herausforderungen für Regulierungsbehörden darstellen. Dies hat weitreichende Auswirkungen auf den Kampf gegen Geldwäsche, da die traditionellen Methoden und Ansätze zur Identifizierung und Verfolgung von Geldwäscheaktivitäten oft bei Transaktionen mit Kryptowährungen an ihre Grenzen stossen. Das Versäumnis, diese neuen Herausforderungen auf internationaler Ebene angemessen zu adressieren, könnte es Kriminellen ermöglichen, die Lücken im gegenwärtigen regulatorischen Rahmen auszunutzen und Geldwäscheaktivitäten durchzuführen.

Die Risiken im Zusammenhang mit Kryptowährungen und Geldwäscheprävention lassen sich am besten durch internationale Regulierungsbemühungen angehen, anstatt dass jedes Land eigenständig Massnahmen definiert. Durch eine einheitliche und koordinierte Vorgehensweise können Schlupflöcher vermieden werden, die bei nationalen Alleingängen entstehen könnten. Internationale Regulierungsbemühungen ermöglichen eine gemeinsame Basis für die Prävention von Geldwäsche und anderen kriminellen Aktivitäten im Kryptowährungsbereich. Es ist wichtig, dass Länder zusammenarbeiten, um einheitliche Standards und Best Practices zu etablieren, die auf globaler Ebene gelten. Dadurch wird sichergestellt, dass die Risiken der Geldwäsche effektiv bekämpft werden können.

Gleichzeitig ist es entscheidend, dass Finanzintermediäre, wie Kryptobörsen und Wallet-Anbieter, sich an die bereits existierenden Regulierungen halten. Viele Länder haben bereits Vorschriften eingeführt, die auf Kryptowährungen anwendbar sind, um Geldwäsche und andere illegale Aktivitäten zu verhindern. Diese Regulierungen sollten konsequent durchgesetzt und von den Finanzintermediären eingehalten werden. Zusätzlich zur internationalen Regulierung und Einhaltung bestehender Vorschriften sollten Finanzintermediäre auch auf Kryptotransaktions-Tools zurückgreifen, um die Risiken bestmöglich zu mindern. Es gibt bereits verschiedene Technologien und Lösungen, die bei der Überwachung von Transaktionen und der Identifizierung verdächtiger Aktivitäten in Kryptowährungen helfen können. Durch den Einsatz solcher Tools können potenzielle Geldwäscheaktivitäten frühzeitig erkannt und verhindert werden.

Insgesamt ist eine Kombination aus internationaler Regulierung, Einhaltung bestehender Vorschriften und dem Einsatz von Kryptotransaktionstools erforderlich, um die Risiken im Zusammenhang mit Kryptowährungen und Geldwäscheprävention wirksam zu mindern. Durch eine koordinierte und gemeinsame Anstrengung können wir sicherstellen, dass Kryptowährungen als Finanzinstrumente sicher und transparent genutzt werden können.

Mit dieser Arbeit wurde ein Beitrag zur aktuellen wissenschaftlichen und politischen Debatte über die Rolle von Kryptowährungen im Finanzsystem und die Notwendigkeit einer angemessenen Regulierung dieses innovativen und dynamischen Sektors geleistet.

9 Anhang

9.1 Transkript Experteninterview mit Marc Baumann

- *Welche konkreten Massnahmen könnten ergriffen werden, um die negativen Auswirkungen der Anonymität von Kryptowährungen auf die Geldwäscherei einzudämmen?*

Ich glaube daran, dass Kryptowährungen eine innovative und revolutionäre Technologie darstellen, die das Potenzial hat, das traditionelle Finanzsystem zu transformieren und zu verbessern. Ich denke jedoch auch, dass die Anonymität von Kryptowährungen ein ernstes Problem darstellt, da sie von Kriminellen genutzt werden kann, um Geldwäsche, Steuerhinterziehung und andere illegale Aktivitäten durchzuführen.

Es gibt mehrere konkrete Massnahmen, die ergriffen werden können, um die negativen Auswirkungen der Anonymität von Kryptowährungen auf die Geldwäsche einzudämmen. Einige dieser Massnahmen sind:

- Regulierung von Kryptobörsen: Eine Möglichkeit, die Anonymität von Kryptowährungen einzudämmen, besteht darin, Kryptobörsen zu regulieren. Die meisten Kryptobörsen verlangen bereits eine Identitätsprüfung, bevor ein Benutzer ein Konto eröffnen kann. Dies kann durch die Einführung strengerer Regulierungsmassnahmen wie KYC und Anti-Money-Laundering (AML) noch verbessert werden. Dadurch werden die Benutzer gezwungen, ihre Identität offenzulegen, was es den Strafverfolgungsbehörden erleichtert, verdächtige Transaktionen zu identifizieren und zu überwachen.
- Verwendung von Blockchain-Analyse-Tools: Blockchain-Analyse-Tools sind Softwareprogramme, die es ermöglichen, Transaktionen auf der Blockchain zu verfolgen und zu analysieren. Diese Tools können dazu beitragen, verdächtige Transaktionen zu identifizieren und Kriminelle aufzudecken. Einige der bekanntesten Blockchain-Analyse-Tools sind Chainalysis, Elliptic und CipherTrace.
- Zusammenarbeit zwischen Regierungen und Kryptowährungsunternehmen: Eine enge Zusammenarbeit zwischen Regierungen und Kryptowährungsunternehmen kann dazu beitragen, die Anonymität von Kryptowährungen zu verringern. Die

Regierungen können beispielsweise Anforderungen an die Kryptowährungsunternehmen stellen, um ihnen bei der Identifizierung von verdächtigen Transaktionen zu helfen. Umgekehrt können Kryptowährungsunternehmen den Regierungen Informationen über verdächtige Transaktionen bereitstellen, um bei der Strafverfolgung zu helfen.

- Verbesserung der öffentlichen Aufklärung: Eine bessere öffentliche Aufklärung über Kryptowährungen und ihre potenziellen Risiken kann dazu beitragen, die Anonymität von Kryptowährungen zu verringern. Wenn die Benutzer besser über die Risiken von Kryptowährungen informiert sind, werden sie vorsichtiger sein und weniger wahrscheinlich in illegale Aktivitäten verwickelt sein.

Zusammenfassend lässt sich sagen, dass die Anonymität von Kryptowährungen ein ernstes Problem darstellt, das angegangen werden muss. Durch die Einführung strengerer Regulierungsmassnahmen, die Verwendung von Blockchain-Analyse-Tools, die Zusammenarbeit zwischen Regierungen und Kryptowährungsunternehmen sowie die Verbesserung der öffentlichen Aufklärung können wir jedoch die negativen Auswirkungen der Anonymität von Kryptowährungen auf die Geldwäsche eindämmen. Es ist wichtig, dass die Kryptowährungsbranche mit den Regierungen und Strafverfolgungsbehörden zusammenarbeitet, um sicherzustellen, dass Kryptowährungen nicht für illegale Aktivitäten genutzt werden.

Es ist auch wichtig zu betonen, dass nicht alle Kryptowährungen anonym sind. Zum Beispiel ist Bitcoin nicht vollständig anonym, da alle Transaktionen auf der Blockchain öffentlich sichtbar sind. Es gibt jedoch andere Kryptowährungen, wie Monero und Zcash, die aufgrund ihrer Datenschutzfunktionen eine höhere Anonymität bieten.

Als Kryptowährungsbefürworter glaube ich, dass wir die Vorteile von Kryptowährungen geniessen können, ohne dabei die Risiken zu ignorieren. Durch die Einführung von Massnahmen wie KYC und AML, die Verwendung von Blockchain-Analyse-Tools und eine engere Zusammenarbeit zwischen Regierungen und Kryptowährungsunternehmen können wir sicherstellen, dass Kryptowährungen sicher und verantwortungsvoll genutzt werden.

- *Wie lässt sich das Ausmass quantifizieren, in dem die Dezentralität von Kryptowährungen als Triebkraft für die Geldwäscherei wirkt, insbesondere im Vergleich zu herkömmlichen Finanzinstrumenten und -dienstleistungen?*

Es ist schwierig, das Ausmass zu quantifizieren, in dem die Dezentralität von Kryptowährungen als Triebkraft für die Geldwäsche wirkt, da es nur begrenzte Daten und Untersuchungen zu diesem Thema gibt. Allerdings gibt es einige Faktoren, die darauf hindeuten, dass Kryptowährungen aufgrund ihrer dezentralen Natur ein erhöhtes Risiko für Geldwäsche darstellen könnten.

Ein Hauptmerkmal von Kryptowährungen ist ihre Pseudonymität, was bedeutet, dass Transaktionen zwar öffentlich zugänglich sind, aber die Identität der beteiligten Personen nicht automatisch bekannt ist. Dies könnte es Kriminellen erleichtern, Gelder zu waschen und anonyme Transaktionen durchzuführen.

Darüber hinaus ermöglicht die dezentrale Natur von Kryptowährungen den Nutzern, Transaktionen ohne die Notwendigkeit eines Dritten wie einer Bank durchzuführen. Dies bedeutet, dass es schwieriger sein kann, Geldwäscheaktivitäten zu überwachen und zu regulieren.

Es ist jedoch wichtig zu beachten, dass traditionelle Finanzinstrumente und -dienstleistungen auch für Geldwäsche genutzt werden können und dass es keine klaren Beweise dafür gibt, dass Kryptowährungen im Vergleich dazu ein grösseres Risiko darstellen. In der Tat gibt es auch positive Entwicklungen im Krypto-Bereich, die auf die Eindämmung von Geldwäscheaktivitäten abzielen, wie z. B. die Implementierung von KYC- und AML-Verfahren sowie die Zusammenarbeit mit Regulierungsbehörden.

Insgesamt bleibt die Frage nach dem Ausmass, in dem die Dezentralität von Kryptowährungen die Geldwäsche begünstigt, umstritten und erfordert weitere Untersuchungen und Daten, um eine genaue Quantifizierung zu ermöglichen.

- *Inwiefern haben die aktuellen regulatorischen Massnahmen gegen die Geldwäscherei in Bezug auf Kryptowährungen zu einer Einschränkung der Nutzung von Mischdiensten geführt, und welche weiteren Massnahmen könnten ergriffen werden, um ihre Wirksamkeit zu verbessern?*

Da Kryptowährungen in der Regel dezentralisiert und anonym sind, ist es schwierig, sie zu kontrollieren, was sie zu einem bevorzugten Instrument für Geldwäsche macht.

Eine der Auswirkungen dieser Massnahmen war eine Einschränkung der Nutzung von Mischdiensten. Mischdienste sind Dienste, die es den Benutzern ermöglichen, ihre Kryptowährungen zu mischen, um ihre Identität zu verbergen und ihre Transaktionen unkenntlich zu machen. Diese Dienste wurden oft von Kriminellen genutzt, um ihre illegalen Aktivitäten zu verschleiern. Die regulatorischen Massnahmen haben jedoch dazu geführt, dass viele dieser Mischdienste geschlossen wurden oder ihre Dienste einschränken mussten, um den Anforderungen der Geldwäschebekämpfung gerecht zu werden.

Darüber hinaus gibt es noch weitere Massnahmen, die ergriffen werden könnten, um die Wirksamkeit der regulatorischen Massnahmen zu verbessern. Eine Möglichkeit besteht darin, die Zusammenarbeit zwischen Regulierungsbehörden und Kryptobörsen zu stärken. Kryptobörsen könnten verpflichtet werden, ihre Kunden besser zu überprüfen und verdächtige Transaktionen an die Behörden zu melden.

Eine weitere Möglichkeit besteht darin, die Verwendung von Kryptowährungen für illegale Aktivitäten stärker zu sanktionieren. Dies könnte beispielsweise durch die Erhöhung von Strafen oder die Verfolgung von Straftaten im Zusammenhang mit Kryptowährungen als schwerwiegende Verbrechen erfolgen.

Insgesamt sind die regulatorischen Massnahmen gegen Geldwäsche in Bezug auf Kryptowährungen ein wichtiger Schritt, um die Nutzung von Kryptowährungen für illegale Aktivitäten zu reduzieren und das Vertrauen in den Kryptowährungsmarkt zu stärken. Weitere Massnahmen könnten ergriffen werden, um die Wirksamkeit dieser Massnahmen zu verbessern, aber es ist wichtig, dass diese Massnahmen sorgfältig abgewogen werden, um die Integrität des Kryptowährungsmarkts zu erhalten.

- *Wie haben die unterschiedlichen Regulierungsansätze in Grossbritannien, der Schweiz und in Deutschland die Entwicklung von Kryptowährungen und DLT-Technologien in diesen Ländern beeinflusst?*

Das ist eine sehr interessante Frage. Persönlich unterscheide ich immer zwischen Ländern, die Kryptowährungen befürworten. Dazu zähle ich jetzt auch die Schweiz und Grossbritannien. In der Schweiz, genauer gesagt in Zug und bald auch in Lugano, sind die meisten Unternehmen in diesem Bereich ansässig. In England haben wir nicht so viele Unternehmen in diesem Bereich, aber qualitativ hochwertige und vor allem innovative Unternehmen.

Im Gegensatz dazu kenne ich in Deutschland, wo die Regierung eine eher restriktive Haltung gegenüber Kryptowährungen und DLT-Technologien einnimmt, kaum Unternehmen aus dem Krypto-Space. Tatsächlich existiert das Unternehmen, das lange als das innovative deutsche Startup galt, nämlich Wirecard, heute nicht mehr. Ohne klare regulatorische Rahmenbedingungen können diese Unternehmen Schwierigkeiten haben, ihre Geschäftsmodelle zu skalieren und auszubauen. Dies kann dazu führen, dass Investoren und Nutzer das Vertrauen in die Branche verlieren, was sich wiederum auf die Marktkapitalisierung und die Preise von Kryptowährungen auswirken kann. Dies kann dazu führen, dass sie den Zugang zu wichtigen Ressourcen wie Talent, Kapital und Kunden verlieren und somit ihre Wachstumschancen begrenzt werden. Gleichzeitig werden talentierte Mitarbeiter ins Ausland abwandern, um ihre Karrieren voranzutreiben. Dies kann dazu führen, dass das Land wichtige Talente und Innovationen verliert, die für die Zukunft des Landes von Bedeutung sind.

Diese Tatsache zeigt mir, dass technologiefreundliche Regulierungsansätze dazu führen, dass sich innovative Unternehmen in einem Land niederlassen, wo die gesetzlichen Grundlagen für ihr Geschäftsmodell passen und es ihnen auch erlauben, in einem solchen Gebiet tätig zu sein. Wenn nämlich das Umfeld stimmt, werden automatisch jene Unternehmen angezogen, die die gesetzlichen Anforderungen einhalten. Nur wenn Länder Kryptowährungen und DLT-Technologien gestatten oder positive Anreize schaffen, kann sichergestellt werden, dass sich die Technologie weiterentwickelt. Wenn sich die Technologie weiterentwickelt, entstehen nicht nur neue Protokolle für Kryptowährungen, sondern auch neue Unternehmen, die sich ganz allgemein mit der Technologie befassen, wie z. B. RegTech-Unternehmen, die es ermöglichen, AML-Vorschriften einfacher und effizienter einzuhalten. Dadurch profitiert auch die Geldwäschereibekämpfung.

- *Welche regulatorischen Massnahmen hat die Schweizer FINMA ergriffen, um die Entwicklung von Kryptowährungs- und DLT-Unternehmen in Zug zu fördern und zu kontrollieren?*

Die FINMA hat in den letzten Jahren mehrere regulatorische Massnahmen ergriffen, um die Entwicklung von Kryptowährungs- und DLT-Unternehmen zu fördern und zu kontrollieren. So wurden klare Regulierungsrahmen geschaffen, die es Kryptowährungs- und DLT-Unternehmen ermöglichen, ihre Geschäfte legal zu betreiben. Im Jahr 2018 hat die FINMA Richtlinien für ICO veröffentlicht, die es Unternehmen ermöglichen, ihre Token-Verkäufe zu regulieren und zu kontrollieren. Im Jahr 2019 hat die FINMA die Bankenregulierung für Kryptounternehmen aktualisiert und klare Anforderungen für die Einhaltung von Geldwäsche- und Terrorismusfinanzierungsbestimmungen festgelegt. Gleichzeitig wurde ein spezielles Bewilligungsverfahren für Kryptounternehmen eingeführt. Die Unternehmen müssen eine Bewilligung von der FINMA erhalten, um ihre Geschäfte in der Schweiz legal zu betreiben. Die Bewilligung stellt sicher, dass das Unternehmen die Anforderungen der FINMA erfüllt und die gesetzlichen Bestimmungen einhält. Ferner überwacht die FINMA auch Krypto-Vermögensverwalter, um sicherzustellen, dass sie ihre Geschäfte in Übereinstimmung mit den geltenden Gesetzen und Vorschriften betreiben. Die Vermögensverwalter müssen sich bei der FINMA registrieren lassen und ihre Geschäftspraktiken offenlegen.

Im Zusammenhang mit der Geldwäschereibekämpfung ist jedoch die enge Zusammenarbeit mit anderen Aufsichtsbehörden erforderlich, um die Entwicklung von Kryptowährungs- und DLT-Unternehmen zu fördern und zu kontrollieren. Im Jahr 2019 hat die FINMA beispielsweise eine Zusammenarbeit mit der US-amerikanischen Securities and Exchange Commission (SEC) angekündigt, um den Informationsaustausch zu erleichtern und die Zusammenarbeit zu verbessern.

9.2 Transkript Experteninterview mit Nicolas Kilchenmann

- *Welche konkreten Massnahmen könnten ergriffen werden, um die negativen Auswirkungen der Anonymität von Kryptowährungen auf die Geldwäscherei einzudämmen?*

Die Anonymität spielt eine sehr wichtige Rolle bei der Geldwäscherei. Geldwäscherei ist ein Prozess, bei dem illegale Einkünfte oder Vermögenswerte in den legalen Finanz- und Wirtschaftskreislauf eingeführt werden, um ihre Herkunft zu verschleiern. Um dies zu erreichen, müssen Geldwäscher ihre Identität und die Herkunft des Geldes verbergen. Wenn sie erwischt werden, können sie strafrechtlich verfolgt werden. Die Anonymität ermöglicht es den Geldwäscherinnen bzw. Geldwäschern, ihre Identität zu verbergen und somit die Entdeckung vermeiden. Auch ohne Kryptowährungen können sie bereits heute Bankkonten unter falschen Namen eröffnen oder Mittelsmänner einschalten, um das Geld zu waschen. Ferner kann die Anonymität dazu beitragen, dass das Geld nicht mit illegalen Aktivitäten in Verbindung gebracht wird, da es schwerer zu verfolgen ist.

Somit lässt sich feststellen, dass die Anonymität in Bezug auf die Geldwäscherei kein neuer Faktor ist. Die Anonymität bildete schon immer ein Anreiz, Geldwäscherei zu betreiben. Folglich bestehen heute bereits Massnahmen, welche auf die Aufhebung der Anonymität abzielen. So auch die Sorgfaltspflichten nach dem GWG. Es handelt sich dabei um grundlegende Verpflichtungen zur Prävention von Geldwäsche, die darauf abzielen, Anonymität zu bekämpfen, indem sie die Offenlegung der Identität von Kunden und wirtschaftlichen Eigentümern fordern sowie eine Risikoanalyse durchführen, um Transaktionen zu überwachen und verdächtige Aktivitäten zu erkennen und zu melden.

Daher stellt sich die Frage, wie die Sorgfaltspflichten auch auf Kryptowährungen angewendet werden können. Wenn eine Finanzmarkttätigkeit unter den Anwendungsbereich des GWG fällt, sind die Finanzintermediäre verpflichtet, die Sorgfaltspflichten einzuhalten. Es ist wichtig zu beachten, dass diese Verpflichtung für alle Geschäftsbeziehungen und Transaktionen gilt, unabhängig von der Herkunft der Vermögenswerte der Vertragspartei. Die Sorgfaltspflichten gelten sowohl bei der Eröffnung einer neuen Geschäftsbeziehung als auch während der laufenden Geschäftsbeziehung. Da die Geldwäschebekämpfungsregulierungen in der Schweiz auf

Prinzipien basieren und technologieneutral gestaltet sind, ist es anzunehmen, dass diese Pflichten immer Anwendung finden, selbst wenn die Vertragspartei oder die betreffenden Vermögenswerte mit Kryptowährungen in Verbindung stehen.

Die Erfüllung und Umsetzung der formalen Sorgfaltspflichten in Bezug auf Kryptowährungen unterscheiden sich heute bei Banken im Wesentlichen nicht von herkömmlichen Bankdienstleistungen. Bevor eine Geschäftsbeziehung aufgenommen wird, muss die Vertragspartei anhand eines überzeugenden Dokuments identifiziert werden, und es muss festgestellt werden, wer die wirtschaftlich berechtigte Person ist. Gemäss dem KYC-Grundsatz müssen auch Informationen vom Vertragspartner eingeholt werden, um die Herkunft der Vermögenswerte plausibel zu prüfen.

Im Vergleich zu den formalen Sorgfaltspflichten stellen die materiellen oder speziellen Sorgfaltspflichten, die von Finanzintermediären, die Dienstleistungen im Zusammenhang mit Kryptowährungen anbieten, eingehalten werden müssen, grössere Herausforderungen dar. Bei herkömmlichen FIAT-Währungstransaktionen werden detaillierte Informationen über den Absender und den Empfänger bereitgestellt. Bei Krypto-Transaktionen hingegen sind nur pseudonyme Wallet-Adressen verfügbar, die von der Blockchain beliebig generiert werden können. Bitcoin und Ether verknüpfen diese pseudonymen Wallet-Adressen nicht automatisch mit nachverfolgbaren Identitäten im herkömmlichen Sinne. Bei einer Krypto-Transaktion werden jedoch allgemeine Informationen zu den Sender- und Empfängeradressen auf der Blockchain gespeichert. Die Informationen, die in der Blockchain enthalten sind, sind daher nicht mit dem Informationsgehalt herkömmlicher FIAT-Währungstransaktionen vergleichbar.

Daher sind neue Überwachungs- und Analysemethoden sowie spezialisierte Instrumente erforderlich, um gezielt die blockchainspezifische Transaktionsanalyse durchzuführen und insbesondere die Ein- und Auszahlungen von Wallet-Adressen genau zu untersuchen. Mithilfe einer solchen Transaktionsanalyse kann die Transaktionshistorie nachträglich rekonstruiert werden und die Herkunft der Kryptowährungen kann bis zu ihrem Ursprung zurückverfolgt werden. Inzwischen gibt es sowohl Kryptowährungen (wie Monero, Verge und Dash) als auch Blockchain-Dienstleistungen (wie Mixer oder Tumbler), die dazu dienen, die Transaktionsketten zu verschleiern und Anonymität zu gewährleisten, was auch für Geldwäschezwecke genutzt werden kann.

In der Theorie ist es möglich, solche Anonymisierungsdienste mithilfe komplexer forensischer und hochkomplexer Berechnungen zu entwirren. Es ist jedoch wichtig zu beachten, dass dies in der Praxis nicht realisierbar ist, insbesondere da den meisten Banken das erforderliche forensische Know-how fehlt und es wirtschaftlich nicht sinnvoll wäre.

In der Praxis genügt es bereits, wenn eine Bank die Wallet-Adresse ihrer Kunden mit handelsüblichen Transaktionsanalyse-Tools wie z. B. Elliptic verwendet, um die vom Kunden erhaltenen KYC-Informationen zu plausibilisieren. Sobald aber die Analysetools auf Wallet-Adresse des Kunden allfällige Verbindungen zum Darknet, zu Mixer oder zu Tumbler aufweisen, ist die Geschäftsbeziehung als eine Geschäftsbeziehung mit erhöhten Risiken (GmeR) zu betrachten. Der Kunde muss dann die Gründe dafür darlegen, dass die Vermögenswerte nicht aus kriminellen Machenschaften stammen. Sollten die Ausführungen für die Bank nicht nachvollziehbar und plausibel erscheinen, liegt bereits ein solcher Verdacht auf Geldwäscherei vor, dass die Bank die Absetzung einer MROS-Meldung prüfen sollte.

Zusammenfassend lässt sich also sagen, dass die Blockchain nicht nur der Anonymisierung dient und demnach Geldwäscherei begünstigt, sondern den Banken hilft, erhaltene Kundeninformationen bis ins letzte Detail prüfen zu können.

- *Wie lässt sich das Ausmass quantifizieren, in dem die Dezentralität von Kryptowährungen als Triebkraft für die Geldwäscherei wirkt, insbesondere im Vergleich zu herkömmlichen Finanzinstrumenten und -dienstleistungen?*

Die aktuelle Datengrundalge lässt die Beantwortung einer solchen Frage noch gar nicht zu. Zum Beispiel wurde im Dezember des Jahres 2018 dem Bundesrat der Bericht der KGGT zu Gelwäscherei- und Terrorismusfinanzierungsrisiken im Zusammenhang mit Kryptowährungen übermittelt. Damals waren kaum Fälle von Geldwäscherei durch die Nutzung von Kryptowährungen bekannt. Trotzdem hiess es in dem Bericht, dass die Geldwäschereirisiken durch dezentrale Technologien auf der ganzen Welt erheblich seien.

In Anbetracht des rasanten Wachstums solcher dezentralen Technologien müssen Politiker/-innen diesen Markt genauer beobachten, um die damit einhergehenden Mechanismen und Risken besser zu verstehen. Mittels besserer Datengrundlage können die entstehenden Risken gemildert werden, um einen sicheren Markt für dezentralisierte Finanzprodukte zu unterstützen. Ein besseres Verständnis der dezentralen Marktmechanismen erlaubt den Politikerinnen und Politikern darüber zu urteilen, ob allfällige regulatorische Lücken vorliegen, neue Regulierungsansätze benötigt werden oder ob bereits existierende Rahmenregelwerke effizient angepasst werden müssen, sodass sie ähnlichen AML-Regulierungen unterliegen. Ferner werden für DeFi- und Krypto-Märkte mehr und vor allem qualitative hochwertigere Daten benötigt, um die Märkte und ihre Auswirkungen auf die Geldwäschereibekämpfung besser analysieren und möglich Eingriffe prüfen zu können.

Neben den erläuterten Erkenntnissen bezüglich allfälliger Möglichkeiten zur Durchsetzung bereits existierender Regularien bezüglich der dezentralen Strukturen könnten Politiker/-innen die Erkenntnisse aus DeFi für den Einsatz von DLT im traditionellen Finanzwesen anwenden. Es bleibt abzuwarten, ob solche dezentralen Strukturen nur ein kurzlebiges Phänomen sind. Ferner stellt sich auch die Frage, ob dezentrale Dienstleistungen einen Mehrwert für Nutzer, das Finanzsystem und die Wirtschaft erbringen. Meines Erachtens können DeFi- und auch DLT-Technologien durchaus Treiber für konventionelle und disruptive Innovation sein. Bereits heute müssen sich etablierte Akteure in der Finanzbrache damit befassen und bestehende Prozesse (z. B. den Nachhandel und die Finanzintermediation) überprüfen, um sie effizienter auszugestalten.

Ganz so einfach sind die soeben erläuterte Überwachung und Einhaltung der Vorschriften für dezentrale Netzwerke in der Praxis doch nicht. Diese werden nämlich dadurch erschwert, dass die Anbieter solcher dezentralen Dienstleistungen und folglich auch Kryptowährungen weltweit tätig sind, sodass sie in der Regel keine bestimmte Gerichtsbarkeit und keinen bestimmten geografischen Standort ihrer Tätigkeit aufweisen. Eine solche Unsicherheit in Bezug auf die Rechtsprechung stellt nämlich eine Herausforderung für die Durchsetzung dar. Dezentrale Systeme weisen eine höhere Schnelligkeit und Leichtigkeit auf, mit welcher die Anbieter als Reaktion auf regulatorische Anpassungen ihren Standort wechseln können. Daher benötigt es

zusätzlich zur Überwachung und Einhaltung der Vorschriften für dezentrale Netzwerke eine effizientere politische Zusammenarbeit und Diskussion, um die Herausforderungen in Bezug auf grenzüberscheitende Ebenen zu meistern und Probleme der Aufsichtsarbitrage zu reduzieren. Ferner wäre als weitere Zusammenarbeit zwischen allen dezentralen Finanzakteuren zu begrüssen, wo auch Politiker/-innen eine aktive Rolle bei der Schaffung eines kooperativeren Umfelds zwischen allen Stakeholdern einnehmen könnten. Die Entwickler sollten unbedingt in einen solchen Austausch miteinbezogen werden, zumal die Codierung solcher dezentralen Systeme in die Diskussion über die angemessene Aufsicht über die Aktivität solcher Systeme trotz unterschiedlicher Anreize und Anschichten dieser Gemeinschaften einfliessen müssen

- *Inwiefern haben die aktuellen regulatorischen Massnahmen gegen die Geldwäscherei in Bezug auf Kryptowährungen zu einer Einschränkung der Nutzung von Mischdiensten geführt, und welche weiteren Massnahmen könnten ergriffen werden, um ihre Wirksamkeit zu verbessern?*

Es scheint, dass die aktuellen regulatorischen Massnahmen gegen Geldwäsche in Bezug auf Kryptowährungen nur eine begrenzte Auswirkung auf die Nutzung von Mischdiensten haben, da es heutzutage auch ohne solche Dienste möglich ist, die Spur von Kryptowährungen zu verwischen.

Bitte beachte, dass die Transaktionsanalyse- und die Blockchain-Analyse-Tools weiterhin wichtige Instrumente sind, um Geldwäsche im Zusammenhang mit Kryptowährungen zu bekämpfen. Es gibt keine spezifischen regulatorischen Massnahmen, die auf Mischdienste abzielen müssen, sondern es geht darum, dass bestehende Regulierungen konsequent durchgesetzt werden und dass technologische Lösungen wie die Transaktionsanalyse verbessert werden, um die Wirksamkeit bei der Bekämpfung von Geldwäsche im Zusammenhang mit Kryptowährungen zu erhöhen.

Ein Blockchain-Analyse-Tool analysiert die Blockchain-Transaktionen, um verdächtige Aktivitäten aufzudecken. Es gibt bestimmte Muster und Verhaltensweisen, auf die das Tool achten kann, um einen Mixer zu erkennen.

Ein Mixer ist ein Service, der Kryptowährungen von verschiedenen Benutzern bündelt und dann mischt, um die Verfolgbarkeit der Transaktionen zu verringern. Dies geschieht

typischerweise durch die Übertragung von Kryptowährungen von einer Adresse zu einer anderen in einer scheinbar zufälligen Reihenfolge, bevor sie an den Empfänger geschickt werden.

Ein Blockchain-Analyse-Tool kann diese Muster von Transaktionen erkennen, die typisch für Mixer sind. Dazu gehört zum Beispiel das Vorhandensein von mehreren Eingangsadressen und der gleichen Menge an Kryptowährungen, die zu einem Zeitpunkt eingezahlt werden. Dies sind Hinweise darauf, dass mehrere Benutzer ihre Kryptowährungen durch den Mixer geschickt haben.

Ein weiterer Hinweis auf einen Mixer kann sein, wenn es eine grosse Anzahl von Transaktionen gibt, die alle in einem sehr kurzen Zeitraum erfolgen. Dies deutet darauf hin, dass ein automatisiertes System wie ein Mixer verwendet wird, um die Transaktionen zu verarbeiten.

Wenn ein Blockchain-Analyse-Tool diese Hinweise auf Mixer in einer Transaktion erkennt, wird die Transaktion mit einem höheren Risiko geflaggt. Das bedeutet, dass die Transaktion genauer untersucht werden sollte, um sicherzustellen, dass sie keine verdächtigen Aktivitäten aufweist.

- *Wie haben die unterschiedlichen Regulierungsansätze in Grossbritannien, der Schweiz und in Deutschland die Entwicklung von Kryptowährungen und DLT-Technologien in diesen Ländern beeinflusst?*

Einige Länder, wie China, Iran und Indien, haben in den letzten Monaten restriktive Massnahmen gegen Kryptowährungen ergriffen, um Geldwäsche und Spekulation zu bekämpfen. In China hat die Regierung den Kryptowährungshandel verboten und die Kryptowährungs-Mining-Industrie stark eingeschränkt. In Indien hat die Zentralbank den Banken verboten, Kryptounternehmen zu unterstützen, was zu Schwierigkeiten für die Branche führte.

Andere Länder, wie die USA und die Schweiz, haben hingegen eine offene Haltung gegenüber Kryptowährungen eingenommen und setzen auf eine Regulierung, um die Sicherheit für Anleger zu erhöhen. Die USA haben sogar eine spezielle Taskforce eingerichtet, um Cyberkriminalität im Zusammenhang mit Kryptowährungen zu bekämpfen.

Einige Länder, wie El Salvador und die Bahamas, haben sogar Bitcoin als offizielle Währung anerkannt und setzen darauf, dass die Verwendung von Kryptowährungen zur Stärkung der Wirtschaft beitragen kann.

Zusammenfassend lässt sich sagen, dass es in Bezug auf Kryptowährungen unterschiedliche Ansätze und Strategien gibt – je nachdem, wie die jeweiligen Länder die Chancen und Risiken dieser neuen Technologie einschätzen.

Insgesamt hat jedes dieser Länder seine eigene Herangehensweise an die Regulierung von Kryptowährungen und DLT-Technologien. Während Grossbritannien und die Schweiz sich auf die Förderung von Innovationen konzentrieren, hat Deutschland eine strengere Regulierung eingeführt, um Geldwäsche und Terrorismusfinanzierung zu bekämpfen. Trotz dieser Unterschiede haben alle drei Länder ein Interesse an der Entwicklung von Krypto- und Blockchain-Unternehmen und bemühen sich, ein günstiges Umfeld dafür zu schaffen.

- *Welche regulatorischen Massnahmen hat die Schweizer FINMA ergriffen, um die Entwicklung von Kryptowährungs- und DLT-Unternehmen in Zug zu fördern und zu kontrollieren?*

Die FINMA hat verschiedene regulatorische Massnahmen ergriffen. Sie hat klare Richtlinien für Initial Coin Offerings (ICO) entwickelt, um sicherzustellen, dass sie den Schweizer Finanzmarktgesetzen entsprechen. Die ICO-Emittenten müssen sich bei ihr registrieren lassen und bestimmte Anforderungen erfüllen, wie z. B. die Offenlegung von Informationen über das Projekt und die Strukturierung des Tokens. Ferner wurden diverse Aufsichtsmitteilungen und Merkblätter veröffentlicht, die den Unternehmen helfen, die regulatorischen Anforderungen zu verstehen und einzuhalten. Diese Dokumente geben auch Rechtssicherheit für die Unternehmen, da sie ihnen eine klare Vorstellung davon geben, was von ihnen erwartet wird.