sui generis

EREI

SIERTER
ENDUNGEN

Geldwäscherei mittels dezentralisierter Finanzanwendungen

Mit besonderer Berücksichtigung der Unterlassungsstrafbarkeit von Betreiberinnen

Lisa Reggiani

Hinweise zur digitalen Fassung dieses Buches:

— Die digitale Fassung (Open Access) ist sowohl auf der Webseite des Verlags (www.suigeneris-verlag.ch), auf Google Books als auch direkt über den Digital Object Identifier (DOI) zugänglich. Der DOI zum vorliegenden Buch ist im Impressum angegeben.
— Sämtliche Gesetzesartikel sowie alle frei zugänglichen Gerichtsurteile und Behördenentscheidungen sind in der digitalen Fassung verlinkt.
— Häufig verwenden die AutorInnen in ihrem Manuskript Links auf weitere Quellen. Diese werden in den Büchern nicht abgedruckt, aber in der digitalen Fassung den entsprechenden Textstellen hinterlegt.
— Für die Verlinkung werden Permalinks eingesetzt. Es handelt sich dabei um Links auf eine archivierte Version der Webseiten im Zeitpunkt der Linksetzung. Die Links sind beständig, d.h. sie funktionieren auch dann noch, wenn die Originalseite nicht mehr zugänglich ist und ihr Inhalt ändert nicht, wenn sich die Originalseite ändert.

Lisa Reggiani

Geldwäscherei mittels dezentralisierter Finanzanwendungen

Mit besonderer Berücksichtigung der Unterlassungsstrafbarkeit von Betreiberinnen

sui generis, Zürich 2026

non mollare mai

Vorwort

Ein Vorwort zu schreiben, fällt vielen schwerer als manches Kapitel der eigentlichen Dissertation. Vielleicht, weil man hier zum ersten Mal nicht mehr versucht, besonders präzise, dogmatisch sauber oder quellenbasiert zu formulieren, sondern persönlich. Diese Arbeit mag meinen Namen tragen, entstanden ist sie jedoch nur durch die Unterstützung vieler Menschen, denen ich an dieser Stelle danken möchte.

Mein besonderer Dank gilt meinem Doktorvater, Prof. Dr. Gian Ege. Sein Vertrauen, seine Unterstützung und seine Offenheit gegenüber einem anspruchsvollen und noch wenig erschlossenen Forschungsthema haben diese Arbeit erst ermöglicht. Er hat mich während der gesamten Entstehung begleitet, gefördert und stets dazu ermutigt, eigene Überlegungen konsequent weiterzuverfolgen. Ohne ihn stünde ich heute wohl nicht dort, wo ich stehe. Ebenso danke ich Prof. Dr. Monika Simmler für ihre wertvollen Anregungen und die Übernahme des Zweitgutachtens.

Mein Dank gilt auch allen Weggefährtinnen und Weggefährten an der T10. Viele Gedanken dieser Arbeit entstanden nicht nur am Schreibtisch, sondern ebenso in Gesprächen auf dem Gang, bei einer Tasse Kaffee oder in gemeinsamen Momenten akademischer Verzweiflung. Besonders danken möchte ich meinen Mitdoktoranden RA MLaw Luca Schoop und RA MLaw Patricia Soltani. Unsere gemeinsamen Schreibretraiten, Diskussionen und unzähligen Gespräche haben die Entstehung dieser Arbeit wesentlich geprägt. Ebenso danke ich MLaw Sarina Kübler, BLaw Michelle Sauter, Sarah Schmid und MLaw Niklaus Sempach für die sorgfältige Durchsicht des Manuskripts und ihre hilfreichen Anmerkungen.

Ein besonderer Dank gebührt meiner Familie. Ich hatte das Privileg, meinen eigenen Weg gehen zu dürfen, ohne Druck, dafür stets begleitet von Vertrauen, Unterstützung und Liebe. Mami, Papi und Noa: Ihr habt mich während des gesamten Entstehungsprozesses getragen, auch dann, wenn ich selbst an dieser Arbeit gezweifelt habe. Ohne euch gäbe es diese Arbeit nicht.

Während der Entstehung dieser Dissertation gab es Zeiten, in denen ich mir selbst einen enormen Druck auferlegte und zeitweise befürchtete, daran zu zerbrechen. Rückblickend hat mich diese Erfahrung gelehrt, dass wissenschaftliche Arbeit nicht nur aus Erkenntnissen, sondern auch aus Beharrlichkeit entsteht. Diese Arbeit ist deshalb all jenen gewidmet, die das Leben schon einmal aus der Bahn geworfen hat, die an sich selbst gezweifelt haben oder die sich irgendwann am tiefsten Punkt ihres Weges wiederfanden. Möge sie

daran erinnern, dass man weitergehen kann, auch wenn der nächste Schritt manchmal unmöglich erscheint.

Die Dissertation entstand während meiner Tätigkeit als wissenschaftliche Assistentin am Lehrstuhl von Prof. Dr. Christian Schwarzenegger sowie Prof. Dr. Gian Ege an der Universität Zürich. Für die Schlussphase wurde mir von der Universität Zürich ein Candoc Grant verliehen, der mir die notwendige Zeit und die finanziellen Mittel verschaffte, die Arbeit abzuschliessen. Für diese Unterstützung bin ich der Universität Zürich sehr dankbar.

Die vorliegende Abhandlung wurde im Mai 2026 von der Rechtswissenschaftlichen Fakultät der Universität Zürich als Dissertation angenommen.

Eschenbach SG, im Juni 2026
Lisa Reggiani

Inhaltsübersicht

Vorwort ... V
Inhaltsübersicht ... VII
Inhaltsverzeichnis ... IX
Literaturverzeichnis ... XV
Materialien und weitere amtliche Publikationen ... XLIII
Abkürzungsverzeichnis ... XLVII
Glossar ... LIII

Einleitung ... 1

Ausgangslage und Forschungsfrage ... 1
Untersuchungsgegenstand ... 3
Gang der Untersuchung ... 5
Methodik und Terminologie ... 6

Teil 1: Grundlagen ... 9

Kapitel 1: Blockchain und dezentralisierte Finanzanwendungen ... 9
I. Blockchain-Technologie ... 9
II. Smart Contracts ... 20
III. Dezentralisierte Finanzanwendungen ... 25
IV. Akteure im Umfeld von dezentralisierten Anwendungen ... 36
Kapitel 2: Geldwäschereihandlungen von Nutzern dezentralisierter Finanzanwendungen ... 48
I. Phänomen ... 48
II. Geldwäschereirelevante Nutzungsmuster im Umgang mit dezentralisierten Protokollen ... 58
III. Zusammenfassung ... 69

Teil 2: Betreiberverantwortlichkeit für Geldwäscherei ... 71

Kapitel 1: Begehensstrafbarkeit nach Art. 305bis StGB ... 71
I. Rechtsgut, Geldwäschereiobjekt und Vortat ... 72
II. Täterschaft ... 74
III. Teilnahme ... 81
IV. Fazit ... 97

Kapitel 2: Strafbarkeit durch Unterlassen 99
I. Täterschaftliche Geldwäscherei durch Unterlassen 99
II. Garantenstellung 105
III. Weitere objektive Tatbestandsmerkmale der unechten Unterlassung 136
IV. Subjektiver Tatbestand 140
V. Versuch 151
VI. Fazit 152
Kapitel 3: Strafrechtliche Anschlussfragen 154
I. Schwere Fälle von Geldwäscherei 155
II. Konkurrenzen 164
III. Strafanwendungsrecht 168

Schlussbetrachtung 177

Zusammenfassung der wesentlichen Ergebnisse 177
Schlussfolgerungen 179

Inhaltsverzeichnis

Vorwort ... V
Inhaltsübersicht ... VII
Inhaltsverzeichnis ... IX
Literaturverzeichnis ... XV
Materialien und weitere amtliche Publikationen ... XLIII
Abkürzungsverzeichnis ... XLVII
Glossar ... LIII

Einleitung ... 1

Ausgangslage und Forschungsfrage ... 1
Untersuchungsgegenstand ... 3
Gang der Untersuchung ... 5
Methodik und Terminologie ... 6

Teil 1: Grundlagen ... 9

Kapitel 1: Blockchain und dezentralisierte Finanzanwendungen ... 9
I. Blockchain-Technologie ... 9
A. Hintergrund und Definition ... 9
B. Blockchain-Typen ... 10
C. Funktionsweise der Blockchain-Technologie ... 12
1. Verteiltes Register und Netzwerkteilnehmer (Nodes) ... 12
2. Kryptographie ... 13
a) Digitale Signatur und Schlüsselverwaltung ... 13
b) Kryptographische Verbindung der Blöcke: Hash-Funktionen ... 15
3. Transaktionsablauf ... 16
D. Zusammenfassung ... 19
II. Smart Contracts ... 20
A. Hintergrund ... 21
B. Definition ... 22
C. Zusammenfassung ... 25
III. Dezentralisierte Finanzanwendungen ... 25
A. Begriff und Merkmale ... 25
B. Kryptowerte ... 28

C. Typologie dezentralisierter Finanzanwendungen ... 30
1. Dezentralisierte Handelsplattformen ... 30
2. Kryptomixer ... 32
3. Weitere Typen ... 34
D. Zusammenfassung ... 35
IV. Akteure im Umfeld von dezentralisierten Anwendungen ... 36
A. Smart Contracts ... 37
1. Autonomie und Automation ... 37
2. Technische Einordnung von Smart Contracts ... 39
B. Betreiberschaft ... 41
1. Lebenszyklus von Finanzanwendungen ... 41
2. Betreiben ... 42
C. Nutzer ... 45
D. Zusammenfassung ... 47
Kapitel 2: Geldwäschereihandlungen von Nutzern dezentralisierter Finanzanwendungen ... 48
I. Phänomen ... 48
A. Einführung und Relevanz ... 48
B. Modi operandi der Herkunftsverschleierung ... 50
1. ‹Tatort› Blockchain ... 50
2. Deliktische Herkunft von Kryptowerten ... 52
3. Drei-Phasen-Modell ... 55
II. Geldwäschereirelevante Nutzungsmuster im Umgang mit dezentralisierten Protokollen ... 58
A. Tatbestandliche Grundlagen von Art. 305bis Ziff. 1 StGB ... 59
B. Nutzungsmuster bei der Verschleierung deliktischer Kryptowerte ... 62
1. Dezentralisierte Handelsplattformen ... 62
2. Kryptomixer ... 66
C. Nutzungsmuster bei der Konvertierung von Fiatgeld in Kryptowerte ... 67
III. Zusammenfassung ... 69

Teil 2: Betreiberverantwortlichkeit für Geldwäscherei ... 71

Kapitel 1: Begehensstrafbarkeit nach Art. 305bis StGB ... 71
I. Rechtsgut, Geldwäschereiobjekt und Vortat ... 72
II. Täterschaft ... 74
A. Tun durch Bereitstellen einer Infrastruktur ... 74
B. Unmittelbare Täterschaft ... 75

C. Mittäterschaft ... **76**
1. (Mit-)Tatherrschaft ... **76**
2. Gemeinsamer Tatentschluss ... **79**
D. Zwischenfazit ... **80**
III. Teilnahme ... **81**
A. Anstiftung ... **81**
B. Gehilfenschaft ... **83**
1. Objektiver Beihilfetatbestand ... **83**
2. Harmlose Gehilfenschaft ... **85**
a) Überblick ... **85**
b) Deliktischer Sinnbezug ... **87**
c) Vorsatz bezüglich der Hilfeleistung ... **89**
d) Vorsatz bezüglich der Bestimmtheit der Haupttat ... **92**
3. Beihilfe am Versuch ... **95**
C. Zwischenfazit ... **96**
IV. Fazit ... **97**
Kapitel 2: Strafbarkeit durch Unterlassen ... **99**
I. Täterschaftliche Geldwäscherei durch Unterlassen ... **99**
A. Begehung durch Unterlassen bei Tätigkeitsdelikten ... **100**
B. Täterschaft und Teilnahme ... **102**
C. Zwischenfazit ... **104**
II. Garantenstellung ... **105**
A. Geldwäschereigesetz ... **106**
1. Persönlicher und sachlicher Geltungsbereich ... **107**
a) Hilfe bei der Übertragung von virtuellen Vermögenswerten ... **109**
aa) Virtuelle Währungen ... **110**
bb) Hilfe zur Übertragung ... **110**
cc) Erste Tatbestandsvariante: Verfügungsmacht ... **112**
dd) Zweite Tatbestandsvariante: dauernde Geschäftsbeziehung ... **113**
ee) Berufsmässigkeit und Fremdheit der Vermögenswerte ... **115**
ff) Würdigung ... **115**
b) Geld- und Wertübertragung ... **117**
c) Prudenzielle Finanzintermediäre ... **118**
aa) Bank ... **118**
bb) Finanzmarktinfrastrukturen ... **120**
2. Örtlicher Geltungsbereich ... **121**
3. Zwischenfazit ... **124**

4. Qualifizierte Handlungspflichten des Geldwäschereigesetzes 125
a) Meinungsstand 125
b) Würdigung 127
5. Zwischenfazit 128
B. Garantenstellungen im Kontext von Gefahrenquellen 128
1. Ingerenz und Herrschaft über eine Gefahrenquelle 129
2. Geschäftsherrenhaftung 132
3. Qualifizierte Handlungspflicht 134
C. Zwischenfazit 135
III. Weitere objektive Tatbestandsmerkmale der unechten Unterlassung 136
A. Hypothetische Kausalität 136
B. Tatmacht 139
C. Gleichwertigkeit von Tun und Unterlassen 140
IV. Subjektiver Tatbestand 140
A. (Eventual-)Vorsatz 140
1. Wissenselement 141
a) Wissen um Garantenstellung und Handlungspflicht 141
b) Wissen um Gefahr, Handlungsmöglichkeit und Kausalität 143
2. Willenselement 145
B. Irrtümer 150
C. Zwischenfazit 150
V. Versuch 151
VI. Fazit 152
Kapitel 3: Strafrechtliche Anschlussfragen 154
I. Schwere Fälle von Geldwäscherei 155
A. Mitglieder einer kriminellen oder terroristischen Organisation 155
1. Betreiberschaft als kriminelle oder terroristische Organisation 157
2. Betreiberinnen als Mitglieder krimineller oder terroristischer Organisationen 159
B. Bandenmitglied 159
C. Gewerbsmässige Geldwäscherei 161
D. Weitere schwere Fälle 163
E. Fazit 163
II. Konkurrenzen 164
A. Gehilfenschaft und täterschaftliche Unterlassung 164
B. Mehrfache Geldwäscherei 165

C. Konkurrenztatbestände bei Sorgfaltspflichtverletzungen 167
D. Fazit 167
III. Strafanwendungsrecht 168
A. Inlandtaten 168
1. Unterlassung 169
2. Gehilfenschaft 171
B. Extraterritoriale Strafanwendung 172
C. Fazit 174

Schlussbetrachtung 177

Zusammenfassung der wesentlichen Ergebnisse 177
Schlussfolgerungen 179

Literaturverzeichnis

ACKERMANN JÜRG-BEAT
- Geldwäschereistrafrecht, in: Jürg-Beat Ackermann (Hrsg.), Wirtschaftsstrafrecht der Schweiz, Hand- und Studienbuch, 2. Aufl., Bern 2021 (zit. ACKERMANN, Wirtschaftsstrafrecht)
- Wann ist abstrakt konkret genug? – vom Eignungsdelikt Geldwäscherei und der «Rechtgutsverschiebung», in: Jeanneret Yvan / Sträuli Bernhard (Hrsg.), Empreinte d'une pionnière sur le droit pénal, Mélanges en l'honneur de Ursula Cassani, Zürich 2021, S. 1 ff. (zit. ACKERMANN, Eignungsdelikt)
- Unterlassungsrisiken in der Unternehmensleitung, am Beispiel der Geldwäscherei, in: Ackermann Jürg-Beat / Hilf Marianne J. (Hrsg.), Geldwäscherei – Asset Recovery, 6. Schweizerische Tagung zum Wirtschaftsstrafrecht, Zürich/Basel/Genf 2012, S. 133 ff. (zit. ACKERMANN, Unterlassungsrisiken)

ACKERMANN JÜRG-BEAT (Hrsg.), Kommentar Kriminelles Vermögen, Kriminelle Organisationen, Band II, Zürich 2018 (zit. KV/KO StGB/GwG-BEARBEITERIN)

ACKERMANN JÜRG-BEAT et al., Strafrecht Individualinteressen, Gesetz, System und Lehre im Lichte der Rechtsprechung, Bern 2019

ACKERMANN JÜRG-BEAT / ZEHNDER STEPHANIE, Praxistaugliche Dogmatik und Beweisanforderungen, forumpoenale 1/2014, S. 45 ff. (zit. ACKERMANN/ZEHNDER, Dogmatik)

AEBI-MÜLLER REGINA E. / MÜLLER CHRISTOPH (Hrsg.), Berner Kommentar, Kommentar zum schweizerischen Privatrecht, Band VI: Obligationenrecht, 2. Abteilung: Die einzelnen Vertragsverhältnisse, 8. Teilband: Die einfache Gesellschaft, Art. 530–544 OR, Bern 2006 (zit. BK OR-BEARBEITERIN)

AKARTUNA ERAY ARDA, Around $1.2 billion from crypto hacks funneled through decentralized exchanges, 2022

AKARTUNA ERAY ARDA / MADELIN THIBAUD, Elliptic Cross-Chain Report 2023, The state of cross-chain crime, Countering the new age of crypto crime and money laundering in a cross-chain world, 2023

ALONSO EDUARDO / MONDRAGÓN ESTHER, Agency, Learning and Animal-Based Reinforcement Learning, in: Nickles Matthias / Rovatsos Michael / Weiss Gerhard (Hrsg.), Agents and Computational Autonomy, Potential, Risks, and Solutions, Berlin/Heidelberg 2004, S. 1 ff.

ANDREOTTI FABIO, Dezentrale Handelsplattformen im Schweizer Finanzmarktrecht, Eine Analyse unter Erarbeitung eines Rechtsprinzips der Dezentralität, Diss. Zürich 2022, Zürich 2024

ANDREOTTI FABIO / ZIMMERMANN STEPHAN / PRANTL FLORIAN, Custodial Staking, GesKR 3/2023, S. 333 ff.

ANKER-SØRENSEN LINN / ZETZSCHE DIRK A., From Centralized to Decentralized Finance: The Issue of ‹Fake-DeFi›, 2021

ANTENEN JACQUES, Problématique nouvelle relative à la poursuite pénale du blanchissage d'argent, à la confiscation et au sort des avoirs confisqués, ZStrR 1/1996, S. 42 ff.

ANTONOPOULOS ANDREAS, Mastering Bitcoin, 2. Aufl., Sebastopol 2017

ANTONOPOULOS ANDREAS / WOOD GAVIN, Mastering Ethereum, Building Smart Contracts and DApps, Sebastopol 2018

ARZT GUNTHER, Das schweizerische Geldwäschereiverbot im Lichte amerikanischer Erfahrungen, ZStrR 106/1989, S. 160 ff.

ASSION SIMON (Hrsg.), TTDSG, Telekommunikation-Telemedien-Datenschutz-Gesetz, Handkommentar, Baden-Baden 2022 (zit. HK TTDSG-BEARBEITERIN)

BABEY FABIO / HOANG NGUYEN, Geldwäscherei und Compliance: Aktuelle Entwicklungen, GesKR 4/2023, S. 488 ff.

BACHARACH JEREMY, Cryptoactifs et lutte contre le blanchiment d'argent, Étude en droit suisse, Diss. Genf 2023, Genf/Zürich 2025

BACHER JEAN-LUC, Jurisprudence du TPF en matière de blanchiment d'argent, Der Schweizer Treuhänder 4/2012, S. 235 ff.

BÄCHER THERESA, Zur strafrechtlichen Verantwortlichkeit des Betreibers einer Plattform im Darknet, Diss. Bayreuth 2023, Berlin 2024

BACHMANN MARIO / ARSLAN NERGIZ, «Darknet»-Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber?, NZWiSt 7/2019, S. 241 ff.

BADEV ANTON / CHEN MATTHEW, Bitcoin: Technical Background and Data Analysis, Washington 2014

BARBON ANDREA / RANALDO ANGELO, On The Quality Of Cryptocurrency Markets Centralized Versus Decentralized Exchanges, Swiss Finance Institute Research, 2024

BAUMANN DANIEL, Verhaltensregeln im Finanzmarktrecht: Unter besonderer Berücksichtigung des Börsen- und Kollektivanlagenrechts sowie des geplanten FIDLEG, Diss. Bern 2017, Zürich/Basel/Genf 2018

BAUMGARTNER FABIAN, Die berüchtigtste Hackergruppe attackiert die Schweiz und erbeutet Millionen. Ein Leak zeigt jetzt, wie sie arbeiten, NZZ vom 30. Mai 2025

BENHAMOU YANIV / WANG LOUISE, Cyberattaque et ransomware: risques juridiques à payer et assurabilité des rançons, SZW 1/2023, S. 80 ff.

BENSON VLADLENA / TURKSEN UMUT / ADAMYK BOGDAN, Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities, Journal of Financial Regulation and Compliance 1/2024, S. 80 ff.

BERENTSEN ALEKSANDER / SCHÄR FABIAN, Bitcoin, Blockchain, and Cryptoassets, A Comprehensive Introduction, London 2020

BERGAULT PHILIPPE et al., Automated Market Makers: Mean-Variance Analysis of LPs Payoffs and Design of Pricing Functions, 2022

BERNASCONI PAOLO, Die Geldwäscherei im schweizerischen Strafrecht. Bericht mit Vorschlägen zu einer Gesetzesrevision (neuer Art. 305bis StGB), im Auftrag des Eidgenössischen Justiz- und Polizeidepartementes, Lugano 1986

BERTOSSA CARLO, Unternehmensstrafrecht – Strafprozess und Sanktionen, Diss. Basel, Bern 2003

BIERMANN FRIEDRICH G., Wissenszurechnung und Künstliche Intelligenz, Diss. Halle-Wittenberg, Baden-Baden 2022

BLANDIN APPOLINE et al., 3rd Global Cryptoasset Benchmarking Study, 2020

BLATTER MANUEL, Rechtsstaatliche Garantien im Enforcementverfahren der FINMA, Diss. Zürich, Zürich 2019

BLOCHER WALTER, Fehlerhafte Smart Contracts, in: Braegelmann Tom / Kaulartz Markus (Hrsg.), Rechtshandbuch Smart Contracts, München 2019

BÖHME RAINER et al., Bitcoin: Economics, Technology, and Governance, Journal of Economic Perspectives 2/2016, S. 213 ff.

BOHRER ANDREAS et al., Finanzmarktrecht, Entwicklungen 2023, Bern 2024

BOMMER FELIX
- Die strafrechtliche Rechtsprechung des Bundesgerichts im Jahr 2010, ZBJV 4/2015, S. 350 ff. (zit. BOMMER, ZBJV 2015)
- Die strafrechtliche Rechtsprechung des Bundesgerichts im Jahr 2006, ZBJV 11/2008, S. 850 ff. (zit. BOMMER, ZBJV 2008)
- Anstiftung und Selbstverantwortung, plädoyer 3/2002, S. 34 ff. (zit. BOMMER, Anstiftung)

BÖRDING ANDREAS et al., Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, Computer und Recht 2/2017, S. 134 ff.

BOŠKIĆ MAGDALENA / HEPP SEBASTIAN, zkKYC in Decentralized Finance (DeFi), Unter besonderer Berücksichtigung des Geldwäschereigesetzes, GesKR 2/2023, S. 209 ff.

BOURQUIN GABRIEL, Steuergeldwäscherei in Bezug auf direkte Steuern: Ein Beitrag zur Auslegung von Art. 305bis Ziff. 1 und Ziff. 1bis StGB, Diss. Zürich 2016, Berlin/Bern 2017

BOVET CHRISTIAN / ANNE HÉRITIER LACHAT, Intermédiaires financiers, in: Christian Bovet (Hrsg.), Finanzmarktaufsicht / Surveillance des marchés financiers, Basel 2016

BRADSHAW JEFFREY et al., Dimensions of Adjustable Autonomy and Mixed-Initiative Interaction, in: Nickles Matthias / Rovatsos Michael / Weiss Gerhard (Hrsg.), Agents and Computational Autonomy, Potential, Risks, and Solutions, Berlin/Heidelberg 2004, S. 17 ff.

BRINKMANN MARCO, Besteuerung der Erträge aus Kryptowährungen, in: Omlor Sebastian / Link Mathias (Hrsg.), Kryptowährungen und Token, 3. Aufl., Frankfurt am Main 2026, S. 769 ff.

BURGWINKEL DANIEL, Blockchaintechnologie und deren Funktionsweise verstehen, in: Burgwinkel Daniel (Hrsg.), Blockchain Technology, Einführung für Business- und IT Manager, München 2016, S. 3 ff.

BUTERIN VITALIK
- The Meaning of Decentralization, 2017 (zit. BUTERIN, Decentralization)
- DAOs, DACs, DAs and More: An Incomplete Terminology Guide, 2014 (zit. BUTERIN, Terminology)

– Ethereum White Paper, A Next Generation Smart Contract & Decentralized Application Platform, 2013 (zit. BUTERIN, White Paper)

CAPRARA TOMMASO, Strafrechtliche Verantwortlichkeit bei der Organisation und Durchführung von Grossveranstaltungen, Diss. Zürich 2020

CASSANI URSULA / BOVET CHRISTIAN / VILLARD KATIA (Hrsg.), Commentaire Romand, Loi sur le blanchiment d'argent, Basel 2022 (zit. CR LBA-BEARBEITERIN)

CASSANI URSULA / VILLARD KATIA, Droit pénal économique, 2. Aufl., Basel 2020

CEFFINATO TOBIAS
– Bereitstellen krimineller Infrastruktur im Internet, Zeitschrift für Rechtspolitik 6/2019, S. 161 ff. (zit. CEFFINATO, kriminelle Infrastruktur)
– Die strafrechtliche Verantwortlichkeit von Internetplattformbetreibern, Jus 5/2017, S. 403 ff. (zit. CEFFINATO, Internetplattformbetreiber)

CHAINALYSIS
– The 2025 Crypto Crime Report, The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation, 2025 (zit. Chainalysis, 2025)
– The 2024 Crypto Crime Report, The latest trends in ransomware, scams, hacking, and more, 2024 (zit. Chainalysis, 2024)
– The 2022 Crypto Crime Report, Original data and research into cryptocurrency-based crime, 2022 (zit. Chainalysis, 2022)

CHRISTALLER THOMAS et al., Robotik, Perspektiven für menschliches Handeln in der zukünftigen Gesellschaft, Berlin/Heidelberg 2001

CLACK CHRISTOPHER / BAKSHI VIKRAM / BRAINE LEE, Smart Contract Templates: foundations, design landscape and research directions, 2017

CIRENER GABRIELE et al. (Hrsg.), Leipziger Kommentar, StGB, 14. Aufl., Berlin 2024 (zit. LK StGB-BEARBEITERIN)

CIPHERTRACE, Cryptocurrency crime and anti-money laundering, Report, 2022

COLLINS JOHN, Crypto, crime and control, Cryptocurrencies as an enabler of organized crime, 2022

CONDOS JAMES et al., Blockchain Technology: Opportunities and Risks, Vermont 2016

CONRAD HARI AURÉLIE, Le blanchiment d'argent par omission, Quelques réflexions découlant de l'ATF 136 IV 188, SZW 4/2012, S. 361 ff.

CONSTANTIN ARNAUD, Le droit de réponse en ligne, Diss. Fribourg, Zürich 2019

CORBOZ BERNARD, Les infractions en droit suisse, Volume II, 3. Aufl., Bern 2010

COVIELLO MICHELE / MÄDER LUKAS / BAUMGARTNER FABIAN, Kriminelle haben über einen Server in Zürich einen Milliardenbetrag an dreckigem Geld gewaschen. Nun ist den Ermittlern ein grosser Schlag gelungen, NZZ vom 1. Dezember 2025

CROSBY MICHAEL et al., BlockChain Technology: Beyond Bitcoin, AIR 2/2016, S. 6 ff.

CURCHOD NICOLAS / PASQUIER BRUNO, Private Law Aspects of Liquidity Pools in Decentralized Finance (DeFi), sui generis 2024, S. 243 ff.

CURRY DAVID, Coinbase Revenue and Usage Statistics (2025), 2025

DAN ADRIAN, Le délit de commission par omission: éléments de droit suisse et comparé, Diss. Genf 2014, Zürich 2015

DECKER MICHAEL, Adaptive Robotik und Verantwortung, in: Gless Sabine / Seelmann Kurt (Hrsg.), Intelligente Agenten und das Recht, Baden-Baden 2016, S. 23 ff.

DE COL DEBORAH, Zivilrechtliche Herausforderungen der Blockchain-Technologie: die schweizerischen und liechtensteinischen Lösungsansätze im Vergleich, Zürich 2021

DE FILIPPI PRIMAVERA / WRAY CHRIS / SILENO GIOVANNI, Smart contracts, Internet Policy Review 2/2021, S. 1 ff.

Deutsche Bundesbank, Crypto tokens and decentralised financial applications, 2021

DICKMANN ROMAN, Cyberversicherung, München 2025

DIEHL MARTIN, Formen programmierbaren Geldes und Rolle der Zentralbank, in: Omlor Sebastian / Link Mathias (Hrsg.), Kryptowährungen und Token, 3. Aufl., Frankfurt am Main 2026, S. 37 ff.

DONATSCH ANDREAS / HEIMGARTNER STEFAN (Hrsg.), Orell Füssli StGB/JStG Kommentar, Mit weiteren Erlassen und Kommentar zu den Strafbestimmungen des SVG, BetmG, AuG sowie OBG, 22. Aufl., Zürich 2026 (zit. OFK StGB-BEARBEITERIN)

DONATSCH ANDREAS / CAVALLO ANGELA, Entwicklungen im Strafrecht / Le point sur le droit pénal, SJZ 22/2011, S. 521 ff.

DONATSCH ANDREAS / GODENZI GUNHILD / TAG BRIGITTE, Strafrecht I, Verbrechenslehre, 10. Aufl., Zürich 2022

DONATSCH ANDREAS / THOMMEN MARC / WOHLERS WOLFGANG, Strafrecht IV, Delikte gegen die Allgemeinheit, 5. Aufl., Zürich 2017

DRITTENBASS JOEL, Regulierung von autonomen Robotern, Angewendet auf den Einsatz von autonomen Medizinrobotern: Eine datenschutzrechtliche und medizinprodukterechtliche Untersuchung, Diss. St. Gallen, Baden-Baden 2021

DRUMMER DANIEL / NEUMANN DIRK, Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts, Journal of Information Technology 4/2020, S. 337 ff.

DUARTE LUDOVIC, Sorgfaltspflichten für Finanzintermediäre und Händler, in: Sester Peter et al. (Hrsg.), St. Galler Handbuch zum Schweizer Finanzmarktrecht, Finanzmarktaufsicht und Finanzmarktinfrastrukturen, St. Gallen / Zürich 2018

DUPUIS DANIEL / GLEASON KIMBERLY, Money laundering with cryptocurrency: open doors and the regulatory dialectic, Journal of Financial Crime 1/2021, S. 60 ff.

DYENS ALEXANDRE, Territorialité et ubiquité en droit pénal international suisse, Diss. Lausanne 2013, Basel 2014

EGGER TANNER CHRISTINE, Die strafrechtliche Erfassung der Geldwäscherei, Ein Rechtsvergleich zwischen der Schweiz und der Bundesrepublik Deutschland, Diss. Zürich 1998, Zürich 1999

EICHHORN ALEXANDER, Kollektive Kapitalanlagen für qualifizierte Anlegerinnen und Anleger nach dem Bundesgesetz über die kollektiven Kapitalanlagen (KAG), Diss. St. Gallen, Zürich / St. Gallen 2014

EIDAM LUTZ, Der Organisationsgedanke im Strafrecht, Tübingen 2015

EISELE JÖRG / BOSCH NIKOLAUS (Hrsg.), Tübinger Kommentar, Strafgesetzbuch, Kommentar, 31. Aufl., München 2025 (zit. Tübinger Kommentar StGB-BEARBEITERIN)

Elliptic, DeFi: Risk, Regulation, and the Rise of DeCrime, 2021

ENDSLEY MICA, The application of human factors to the development of expert systems for advanced cockpits, Proceedings of the Human Factors Society Annual Meeting, 1987, S. 1388 ff.

ENGLER MARC
– Die strafrechtliche Verantwortlichkeit des Veranstalters von Sportanlässen, in: Kleiner Jan / Baddeley Margareta / Arter Oliver (Hrsg.), Sportrecht, Bd. I, Bern 2013, S. 489 ff. (zit. ENGLER, Sportanlässe)
– Die Vertretung des beschuldigten Unternehmens, Diss. Zürich 2008 (zit. ENGLER, Diss.)

ERARD FRÉDÉRIC, Blockchain et santé: perspectives juridiques en Suisse, in: Dunand Jean-Philippe / Dupont Anne-Sylvie / Mahon Pascal (Hrsg.), Le Droit face à la révolution 4.0, Zürich 2019, S. 215 ff.

ERB VOLKER / SCHÄFER JÜRGEN (Hrsg.), Münchner Kommentar, StGB, Bd. 1, 5. Aufl., München 2025 (zit. MüKo StGB-BEARBEITERIN)

ERBGUTH JÖRN, Kryptowerte und der Datenschutz, ZVglRWiss 3/2023, S. 338 ff.

EQUEY DAVID, La responsabilité pénale des fournisseurs de services Internet, Etude à la lumière des droits suisse, allemand et français, Diss. Lausanne 2015, Bern 2016

European Banking Authority / European Securities and Markets Authority, Joint Report, Recent developments in crypto-assets (Article 142 of MiCAR), 2025 (zit. EBA/ESMA)

European Securities and Markets Authority, Crypto assets: Market structures and EU relevance, 2024 (zit. ESMA)

FAVROD-COUNE PASCAL, Les cryptoactifs dans la procédure d'exécution forcée: saisie, revendication, réalisation, JdT II 1/2023, S. 45 ff.

FAVROD-COUNE PASCAL / BELET KÉVIN, La convention d'arbitrage dans un smart contract, AJP 9/2018, S. 1105 ff.

FELBER TOM, Über 7000 anonyme Drogenverkäufe übers Internet, NZZ vom 27. Mai 2025

Financial Crime Academy, The Stages of Cryptocurrency Laundering: A Comprehensive Overview of the Stages of Cryptolaundering, 2025

Financial Stability Board, The Financial Stability Risks of Decentralised Finance, Basel 2023

FINCK MICHÈLE, Grundlagen und Technologie von Smart Contracts, in: Fries Martin / Paal Boris (Hrsg.), Smart Contracts, Tübingen 2019

FLACHSMANN STEFAN, Fahrlässigkeit und Unterlassung, Diss. Zürich 1992

FLEMISCH FRANK et al., Towards a dynamic balance between humans and automation: authority, ability, responsibility and control in shared and cooperative control situations, in: Cognition, Technology & Work 1/2012, S. 3 ff.

FOERSTER MAX, Automatisierung und Verantwortung im Zivilrecht, ZfPW 4/2019, S. 418 ff.

FOLEY SEAN / KARLSEN JONATHAN R. / PUTNIŅŠ TĀLIS J., Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?, Review of Financial Studies 5/2019, S. 1798 ff.

FORSTER MARC, Der Wirtschaftsalltag als strafrechtsdogmatischer «Hort des Verbrechens»: Zum «zielobjektivierten Beihilfetatbestand» bei sogenannten Alltagsgeschäften und berufstypischen Dienstleistungen, in: Ackermann Jürg-Beat / Donatsch Andreas / Rehberg Jörg (Hrsg.), Wirtschaft und Strafrecht, Festschrift für Niklaus Schmid zum 65. Geburtstag, Zürich 2001 (zit. FORSTER, FS Schmid)

FORSTER MATTHIAS, Die strafrechtliche Verantwortlichkeit des Unternehmens nach Art. 102 StGB, Diss. Bern 2006 (zit. FORSTER, Diss.)

FRANCO PEDRO, Understanding Bitcoin: Cryptography, Engineering, and Economics, Chichester 2015

FRISTER HELMUT, Strafrecht Allgemeiner Teil, 10. Aufl., München 2023

FRITSCH ROBIN / MÜLLER MARINO / WATTENHOFER ROGER, Analyzing Voting Power in Decentralized Governance: Who controls DAOs?, Blockchain: Research and Applications 3/2024, S. 1 ff.

FUCHS STEFAN, Die Steuergeldwäscherei im Schweizer Recht: Darstellung und Würdigung des Bundesgesetzes zur Umsetzung der 2012 revidierten Empfehlungen der GAFI/FATF im Steuerbereich, Diss. St. Gallen, Bern 2017

FURRER ANDREAS, Die Einbettung von Smart Contracts in das schweizerische Vertragsrecht, Anwaltsrevue 3/2018, S. 103 ff.

GABBIADINI ROMINA / GOBBI LORENZO / RUBERA EUGENIO, Money laundering and blockchain technology: can you follow the trail of cryptocurrency transactions?, Questioni di Economia e Finanza 893/2024, S. 1 ff.

GETH CHRISTOPHER, Strafrecht Allgemeiner Teil, 7. Aufl., Basel 2021

GETH CHRISTOPHER / NICOLAS LEU, Gehilfenschaft durch berufsbedingtes Handeln bei vertragswidrigem Verhalten des Haupttäters, in: Jositsch Daniel / Schwarzenegger Christian / Wohlers Wolfgang (Hrsg.), Festschrift für Andreas Donatsch, Zürich 2017, S. 29 ff.

GERMANN SANDRO / WICKI-BIRCHLER DAVID, Hacking und Hacker im Schweizer Recht, AJP 1/2020, S. 83 ff.

GIANNINI MARIO, Anwaltliche Tätigkeit und Geldwäscherei, Zur Anwendbarkeit des Geldwäschereitatbestandes (Art. 305bis StGB) und des Geldwäschereigesetzes (GwG) auf Rechtsanwälte, Diss. Zürich 2005

GLARNER ANDREAS / MEYER STEPHAN, Smart Contracts in Escrow-Verhältnissen, Jusletter vom 4. Dezember 2017

GLESS SABINE, Internationales Strafrecht, 3. Aufl., Basel 2021

GLESS SABINE / BACHMANN LEA, § 21 Internationales Strafrecht, in: Zellweger-Gutknecht Corinne / Tschudi Dominik / MacCabe Kevin P. (Hrsg.), Kryptowerte, Basel 2024, N 21.01 ff.

GLESS SABINE / SILVERMAN EMILY / WEIGEND THOMAS, If Robots cause harm, Who is to blame? Self-driving Cars and Criminal Liability, New Criminal Law Review 3/2016, S. 412 ff.

GLESS SABINE / WEIGEND THOMAS, Intelligente Agenten und das Strafrecht, ZStW 3/2014, S. 561 ff.

GODENZI GUNHILD, Strafbare Beteiligung am kriminellen Kollektiv, Eine Explikation von Zurechnungsstrukturen der Banden-, Organisations- und Vereinigungsdelikte, Bern 2015

GOGEL DAVID et al.
- World Economic Forum, Decentralized Autonomous Organization Toolkit, Insight Report, 2023 (zit. GOGEL et al., Toolkit)
- World Economic Forum, Decentralized Autonomous Organizations: Beyond the Hype, White Paper, 2022 (zit. GOGEL et al., DAO)
- World Economic Forum, DeFi Beyond the Hype, Wharton Blockchain and Digital Asset Project, University of Pennsylvania, 2021 (zit. GOGEL et al., DeFi)

GOGOL KRZYSZTOF et al., Liquid Staking Tokens in Automated Market Makers, 2024

GÖHSL JAN-FREDERICK / ZIMMER DANIEL, VO (EU) 2022/1925 Art. 2, in: Immenga Ulrich / Mestmäcker Ernst-Joachim (Hrsg.), Wettbewerbsrecht, Bd. 1, 7. Aufl., München 2025

GORDON CLARA-ANN / LUTZ TANJA, Haftung für automatisierte Entscheidungen – Herausforderungen in der Praxis, SZW 1/2020, S. 53 ff.

GRABER CHRISTOPH, Geldwäscherei: Ein Kommentar zu Art. 305bis und 305ter StGB, Diss. Bern 1989, Bern 1990

GRAF DAMIAN (Hrsg.), StGB, Annotierter Kommentar, 2. Aufl., Bern 2025 (zit. AK StGB-BEARBEITERIN)

GRAF DAMIAN, Zurechnung von Unternehmensbussen, GesKR 3/2015, S. 356 ff.

GRAVEN PHILIPPE / STRÄULI BERNHARD, L'infraction pénale punissable, 2. Aufl., Bern 1995

GRECO LUÌS, Strafbarkeit des Unterhaltens einer Handels- und Diskussionsplattform insbesondere im sog. Darknet, ZIS 9/2019, S. 435 ff.

GRUBMILLER PETER, Unterlassen im Strafrecht, Eine vergleichende Darstellung der gesetzlichen Regelungen in der Schweiz und in Deutschland, Diss. Zürich 2010, Zürich 2011

GRZYWOTZ JOHANNA / KÖHLER OLAF M. / RÜCKERT CHRISTIAN, Cybercrime mit Bitcoins, Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention, StV 11/2016, S. 753 ff.

GUILLAUME FLORENCE, L'effet disruptif des smart contracts et des DAOs sur le droit international privé, in: Richa Alexandre / Canapa Damiano (Hrsg.), Droit et économie numérique, Bern 2021, S. 35 ff.

GUILLAUME FLORENCE / RIVA SVEN, DAO, code et loi: le régime technologique et juridique de la decentralized autonomous organization, Revue de droit d'Assas 4/2021, S. 206 ff.

GYARMATI NIKOLAUS, Phänomen Cybercrime und seine Bekämpfung, SKZ 2/2019, S. 86 ff.

GYR ELEONOR
- Blockchain und Smart Contracts, Die vertragsrechtlichen Implikationen einer neuen Technologie, Diss. Basel 2019 (zit. GYR, Smart Contracts)
- Dezentrale Autonome Organisation DAO, Jusletter vom 4. Dezember 2017 (zit. GYR, DAO)

HAAS JANICK, Zur Notwendigkeit und Umsetzung einer eigenständigen Strafbarkeit des Betreibens von digitalen Handelsplattformen, Eine kritische Analyse von § 127 StGB n. F. im Lichte des Vorbereitungsstrafrechts, Diss. Marburg 2023, Berlin 2024

HABERBECK PHILIPP H., Von der Kryptohandelsplattform unrechtmässig verwertete Kryptowährungen, AJP 3/2023, S. 312 ff.

HÄFELIN ULRICH / MÜLLER GEORG / UHLMANN FELIX, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich / St. Gallen 2020

HANDSCHIN LUKAS / CHOU HAN-LIN, Zürcher Kommentar, Kommentar zum schweizerischen Zivilrecht, Teilband V/4b, Die Kollektivgesesellschaft, Die Kommanditgesellschaft, Art. 552-619 OR, 4. Aufl., Zürich 2009 (zit. ZK OR-HANDSCHIN/CHOU)

HANDSCHIN LUKAS / VONZUN RETO, Zürcher Kommentar, Kommentar zum schweizerischen Zivilrecht, Teilband V/4a, Die einfache Gesellschaft, Art. 530–551 OR, 4. Aufl., Zürich 2009 (zit. ZK OR-HANDSCHIN/VONZUN)

HASSAN SAMER / DE FILIPPI PRIMAVERA, Decentralized Autonomous Organization, Internet Policy Review 2/2021, S. 1 ff.

HASSEMER WINFRIED, Professionelle Adäquanz. Bankentypisches Verhalten und Beihilfe zur Steuerhinterziehung, Wistra 1995, S. 41 ff.

HAUSER-SPÜHLER GABRIELA, Innovation vs. Regulation Compliance im Digital-Finance-Bereich, Zürich 2017

HECKELMANN MARTIN, Zulässigkeit und Handhabung von Smart Contracts, NJW 8/2018, S. 504 ff.

HEIERLI MARCUS, Zivilrechtliche Haftung für Geldwäscherei, Diss. Zürich 2012

HEIMGARTNER STEFAN, Die internationale Dimension von Internetstraffällen – Strafhoheit und internationale Rechtshilfe in Strafsachen, in: Schwarzenegger Christian / Arter Oliver / Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 117 ff.

HEIN CATHRIN / WELLBROCK WANJA / HEIN CHRISTOPH, Rechtliche Herausforderungen von Blockchain-Anwendungen, 2. Aufl., Wiesbaden 2023

HEINE GÜNTER / TRUNIGER PHILIPP, Die strafrechtliche Verantwortlichkeit des Konzertveranstalters, ZStrR 1/2010, S. 83 ff.

HEINIGER MATTHIAS, Der Konzern im Unternehmensstrafrecht gemäss Art. 102 StGB, Die strafrechtliche Erfassung eines wirtschaftlichen Phänomens, Diss. Bern 2010, Bern 2011

HERREN NICOLAS, Le blanchiment d'argent dans la jurisprudence des tribunaux fédéraux, AJP 9/2017, S. 1112 ff.

HESS MARTIN / LIENHARD STEPHANIE, Übertragung von Vermögenswerten auf der Blockchain, Darstellung der technischen Grundlagen und der Übertragungsformen de lege lata et ferenda, Jusletter vom 4. Dezember 2017

HILGENDORF ERIC, Können Roboter schuldhaft handeln?, in: Beck Susanne (Hrsg.), Jenseits von Mensch und Maschine, Baden-Baden 2012, S. 119 ff.

HSU PETER / FLÜHMANN DANIEL (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021 (zit. BSK GwG-BEARBEITERIN)

HUMBEL CLAUDE, Decentralized Finance, A new frontier of global financial markets regulation, GesKR 1/2022, S. 9 ff.

HUMBEL CLAUDE / ECKERT FABRICE, Decentralized Exchanges: Grundlagen, Risiken und ausgewählte aufsichtsrechtliche Aspekte, SZW 1/2023, S. 10 ff.

HURTADO POZO JOSÉ / GODEL THIERRY, Droit pénal général, 4. Aufl., Zürich 2023

HUWILER SIMON, Die berüchtigte Hackergruppe Lockbit attackiert die Schweiz und erbeutet Millionen. Jetzt zeigt ein Leak, wie sie arbeiten, NZZ vom 30. Mai 2025

IKEMEYER RAPHAEL / KRIMPHOVE DIETER, Geldwäsche: Tatbestände, Aufgriffsmöglichkeiten, Indizien im Zahlungs- und Kapitalmarkt, Compliance Berater 11/2022, S. 432 ff.

IVANOV NIKOLAY / GUO HANQING / YAN QIBEN, Rectifying Administrated ERC-20 Tokens, 2021

JACCARD MICHEL / TORAL MEHMET, Smart contracts – de la théorie à la pratique, in: Richa Alexandre / Canapa Damiano (Hrsg.), Droit et économie numérique, Bern 2021, S. 1 ff.

JACQUEMART NICOLAS, Offene Blockchainsysteme und die Schutzziele des schweizerischen Finanzmarktrechts, Unter Berücksichtigung möglicher Ansatzpunkte einer Regulierung, Diss. Zürich 2020

JAKOBS GÜNTHER, Strafrechtliche Haftung durch Mitwirkung an Abstimmungen, in: Kühne Hans-Heiner (Hrsg.), Festschrift für Koichi Miyazawa, Dem Wegbereiter des japanisch-deutschen Strafrechtsdiskurses, S. 419 ff.

JEANNERET YVES, La responsabilité pénale de l'entreprise et le droit de la circulation routière, AJP 8/2004, S. 917 ff.

JESCHECK HANS-HEINRICH / WEIGEND THOMAS, Lehrbuch des Strafrechts, Allgemeiner Teil, 5. Aufl., Berlin 1996

JIMENEZ ALISON, 3 Misconceptions about Cryptocurrency Crime Estimates, 2022

JOSITSCH DANIEL / VON ROTZ MADELEINE, Das Finanzmarktstrafrecht der Schweiz – Status quo unter Einbezug der neusten Gesetzesänderungen, des internationalen Einflusses sowie der anstehenden Neuerungen, SZW 6/2016, S. 592 ff.

JUTZI THOMAS / ABBÜHL ANDRI, Fintech und DLT, Privat- und finanzmarktrechtliche Grundlagen in der Schweiz, Bern 2023

KAUFMANN ARMIN, Die Dogmatik der Unterlassungsdelikte, 2. Aufl., Göttingen 1988

KAULARTZ MARKUS / HECKMANN JÖRN, Smart Contracts – Anwendungen der Blockchain-Technologie, Computer und Recht 9/2016, S. 618 ff.

KERN MARTIN
- Anwaltliche Tätigkeit und Geldwäschereibekämpfung, Anwaltsrevue 2/2022, S. 81 ff. (zit. KERN, Geldwäschereibekämpfung)
- Geldwäschereirisiken im Kunsthandel, SJZ 8/2021, S. 375 ff. (zit. KERN, Kunsthandel)

KILLIAS MARTIN / KUHN ANDRÉ / DONGOIS NATHALIE, Précis de droit pénal général, 4. Aufl., Bern 2016

KIPKER DENNIS-KENJI et al. Rechtliche und technische Rahmenbedingungen der «Smart Contracts», Eine zivilrechtliche Betrachtung, MMR 8/2020, S. 509 ff.

KLAAS ARNE, Geldwäsche und dezentrale autonome Organisationen (DAO), Wer wird verpflichtet und wer kann Adressat aufsichtsbehördlicher Maßnahmen werden?, BKR 3/2023, S. 162 ff.

KMIELIAUSKAS LINAS, Lagging in illicit stablecoin freezing helps criminals launder funds, 2025

KRAMER STEFAN / MEIER URS, Tokenisierung von Finanzinstrumenten, GesKR 1/2020, S. 60 ff.

KRAMER STEFAN / WYSS STEFAN, Verwahrung von digitalen Aktiven, in: Weber Rolf / Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, S. 145 ff.

KRONENBERG SABRINA, Der Bandenbegriff im schweizerischen Strafrecht, forumpoenale 1/2011, S. 50 ff.

KUHN HANS, Taxonomie, in: Weber Rolf / Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, S. 35 ff.

KUNZ MICHAEL, Die strafrechtliche Garantenstellung von Bankorganen bei der Geldwäscherei, Jusletter vom 14. Februar 2011

KUNZ PETER V. / JUTZI THOMAS / SCHÄREN SIMON (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz (GwG), Bern 2017 (zit. SHK GwG-BEARBEITERIN)

LAGISTORFER RENÉ / GÜDEL BENJAMIN, «Jetzt fahren wir zur Bank»: Krypto-Betrüger lassen in Zürich Zehntausende Franken verschwinden, Tagesanzeiger vom 23. April 2025

LEE SUNG-SHINE et al., Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks, 2022

LEHMANN MATTHIAS, Zivilrecht, in: Omlor Sebastian / Link Mathias (Hrsg.), Kryptowährungen und Token, 3. Aufl., Frankfurt am Main 2026, S. 177 ff.

LENGAUER DANIEL / RUCKSTUHL LEA, Compliance, Zürich 2017

LI LI / WU JIAHAO / CUI WEI, A review of blockchain cross-chain technology, IET Blockchain 3/2023, S. 149 ff.

LOH JANINA
- Maschinenethik und Roboterethik, in: Oliver Bendel (Hrsg.), Handbuch Maschinenethik, Wiesbaden 2019, S. 75 ff. (zit. LOH, Ethik)
- Verantwortung und Roboterethik – ein kleiner Überblick – Teil 2, InTeR 1/2018, S. 29 ff. (zit. LOH, Roboterethik)

LOH WULF / LOH JANINA, Autonomy and Responsibility in Hybrid Systems: The Example of Autonomous Cars, in: Lin Patrick / Abney Keith / Jenkins Ryan (Hrsg.), Robot Ethics 2.0, From Autonomous Cars to Artificial Intelligence, Oxford 2017, S. 35 ff.

LOHMANN ANNA, Strafrecht im Zeitalter von Künstlicher Intelligenz, Der Einfluss von autonomen Systemen und KI auf die tradierten strafrechtlichen Verantwortungsstrukturen, Diss. Würzburg, Baden-Baden 2021 (zit. LOHMANN, KI)

LOHMANN MELINDA FLORINA, Wissen, Wille und Erklärungen von Maschinen, Zürich / St. Gallen 2024 (zit. LOHMANN, Maschinenerklärung)

LUCHSINGER ROLAND / PORTMANN MATTHIAS, Geldwäscherei-Risiken, SZW 1/2025, S. 40 ff.

LUTHIGER RETO, Geldwäschereibekämpfung bei Investmentgesellschaften, Die Anteilsbeziehung im GwG, Diss. St. Gallen, Zürich 2017

MACALUSO ALAIN, La responsabilité pénale des personnes morales et de l'entreprise: éléments de droit comparé et étude des articles 100quater et 100quinquies CPS, Diss. Lausanne 2004

MACALUSO ALAIN / GARBARSKI ANDREW, Communication de soupçons de blanchiment après la fin de la relation d'affaires, AJP 10/2016, S. 1318 ff.

MACALUSO ALAIN / MOREILLON LAURENT / QUELOZ NICOLAS (Hrsg.), Commentaire Romand, Code pénal II, Art. 111-392 CP, Art. 154 et 155 LIMF, Basel 2025 (zit. CR CP II-BEARBEITERIN)

MANTZ RETO, Open Source Software, in: Taeger Jürgen / Pohle Jan (Hrsg.), Computerrechts-Handbuch, 40. Aufl., München 2025

MARKWALDER NORA / SIMMLER MONIKA, Roboterstrafrecht, AJP 2/2017, S. 171 ff.

MARRINAN PAUL, Crypto-crime & caveats, 2021

MATSUOKA DAREN / HACKETT ROBERT / LAZZARIN EDDY, State of Crypto Report 2024: New data on swing states, stablecoins, AI, builder energy, and more, 2024

MAUCHLE YVES
- Die Registrierungsvereinbarung – insbesondere bei tokenisierten Forderungsrechten, SZW 6/2023, S. 683 ff. (zit. MAUCHLE, Registrierungsvereinbarung)
- Die regulatorische Antwort auf Fintech: Evolution oder Revolution? Eine Verortung aktueller Entwicklungen, SZW 6/2017, S. 810 ff. (zit. MAUCHLE, Fintech)

MAURENBRECHER BENEDIKT / LEISINGER BENJAMIN
– Decentralized Finance (Teil 2), SJZ 14/2022, S. 704 ff. (zit. MAURENBRECHER/LEISINGER, Teil 2)
– Decentralized Finance (Teil 1), SJZ 13/2022, S. 647 ff. (zit. MAURENBRECHER/LEISINGER, Teil 1)

MEIER-HAYOZ ARTHUR / FORSTMOSTER PETER / SETHE ROLF, Schweizerisches Gesellschaftsrecht, 13. Aufl., Bern 2023

MEIRICH DAVID, Regulatorische Einordnung von Decentralized Finance, Diss. Zürich 2023

MEISSER LUZIUS, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Weber Rolf / Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich/Basel/Genf 2015, S. 74 ff.

MELE VALENTINA / PETERS RENA, Entscheidbesprechung zu BGer, StA, 6B_1437/2020 vom 22. September 2021 (zur Publikation vorgesehen), A. gegen Staatsanwaltschaft des Kantons Basel-Landschaft und B., Vergewaltigung und sexuelle Nötigung, Täterschaft und Teilnahme, AJP 4/2022, S. 384 ff.

MEYER STEPHAN
– Dezentrale autonome Organisationen (DAOs) und das Gesellschaftsrecht der Zukunft, AJP 3/2023 (zit. MEYER, DAO)
– Rechte an und aus Blockchain-basierten Crypto Tokens, Diss. Zürich 2022 (zit. MEYER, Token)

MEYER STEPHAN / SCHUPPLI BENEDIKT, «Smart Contracts» und deren Einordnung in das schweizerische Vertragsrecht, recht 3/2017, S. 204 ff.

MIENERT BIYAN, Dezentrale autonome Organisationen (DAOs) und Gesellschaftsrecht, Zum Spannungsverhältnis Blockchain-basierter und juristischer Regeln, Diss. Marburg 2021, Tübingen 2022

MIGNON VINCENT, Blockchains – perspectives and challenges, in: Kraus Daniel / Obrist Thierry / Hari Olivier (Hrsg.), Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law, Cheltenham 2019, S. 1 ff.

MÖCKLI ALEKSANDRA / REBER MARTINA, Bankhaftung bei pflichtwidriger externer Vermögensverwaltung, recht 3/2023, S. 152 ff.

MOLO GIOVANNI / BRUNONE MATTEO, Kryptowährungen im Visier der staatlichen Kontrolle, sic! 7-8/2022, S. 299 ff.

MOLO GIOVANNI / DRZALIC JANA, Können Kryptowährungen compliant sein?, AJP 1/2019, S. 40 ff.

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/Genf 2022

MOOS REINHARD, Objektive Zurechnung und sozialadäquates Verhalten bei wertneutraler Gehilfenschaft, in: Donatsch Andreas / Forster Marc / Schwarzenegger Christian (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag, S. 477 ff.

MOREILLON LAURENT, L'infraction par omission: étude des infractions à la vie et à l'intégrité corporelle en droits anglais, français, allemand et suisse, Genf 1993

MOREILLON LAURENT et al. (Hrsg.), Commentaire Romand, Code pénal I, Art. 1-110 CP, 2. Aufl., Basel 2021 (zit. CR CP I-BEARBEITERIN)

MÜLLER CHRISTOPH
- Die Smart Contracts aus Sicht des Schweizerischen Obligationenrechts, ZBJV 5/2019, S. 330 ff. (zit. MÜLLER, Smart Contracts)
- Berner Kommentar zum schweizerischen Privatrecht, Obligationenrecht, Allgemeine Bestimmungen, Art. 1-18 OR mit allgemeiner Einleitung in das Schweizerische Obligationenrecht, Bern 2018 (zit. BK OR-MÜLLER)

MÜLLER JÜRG, Initial Coin Offering: Regeln durchforsten, nicht aufforsten, NZZ vom 19. Juni 2018 (zit. MÜLLER, Initial Coin Offering)

MÜLLER LUKAS / SEILER RETO, Smart Contracts aus Sicht des Vertragsrechts, AJP 3/2019, S. 317 ff.

MÜLLER VAÏK, Les règles de conduite sur le marché à l'épreuve de la Market Extractable Value, GesKR 1/2025, S. 96 ff. (zit. MÜLLER, Règles)

MÜLLER-HENGSTENBERG CLAUS / KIRN STEFAN, Rechtliche Risiken autonomer und vernetzter Systeme, Eine Herausforderung, Berlin/Boston 2016

MÜNCH FLORIAN, Autonome Systeme im Krankenhaus, Datenschutzrechtlicher Rahmen und strafrechtliche Grenzen, Diss. Würzburg 2016, Baden-Baden 2017

MURPHY HANNAH, Monero emerges as crypto of choice for cybercriminals, Financial Times vom 21. Juni 2021

MUSKENS LOUIS FRÉDÉRIC / NIGGLI MARCEL A., Geldwäscherei durch Unterlassen, Grenzen des unechten Unterlassungsdelikts am Beispiel der Geldwäscherei, zugleich eine Kritik von BGE 136 IV 188, ContraLegem 1/2019, S. 16 ff.

NADELHOFER DO CANTO SIMONE, Geldwäscherei und Einziehung – Risiken für Anwälte, SJZ 15/2006, S. 345 ff.

NADLER MATHIAS / SCHÄR FABIAN
- Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers, Federal Reserve Bank of St. Louis Review 2023, S. 122 ff. (zit. NADLER/SCHÄR, Tornado Cash)
- Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution, Journal of Blockchain Research 1/2022, S. 29 ff. (zit. NADLER/SCHÄR, Decentralized Finance)

NAGEL THOMAS
- Dienstleistungen für den Zahlungsverkehr unter dem Geldwäschereigesetz, GesKR 2023, S. 72 ff. (zit. NAGEL, Zahlungsverkehr)
- Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes (GwG), Diss. Zürich 2019, Zürich 2020 (zit. NAGEL, Diss.)

NAKAMOTO SATOSHI, Bitcoin: A Peer-to-Peer Electronic Cash System, 2018

NIEDERNHUBER TANJA, Blockchain und Kryptowerte im Strafrecht, in: Wabnitz Heinz / Janovsky Thomas / Schmitt Lothar (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, 6. Aufl., München 2025, § 16 N 1 ff.

NIGGLI MARCEL A. / WIPRÄCHTIGER HANS (Hrsg.)
- Basler Kommentar, Strafrecht I, Art. 1-136, Jugendstrafgesetz, 4. Aufl., Basel 2019 (zit. BSK StGB I-BEARBEITERIN)
- Basler Kommentar, Strafrecht II, Art. 137-392, 4. Aufl., Basel 2019 (zit. BSK StGB II-BEARBEITERIN)
- Basler Kommentar, Strafrecht I, Art. 1-110, Jugendstrafgesetz, 2. Aufl., Basel 2007 (zit. aBSK StGB I-BEARBEITERIN)

NOSER SAMUEL / INFANGER SVEN / LÜDI YANICK, § 12 Decentralized Finance, in: Zellweger-Gutknecht Corinne / Tschudi Dominik / MacCabe Kevin P. (Hrsg.), Kryptowerte, Basel 2024, N 18.01 ff.

NYDEGGER MICHA, Zurechnungsfragen der Anstiftung im System strafbarer Beteiligung, Diss. Luzern, Zürich 2012

OSWALD DOMINIK, Erlös aus Kryptowährungen, Ein unterschätztes Geldwäscherei-Risiko der Banken, Zürich 2021

OU WEI et al., An overview on cross-chain: Mechanism, platforms, challenges and advances, Computer Networks 2022, S. 1 ff.

PAJAROLA UMBERTO, Bekämpfung von Terrorismus und Organisierter Kriminalität, Zürich 2022

PAKKI JASWANT et al., Everything You Ever Wanted to Know About Bitcoin Mixers (But Were Afraid to Ask), 2020

PALLADINO SANTIAGO, The State of Smart Contract Upgrades, 2020

PARASURAMAN RAJA / SHERIDAN THOMAS / WICKENS CHRISTOPHER, A model for types and levels of human interaction with automation, IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans 3/2000, S. 286 ff.

PASQUIER BRUNO / BÄRTSCHI HARALD, Dezentrale autonome Organisationen für Immobilien, GesKR 2/2024, S. 200 ff.

PETERS GARETH / PANAYI EFSTATHIOS, Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, in: Tasca Paolo et al. (Hrsg.), Banking Beyond Banks and Money, Cham 2016, S. 239 ff.

PODSZUN RUPPRECHT (Hrsg.), Digital Markets Act, Gesetz über digitale Märkte, Handkommentar, Baden-Baden 2023 (zit. DMA-BEARBEITERIN)

REDMANN-WIPPEL CARMEN / STADLER MICHAEL, Decentralised Finance – a growing but grey area, 2015

REGGIANI LISA, Kryptomixer im Lichte des Geldwäschereitatbestandes nach Art. 305bis StGB, in Bayana Serdar et al. (Hrsg.), Recht und Realität, Zürich 2025, S. 111 ff.

REINLE MICHAEL, Die Meldepflicht im Geldwäschereigesetz, Diss. St. Gallen, Zürich 2007

REMUND CÉDRIC / MEIER FRANÇOIS, Marktmissbrauch auf Kryptomärkten (Teil 1), SJZ 7/2025, S. 339 ff.

RIEDO CHRISTOF, Kausalität im Strafrecht, Von ruchlosen Erben und zuckenden Blitzen oder Verursachung durch aktives Tun, Zürich/Genf 2025

RIKLIN FRANZ
- Schweizerisches Strafrecht, Allgemeiner Teil I, Verbrechenslehre, 3. Aufl., Zürich 2007 (zit. RIKLIN, AT I)
- Mailbox-Betreiber wegen Pornographie verurteilt, medialex 2/1999, S. 106 ff. (zit. RIKLIN, Mailbox)

RIMLE ALOIS, Recht des schweizerischen Finanzmarktes, Zürich 2004

RIVA SVEN, Decentralized Autonomous Organizations (DAOs) in the Swiss Legal Order, in: Bonomi Andrea / Romano Gian Paolo (Hrsg.), Yearbook of Private International Law, Vol. XXI, Köln 2021, S. 601 ff.

ROHR ANDREAS, Bin ich Finanzintermediär?, Ein Handbuch zur Auslegung von Art. 2 Abs. 3 GwG, Bern 2004

RONC PASCAL / SCHUPPLI BENEDIKT, Kryptowährungen im Lichte der schweizerischen Geldwäschereigesetzgebung, forumpoenale 6/2018, S. 529 ff.

ROSENTHAL DAVID, Internet-Provider-Haftung – ein Sonderfall?, in: Jung Peter (Hrsg.), Aktuelle Entwicklungen im Haftungsrecht, Referate der Tagung Recht aktuell 2006 der Juristischen Fakultät der Universität Basel, Zürich/Basel/Genf 2007, S. 147 ff.

ROTH MONIKA
- Compliance: Verantwortung und Verantwortlichkeit von Bankmitarbeitenden, recht 3/2022, S. 119 ff. (zit. ROTH, Compliance)
- Geldwäscherei im Kunsthandel, Kunst & Recht 2014, S. 43 ff. (zit. ROTH, Kunsthandel)

ROXIN CLAUS, Was ist Beihilfe?, in: Kühne Hans-Heiner (Hrsg.), Festschrift für Koichi Miyazawa. Dem Wegbereiter des japanisch-deutschen Strafrechtsdiskurses, Baden-Baden 1995, S. 501 ff.

RUTISHAUSER DANIEL / KUBLI RALF / WEBER ROLF, Grundlagen, in: Weber Rolf / Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, S. 9 ff.

RYSER ROLAND M., Outsourcing – eine unternehmensstrafrechtliche Untersuchung, Diss. St. Gallen, Zürich 2007

SAFFERLING CHRISTOPH / RÜCKERT CHRISTIAN, Das Strafrecht und die Underground Economy, Analysen & Argumente 2019, S. 1 ff.

SALEHI MEHDI / CLARK JEREMY / MANNAN MOHAMMAD, Not so immutable: Upgradeability of Smart Contracts on Ethereum, 2022

SARTOR GIOVANNI / OMICINI ANDREA, The autonomy of technological systems and responsibilities for their use, in: Bhuta Nehal et al. (Hrsg.), Autonomous Weapons Systems, Law, Ethics, Policy, Cambridge 2016, S. 39 ff.

SCHÄR FABIAN, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis Review 2021, S. 153 ff.

SCHÄRLI PATRICK, § 9 Finanzmarktrechtliche Kategorisierung von Kryptowerten, in: Zellweger-Gutknecht Corinne / Tschudi Dominik / MacCabe Kevin P. (Hrsg.), Kryptowerte, Basel 2024, N 9.01 ff.

SCHLATT VINCENT et al., Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth 2016

SCHMID NIKLAUS, Aspekte der Strafbarkeit des Unternehmens nach dem neuen Allgemeinen Teil des Schweizerischen Strafgesetzbuches, in: von der Crone Hans Caspar et al. (Hrsg.), Festschrift für Peter Forstmoser zum 60. Geburtstag, Zürich 2003, S. 761 ff.

SCHÖNKNECHT FLORIAN
- Vorabklärungen im FINMA-Enforcement, in Zulauf Urs / Wyss David (Hrsg.), Finanzmarktenforcement, 3. Aufl., Bern 2022, S. 65 ff. (zit. SCHÖNKNECHT, Vorabklärungen)
- Der Einlagebegriff nach Bankengesetz, GesKR 3/2016, S. 300 ff. (zit. SCHÖNKNECHT, Einlagebegriff)

SCHUBARTH MARTIN, Dolus eventualis – positive und negative Indikatoren; Analyse der Rechtsprechung des Bundesgerichtes von 1943-2007, AJP 5/2008, S. 519 ff.

SCHULER KATRIN / CLOOTS ANN SOFIE / SCHÄR FABIAN, On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance, Journal of Financial Regulation 2/2024, S. 213 ff.

SCHWARZENEGGER CHRISTIAN, Der räumliche Geltungsbereich des Strafrechts im Internet, Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 2/2000, S. 109 ff.

SEHER GERHARD, Intelligente Agenten als «Personen» im Strafrecht?, in: Gless Sabine / Seelmann Kurt (Hrsg.), Intelligente Agenten und das Recht, Baden-Baden 2016, S. 45 ff.

SEIFFERT RINO, Berner Kommentar, Kommentar zum schweizerischen Privatrecht, Obligationenrecht, Die Geschäftsfirmen, Art. 944-956 OR, Bern 2017 (zit. BK OR-SEIFFERT)

SETHE ROLF et al. (Hrsg.), Schulthess Kommentar, Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG, Zürich 2017 (SK FinfraG-BEARBEITERIN)

SIDORENKO ELINA L., Legalization of criminal income using DeFi: typical schemes and risk indicators, Russian Journal of Economics and Law 4/2023, S. 822 ff.

SIEBER ULRICH, Teil 19 Strafrecht und Strafprozessrecht, in: Hoeren Thomas / Sieber Ulrich / Holznagel Bernd (Hrsg.), Handbuch Multimedia-Recht, 62. Aufl., München 2024

SIEGEL DIRK, Technische Grundlagen in: Omlor Sebastian / Link Mathias (Hrsg.), Kryptowährungen und Token, 3. Aufl., Frankfurt am Main 2026, S. 72 ff.

SIMMLER MONIKA, Strafrechtliche Verantwortung beim Zusammenwirken von Mensch und Maschine, Basel 2025

SIMMLER MONIKA / FRISCHKNECHT RUTH, A taxonomy of human-machine collaboration: capturing automation and technical autonomy, in: AI & Society 1/2021, S. 239 ff.

SIMMLER MONIKA / SELMAN SINE / BURGERMEISTER DANIEL, Beschlagnahme von Kryptowährungen im Strafverfahren, AJP 8/2018, S. 963 ff.

SIMMLER MONIKA / WEDER REGINA / FRISCHKNECHT RUTH, Rechtliche Verfahren als sozio-technische Systeme, Eine Taxonomie des Zusammenwirkens von Mensch und Maschine in der Rechtsanwendung, in: Simmler Monika (Hrsg.), Smart Criminal Justice, Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege, Basel 2021, S. 81 ff.

SOSNITZA OLAF, Das Internet der Dinge – Herausforderungen oder gewohntes Terrain für das Zivilrecht?, Computer und Recht 11/2016, S. 764 ff.

SPECHT LOUISA / HEROLD SOPHIE, Roboter als Vertragspartner?, MMR 2018, S. 40 ff.

SPECOGNA RHEA, Codebasiertes Regelsystem, Diss. Zürich 2022, Zürich 2023

STALLINGS WILLIAM Network Security Essentials: Applications and Standards, 4. Aufl., Upper Saddle River 2003

STENGEL CORNELIA / AUS DER AU ROMAN, Blockchain: Eine Technologie für effektiven Datenschutz?, sic! 9/2018, S. 439 ff.

STENGEL CORNELIA / BIANCHI LUCA, Geldwäscherei und Terrorismusfinanzierung, in: Weber Rolf / Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, S. 223 ff.

STENGEL CORNELIA / RUCKSTUHL LEA, 3. Teil: Regulatorische Themen / 2. Kapitel: Finanzmarktrecht Schweiz / III. Geldwäschereigesetzgebung, in: Stengel Cornelia / Weber Thomas (Hrsg.), Digitale und mobile Zahlungssysteme, Kredit- und Debitkarten, Wallets, virtuelle Währungen und Kryptowerte, 2. Aufl., Zürich 2024

STENGEL CORNELIA / PAYDAR RAMIN, § 18 Geldwäscherei- und Terrorismusbekämpfung, in: Zellweger-Gutknecht Corinne / Tschudi Dominik / MacCabe Kevin P. (Hrsg.), Kryptowerte, Basel 2024, N 18.01 ff.

STILLER BURKHARD / RODRIGUES BRUNO / NEZHADSISTANI NASIM, § 2 Technische Grundlagen der Blockchains, in: Zellweger-Gutknecht Corinne / Tschudi Dominik / MacCabe Kevin P. (Hrsg.), Kryptowerte, Basel 2024, N 2.01 ff.

STRASSER OTHMAR, Aufsichts- und verwaltungsstrafrechtliche Verantwortlichkeit bei Gremienentscheidungen in der Geldwäschereibekämpfung von Banken, SJZ 118/2022, S. 691 ff.

STRATENWERTH GÜNTHER / BOMMER FELIX
- Schweizerisches Strafrecht, Allgemeiner Teil I: Die Straftat, 5. Aufl., Bern 2024 (zit. STRATENWERTH/BOMMER, AT I)
- Schweizerisches Strafrecht, Besonderer Teil I, Straftaten gegen Individualinteressen, 8. Aufl., Bern 2022 (zit. STRATENWERTH/BOMMER, BT I)
- Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 7. Aufl., Bern 2013 (zit. STRATENWERTH/BOMMER, BT II)

STÜRMER JONAS, Kryptowerte als Tatertrag, Tatmittel, Tatobjekt und Tatprodukt, ZVglRWiss 3/2023, S. 289 ff.

SUMMERMATTER DANIEL, Kausalität, Ein Handbuch, Bern 2019

SURY URSULA, Digital in Law, 2. Aufl., Bern 2021

SUTER CHRISTOPH / REMUND CÉDRIC, Infractions fiscales, blanchiment et intermédiaires financiers, GesKR 1/2015, S. 54 ff.

SZABO NICK
- Formalizing and Securing Relationships on Public Networks, First Monday Internet Journal 9/1997 (zit. SZABO, Networks)
- Smart Contracts: Building Blocks for Digital Markets, 1996 (zit. SZABO, Blocks)
- Smart Contracts, 1994 (zit. SZABO, Smart Contracts)

TEICHMANN FABIAN, Ransomware-Erpressung: Umgang, Rechtsfragen und Cyberversicherung, ZBJV 9/2025, S. 553 ff.

THELESKLAF DANIEL et al. (Hrsg.), Orell Füssli GwG Kommentar, AMLA Commentary, Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, Swiss Anti-Money Laundering Act with other Laws, 3. Aufl., Zürich 2019 (zit. OFK GwG-BEARBEITERIN)

THOMMEN MARC, Geldwäscherei durch Unterlassen?, in: Jeanneret Yvan / Sträuli Bernhard (Hrsg.), Empreinte d'une pionnière sur le droit pénal, Mélanges en l'honneur d'Ursula Cassani, Zürich 2021, S. 425 ff.

TRECHSEL STEFAN et al., Schweizerisches Strafrecht, Allgemeiner Teil I, Allgemeine Voraussetzungen der Strafbarkeit, 8. Aufl., Zürich 2026

TRECHSEL STEFAN / PIETH MARK / CHRISTOPHER GETH (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 5. Aufl., Zürich 2025 (zit. PK StGB-BEARBEITERIN)

TSCHUDI DOMINIK, § 20 Beschlagnahme und Einziehung von Kryptowerten, in: Zellweger-Gutknecht Corinne / Tschudi Dominik / MacCabe Kevin P. (Hrsg.), Kryptowerte, Basel 2024, N 20.01 ff.

VAGIA MARIALENA / TRANSETH AKSEL / FJERDINGEN SIGURD, A literature review on the levels of automation during the years. What are the different taxonomies that have been proposed?, Applied Ergonomics 2016, S. 190 ff.

VAHRENHOLT DE LUCENA OLIVER, Regulierung von Innovation und Disruption im digitalen Finanzsystem, am Beispiel der brasilianischen FinTech-Regulierung, Zürich / St. Gallen 2024

VAN DEN HOVEN VAN GENDEREN ROBERT, Robot as Legal Entity, Legal Dream or Nightmare?, Jusletter IT vom 23. November 2017

VAN WEGBERG ROLF / OERLEMANS JAN-JAAP/VAN DEVENTER OSKAR, Bitcoin money laundering: mixed results?, An explorative study on money laundering of cybercrime proceeds using bitcoin, Journal of Financial Crime 2/2018, S. 419 ff.

VERMANDE NIC, A Story of Burning Bridges: Fixing Cross-Chain Transfers for Good, 2025

VEST HANS
- «Vom Zufall abhängt»?, AJP 8/2018, S. 945 ff. (zit. VEST, Zufall)
- Anwendungsprobleme im Bereich der Geldwäscherei, SJZ 3/2004, S. 53 ff. (zit. VEST, Geldwäscherei)

VEST HANS et al., StGB AT Kompakt, Ein Lehr- und Lernbuch zum Allgemeinen Teil I des Strafgesetzbuches, 3. Aufl., Bern 2023 (zit. VEST et al., AT)

VILLARD KATIA, La compétence territoriale du juge pénal suisse (art. 3 et 8 CP): réflexions autour d'évolutions récentes, ZStrR 2/2017, S. 145 ff.

VON ROTZ MADELEINE, Die Garantenstellung und die Garantenpflicht des Compliance Officers einer Bank, Diss. Zürich 2019

WAGNER GERHARD / LUYKEN LINA, Haftung für Robo Advice, in: Bachmann Gregor et al. (Hrsg.), Festschrift für Christine Windbichler zum 70. Geburtstag am 8. Dezember 2020, Berlin 2020, S. 155 ff.

WALPORT MARK, Distributed Ledger Technology beyond blockchain, 2015

WATTER ROLF / BAHAR RASHID (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz, Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2018 (zit. BSK FINMAG/FinfraG-BEARBEITERIN)

WATTER ROLF et al. (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013 (zit. BSK BankG-BEARBEITERIN)

WATTER ROLF / VOGT HANS-UELI (Hrsg.), Basler Kommentar, Obligationenrecht II, Art. 530–964l, inkl. Schluss- und Übergangsbestimmungen, 6. Aufl., Basel 2023 (zit. BSK OR II-BEARBEITERIN)

WEBER ALEXA, Die Strafbarkeit von Plattformbetreibern im Darknet, Diss. Würzburg 2021, Baden-Baden 2022 (zit. WEBER, Darknet)

WEBER ROLF
- Neues «Kleid» für Dezentrale Autonome Organisationen?, Jusletter vom 3. Juni 2024 (zit. WEBER, DAO)
- Handel mit digitalen Aktiven, in: Weber Rolf / Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, S. 165 ff. (zit. WEBER, Aktiven)
- Zivilrechtliche Aspekte von Geschäftsabwicklungen auf DLT-Handelsplattformen, SZW 4/2021, S. 450 ff. (zit. WEBER, DLT)
- Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts, Jusletter vom 4. Dezember 2017 (zit. WEBER, Leistungsstörungen)

WELZEL HANS, Das Deutsche Strafrecht, 11. Aufl., Berlin 1969

WERBACH KEVIN (Hrsg.), World Economic Forum, Decentralized Finance (DeFi) Policy-Maker Toolkit, White Paper, 2021 (zit. WEF, DeFi)

WIDMER LÜCHINGER CORINNE, Apps, Algorithmen und Roboter in der Medizin: Haftungsrechtliche Herausforderungen, HAVE 1/2019, S. 3 ff.

WILDHABER ISABELLE / LOHMANN MELINDA FLORINA, Roboterrecht – eine Einleitung, AJP 2/2017, S. 153 ff.

WILKENS ROBERT / FALK RICHARD, Smart Contracts, Grundlagen, Anwendungsfelder und rechtliche Aspekte, Wiesbaden 2019

WIPRÄCHTIGER HANS, Revision des Allgemeinen Teils des StGB, Änderungen im Schatten des Sanktionenrechts, Überblick über diverse kleinere Neuerungen (Art. 1-33, 52-55a, 97-101 und 103-110 nStGB), ZStrR 4/2005, S. 403 ff.

WOHLERS WOLFANG, Gehilfenschaft durch «neutrale» Handlungen – Ausschluss strafrechtlicher Verantwortlichkeit bei alltäglichem bzw. berufstypischem Verhalten?, ZStrR 4/1999, S. 425 ff.

WOHLERS WOLFANG / GODENZI GUNHILD / SCHLEGEL STEPHAN (Hrsg.), Schweizerisches Strafgesetzbuch, Handkommentar, 5. Aufl., Bern 2024 (zit. HK StGB-BEARBEITERIN)

WOHLLEBEN MARCUS, Beihilfe durch äusserlich neutrale Handlungen, Diss. München 1996

WÜST MARLENE, Die Underground Economy des Darknets, Die Strafbarkeit des Betreibens «illegaler» Handelsplattformen, Diss. Nürnberg 2021, Berlin 2022

ZETZSCHE DIRK / ARNER DOUGLAS / BUCKLEY ROSS, Decentralized Finance, Journal of Financial Regulation 6/2020, S. 172 ff.

ZHOU YI et al., Erays: Reverse Engineering Ethereum's Opaque Smart Contracts, Proceedings of the 27th USENIX Security Symposium 2018, S. 1371 ff.

ZIESCHANG FRANK, Zur strafrechtlichen Verantwortlichkeit eines Host-Providers für rechtswidrige Inhalte, GA 2020, S. 57 ff.

ZOGG SAMUEL, Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung, recht 2/2019, S. 95 ff.

ZÖLLER MARK A.
- Die Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet – Der neue § 127 StGB, International Cybersecurity Law Review 2/2021, S. 279 ff. (zit. ZÖLLER, Handelsplattformen)
- Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet, KriPoZ 2/2021, S. 79 ff. (zit. ZÖLLER, Strafbarkeit)

ZYSSET PASCAL / NAGEL THOMAS, Der räumliche Geltungsbereich des Geldwäschereigesetzes, GesKR 2/2018, S. 140 ff.

Materialien und weitere amtliche Publikationen

Schweiz

Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25. Juni 2014 (zit. Bundesrat, Virtuelle Währungen)

Bericht des Bundesrates, Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz, Eine Auslegeordnung mit Fokus auf dem Finanzsektor, Bern 2018 (zit. Bundesrat, DLT)

Botschaft über die Änderung des Schweizerischen Strafgesetzbuches (Gesetzgebung über Geldwäscherei und mangelnde Sorgfalt bei Geldgeschäften) vom 12. Juni 1989, BBl 1989 II 1061 ff. (zit. Botschaft StGB 1989)

Botschaft über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Revision des Einziehungsrechts, Strafbarkeit der kriminellen Organisation, Melderecht des Financiers) vom 30. Juni 1993, BBl 1993 III 277 ff. (zit. Botschaft StGB 1993)

Botschaft zu einem Bundesgesetz über die Börsen und den Effektenhandel (Börsengesetz, BEHG) vom 24. Februar 1993, BBl 1993 I 1369 ff. (zit. Botschaft BEHG 1993)

Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 27. November 2019, BBl 2020 233 ff. (zit. Botschaft DLT)

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

Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21. September 1998, BBl 1999 II 1979 ff. (zit. Botschaft StGB 1998)

Botschaft zur Genehmigung und zur Umsetzung des Übereinkommens des Europarats zur Verhütung des Terrorismus mit dem dazugehörigen Zusatzprotokoll sowie zur Verstärkung des strafrechtlichen Instrumentariums

gegen Terrorismus und organisierte Kriminalität vom 14. September 2018, BBl 2018 6427 ff. (zit. Botschaft organisierte Kriminalität 2018)

Botschaft zur Umsetzung der revidierten Empfehlungen der Groupe d'action financière (GAFI) vom 15. Juni 2007, BBl 2007 6269 ff. (zit. Botschaft GAFI 2007)

Bundesamt für Justiz
- Bericht zur Revision des Allgemeinen Teils und des Dritten Buches des Strafgesetzbuches und zu einem Bundesgesetz über die Jugendstrafrechtspflege, Bern 1993 (zit. Bundesamt für Justiz, Bericht 1993)
- Gutachten zur Frage der strafrechtlichen Verantwortlichkeit von Internet-Access-Providern gemäss Art. 27 und 322bis StGB, 75. Gutachten des Bundesamtes für Justiz vom 24. Dezember 1999, VPB 2000 Nr. 75 S. 820 ff. (zit. Bundesamt für Justiz, Internet)

Bundesrat
- Digital Finance: Handlungsfelder 2022+ vom 2. Februar 2022 (zit. Bundesrat, Digital Finance)
- Weltweit führend, verankert in der Schweiz: Politik für einen zukunftsfähigen Finanzplatz Schweiz vom 4. Dezember 2020 (zit. Bundesrat, Finanzplatz)

Eidgenössische Finanzmarktaufsicht
- FINMA-Aufsichtsmitteilung 08/2023, Staking vom 20. Dezember 2023 (zit. FINMA, Staking)
- Risikomonitor 2022 vom 10. November 2022 (zit. FINMA, Risikomonitor)
- Teilrevision der Geldwäschereiverordnung der FINMA (GwV-FINMA), Erläuterungen, 27. Oktober 2022 (zit. FINMA, Teilrevision)
- Faktenblatt Kryptobasierte Vermögenswerte, 1. Mai 2022 (zit. FINMA, Vermögenswerte)
- Jahresbericht 2021, Bern 2021 (zit. FINMA, Jahresbericht)
- Leitlinien zur Finanzmarktregulierung vom 5. Dezember 2019 (zit. FINMA, Leitlinien)
- Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Ausgabe vom 16. Februar 2018, Ziff. 3.1 ff. (zit. FINMA, Wegleitung)
- Geldwäschereiverordnung-FINMA (GwV-FINMA), Erläuterungsbericht zur Totalrevision der GwV-FINMA, 11. Februar 2015 (zit. FINMA, Erläuterungsbericht)
- Rundschreiben 2011/1, Tätigkeit als Finanzintermediär nach GwG, Ausführungen zur Geldwäschereiverordnung (GwV) vom 20. Oktober 2010, letzte Änderung am 4. November 2020 (zit. FINMA-RS-11/1)

Eidgenössisches Finanzdepartement
- Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Erläuterungsbericht vom 18. Juni 2021 (zit. EFD, Erläuterungen)
- Änderung des Bankengesetzes und der Bankenverordnung (FinTech), Erläuternder Bericht zur Vernehmlassungsvorlage, 1. Februar 2017 (zit. EFD, Vernehmlassungsvorlage)

Eidgenössisches Justiz- und Polizeidepartement
- Eidgenössisches Justiz- und Polizeidepartement, National Risk Assessment (NRA), Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets, 2024 (zit. EJPD, NRA)
- Netzwerk-Kriminalität, Bericht der Expertenkommission «Netzwerkkriminalität», 2003 (zit. EJPD, Netzwerkkriminalität)
- Die strafrechtliche Verantwortung von Internet Service Providern, Positionspapier der Bundespolizei, 2000 (zit. EJPD, Internet)

Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT)
- National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets, 2024 (zit. KGGT, NRA 2024)
- National Risk Assessment (NRA): Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding, 2018 (zit. KGGT, NRA 2018)
- Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz, 2015 (zit. KGGT, 2015)

Meldestelle für Geldwäscherei (MROS), Jahresbericht 2024, 2025 (zit. MROS, Jahresbericht)

International

Bundeskriminalamt Deutschland, Cybercrime, Bundeslagebild 2021, Wiesbaden 2022

Estonian Financial Intelligence Unit, Yearbook 2024, 2025 (zit. FIU Estland)

EU Blockchain Observatory and Forum, Decentralized Finance, 2022 (zit. EUBOF)

Europol, Europol Spotlight, Cryptocurrencies – Tracing the Evolution of Criminal Finances, 2021 (zit. Europol, Spotlight)

Financial Intelligence Unit – the Netherlands
- Annual Review 2023, 2024 (zit. FIU Niederlande, 2023)
- Annual Review 2021, 2022 (zit. FIU Niederlande, 2021)

Financial Intelligence Unit Deutschland
- Jahresbericht 2022, 2023 (zit. FIU Deutschland, 2022)
- Jahresbericht 2021, 2022 (zit. FIU Deutschland, 2021)

Groupe d'action financière
- International Standards on Combating Money Laundering And The Financing of Terrorism & Proliferation, The FATF Recommendations, 2025 (zit. GAFI, Standards)
- Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, 2025 (zit. GAFI, Update)
- FATF Report, Countering Ransomware Financing, 2023 (zit. GAFI, Ransomware)
- Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2021 (zit. GAFI, VASP)
- Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, 2020 (zit. GAFI, Indicators)

Organisation for Economic Co-operation and Development
- Lessons from the crypto winter, DeFi versus CeFi, OECD Business and Finance Policy Papers, 2022 (zit. OECD, Lessons)
- Why Decentralised Finance (DeFi) Matters and the Policy Implications, 2022 (zit. OECD, DeFi)

President's Commission on Organized Crime USA, The Cash Connection: Organized Crime, Financial Institutions and Money Laundering, 1984

Stabsstelle Financial Intelligence Unit (FIU) des Fürstentums Liechtenstein, Jahresbericht 2021, 2022 (zit. FIU Liechtenstein)

United States Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance, 2023

United Nations Office on Drugs and Crime, Money laundering through cryptocurrencies (zit. UNODC)

Abkürzungsverzeichnis

a.M.	anderer Meinung
AB	Amtliches Bulletin
Abs.	Absatz
aBSK	alte Auflage des Basler Kommentars
AG	Kanton Aargau
AGe	Appellationsgericht
AI	Artificial Intelligence
AlG	Bundesgesetz über die Ausländerinnen und Ausländer und über die Integration (Ausländer- und Integrationsgesetz, AIG) vom 16. Dezember 2005 (SR 142.20)
AIR	Applied Innovation Review
AJP	Aktuelle juristische Praxis
AK	Annotierter Kommentar
AMLA	Federal Act on Combating Money Laundering and Terrorist Financing
Art.	Artikel
AT	Allgemeiner Teil
ATF	Arrêts du Tribunal fédéral
Aufl.	Auflage
BankG	Bundesgesetz über die Banken und Sparkassen (Bankengesetz, BankG) vom 8. November 1934 (SR 952.0)
BankV	Verordnung über die Banken und Sparkassen (Bankenverordnung, BankV) vom 30. April 2014 (SR 952.02)
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
Bd.	Band
BE	Kanton Bern
BeckRS	Beck'sche Rechtsprechungssammlung
BEHG	Bundesgesetz über die Börsen und den Effektenhandel (Börsengesetz, BEHG) vom 24. März 1995 (SR 954.1) (ersetzt durch FINIG)
BetmG	Bundesgesetz über die Betäubungsmittel und die psychotropen Stoffe (Betäubungsmittelgesetz, BetmG) vom 3. Oktober 1951 (SR 812.121)
BG	Bezirksgericht
BGE	Entscheidungen des Schweizerischen Bundesgerichts (Amtliche Sammlung)
BGH	Bundesgerichtshof (Deutschland)

BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen (Deutschland)
BK	Berner Kommentar
BKR	Zeitschrift für Bank- und Kapitalmarktrecht
BR	Bundesrat
BS	Kanton Basel-Stadt
BSK	Basler Kommentar
bspw.	beispielsweise
BstGer	Bundesstrafgericht
BT	Besonderer Teil
BVGer	Bundesverwaltungsgericht
bzw.	beziehungsweise
CeFi	Centralized Finance
CHF	Schweizer Franken
CP	Code pénal
CR	Commentaire Romand
DAC	Decentralized Autonomous Corporation
DAO	Dezentrale Autonome Organisation
DApp	Dezentrale Applikation
DeFi	Decentralized Finance
d.h.	das heisst
Diss.	Dissertation
DLT	Distributed Ledger Technology
DMA	Digital Markets Act
E.	Erwägung(en)
EBA	European Banking Authority
EBG	Eisenbahngesetz (EBG) vom 20. Dezember 1957 (SR 742.101)
EFD	Eidgenössisches Finanzdepartement
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EOA	Externally Owned Account
ESMA	European Securities and Markets Authority
ESTV	Eidgenössische Steuerverwaltung
et al.	et alii = und weitere
ETH	Ether
EU	Europäische Union
EUBOF	EU Blockchain Observatory and Forum
EUR	Euro (Währung der Europäischen Wirtschafts- und Währungsunion)
EVM	Ethereum Virtual Machine
f./ff.	folgende

FIDLEG	Bundesgesetz über die Finanzdienstleistungen (Finanzdienstleistungsgesetz, FIDLEG) vom 15. Juni 2018 (SR 950.1)
FinfraG	Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarktinfrastrukturgesetz, FinfraG) vom 19. Juni 2015 (SR 958.1)
FINIG	Bundesgesetz über die Finanzinstitute (Finanzinstitutsgesetz, FINIG) vom 15. Juni 2018 (SR 954.1)
FINMA	Eidgenössische Finanzmarktaufsicht
FINMAG	Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz, FINMAG) vom 22. Juni 2007 (SR 956.1)
FIT	Fraunhofer-Institut für Angewandte Informationstechnik
FIU	Financial Intelligence Unit
FMG	Fernmeldegesetz (FMG) vom 30. April 1997 (SR 784.10)
FR	Kanton Fribourg
FS	Festschrift
FSB	Financial Stability Board
GA	Goltdammer's Archiv für Strafrecht
GAFI (= FATF)	— Groupe d'action financière (= Financial Action Task Force)
GE	Kanton Genf
GesKR	Schweizerische Zeitschrift für Gesellschafts- und Kapitalmarktrecht sowie Umstrukturierungen
gl.M.	gleicher Meinung
GwG	Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG) vom 10. Oktober 1997 (SR 955.0)
GwV	Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereiverordnung, GwV) vom 11. November 2015 (SR 955.01)
GwV-FINMA	Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor (Geldwäschereiverordnung-FINMA, GwV-FINMA) vom 3. Juni 2015 (SR 955.033.0)
HAVE	Haftung und Versicherung
HK	Handkommentar
HRegV	Handelsregisterverordnung (HRegV) vom 17. Oktober 2007 (SR 221.411)
Hrsg.	Herausgeber
ICO	Initial Coin Offering

IEEE	Institute of Electrical and Electronics Engineers
IEO	Initial Exchange Offering
IET	The Institution of Engineering and Technology
InTeR	Zeitschrift für Innovations- und Technikrecht
IOSCO	International Organization of Securities Commissions
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG) vom 20. März 1981 (SR 351.1)
ISG	Bundesgesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG) vom 18. Dezember 2020 (SR 128)
IT	Informationstechnologie
i.V.m.	in Verbindung mit
JdT II	Journal des Tribunaux, Partie II
KAG	Bundesgesetz über die kollektiven Kapitalanlagen (Kollektivanlagengesetz, KAG) vom 23. Juni 2006 (SR 951.31)
Kap.	Kapitel
KEG	Kernenergiegesetz (KEG) vom 21. März 2003 (SR 732.1)
KGGT	Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung
KI	Künstliche Intelligenz
KriPoZ	Kriminalpolitische Zeitschrift
krit.	kritisch
KV/KO	Kommentar Kriminelles Vermögen – Kriminelle Organisationen
LBA	Loi sur le blanchiment d'argent
LG	Landgericht
lit.	litera
LK	Leipziger Kommentar
LP	Liquidity Provider
MiCAR	Markets in Crypto-Assets Regulation
MMR	Multimedia und Recht
MROS	Money Laundering Reporting Office Switzerland
MüKo	Münchner Kommentar
Multisig	Multisignature
m.V.a.	mit Verweis auf
m.w.H.	mit weiteren Hinweisen
m.w.V.	mit weiteren Verweisen
N	Randnummer
n.F.	neue Fassung
NJW	Neue Juristische Wochenschrift
NR	Nationalrat
Nr.	Nummer

NRA	National Risk Assessment
NStZ	Neue Zeitschrift für Strafrecht
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht
NZZ	Neue Zürcher Zeitung
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
OFK	Orell Füssli Kommentar
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (SR 220)
PK	Praxiskommentar
P2P	Peer-to-Peer
recht	Zeitschrift für juristische Weiterbildung und Praxis
resp.	respektive
S.	Seite(n)
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) vom 11. April 1889 (SR 281.1)
SHA	Secure Hash Algorithm
SHK	Stämpflis Handkommentar
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
SJZ	Schweizerische Juristen-Zeitung
SK	Schulthess Kommentar
SKZ	Schweizerische Zeitschrift für Kriminologie
SO	Kanton Solothurn
SPV	Simplified Payment Verification Node
SRO	Selbstregulierungsorganisation
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
STO	Security Token Offering
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)
StV	Zeitschrift Strafverteidiger
SVG	Strassenverkehrsgesetz (SVG) vom 19. Dezember 1958 (SR 741.01)
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht
TPF	Tribunal pénal fédéral
TradFi	Traditionelles Finanzsystem

TTDSG	Telekommunikations-Telemedien-Datenschutz-Gesetz (Deutschland)
UNODC	United Nations Office on Drugs and Crime
US	United States
USD	United States Dollar
USDC	USD Coin
USG	Bundesgesetz über den Umweltschutz (Umweltschutzgesetz, USG) vom 7. Oktober 1983 (SR 814.01)
usw.	und so weiter
UTXO	Unspent Transaction Outputs
VASP	Virtual Asset Service Provider
vgl.	vergleiche
VO	Verordnung
Vol.	Volumen
Vorb.	Vorbemerkungen
VPB	Verwaltungspraxis des Bundes
vs.	versus
WEF	World Economic Forum
wistra	Zeitschrift für Wirtschaft, Steuer, Strafrecht
z.B.	zum Beispiel
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZH	Kanton Zürich
Ziff.	Ziffer
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
zit.	zitiert als
ZK	Zürcher Kommentar
zkKYC	Zero-Knowledge Know Your Customer
ZStrR	Schweizerische Zeitschrift für Strafrecht
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZVglRWiss	Zeitschrift für Vergleichende Rechtswissenschaft

Glossar

Admin Keys
: Kryptographische Schlüssel, mit denen Betreiberinnen Eingriffe in Smart Contracts oder Protokollfunktionen vornehmen können

Backend
: Technischer Kernbereich einer Anwendung, der im Hintergrund die Systemlogik und Protokollfunktionen ausführt

Bitcoin
: Dezentrale digitale Währung, deren Transaktionen auf einer öffentlich einsehbaren Blockchain verzeichnet werden

Block-Header
: Strukturteil eines Blocks, der Metadaten wie Zeitstempel, Hash-Werte und Verweise auf Vorgängerblöcke enthält

Blockchain-Explorer
: Webbasierte Anwendung zur Suche, Aufbereitung und Anzeige von Blockchain-Daten wie Transaktionen, Blöcken oder Adressen

Blockchain-Technologie
: Verteiltes, kryptographisch gesichertes Datensystem, in dem Transaktionen in chronologisch verknüpften Datenblöcken gespeichert und manipulationsresistent dokumentiert werden

Blöcke
: Dateneinheiten innerhalb einer Blockchain, die Transaktionen sowie zugehörige Metadaten enthalten und durch Hash-Verweise miteinander verkettet sind

Blockmetadaten
: Strukturelle Informationen eines Blocks, wie Zeitstempel, Verweise auf vorherige Blöcke, Nonce oder Protokollversion, die der Validierung und Einordnung dienen

Bugfix
: Korrekturen an bestehendem Code, die Programmfehler beheben und die Funktionsfähigkeit einer Anwendung oder eines Smart Contracts wiederherstellen

Bytecode
Maschinennahe Codeform, in die Smart Contracts kompiliert werden und die von der Ausführungsumgebung interpretiert wird

Chain-Hopping
Sequenzielles Verschieben von Vermögenswerten über mehrere Blockchains zur Erschwerung der Nachverfolgung

Coin
Nativer Vermögenswert einer Blockchain, der unmittelbar durch das zugrunde liegende Protokoll erzeugt und verwaltet wird

Cold / Hot Storage
Offline-Speicherung von Private Keys (Cold) bzw. Online-Speicherung mit Netzwerkanbindung (Hot)

Cross-Chain-Technologie
Technische Verfahren zur Übertragung oder Nutzung von Vermögenswerten über verschiedene Blockchains hinweg

Custodial / Non-Custodial
Unterscheidung zwischen Lösungen mit Verwahrung der Private Keys durch einen Dritten (custodial) und solchen ohne Fremdverwahrung (non-custodial)

DApp (Decentralized Application)
Dezentral ausgeführte Anwendung, die auf Smart Contracts basiert und über ein Frontend für Nutzerinteraktionen zugänglich ist

DeFi (Decentralized Finance)
Blockchainbasierte Architektur, die mittels Smart Contracts Finanzdienstleistungen ohne zentrale Intermediäre automatisiert bereitstellt

Deployment (von Smart Contracts)
Vorgang der Veröffentlichung und Aktivierung eines Smart Contracts auf einer Blockchain

Dezentrale Autonome Organisation (DAO)
Blockchainbasierte Organisationsform, bei der Entscheidungen typischerweise durch Abstimmungen der Governance-Teilnehmer getroffen und mittels Smart Contracts umgesetzt werden

dezentralisierte Finanzanwendungen *Siehe DeFi*

dezentralisierte Handelsplattform
Blockchainbasierte Plattform, auf der Vermögenswerte ohne zentrale Vermittlungsstelle gehandelt werden können

digitale Signatur
Kryptographisches Verfahren zur Authentifizierung von Transaktionen und zum Nachweis der Inhaberschaft eines Private Keys

Distributed Ledger Technology (DLT)
Technologie zur dezentralen Speicherung und Synchronisierung von Daten über mehrere unabhängige Knoten hinweg

Ether (ETH)
Native Kryptowährung der Ethereum-Blockchain, verwendet zur Bezahlung von Transaktionen und zum Betrieb von Smart Contracts

Ethereum
Blockchain-Protokoll mit integrierter Ausführungsumgebung für Smart Contracts und dezentralisierte Anwendungen

Ethereum Virtual Machine (EVM)
Ausführungsumgebung der Ethereum-Blockchain, die Smart Contracts verarbeitet und deren Zustand verwaltet

Externally Owned Account (EOA)
Blockchain-Konto, das durch einen Private Key kontrolliert wird und Transaktionen initiieren kann

Fiat On-Ramp / Off-Ramp
Dienstleistungen zum Wechsel zwischen Fiatwährungen und Kryptowerten in beide Richtungen

Fiatwährung / Fiatgelder
Staatlich ausgegebenes Zahlungsmittel unter Kontrolle einer Zentralbank

Flash Loans
Unbesicherter Blockchain-Kredit, der innerhalb derselben Transaktion aufgenommen und zurückgeführt werden muss

Frontend
Benutzeroberfläche einer Anwendung, über die Nutzer mit dem zugrundeliegenden Protokoll interagieren

Full Node
Knoten, der die gesamte Blockchain speichert, alle Transaktionen und Blöcke validiert und zur Netzwerksicherheit beiträgt

Fungibilität
Austauschbarkeit gleichartiger Einheiten eines Vermögenswerts ohne Wert- oder Bedeutungsunterschied

Gas / Gasgebühren
Rechenentgelt für die Ausführung von Transaktionen und Smart Contracts auf Blockchain-Netzwerken wie Ethereum

Governance
Mechanismen und Verfahren, durch die Änderungen, Parameteranpassungen oder Entscheidungen über den Betrieb eines dezentralisierten Protokolls getroffen werden

Hash
Algorithmisch erzeugter, fester Prüfwert (‹Fingerabdruck›) einer beliebigen Datenmenge

idealtypisch dezentrale Protokolle
Protokolle, deren Smart Contracts unveränderlich ausgeführt werden und bei denen Betreiberinnen über keine administrativen Eingriffs- oder Steuerungsmöglichkeiten verfügen

Interface
Schnittstelle, welche die Interaktion zwischen Nutzer, Anwendung oder Protokoll ermöglicht

Kill Switch
Mechanismus in einem Smart Contract oder einer Anwendung, der den Betrieb teilweise oder vollständig stoppen oder bestimmte Funktionen deaktivieren kann

Knoten(-punkt)
Computer im Netzwerk einer Blockchain, der Transaktionen validiert, speichert und zur Verteilung des Datenbestands beiträgt

Konsensmechanismus
Verfahren, mit dem die Teilnehmer eines verteilten Netzwerks einen einheitlichen Zustand der Blockchain feststellen und Transaktionen validieren

Kryptoautomat
Physische Geräte zum Kauf und Verkauf von Kryptowährungen gegen Bargeld

Kryptographie
Einsatz mathematischer Verfahren zur Sicherung, Authentifizierung und Integrität digitaler Informationen

Kryptomixer
Protokoll zur Erschwerung der Rückverfolgbarkeit von Kryptowerttransaktionen durch die Auflösung oder Verschleierung von Transaktionszusammenhängen

Kryptowerte
Digitale, auf einer Blockchain geführte Vermögenswerte, deren Verfügung ausschliesslich durch kryptographische Schlüssel kontrolliert wird

Lending-Protokolle
Dezentralisierte Anwendungen, die automatisierte Kreditvergaben und -aufnahmen über Smart Contracts ermöglichen

Light Node / Light Client
Knoten, der nur einen Teil der Blockchain-Daten speichert und die Gültigkeit von Blöcken über vereinfachte Verifizierungsverfahren prüft

Liquiditätspool
Smart-Contract-basierter Pool von Token, die von Nutzern bereitgestellt werden und den automatisierten Handel auf dezentralen Plattformen ermöglichen

Liquidity Mining
Mechanismus, bei dem Nutzer für die Bereitstellung von Token in einem Liquiditätspool zusätzliche Vergütungen erhalten

Matching Engine
Technische Komponente einer Handelsplattform, welche Kauf- und Verkaufsaufträge automatisiert miteinander abgleicht

Memory Pool
Zwischenspeicher für gültige, aber noch nicht in einen Block aufgenommene Transaktionen

Merkle Root
Kryptographischer Hash, der die Gesamtheit der Transaktions-Hashes eines Blocks repräsentiert und als komprimierte Integritätsprüfung dient

Merkle Tree
Baumstruktur kryptographischer Hashes, die eine effiziente und sichere Verifizierung grosser Datenmengen ermöglicht

Miner
Netzwerkteilnehmer in Proof-of-Work-Systemen, der durch das Lösen kryptographischer Aufgaben neue Blöcke erzeugt und dafür eine Blockbelohnung sowie Transaktionsgebühren erhält

Monero
Kryptowährung mit datenschutzorientierter Architektur, die Transaktionsbeträge, -herkunft und -empfänger verschleiert

Multisignature
Verfahren, bei dem mehrere kryptographische Signaturen erforderlich sind, um eine Transaktion oder administrative Aktion auszuführen

Native Token
Blockchain-eigener Vermögenswert, der direkt aus dem Protokoll stammt und zur Ausführung von Transaktionen sowie zur Nutzung von Netzwerkfunktionen dient

Node *Siehe Knotenpunkt*

Nonce
Protokollabhängiger Wert zur Sicherstellung der Eindeutigkeit von Transaktionen oder Blöcken und zur Verhinderung bestimmter Angriffe

On-chain / Off-chain
Vorgänge auf der Blockchain bzw. Vorgänge ausserhalb der Blockchain

Oracle
System, das externe Informationen in eine Blockchain einspeist

Orderbuch
Strukturierte Auflistung offener Kauf- und Verkaufsaufträge in einer Handelsanwendung

Peer-to-Peer-Netzwerk (P2P)
Direktes Netzwerk ohne zentrale Instanz, in dem Teilnehmer Daten unmittelbar miteinander austauschen

Privacy Coins
Kryptowährungen mit integrierten Anonymisierungsmechanismen zur Verschleierung von Transaktionen und Adressen

Private Key
Kryptographischer Geheimschlüssel zur Autorisierung von Transaktionen und zur Verfügung über digitale Vermögenswerte

Proof of Stake
Konsensverfahren, bei dem Validatoren Transaktionen anhand ihres hinterlegten Einsatzes (Stake) bestätigen

Proof of Work
Konsensverfahren, bei dem Miner durch rechenintensive Aufgaben neue Blöcke erzeugen und das Netzwerk sichern

Protokollparameter
Technische Einstellungen, welche die Funktionsweise eines Protokolls bestimmen

Proxy-Architektur
Smart-Contract-Struktur, die durch Trennung von Zustand (Proxy) und Logik austauschbare Updates ohne Änderung der Nutzerinteraktion ermöglicht

Pseudonymität
Adressbasierte Identität ohne direkte Personenzuordnung

Public Key
Öffentlich einsehbarer kryptographischer Schlüssel zur Adressbildung und Verifikation digitaler Signaturen

Release
Freigabe zuvor in Smart Contracts gesperrter Token

Revert
Automatischer Abbruch einer Smart-Contract-Transaktion, bei dem sämtliche vorgesehenen Zustandsänderungen rückgängig gemacht werden und die Blockchain unverändert bleibt

Reward
Vergütung für Beiträge zum Netzwerkbetrieb

Simplified Payment Verification Node (SPV) *Siehe Light Node*

Slippage
Abweichung zwischen erwartetem und effektivem Ausführungspreis einer Transaktion aufgrund von Marktbewegungen oder geringer Liquidität

Smart Contract
Programmierter Code auf einer Blockchain, der vordefinierte Abläufe automatisch ausführt

Stablecoin
Token mit wertstabiler Bindung an eine Referenzgrösse (z.B. Fiatwährung)

Staking
Bindung von Token zur Teilnahme an einem Proof-of-Stake-Verfahren und zum Erhalt von Rewards

Swapping
Automatisierter Tausch eines Tokens gegen einen anderen über eine (zentralisierte oder dezentralisierte) Handelsplattform

Tainted Coins
Kryptowerte, die mit Delikten oder sanktionierten Adressen in Verbindung stehen

Tether
Bekannter US-Dollar-gebundener Stablecoin (USDT) des Unternehmens Tether

Token
Digitale Einheit auf einer Blockchain, die einen Wert, ein Recht oder eine Funktion repräsentiert

TradFi (Traditional Finance)
Sammelbegriff für das traditionelle, zentral organisierte Finanzsystem

Transaction Pool *Siehe Memory Pool*

Tumbler *Siehe Kryptomixer*

Turing-Vollständigkeit
Fähigkeit eines Systems, beliebige berechenbare Programme auszuführen

Unfreezable / Freezable Token
Token mit der (nicht) bestehenden Möglichkeit, sie technisch zu sperren

Unspent Transaction Outputs (UTXOs)
Nicht ausgegebene Transaktionsausgänge, die in UTXO-basierten Blockchains als verfügbare Guthaben gelten

USD Coin (USDC)
Stablecoin, der den US-Dollar abbildet

Validatoren
Netzwerkteilnehmer in Proof-of-Stake-Blockchains, die durch Hinterlegung eines Einsatzes (Stake) Transaktionen prüfen und an der Erstellung sowie Bestätigung neuer Blöcke mitwirken

virtuelle Vermögenswerte *Siehe Kryptowerte*

Wallet
Software oder Hardware zur Verwaltung von Private Keys

Watchlists
Von Behörden oder Analysefirmen geführte Listen auffälliger oder sanktionierter Blockchain-Adressen

Webinterface
Browserbasierte Benutzeroberfläche für den Zugang zu einer Anwendung

Whitelist
Liste zugelassener Adressen oder Entitäten, die für bestimmte Transaktionen oder Funktionen freigeschaltet sind

Wrapped Token
Tokenisierte Repräsentation eines Vermögenswerts auf einer anderen Blockchain

Yield Farming
Strategie zur Erzielung von Erträgen durch die Bereitstellung von Liquidität oder die Nutzung von Anreizmechanismen in DeFi-Protokollen

Zahlungs-Token
Token, die primär als Zahlungsmittel innerhalb oder ausserhalb der Blockchain verwendet werden

Einleitung

Ausgangslage und Forschungsfrage

Kryptowerte haben sich innert weniger Jahre von einem technologischen Nischenphänomen zu einem strukturell relevanten Bestandteil des globalen Finanzsystems entwickelt und sind zugleich zu einem dynamischen Schauplatz moderner Kriminalität geworden.[1] Parallel zu ihrer zunehmenden Einbindung in den legalen Finanzmarkt hat sich gezeigt, dass gerade jene technologischen Eigenschaften, welche Innovation ermöglichen, gleichzeitig neue Angriffs- und Missbrauchsflächen eröffnen: So dienen virtuelle Vermögenswerte heute nicht nur als Anlageinstrumente, sondern auch als Lösegeld bei Ransomware-Attacken, als Zahlungsmittel auf Darknet-Marktplätzen oder geraten regelmässig ins Visier koordinierter Hackerangriffe.[2] Die für diese Entwicklung zentrale technologische Grundlage öffentlicher Blockchains besteht in ihrer globalen Verfügbarkeit, der pseudonymen Ausgestaltung von Transaktionen und dem intermediärlosen Zugang für Nutzer.[3] 1

Pseudonyme Adressen erlauben es, Vermögenswerte ohne unmittelbar erkennbare Personenbezüge zu übertragen. Demgegenüber dokumentiert die Blockchain jede Transaktion dauerhaft und schafft damit einen digitalen Nachweis, der die Verbindung zwischen Vermögenswert und seiner Herkunft erkennbar hält.[4] Für kriminelle Akteure bedeutet dies: Die Nutzung ist zwar anonymitätsbegünstigend, setzt aber zwingend Verschleierungsmechanismen voraus, um die systembedingte Rückverfolgbarkeit zu durchbrechen.[5] Der zentrale Ansatzpunkt solcher Verschleierungsmechanismen sind dezentralisierte Finanzanwendungen: blockchainbasierte Systeme, über die Nutzer den Austausch, die Umlagerung und die Umwandlung von Kryptovermögen 2

1 Vgl. KGGT, NRA 2024, S. 10 ff.; KGGT, NRA 2018, S. 9 ff.; Bundesrat, DLT, S. 143 ff.

2 KGGT, NRA 2024, S. 52 ff.; KGGT, NRA 2018, S. 21 ff.; U.S. Department of the Treasury, S. 18 ff.; COLLINS, S. 13 ff.

3 Europol, Spotlight, S. 5 f.; KGGT, NRA 2024, S. 23; GAFI, Indicators, S. 3; PAJAROLA, N 533.

4 Vgl. MEYER, Token, N 59; DE COL, S. 11; ERARD, S. 219; GYR, Smart Contracts, N 33; STENGEL / AUS DER AU, S. 441; ZOGG, S. 96.

5 Vgl. KGGT, NRA 2024, S. 48; U.S. Department of the Treasury, S. 16 f.; Europol, Spotlight, S. 7 ff.

allein durch automatisierten Programmcode ausführen können.[6] Im Unterschied zu klassischen Intermediären erfolgt die Abwicklung nicht über eine verantwortliche Stelle, sondern über Software-Logik, deren Grad an administrativer Kontrolle je nach System stark variiert und von weitreichenden Eingriffsmöglichkeiten einzelner Betreiberinnen bis hin zu Konstellationen reicht, die menschliche Steuerung vollständig obsolet machen.[7]

3 Die auf der Funktionsweise dezentralisierter Systeme beruhende Missbrauchsanfälligkeit für Geldwäscherei hat in den vergangenen Jahren einen intensivierten Diskurs nationaler und internationaler Aufsichtsbehörden ausgelöst.[8] Dass es sich dabei nicht um ein rein theoretisches Risiko handelt, zeigt sich auch in der schweizerischen Praxis: Ende November 2025 legten die Strafverfolgungsbehörden des Kantons Zürich im Rahmen eines international koordinierten Ermittlungsverfahrens die Server-Infrastruktur eines seit Jahren betriebenen Bitcoin-Mixers still, über den deliktisch erlangte Vermögenswerte im Umfang von weit über einer Milliarde Franken verschleiert worden sein sollen.[9] Der Fall verdeutlicht exemplarisch, dass dezentralisierte Finanzanwendungen nicht nur als technologische Innovationen, sondern zugleich als infrastrukturelle Knotenpunkte geldwäschereirelevanter Aktivitäten in Erscheinung treten können.

4 Auf strafrechtlicher Ebene zeigt sich indes, dass die relevanten Zurechnungs- und Verantwortlichkeitsfragen in der Literatur bislang kaum behandelt wurden und eine systematische Aufarbeitung noch aussteht.[10] Anders als im klassischen Finanzsektor, in dem die geldwäschereirechtliche Verantwortlichkeit von Intermediären dogmatisch gefestigt ist, stellt sich im Umfeld dezentralisierter Systeme die Frage, wie sich diese Grundsätze auf Strukturen übertragen lassen, in denen eine verantwortliche Stelle nicht ohne Weiteres auszumachen ist und zentrale Funktionen durch automatisierten Programmcode wahrgenommen werden.[11] Die vorliegende Untersuchung widmet sich dem daraus resultierenden Kernproblem: ob und unter welchen Voraussetzungen

6 U.S. Department of the Treasury, S. 16 f.; vgl. Bundesrat, Digital Finance, S. 8; ANDREOTTI, S. 178; HUMBEL, S. 10; SCHÄR, S. 154; WEF, DeFi, S. 6.

7 Vgl. MEIRICH, N 289 ff.; Financial Stability Board, S. 6; OECD, DeFi, S. 18; vgl. auch EJPD, NRA, S. 23; GAFI, VASP, S. 27.

8 Vgl. Bundesrat, DLT, S. 8 ff.; FINMA, Jahresbericht, S. 20; GAFI, Update, S. 2 ff.; GAFI, VASP, S. 4 ff.

9 Vgl. Gemeinsame Medienmitteilung der Zürcher Staatsanwaltschaft, der Stadtpolizei Zürich und der Kantonspolizei Zürich; COVIELLO/MÄDER/BAUMGARTNER.

10 Vgl. z.B. ANDREOTTI, S. 359 ff.; REGGIANI, S. 111 ff.

11 Anstatt vieler BGE 136 IV 188; ACKERMANN, Unterlassungsrisiken, S. 133; BABEY/HOANG, S. 488 ff.; OSWALD, passim; ROTH, Compliance, passim; STRASSER, S. 691 ff.; VON ROTZ, passim.

sich Betreiberinnen dezentralisierter Finanzanwendungen für von Nutzern begangene Geldwäschereihandlungen nach Art. 305bis StGB strafrechtlich verantwortlich machen können.

Untersuchungsgegenstand

Das Ziel dieser Untersuchung ist es, am Beispiel des Geldwäschereitatbestands Fragen der Strafbarkeit solcher Konstrukte im Kontext von Dezentralisierung und Automation zu navigieren. Der Fokus liegt auf Art. 305bis StGB, weil dieser im Zusammenhang mit blockchainbasierten Finanzanwendungen angesichts ihrer risikobehafteten Struktur und der zunehmenden praktischen Relevanz von Kryptokriminalität in besonderem Masse in den Vordergrund tritt.[12] Grundsätzlich stellen sich im Bereich der Geldwäscherei neben kernstrafrechtlichen Fragestellungen auch solche des Aufsichts- und Finanzmarktrechts. Da diese Aspekte bereits vertieft von Praxis und Behörden adressiert wurden,[13] konzentriert sich die Untersuchung auf die strafrechtliche Verantwortlichkeitsfrage im Zusammenhang mit Art. 305bis StGB; aufsichtsrechtliche und nebenstrafrechtliche Fragestellungen werden insoweit ausgeklammert, als sie für die Beantwortung der Forschungsfrage nicht erforderlich sind. 5

Die nachfolgende Untersuchung erfasst sämtliche Ausprägungen dezentralisierter Finanzanwendungen, unabhängig von ihrer technischen Architektur oder ihrem Grad an Dezentralisierung. Wo dies zu Veranschaulichungszwecken erforderlich ist, werden einzelne Fragestellungen exemplarisch am Beispiel von Kryptomixern sowie dezentralisierten Handelsplattformen illustriert. Diese Anwendungen wurden ausgewählt, weil sie aufgrund ihrer Funktionsmechanismen besonders oft zur Verschleierung von Vermögenswerten eingesetzt werden und deshalb im Zentrum der praxisbezogenen Debatte über geldwäschereirelevante Risiken dezentralisierter Systeme stehen.[14] Diese Beispiele dienen ausschliesslich der Konkretisierung abstrakter Problemstellungen und begrenzen den Untersuchungsgegenstand nicht, sondern sind in 6

12 Das Risiko von Geldwäscherei im Bereich dezentralisierter Finanzanwendungen wird sowohl auf nationaler Ebene als auch international übereinstimmend als ‹erheblich› eingestuft (vgl. Bundesrat, Digital Finance, S. 31; FINMA, Risikomonitor, S. 19; KGGT, NRA 2024, S. 64; OECD, DeFi, S. 26; U.S. Department of the Treasury, S. 16 ff.; vgl. auch MROS, Jahresbericht, S. 16, 24; FIU Deutschland, 2022, S. 35 f.).

13 Anstatt vieler MEIRICH, passim; NOSER/INFANGER/LÜDI, N 12.01 ff.; STENGEL/PAYDAR, N 18.01 ff.; WEF, DeFi, passim; vgl. auch Bundesrat, DLT, S. 87 ff.; FINMA, Risikomonitor, S. 19 f.

14 Vgl. hinten N 181 ff.; KGGT, NRA 2024, S. 102 f.; KGGT, NRA 2018, S. 21; U.S. Department of the Treasury, S. 16.

eine umfassende Beurteilung der Strafbarkeit im Kontext dezentralisierter Finanzanwendungen nach Art. 305bis StGB eingebettet.

7 Bei Betreiberinnen von dezentralisierten Protokollen handelt es sich in der Regel um Einzelpersonen oder lose Personenzusammenschlüsse ohne formale Rechtsform.[15] Die Untersuchung konzentriert sich insofern auf die individuelle Strafbarkeit der Betreiberinnen. Die Betreiberschaft als Kollektiv wird derweil punktuell dort aufgegriffen, wo sie für die strafrechtliche Analyse im Zusammenhang mit Art. 305bis StGB – namentlich im Bereich der Qualifikationstatbestände – von Relevanz ist.[16] Kollektive Betreibermodelle wie Dezentrale Autonome Organisationen (DAOs) und Multisignatur-Strukturen werden nicht vertieft behandelt. Sie weichen hinsichtlich Verantwortungszuweisung, Entscheidungsprozessen und Kontrollmechanismen strukturell erheblich von den in dieser Arbeit untersuchten Betreiberkonstellationen ab und bedürften daher einer eigenständigen strafrechtlichen Analyse, die den Rahmen der Untersuchung sprengen würde.[17] Soweit es der Gang der Untersuchung erlaubt, werden solche Konstellationen jedoch punktuell einbezogen.

8 Fragen der Unternehmensstrafbarkeit nach Art. 102 StGB sind nicht Gegenstand dieser Arbeit. Zwar kann sich bei Vorliegen einer Individualstrafbarkeit der Betreiberinnen im Einzelfall zusätzlich die Frage einer subsidiären oder originären Verantwortlichkeit eines Unternehmens nach Art. 102 Abs. 1 bzw. 2 StGB stellen. Die damit verbundenen Fragestellungen betreffen jedoch primär die Zurechnung strafbaren Verhaltens zu einer Unternehmensstruktur und setzen die vorgängige Klärung der individuellen Verantwortlichkeit weitgehend voraus. Für die im Zentrum dieser Arbeit stehende Frage, ob und unter welchen Voraussetzungen Betreiberinnen dezentralisierter Finanzanwendungen für Geldwäschereihandlungen strafrechtlich verantwortlich gemacht werden können, ergibt sich daraus kein wesentlicher zusätzlicher Erkenntnisgewinn.[18]

15 Vgl. OECD, DeFi, S. 11; MAURENBRECHER/LEISINGER, Teil 2, S. 715; NOSER/INFANGER/LÜDI, N 12.14; vgl. auch FINMA, Risikomonitor, S. 19; GAFI, VASP, S. 43; REDMANN-WIPPEL/STADLER.

16 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 716 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 46 ff.; BSK StGB II-PIETH, Art. 305bis N 63 ff.

17 Vgl. MEIRICH, N 145 ff.

18 Vgl. BSK StGB I-NIGGLI/GFELLER, Art. 102 N 426 ff.; FORSTER, Diss., S. 128; SCHMID, S. 781.

Gang der Untersuchung

Um die eingangs formulierte Forschungsfrage tragfähig beantworten zu können, bedarf es zunächst einer technischen und begrifflichen Fundierung *(Teil 1)*. Der erste Teil der Arbeit widmet sich deshalb den Grundlagen derjenigen Technologie, welche dezentralisierten Finanzanwendungen zugrunde liegt (Kap. 1). Ausgangspunkt bildet die Darstellung der Funktionsweise öffentlicher Blockchains (I.), um jene technologischen Merkmale sichtbar zu machen – insbesondere die dezentrale Architektur, die kryptographischen Sicherungsmechanismen sowie den Ablauf von Transaktionen –, die bestimmen, wie Wertübertragungen innerhalb des Blockchain-Systems technisch abgebildet werden. Daran anschliessend folgt eine Einführung in Smart Contracts (II.), die erläutert, wie programmierbare Vertragslogiken auf der Blockchain funktionieren und automatisierte Abläufe ermöglichen. Dieser Abschnitt schafft damit das notwendige technische Fundament für das Verständnis der Infrastruktur, über welche blockchainbasierte Finanztransaktionen abgewickelt werden. 9

Im Anschluss werden dezentralisierte Finanzanwendungen behandelt (III.). Gegenstand dieses Abschnitts sind Begriff, Strukturmerkmale und typische Ausprägungen solcher Anwendungen sowie der Begriff der Kryptowerte, mit denen diese operieren. Dabei wird aufgezeigt, über welche technischen Mechanismen Werttausch, Umlagerung und Umwandlung von Kryptovermögen automatisiert erfolgen können. Auf dieser Grundlage erfolgt sodann die systematische Bestimmung der Akteurslandschaft im Umfeld dezentralisierter Anwendungen (IV.), mit einem Fokus auf das technische ‹Handeln› von Smart Contracts, die Rolle und Eingriffsmöglichkeiten der Betreiberschaft sowie die Stellung der Nutzer. Diese Analyse schafft die Grundlage für die Beurteilung, ob und in welchem Umfang normativ relevantes menschliches Verhalten – und damit strafrechtliche Verantwortlichkeit – in Systemen möglich ist, die von Automatisierung und potenzieller Dezentralisierung geprägt sind. 10

Das zweite Kapitel der Grundlagen widmet sich der Geldwäscherei im Umfeld blockchainbasierter Finanzanwendungen und klärt, in welcher Weise Nutzer solche Systeme zur Herkunftsverschleierung einsetzen (Kap. 2). Dieser Abschnitt fungiert als Bindeglied zwischen der technischen Funktionsweise der Anwendungen und dem Geldwäschereitatbestand nach Art. 305bis StGB. Nur wenn klar umrissen ist, welche Nutzungsmuster als geldwäschereirelevante Tathandlungen zu qualifizieren sind, lässt sich später prüfen und beantworten, ob Betreiberinnen im Zusammenhang mit solchen Vorgängen verantwortlich gemacht werden können. Das Phänomen der Geldwäscherei mit Kryptowerten wird zunächst im Lichte der klassischen Drei-Phasen-Lehre beschrieben und in seinen kriminologischen sowie empirischen Kontext eingebettet. 11

Daran anschliessend werden die Tatbestandsvoraussetzungen von Art. 305bis StGB systematisch auf die Nutzung dezentralisierter Protokolle angewendet. Untersucht wird nicht die Strafbarkeit der Nutzer, sondern die Frage, unter welchen Voraussetzungen Verschleierungsakte unter Einsatz dezentralisierter Anwendungen als tatbestandsmässig relevante Handlungen im Sinne des Geldwäschereitatbestands einzuordnen sind. Nutzerhandlungen werden dabei lediglich in dem Umfang beschrieben, der für die spätere Analyse der Betreiberverantwortlichkeit erforderlich ist.

12 Basierend auf den im ersten Teil erarbeiteten Grundlagen wendet sich der zweite Teil der Untersuchung der Kernfrage zu, ob und unter welchen Voraussetzungen Betreiberinnen dezentralisierter Finanzanwendungen für Geldwäschereihandlungen der Nutzer nach Art. 305bis StGB strafrechtlich verantwortlich gemacht werden können *(Teil 2)*. Den Ausgangspunkt bildet die Prüfung einer Begehensstrafbarkeit (Kap. 1). Untersucht wird, ob und in welcher Form das Bereitstellen bzw. das Deployment eines Protokolls als tatbestandsrelevantes Tun erfasst werden kann und ob es sich dabei um Täterschaft oder Teilnahme handelt. Anschliessend wird geprüft, ob eine Verantwortlichkeit auch in Form einer Unterlassensstrafbarkeit (Kap. 2) in Betracht kommen kann. Im Zentrum stehen dabei die Voraussetzungen einer unechten Unterlassung, insbesondere das Bestehen einer Garantenstellung, die hypothetische Kausalität, die Tatmacht und die Gleichwertigkeit von Tun und Unterlassen sowie der subjektive Tatbestand. In einem abschliessenden Kapitel (Kap. 3) befasst sich die Untersuchung neben der Frage, inwiefern qualifizierte Tatbestände auch Betreiberinnen dezentralisierter Anwendungen erfassen können, mit möglichen Konkurrenzverhältnissen sowie mit den Anknüpfungspunkten einer schweizerischen Strafhoheit.

Methodik und Terminologie

13 Vorliegend handelt es sich um eine rechtsdogmatische Untersuchung, die schwerpunktmässig im Allgemeinen Teil des Strafrechts angesiedelt ist. Die Forschungsfrage wird auf Grundlage des geltenden Rechts beantwortet, unter Rückgriff auf die anerkannten Auslegungsmethoden sowie unter Berücksichtigung von Gesetzeswortlaut, Rechtsprechung, Materialien und einschlägiger Literatur. Im Vordergrund stehen die schweizerische Literatur und Judikatur. Soweit der nationale Diskurs keine hinreichenden dogmatischen Anknüpfungspunkte bietet, wird punktuell auf deutsche Literatur zurückgegriffen, deren Herkunft bei der ersten Erwähnung ausgewiesen wird. Anschliessende Zitate erfolgen ohne erneute Kennzeichnung.

Für die Darstellung der technologischen Grundlagen wird dagegen vermehrt 14
auf englischsprachige Fachliteratur zurückgegriffen, da der einschlägige wissenschaftliche Diskurs zu blockchainbasierten Systemen im deutschsprachigen Raum bislang nur in begrenztem Umfang vorliegt.

Ferner ist zu beachten, dass aus Gründen der terminologischen Einheit- 15
lichkeit technische Fachbegriffe überwiegend in ihrer englischen Originalfassung verwendet werden. Wo sich jedoch im deutschsprachigen Diskurs bereits klare und anerkannte Bezeichnungen etabliert haben, wird aus Gründen der Lesbarkeit auf diese zurückgegriffen. Zur Unterstützung der Verständlichkeit wird zudem ein Glossar bereitgestellt, das die in der Arbeit verwendeten blockchainbezogenen technologischen Fachbegriffe kompakt erläutert und damit insbesondere Leserinnen und Leser ohne technischen Hintergrund einen erleichterten Zugang zur Terminologie ermöglicht.

Teil 1: Grundlagen

Kapitel 1: Blockchain und dezentralisierte Finanzanwendungen

I. Blockchain-Technologie

A. Hintergrund und Definition

Die Blockchain-Technologie trat im Jahr 2008 erstmals in das öffentliche Bewusstsein, als unter dem Pseudonym ‹Satoshi Nakamoto›[19] das Whitepaper ‹Bitcoin: A Peer-to-Peer Electronic Cash System› publiziert wurde.[20] Zwar steht darin die Konzeption eines elektronischen Zahlungssystems im Vordergrund, doch markiert das Dokument zugleich die Geburtsstunde eines neuen technischen Konzepts, das sich seither weit über den Kontext von Kryptowährungen hinaus entwickelt hat: der Blockchain.[21] 16

Der Begriff ‹Blockchain› bezeichnet keine einheitlich definierte Technologie, sondern ein Grundprinzip zur Speicherung und Verwaltung von Daten.[22] Technisch handelt es sich um eine besondere Form der sogenannten Distributed-Ledger-Technologie (DLT).[23] Damit sind Systeme gemeint, bei denen Informationen nicht zentral auf einem Server gespeichert werden, sondern über viele Computer (sogenannte Nodes oder Knotenpunkte) verteilt sind, die gemeinsam denselben Datenbestand führen.[24] Die Blockchain unterscheidet sich von anderen DLT-Formen dadurch, dass neue Daten in einzelnen Einheiten (sogenannten Blöcken) zusammengefasst und durch kryptographische Verfahren manipulationsresistent an eine chronologisch geordnete Kette früherer Blöcke angehängt werden.[25] 17

19 Die Identität der hinter dem Pseudonym stehenden Person(en) ist bis heute ungeklärt. In der Literatur wird diese Anonymität teilweise als Ausdruck der von Bitcoin angestrebten Dezentralität und Autonomie verstanden (vgl. BERENTSEN/SCHÄR, S. 49).

20 BERENTSEN/SCHÄR, S. 49; DIEHL, S. 39 f.; MEYER, DAO, S. 321; SIEGEL, S. 74; STILLER/RODRIGUES/NEZHADSISTAN, N 2.01.

21 Vgl. NAKAMOTO, passim.

22 Vgl. CROSBY et al., S. 8; STENGEL / AUS DER AU, S. 445; STILLER/RODRIGUES/NEZHADSISTAN, N 2.01.

23 STILLER/RODRIGUES/NEZHADSISTAN, N 2.04.

24 DE COL, N 5; MEYER, Token, N 25; OSWALD, S. 17 f.

25 Vgl. Botschaft DLT, S. 18; DE COL, N 7; MEYER, Token, N 24 ff.; SCHLATT et al., S. 7; STENGEL / AUS DER AU, S. 439; vgl. auch CONDOS et al., S. 6; MIGNON, S. 1.

18 Eine einheitliche Definition des Begriffes ‹Blockchain› existiert bislang nicht. Dies hängt nicht zuletzt damit zusammen, dass es nicht ‹die› Blockchain gibt: Die konkrete Ausgestaltung, z.B. hinsichtlich Zugangsrechten oder Netzwerkstruktur, variiert je nach technischer Umsetzung und Anwendungsbereich. Ursprünglich zur Ermöglichung eines digitalen Zahlungssystems konzipiert, hat sich das Konzept seither auf vielfältige Bereiche ausgeweitet, namentlich auf das Finanzwesen, die Lieferkettenverfolgung oder digitale Identitäten.[26] Allen Anwendungsformen gemeinsam ist der Bedarf nach einer manipulationssicheren, transparenten und gemeinschaftlich geführten Datenbasis.

19 In vereinfachter Darstellung lässt sich eine Blockchain als eine Art dezentrale Datenbank beschreiben: Neue Datensätze (wie z.B. Transaktionsdetails) werden in Blöcken gruppiert, kryptographisch gesichert und an die bestehende Kette angehängt.[27] Eine Kopie dieser Kette wird, je nach Art des Knotenpunktes, ganz oder teilweise von den Netzwerkteilnehmern gespeichert.[28] Ob ein neuer Block gültig ist, wird von den Netzwerkteilnehmern nach gemeinsamen, im System festgelegten Regeln überprüft. Diese Regeln werden als Konsensmechanismus bezeichnet und sorgen dafür, dass sich das Netzwerk ohne zentrale Instanz auf denselben Datenstand einigt.[29] Durch die kryptographische Verkettung sind Manipulationen an früheren Datensätzen grundsätzlich nur möglich, wenn gleichzeitig alle nachfolgenden Blöcke angepasst würden und der Angreifer die Kontrolle über den Konsensmechanismus erlangt.[30]

20 Die nachfolgenden Abschnitte widmen sich den grundlegenden technischen Elementen der Blockchain-Technologie. Im Zentrum stehen dabei ihre Netzwerkarchitektur, die zugrunde liegenden kryptographischen Verfahren sowie der Ablauf von Transaktionen.

B. Blockchain-Typen

21 Für die Systematisierung von Blockchains lassen sich zwei grundlegende Kriterien heranziehen: zum einen, wer die gespeicherten Daten einsehen kann, und zum anderen, wer am Konsensmechanismus – insbesondere an

26 Vgl. Botschaft DLT, S. 33 ff.; ERARD, S. 215 ff.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.08 ff.

27 GYR, Smart Contracts, S. 10 ff.; MEYER, DAO, S. 10; BURGWINKEL, S. 5 f.; vgl. CONDOS et al., S. 6.

28 ANTONOPOULOS, S. 172 f.; ANTONOPOULOS/WOOD, S. 42 ff.; MEIRICH, N 52.

29 CONDOS et al., S. 6 f.; MEYER, Token, N 44 ff.; STENGEL / AUS DER AU, S. 440.

30 Botschaft DLT, S. 18; BURGWINKEL, S. 6; CONDOS et al., S. 7; STENGEL / AUS DER AU, S. 441; m.w.H. MEYER, Token, N 44 ff.; BERENTSEN/SCHÄR, S. 99.

der Validierung von Transaktionen und der Erstellung neuer Blöcke – teilnehmen darf.[31] Nach dem Kriterium der Leserechte wird zwischen public und private Blockchains unterschieden. Public Blockchains stehen grundsätzlich allen Personen offen, das heisst, jeder Nutzer kann die entsprechende Software installieren, Transaktionen versenden und eine Kopie der Blockchain speichern; sämtliche Daten sind öffentlich einsehbar und historisch rückverfolgbar.[32] Private Blockchains hingegen beschränken die Leserechte ganz oder teilweise und richten sich in der Regel an einen geschlossenen oder kontrollierten Nutzerkreis.[33]

Bezieht man sich hingegen auf die Teilnahme am Konsensmechanismus, so erfolgt eine Unterscheidung zwischen permissionless und permissioned Blockchains.[34] In permissionless Systemen kann jede Person ohne vorherige Zulassung an der Validierung von Transaktionen mitwirken und neue Blöcke erzeugen. Permissioned Blockchains beschränken diese Funktionen auf einen ausgewählten Teilnehmerkreis, dessen Rolle meist organisatorisch oder vertraglich festgelegt ist.[35] 22

Schliesslich bestehen hybride Ausprägungen, in denen sich beide Dimensionen kombinieren – etwa öffentlich einsehbare Systeme mit einem beschränkten Kreis von Konsensberechtigten oder, umgekehrt, nicht-öffentliche Systeme mit offenem Validierungszugang.[36] 23

Für die vorliegende Untersuchung sind primär public, permissionless Blockchains von Bedeutung, da die relevanten dezentralisierten Finanzanwendungen typischerweise auf offenen Systemen wie der Ethereum-Blockchain aufbauen und die damit verbundene Abwesenheit institutioneller Vermittlungsstellen gerade den Kern der strafrechtlichen Fragestellungen bildet.[37] 24

31 Vgl. MEYER, Token, N 58 ff.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.22 ff.; eine ähnliche Unterscheidung machen auch SCHLATT et al., S. 11.

32 MEYER, Token, N 59; MEIRICH, N 46; vgl. ERARD, S. 219; GYR, Smart Contracts, N 33; STENGEL/AUS DER AU, S. 441.

33 MEYER, Token, N 60; MEIRICH, N 46; vgl. ERARD, S. 219; GYR, Smart Contracts, N 35; PETERS/PANAYI, S. 5; STENGEL/AUS DER AU, S. 441; STILLER/RODRIGUES/NEZHADSISTAN, N 2.22.

34 MEYER, Token, N 58; MEIRICH, N 47; PETERS/PANAYI, S. 5 ff.; STENGEL/AUS DER AU, S. 441; STILLER/RODRIGUES/NEZHADSISTAN, N 2.22; WALPORT, S. 35.

35 Botschaft DLT, S. 24; MEYER, Token, N 62 f.; ERARD, S. 219; SIEGEL, S. 93 ff.; STENGEL/AUS DER AU, S. 441; STILLER/RODRIGUES/NEZHADSISTAN, N 2.22.

36 Botschaft DLT, S. 24; GYR, Smart Contracts, N 37; MEYER, Token, N 64.

37 MAURENBRECHER/LEISINGER, Teil 2, S. 705; GOGEL et al., DeFi, S. 2; SCHÄR, S. 154.

C. Funktionsweise der Blockchain-Technologie

25 Nach der begrifflichen und typologischen Einordnung der Blockchain-Technologie wird im Folgenden ihre grundlegende Funktionsweise anhand der beiden prototypischen Systeme Bitcoin und Ethereum erläutert. Obwohl sich beide Netzwerke in ihrer technischen Architektur unterscheiden, weisen sie zentrale gemeinsame Strukturelemente auf, die das Verständnis der Technologie prägen. Die Darstellung konzentriert sich auf diese Grundmechanismen und vereinfacht technische Einzelheiten dort, wo dies der Verständlichkeit dient.

1. Verteiltes Register und Netzwerkteilnehmer (Nodes)

26 Bei Blockchains wie Bitcoin und Ethereum handelt es sich um Peer-to-Peer-Netzwerke (P2P) von Computern.[38] Das bedeutet, dass viele einzelne Rechner, sogenannte Knotenpunkte oder Nodes, miteinander verbunden sind und gemeinsam das System betreiben, ohne dass eine zentrale Stelle Kontrolle ausübt.[39]

27 Netzwerkknotenpunkte sind also mit dem Internet verbundene Computer, die durch eine kompatible Software an das jeweilige Blockchain-Netzwerk angeschlossen sind und dessen Protokolle ausführen.[40] Je nach Typ empfangen, verifizieren oder übermitteln sie Transaktionen und Blöcke und leisten damit einen Beitrag zur Verteilung, Validierung oder Konsensbildung im Netzwerk. Der Betrieb einer Node steht grundsätzlich jeder interessierten Person offen und bildet einen zentralen Ausdruck des offenen Zugangsprinzips sogenannter permissionless Blockchains.[41]

28 Sowohl in der Bitcoin- als auch in der Ethereum-Blockchain speichern sogenannte Full Nodes eine vollständige Kopie der Blockchain und validieren Transaktionen sowie Blöcke gemäss den Regeln der jeweiligen Protokolle.[42] Ressourcenschonendere Knoten, sogenannte Light Nodes (oder Simplified

38 ANTONOPOULOS/WOOD, S. 2; BERENTSEN/SCHÄR, S. 53; MEYER, Token, N 30; STENGEL/AUS DER AU, S. 440.

39 ANTONOPOULOS, S. 171; BERENTSEN/SCHÄR, S. 69; vgl. GYR, Smart Contracts, N 43; MEYER, Token, N 31.

40 Vgl. Botschaft DLT, S. 22; MEYER, Token, N 37; ANTONOPOULOS/WOOD, S. 45.

41 Vgl. ANTONOPOULOS, S. 172; BERENTSEN/SCHÄR, S. 71; MEYER, Token, N 38; STILLER/RODRIGUES/NEZHADSISTAN, N 2.22.

42 Vgl. ANTONOPOULOS, S. 172 f.; ANTONOPOULOS/WOOD, S. 42 ff.; HEIN/WELLBROCK/HEIN, S. 7; MEIRICH, N 52; MOLO/DRZALIC, S. 54. Die hier beschriebene Validierung durch Full Nodes betrifft die technische Prüfung, ob Transaktionen und Blöcke den Protokollregeln entsprechen. Sie unterscheidet sich von der aktiven Teilnahme am Konsens, also dem Vorschlagen bzw. Bestätigen von Blöcken, die im Bitcoin-Netzwerk von Mining Nodes und im Ethereum-Netzwerk von Validator Nodes übernommen wird (vgl. LINDER, S. 22; ANTONOPOULOS, S. 173; MEIRICH, N 52).

Payment Verification Nodes) im Bitcoin-Netzwerk und Light Clients in Ethereum, speichern hingegen lediglich ausgewählte Blockmetadaten wie Zeitstempel, Verweise sowie Prüfsummen und stützen sich für die Verifikation auf vereinfachte kryptographische Nachweise sowie auf Informationen anderer Netzwerkknoten.[43] Letztere sind insbesondere für ressourcenarme Umgebungen wie mobile Geräte konzipiert und unterstützen keine vollständige Validierung.[44]

2. Kryptographie

Die Sicherheit und Funktionsweise der Blockchain-Technologie, insbesondere bei Bitcoin und Ethereum, beruhen nicht auf zentralem Vertrauen, sondern auf der Anwendung kryptographischer Verfahren. Sie ermöglichen es, dass eine Vielzahl anonymer bzw. pseudonymer Teilnehmer miteinander interagiert, ohne sich gegenseitig kennen oder vertrauen zu müssen. Authentizität, Unverfälschbarkeit und Nachvollziehbarkeit von Transaktionen werden vielmehr durch mathematisch überprüfbare Mechanismen gewährleistet.[45] 29

Im Zentrum stehen dabei zwei Verfahren: digitale Signaturen, die es ermöglichen, Transaktionen eindeutig einem Schlüsselinhaber zuzuordnen und dessen Berechtigung kryptographisch zu bestätigen, sowie Hash-Funktionen, welche die Integrität der Blockchain sicherstellen und Manipulationen erkennbar machen.[46] 30

a) Digitale Signatur und Schlüsselverwaltung

Jeder Nutzer einer Blockchain verfügt über ein kryptographisches Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel (Public Key) und einem privaten Schlüssel (Private Key).[47] Diese Schlüssel sind mathematisch miteinander verknüpft und erscheinen als lange alphanumerische Zeichenketten.[48] Der Private Key ist ein geheimer, zufällig generierter Schlüssel, der ausschliesslich dem Inhaber bekannt ist.[49] Aus ihm wird der Public Key abgeleitet, welcher 31

43 Vgl. ANTONOPOULOS/WOOD, S. 43; ANTONOPOULOS, S. 172 f.; BERENTSEN/SCHÄR, S. 75; RUTISHAUSER/KUBLI/WEBER, S. 16; ZOGG, Fn. 7.

44 Vgl. ANTONOPOULOS/WOOD, S. 55.

45 ERBGUTH, S. 339 f.; SPECOGNA, N 79; SURY, S. 245.

46 Vgl. zum Ganzen ANTONOPOULOS, S. 56 ff.; BÖHME et al., S. 216; MEYER, Token, N 35 f.; STENGEL / AUS DER AU, S. 442; STILLER/RODRIGUES/NEZHADSISTAN, N 2.15.

47 Vgl. Botschaft DLT, S. 19; ANTONOPOULOS, S. 56; BERENTSEN/SCHÄR, S. 119; SCHLATT et. al., S. 8; STENGEL / AUS DER AU, S. 442; STILLER/RODRIGUES/NEZHADSISTAN, N 2.29.

48 Vgl. BERENTSEN/SCHÄR, S. 84; FRANCO, S. 80; HEIN/WELLBROCK/HEIN, S. 8; STILLER/RODRIGUES/NEZHADSISTAN, N 2.29.

49 Vgl. ANTONOPOULOS, S. 56; HEIN/WELLBROCK/HEIN, S. 8; STENGEL / AUS DER AU, S. 442.

wiederum die Grundlage für die Blockchain-Adresse bildet, an welche Vermögenswerte transferiert werden können.[50]

32 Wird eine Transaktion ausgelöst, signiert der Absender sie mit seinem Private Key. Mithilfe des zugehörigen Public Keys kann das Netzwerk überprüfen, ob die Signatur gültig ist und somit vom berechtigten Absender stammt.[51] Die digitale Signatur erfüllt dabei eine doppelte Funktion: Einerseits gewährleistet sie die Authentizität der Transaktion, andererseits schützt sie deren Integrität, da jede nachträgliche Änderung des Transaktionsinhalts die Signatur ungültig machen würde.[52]

33 Das kryptographische Schlüsselpaar wird üblicherweise in einer sogenannten Wallet gespeichert.[53] Dabei handelt es sich um eine Software- oder Hardwarelösung, die mit dem Blockchain-Netzwerk interagiert und als Container für private Schlüssel fungiert. Die Wallet ermöglicht es Nutzern, ihre digitalen Vermögenswerte zu verwalten, zu übertragen oder auf diese zuzugreifen, ohne dass die Vermögenswerte selbst in der Wallet gespeichert werden.[54] Sie kann als digitale Geldbörse verstanden werden, die, anders als ein herkömmliches Portemonnaie, keine Werteinheiten selbst enthält, sondern lediglich den sicheren Zugriff auf die in der Blockchain verzeichneten Guthaben gewährt.[55]

34 Es gibt verschiedene Arten von Wallets, die jeweils unterschiedliche Sicherheits- und Zugriffseigenschaften bieten.[56] Hot Wallets sind mit dem Internet verbunden und ermöglichen einen schnellen Zugriff auf die Schlüssel, wodurch sie für häufige Transaktionen geeignet sind.[57] Im Gegensatz dazu werden Private Keys bei Cold Storage oder Paper Wallets offline aufbewahrt (bspw. auf physischen Datenträgern oder Papier), um sie besser gegen Online-Angriffe zu schützen.[58]

50 Vgl. ANTONOPOULOS, S. 57; BERENTSEN/SCHÄR, S. 84; HEIN/WELLBROCK/HEIN, S. 8; STALLINGS, S. 81; STENGEL / AUS DER AU, S. 442; STILLER/RODRIGUES/NEZHADSISTAN, N 2.29.

51 Vgl. ANTONOPOULOS/WOOD, S. 62; CONDOS et al., S. 8; HEIN/WELLBROCK/HEIN, S. 8; STALLINGS, S. 81 f.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.33.

52 Vgl. ANTONOPOULOS, S. 57; FRANCO, S. 79; STALLINGS, S. 79; vgl. auch BERENTSEN/SCHÄR, S. 101.

53 M.w.H. ANTONOPOULOS, S. 93 ff.; MEYER, Token, N 73 ff.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.81.

54 STILLER/RODRIGUES/NEZHADSISTAN, N 2.81; ANTONOPOULOS/WOOD, S. 79.

55 MEYER, Token, N 73.

56 M.w.H. BERENTSEN/SCHÄR, S. 240 ff.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.81 ff.

57 Vgl. ANTONOPOULOS, S. 7; BERENTSEN/SCHÄR, S. 241; FAVROD-COUNE, S. 52; MONNERAT, S. 5 f.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.83.

58 Vgl. BERENTSEN/SCHÄR, S. 243; FAVROD-COUNE, S. 52; MONNERAT, S. 5 f.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.83.

Auch eine gemeinschaftliche Verwaltung ist möglich: Sogenannte Multisig- 35
nature-Wallets (Multisig) erfordern für eine Transaktion mehrere Signaturen. Je nach Konfiguration sind bspw. zwei von drei oder drei von fünf gültigen Signaturen erforderlich. Solche Systeme erhöhen insbesondere bei institutionellen oder gemeinschaftlich verwalteten Vermögenswerten die Sicherheit.[59]

Neben der unmittelbaren Selbstverwaltung durch Einzelpersonen können 36
Wallets auch von Drittanbietern verwaltet werden. Man unterscheidet dabei zwischen non-custodial Wallets und custodial Wallets. Bei non-custodial Wallets behält der Nutzer die alleinige Kontrolle über den privaten Schlüssel und damit die volle Verfügungsmacht über seine Kryptowerte. Der Wallet-Anbieter beschränkt sich auf die Bereitstellung der technischen Infrastruktur und verfügt über keinerlei Zugriff auf die Vermögenswerte.[60] Demgegenüber verwaltet bei custodial Wallets ein Dritter, z.B. eine Kryptohandelsplattform, die privaten Schlüssel. Der Nutzer hat in diesem Fall oft nur Zugriff auf ein internes Konto, während die tatsächliche Kontrolle über die Vermögenswerte beim Anbieter liegt.[61] Transfers zwischen Nutzern desselben Anbieters können in solchen Fällen auch ausserhalb der Blockchain verbucht werden.[62]

b) Kryptographische Verbindung der Blöcke: Hash-Funktionen

Hash-Funktionen bilden ein zentrales kryptographisches Fundament der 37
Blockchain-Technologie. Sie gewährleisten die Integrität aufgezeichneter Transaktionen, indem jede nachträgliche Veränderung kryptographisch nachweisbar wird.[63]

Technisch handelt es sich dabei um deterministische Algorithmen, die 38
beliebig grosse Datenmengen in eine Zeichenkette fester Länge, den sogenannten Hash-Wert, überführen.[64] Bereits geringfügige Änderungen der Eingabedaten führen zu einem vollständig anderen Hash-Wert.[65] Hash-Funktionen

59 ANTONOPOULOS, S. 82; MEIRICH, N 153; MEYER, Token, N 75.

60 Botschaft DLT, S. 146; MEIRICH, N 82; OSWALD, S. 24 f.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.82.

61 Botschaft DLT, S. 146 f.; MEIRICH, N 83; OSWALD, S. 23 f.; STILLER/RODRIGUES/NEZHADSISTAN, N 2.82.

62 KRAMER/WYSS, S. 149; MEIRICH, N 83.

63 Vgl. STILLER/RODRIGUES/NEZHADSISTAN, N 2.26.

64 Während auf der Bitcoin-Blockchain der Hash-Algorithmus SHA-256 verwendet wird, der für jeden Dateninput einen 256 Bit langen Hash-Wert erzeugt, nutzt Ethereum die Variante Keccak-256, welche ebenfalls einen 256 Bit langen Hash-Wert liefert, jedoch nicht vollständig dem später standardisierten SHA-3 entspricht (vgl. ANTONOPOULOS/WOOD, S. 72; FRANCO, S. 125).

65 BADEV/CHEN, S. 9; BERENTSEN/SCHÄR, S. 99; CONDOS et al., S. 7; DE COL, N 11; MEYER/SCHUPPLI, S. 206.

wirken damit wie digitale Fingerabdrücke von Informationen: Dieselben Eingabedaten erzeugen stets denselben Output, ohne dass die ursprüngliche Eingabe mittels Hash rekonstruiert werden kann (Einwegfunktion). Zudem ist es bei sicheren Hash-Funktionen praktisch ausgeschlossen, zwei verschiedene Eingaben zu finden, die denselben Hash produzieren (Kollisionsresistenz).[66]

39 Diese Eigenschaften werden in Blockchains auf mehreren Ebenen genutzt. Jede Transaktion wird vor ihrer Aufnahme in einen Block gehasht, wobei der resultierende Hash als eindeutiger Identifikator dient. Bereits minimale Abweichungen im Transaktionsinhalt führen zu einem vollständig anderen Hash und machen Manipulationen unmittelbar erkennbar. Die Hash-Werte aller Transaktionen eines Blocks werden anschliessend in einer hierarchischen Struktur – dem sogenannten Merkle Tree – zusammengeführt. Dessen Spitze bildet der Merkle Root, ein einzelner Hash-Wert, der kryptographisch sämtliche Transaktionen des Blocks zusammenfasst.[67] Dieser Merkle Root wird im Block-Header gespeichert und gewährleistet die Integrität der im Block enthaltenen Daten.[68] Darüber hinaus enthält der Block-Header den Hash-Wert des unmittelbar vorhergehenden Blocks. Durch diese fortlaufende Verknüpfung entsteht eine chronologisch geordnete, kryptographisch gesicherte Kette von Blöcken – die Blockchain.[69] Eine nachträgliche Änderung einer Transaktion würde den Hash des entsprechenden Blocks und in der Folge sämtliche nachgelagerten Hash-Werte verändern, sodass die manipulierte Kette nicht mehr der gültigen und vom Netzwerk akzeptierten Version entsprechen würde. Die Verkettung der Blöcke mittels Hash-Funktionen bildet somit die technische Grundlage der Fälschungssicherheit und Unveränderbarkeit von Blockchains.[70]

3. Transaktionsablauf

40 Transaktionen bilden das funktionale Zentrum jeder Blockchain, da sie den digitalen Transfer von Werten zwischen den Teilnehmenden des Netzwerks bewirken. Sowohl bei Bitcoin als auch bei Ethereum handelt es sich dabei nicht um digitale Objekte, die lokal auf Geräten gespeichert sind, sondern um kryptographisch gesicherte Berechtigungen bezüglich bestimmter Einträge in der dezentral geführten Datenbank, der Blockchain. Die technische Ausgestaltung

66 GYR, Smart Contracts, Anhang N 5; MEYER, Token, N 48.

67 ANTONOPOULOS, S. 202; BERENTSEN/SCHÄR, S. 142; FRANCO, S. 126; STILLER/RODRIGUES/NEZHADSISTAN, N 2.27.

68 ANTONOPOULOS, S. 202; BERENTSEN/SCHÄR, S. 142; STILLER/RODRIGUES/NEZHADSISTAN, N 2.27.

69 BERENTSEN/SCHÄR, S. 142; MEYER, Token, N 36; STENGEL / AUS DER AU, S. 443.

70 Vgl. Botschaft DLT, S. 19 ff.; FRANCO, S. 125.

dieser Berechtigungen unterscheidet sich jedoch grundlegend: Während Bitcoin auf dem sogenannten UTXO-Modell basiert, verwendet Ethereum ein kontenbasiertes System.[71]

Im Bitcoin-Netzwerk manifestiert sich der Besitz von Einheiten nicht in 41
einem Kontostand, sondern in der Kontrolle über sogenannte Unspent Transaction Outputs (UTXOs), also über Transaktionsausgänge früherer Zahlungen, die noch nicht erneut ausgegeben wurden. Jede Transaktion referenziert solche UTXOs als Inputs und erzeugt neue Outputs, die wiederum in künftigen Transaktionen verwendet werden können.[72] Technisch gesehen besteht eine Bitcoin-Transaktion aus einer Liste von Inputs, die auf frühere Transaktionen verweisen, und einer Liste von Outputs, welche die Zieladressen und Beträge definieren.[73] Die Gültigkeit der Inputs wird durch die digitale Signatur des Senders nachgewiesen, die mit dem zugehörigen privaten Schlüssel erstellt wird und bestätigt, dass der Absender berechtigt ist, über die entsprechenden UTXOs zu verfügen.[74]

Im Gegensatz dazu verwendet Ethereum ein kontenbasiertes System, 42
das funktional eher einem klassischen Buchhaltungssystem als dem UTXO-Modell gleicht. Während Letzteres dem Umgang mit Bargeld ähnelt, bei dem jede ‹Münze› als separater Transaktionsausgang behandelt wird, funktioniert das Kontenmodell ähnlich wie eine Debitkarte: Der aktuelle Kontostand einer Adresse wird im Netzwerk geführt und bei jeder Transaktion aktualisiert.[75] Dabei wird der entsprechende Betrag direkt vom Konto des Absenders abgezogen und dem Konto des Empfängers gutgeschrieben. Es besteht somit ein globaler Zustand, der sämtliche Kontosalden abbildet und sich mit jedem neuen Block durch die aggregierten Transaktionen fortschreibt.[76]

Unabhängig davon, ob eine Transaktion nach dem UTXO-Modell (Bit- 43
coin) oder nach dem Kontenmodell (Ethereum) aufgebaut ist, muss sie nach ihrer Erstellung und Signatur zunächst vom Netzwerk verifiziert werden.

71 Vgl. STILLER/RODRIGUES/NEZHADSISTAN, N 2.71 ff.; FRANCO, S. 134; ANTONOPOULOS, S. 119; ZOGG, S. 99.

72 M.w.H. BERENTSEN/SCHÄR, S. 118; ANTONOPOULOS, S. 119 ff.; MEYER, Token, N 82; Botschaft DLT, S. 20; FRANCO, S. 103.

73 Vgl. Botschaft DLT, S. 20; ANTONOPOULOS, S. 119; BERENTSEN/SCHÄR, S. 118.

74 Botschaft DLT, S. 20; ANTONOPOULOS, S. 123; MEYER, Token, N 82; FRANCO, S. 103; zur digitalen Signatur vgl. vorne N 31 ff.

75 STILLER/RODRIGUES/NEZHADSISTAN, N 2.75; vgl. MEIRICH, N 62; MEYER, Token, N 86.

76 Vgl. HESS/LIENHARD, N 11; MEIRICH, N 62. Um zu verhindern, dass eine Transaktion mehrfach ausgeführt wird, verwendet Ethereum eine sogenannte Nonce. Hierbei handelt es sich um eine fortlaufende Zahl, die sicherstellt, dass jede Transaktion nur einmal gültig ist und in der richtigen Reihenfolge verarbeitet wird (STILLER/RODRIGUES/NEZHADSISTAN, N 2.75).

Dazu prüfen die Knotenpunkte (Nodes) die Gültigkeit der Signatur sowie die Verfügbarkeit der Mittel – bei Bitcoin anhand der referenzierten UTXOs, bei Ethereum anhand des Kontostands und der Nonce.[77] Besteht die Transaktion diese Prüfung, wird sie vorläufig im sogenannten Memory Pool gespeichert (bei Bitcoin als Mempool, bei Ethereum als Transaction Pool bezeichnet), wo sie auf ihre Aufnahme in den nächsten Block wartet.[78]

44 Bevor eine Transaktion dauerhaft in die Blockchain aufgenommen wird, muss das dezentrale Netzwerk Einigkeit darüber erzielen, welche Transaktionen gültig sind und in welcher Reihenfolge sie gespeichert werden.[79] Da es in Blockchains wie Bitcoin und Ethereum keine zentrale Instanz gibt, welche diese Entscheidung trifft, übernimmt der sogenannte Konsensmechanismus diese Funktion. Er sorgt dafür, dass alle Netzwerkteilnehmer denselben, einheitlichen Datenstand führen und eine gemeinsame Version der Transaktionsgeschichte speichern.[80] Erst wenn eine Transaktion im Rahmen dieses Konsensprozesses in einen gültigen Block aufgenommen wurde, gilt sie als bestätigt.

45 Bei Bitcoin übernehmen sogenannte Miner diese Aufgabe, indem sie mittels hoher Rechenleistung neue Blöcke im Rahmen des Proof-of-Work-Verfahrens erzeugen.[81] Ziel ist es, ein kryptographisches Rätsel zu lösen und einen Hash-Wert zu finden, der bestimmte mathematische Anforderungen erfüllt.[82] Der erste Miner, dem dies gelingt, veröffentlicht den neuen Block im Netzwerk.[83] Die übrigen Nodes überprüfen dessen Gültigkeit sowohl hinsichtlich der enthaltenen Transaktionen als auch bezüglich der Einhaltung der Protokoll- und Konsensregeln.[84] Wird der Block als gültig anerkannt, wird er an die bestehende Blockchain angehängt und von sämtlichen vollständigen Nodes in ihre lokale Kopie übernommen.[85]

77 Vgl. ANTONOPOULOS, S. 192; FRANCO, S. 141; HEIN/WELLBROCK/HEIN, S. 9; MEYER, Token, N 39; MONNERAT, S. 8; STENGEL / AUS DER AU, S. 440; ZOGG, S. 97.

78 Vgl. BERENTSEN/SCHÄR, S. 117; FRANCO, S. 141; LINDER, S. 17; MEYER, Token, N 39, 224; MÜLLER, Règles, S. 98 f.; SCHLATT et al., S. 10.

79 ANDREOTTI, S. 155; BRINKMANN, S. 778; MONNERAT, S. 8 f.; vgl. Botschaft DLT, S. 21.

80 Vgl. SIEGEL, S. 77 f.; MEYER, Token, N 26, 1018.

81 Vgl. MEYER, Token, N 41; MEYER/SCHUPPLI, S. 212 ff.; vgl. auch ANTONOPOULOS, S. 213 ff.

82 Vgl. ANTONOPOULOS, S. 27; BERENTSEN/SCHÄR, S. 149 f.; MEYER/SCHUPPLI, S. 212; SCHLATT et al., S. 10; STILLER/RODRIGUES/NEZHADSISTAN, N 2.36; ZOGG, S. 99.

83 BADEV/CHEN, S. 14; ZOGG, S. 97; vgl. ANTONOPOULOS, S. 213 f.

84 STILLER/RODRIGUES/NEZHADSISTAN, N 2.36.

85 ANTONOPOULOS, S. 27; BERENTSEN/SCHÄR, S. 150; MEYER, Token, N 47.

Im Ethereum-Netzwerk erfolgt die Konsensfindung seit der Umstellung auf Proof of Stake im Jahr 2022 durch sogenannte Validatoren.[86] Diese hinterlegen eine bestimmte Menge Ether als Einsatz (Stake), um am Validierungsprozess teilnehmen zu können.[87] Aus dem Kreis der aktiven Validatoren wird nach einem Zufallsverfahren ein Teilnehmer ausgewählt, der das Recht erhält, einen neuen Block mit Transaktionen aus dem Transaction Pool vorzuschlagen.[88] Weitere Validatoren überprüfen anschliessend den Blockvorschlag und bestätigen oder verwerfen ihn gemäss den Protokollregeln.[89] Wird der Block bestätigt, wird er in die Blockchain aufgenommen. 46

Die jeweils beteiligten Netzwerkteilnehmer (Miner bei Bitcoin, Validatoren bei Ethereum) erhalten für ihre Mitwirkung eine wirtschaftliche Belohnung in Form von protokollseitigen Vergütungen sowie Transaktionsgebühren.[90] 47

D. Zusammenfassung

Die Publikation des Bitcoin-Whitepapers im Jahr 2008 markiert den Ausgangspunkt einer technologischen Entwicklung, aus der hervorgegangen ist, dass der Begriff ‹Blockchain› nicht eine einheitliche Technologie bezeichnet, sondern ein Grundprinzip dezentral organisierter Datenverwaltung. Daten werden in Blöcken kryptographisch gesichert, chronologisch aneinandergefügt und auf vielen Computern gleichzeitig gespeichert, sodass ein gemeinsamer Datenbestand entsteht, der ohne zentrale Kontrollinstanz dauerhaft, transparent und manipulationsresistent geführt werden kann. 48

Die konkrete Ausgestaltung einer Blockchain variiert je nach Anwendungszweck und Netzwerkarchitektur. Insbesondere divergieren Systeme danach, wer die Daten einsehen kann (public vs. private Blockchains) und wer am Konsensmechanismus teilnehmen darf (permissionless vs. permissioned Blockchains). Für die im Folgenden untersuchten dezentralisierten Finanzanwendungen sind primär public, permissionless Blockchains relevant, da sie ohne institutionelle Intermediäre funktionieren und dadurch die strafrechtlich zentrale Frage nach Verantwortlichkeits- und Zurechnungsstrukturen aufwerfen. 49

86 Vgl. BOŠKIĆ/HEPP, S. 212; SIEGEL, S. 90.

87 Vgl. Botschaft DLT, S. 26; ANDREOTTI, S. 156; MAURENBRECHER/LEISINGER, Teil 1, S. 653; MEIRICH, N 55.

88 Vgl. BRINKMANN, S. 780; SIEGEL, S. 90.

89 STILLER/RODRIGUES/NEZHADSISTAN, N 2.36.

90 Vgl. BRINKMANN, S. 779 f.; MEIRICH, N 55; STILLER/RODRIGUES/NEZHADSISTAN, N 2.38.

50 Anhand der prototypischen Systeme Bitcoin und Ethereum wurde die grundlegende Funktionsweise öffentlicher Blockchains herausgearbeitet. Beide Netzwerke sind als Peer-to-Peer-Systeme ausgestaltet, in denen unterschiedliche Knotentypen Transaktionen empfangen, prüfen und speichern. Die Sicherheit beruht dabei nicht auf dem Vertrauen in eine zentrale Instanz, sondern auf kryptographischen Verfahren: Digitale Signaturen ordnen Transaktionen eindeutig einem Schlüsselinhaber zu und sichern ihre Integrität, während Hash-Funktionen durch die Verkettung der Blöcke die Unveränderbarkeit der gespeicherten Daten gewährleisten.

51 Es hat sich ferner gezeigt, dass der Ablauf von Transaktionen in beiden Netzwerken trotz unterschiedlicher Modellansätze vergleichbaren Grundmustern folgt. Während Bitcoin auf dem UTXO-Modell und Ethereum auf einem kontenbasierten System beruht, werden Transaktionen in beiden Fällen kryptographisch signiert, durch das Netzwerk verifiziert und im Rahmen eines Konsensmechanismus dauerhaft in die Blockchain aufgenommen. Bei Bitcoin erfolgt dies mittels Proof of Work durch Miner, bei Ethereum seit 2022 mittels Proof of Stake durch Validatoren. Beide Verfahren gewährleisten eine einheitliche Transaktionshistorie und die Konsistenz des Datenbestands im Netzwerk.

II. Smart Contracts

52 Blockchain-Systeme wie Bitcoin und Ethereum ermöglichen zwar beide die sichere Erfassung und Speicherung von Transaktionen, unterscheiden sich jedoch grundlegend in ihren technischen Fähigkeiten. Während das Bitcoin-Protokoll primär auf den zuverlässigen Transfer digitaler Werte ausgerichtet ist und nur eine sehr eingeschränkte, nicht-Turing-vollständige Skriptsprache zur Verfügung stellt, wurde Ethereum von Beginn an als Plattform für die Ausführung komplexer programmierbarer Logik konzipiert.[91]

53 Diese Erweiterung eröffnet funktional neue Anwendungsbereiche: Nutzer können nicht nur digitale Vermögenswerte übertragen, sondern auch Bedingungen festlegen, unter denen dies automatisch geschieht, etwa nach dem Muster ‹Wenn Ereignis A eintritt, übertrage Betrag X an Adresse B›.[92] Solche in der Blockchain ausgeführten programmierten Abläufe werden als Smart Contracts bezeichnet. Sie bestehen aus Code, der unverändert und deterministisch innerhalb der Ausführungsumgebung von Ethereum ausgeführt wird. Smart Contracts bilden damit eine wesentliche Weiterentwicklung der

91 Vgl. ANTONOPOULOS/WOOD, S. 3 ff.; MAUCHLE, Fintech, S. 826; MEIRICH, N 35; MEYER/SCHUPPLI, S. 204; SIEGEL, S. 96 f.

92 Vgl. MAUCHLE, Fintech, S. 826.

Blockchain-Technologie. Sie ermöglichen die automatisierte Umsetzung von Vereinbarungen zwischen pseudonymen Netzwerkteilnehmern und schaffen die Grundlage für komplexe, dezentral organisierte Anwendungen, insbesondere im Finanzbereich (Decentralized Finance bzw. DeFi), aber auch darüber hinaus.[93]

Im Folgenden wird das Konzept der Smart Contracts hinsichtlich seiner historischen Herkunft, seiner technischen Funktionsweise und seiner Einbettung in die Architektur der Ethereum-Blockchain näher erläutert. 54

A. Hintergrund

Der Begriff ‹Smart Contracts› wurde erstmals in den 1990er-Jahren von NICK SZABO geprägt.[94] In seinem gleichnamigen Whitepaper beschreibt SZABO digitale Protokolle, die vertragliche Vereinbarungen automatisch durchsetzen können, ohne dass eine zentrale Vertrauensinstanz erforderlich ist.[95] Die Grundidee besteht darin, Vertragspflichten technisch so umzusetzen, dass sie sich bei Eintritt bestimmter Bedingungen selbst ausführen.[96] SZABO entwickelte dieses Konzept zu einer Zeit, in der die dafür notwendige Infrastruktur – insbesondere eine dezentrale, manipulationssichere Ausführungsumgebung – noch nicht existierte.[97] Als plastisches Beispiel führte SZABO den Getränkeautomaten an, ein System, das beim Einwurf von Münzen automatisch ein Produkt ausgibt, ohne dass ein weiterer Interaktionsschritt mit dem Verkäufer erforderlich ist.[98] 55

Eine tatsächliche technische Umsetzung der Idee SZABOS wurde erst mit der Einführung der Ethereum-Blockchain durch VITALIK BUTERIN im Jahr 2015 ermöglicht. BUTERIN griff das Konzept der Smart Contracts auf und verband die Programmlogik direkt mit der Blockchain-Infrastruktur, sodass sich Code unveränderbar auf einer dezentralen Datenbasis ausführen lässt.[99] Auf diese Weise unterliegen sämtliche Netzwerkteilnehmer denselben Vertragsbedingungen, deren Einhaltung durch das Protokoll selbst sichergestellt wird.[100] 56

93 Vgl. MEYER/SCHUPPLI, S. 208 f.; SIEGEL, S. 97.

94 GLARNER/MEYER; N 2; GYR, Smart Contracts, N 216; MEYER/SCHUPPLI, S. 207; vgl. SZABO, Smart Contracts.

95 Vgl. SZABO, Smart Contracts.

96 MEIRICH, N 33; vgl. SZABO, Smart Contracts.

97 MAUCHLE, Fintech, S. 826; MEIRICH, N 34; MEYER/SCHUPPLI, S. 208; SPECOGNA, N 45; vgl. GYR, Smart Contracts, S. 86 f.

98 SZABO, Smart Contracts; vgl. auch MÜLLER, Smart Contracts, S. 334 f.; SPECOGNA, N 28.

99 MEIRICH, N 34; SPECOGNA, N 39.

100 MAUCHLE, Fintech, S. 826; MEIRICH, N 34.

57 Während das Bitcoin-Protokoll lediglich eine stark eingeschränkte, nicht-Turing-vollständige Skriptsprache unterstützt und nur einfach strukturierte Bedingungen zulässt, sind Smart Contracts auf Ethereum Turing-vollständig ausgestaltet.[101] Sie ermöglichen die Abbildung beliebig komplexer logischer Abläufe, einschliesslich Bedingungen, Schleifen, Speicheroperationen und potenziell unendlicher Berechnungen.[102] Ausgeführt werden die Programme in der Ethereum Virtual Machine (EVM), einer standardisierten virtuellen Laufzeitumgebung, die in jedem vollständigen Ethereum-Knoten integriert ist.[103]

B. Definition

58 Eine einheitliche Definition des Begriffes Smart Contract existiert bis heute nicht.[104] In der Fachliteratur finden sich sowohl technikorientierte als auch juristisch-funktionale Begriffsansätze, die sich in Abstraktionsgrad und inhaltlicher Ausrichtung teilweise erheblich unterscheiden.[105]

59 Der Begriffsgeber SZABO definierte Smart Contracts in den 1990er-Jahren als computerisiertes Transaktionsprotokoll, das die Bedingungen eines Vertrags ausführt.[106] Ziel solcher Mechanismen sei es, zentrale vertragliche Elemente, wie Zahlungsmodalitäten, Pfandrechte, Vertraulichkeit oder Vollstreckung, technisch abzubilden, dabei Abweichungen zu minimieren und den Bedarf an vertrauenswürdigen Dritten zu reduzieren.[107] Etwas vereinfacht versteht SZABO Smart Contracts als digital spezifizierte Versprechen, die innerhalb eines Protokolls eingelöst werden.[108]

60 Praktische Bedeutung erlangte das Konzept mit der Einführung der Ethereum-Blockchain.[109] VITALIK BUTERIN knüpfte an SZABOS Ansatz an und beschrieb Smart Contracts anschaulich als «cryptographic boxes that contain value and only unlock it if certain conditions are met».[110] In späteren Beiträgen charakterisierte er sie als Mechanismen, bei denen mehrere Parteien digitale

101 ANDREOTTI, S. 152 f.; HAUSER-SPÜHLER, N 57 f.; HUMBEL, S. 11.

102 BUTERIN, White Paper, S. 28; HUMBEL, S. 11; MEIRICH, N 35; WEF, DeFi, Fn. 3; vgl. auch MAUCHLE, Registrierungsvereinbarung, Fn. 47.

103 ANTONOPOULOS/WOOD, S. 297 ff.; SIEGEL, S. 98 f.; SPECOGNA, N 74; vgl. DE FILIPPI/WRAY/SILENO, S. 3.

104 FAVROD-COUNE/BELET, S. 1106; GYR, Smart Contracts, N 215; MÜLLER/SEILER, S. 318.

105 Vgl. SPECOGNA, N 42; GYR, Smart Contract, N 220.

106 SZABO, Blocks; vgl. ANDREOTTI, S. 73; GUILLAUME, S. 42; SPECOGNA, N 28.

107 SZABO, Blocks; ANDREOTTI, S. 73; SPECOGNA, N 29.

108 SZABO, Blocks; vgl. JACCARD/TORAL, S. 4; MEIRICH, N 33.

109 Vgl. MEIRICH, N 34 f.; SPECOGNA, N 39.

110 BUTERIN, Whitepaper, S. 13; vgl. MEIRICH, N 34.

Vermögenswerte in einen gemeinsam kontrollierten Programmcode einbringen, der diese Werte gemäss einer vordefinierten Formel und in Abhängigkeit externer Daten verteilt – wobei diese Daten zum Zeitpunkt des Vertragsschlusses noch unbekannt sein können.[111] BUTERIN betont dabei die programmatische Natur solcher Mechanismen, deren Ausführung durch zuvor festgelegte Bedingungen, nicht jedoch durch nachträgliche menschliche Entscheidungen, gesteuert wird.[112]

Weitere Definitionen in der technischen Literatur betonen ähnliche 61
Elemente, variieren jedoch je nach Anwendungskontext und Abstraktionsebene.[113] So bezeichnen ANTONOPOULOS/WOOD Smart Contracts «als unveränderliche Computerprogramme, die deterministisch innerhalb der Ethereum Virtual Machine als Bestandteil des Ethereum-Protokolls ausgeführt werden».[114] WILKENS/FALK definieren Smart Contracts als «Programme auf der Blockchain, die auf Basis einer Wenn-dann-Logik arbeiten, sodass bei Eintritt eines zuvor festgelegten Ereignisses (sogenannter Trigger) automatisch eine ebenfalls zuvor definierte Aktion (bspw. eine Transaktion) ausgeführt wird».[115]

Trotz unterschiedlicher Schwerpunktsetzungen besteht weitgehende 62
Einigkeit darüber, dass es sich bei Smart Contracts um Programme handelt, die auf einer Blockchain gespeichert sind und unter bestimmten Bedingungen automatisierte Abläufe ohne zentrale Instanz auslösen.

In der juristischen Literatur finden sich vereinzelt technikneutrale Defi- 63
nitionsversuche, welche jede computerbasierte, selbstauslösende Wenn-dann-Beziehung erfassen wollen.[116] Solche Ansätze abstrahieren jedoch von der spezifischen Ausführungsumgebung auf der Blockchain und erfassen weder deren rechtliche noch deren technische Besonderheiten in hinreichendem Masse. In der schweizerischen Doktrin hat sich daher ein technologiegebundener Begriffsansatz durchgesetzt.[117] So definiert etwa MEIRICH Smart Contracts als «blockchain-basierter, algorithmischer Programmcode für einen

111 Vgl. BUTERIN, Terminology.

112 Vgl. BUTERIN, Terminology.

113 Vgl. SPECOGNA, N 42; GYR, Smart Contract, N 220.

114 Vgl. ANTONOPOULOS/WOOD, S. 127.

115 WILKENS/FALK, S. 4.

116 FINCK, S. 5 ff.; für eine technologieneutrale Definition vgl. z.B. BÖRDING et al., S. 139; HECKELMANN, S. 505; KAULARTZ/HECKMANN, S. 618; KIPKER et al., 509; WEBER, Leistungsstörungen, N 4.

117 MÜLLER, Smart Contracts, S. 331; vgl. z.B. in der schweizerischen Literatur FURRER, S. 103; GLARNER/MEYER, N 18; LOHMANN, Maschinenerklärung, N 12; MEYER/SCHUPPLI, S. 208; MÜLLER/SEILER, S. 318 f.

automatisierten Leistungsaustausch nach der Logik einer Wenn-dann-Struktur und auf Basis digital prüfbarer Ereignisse».[118]

64 Überblicksweise lassen sich folgende Begriffsmerkmale identifizieren:[119]
- Software- bzw. Programmcode, basierend auf Blockchain-Technologie,
- der auf einer Blockchain gespeichert und ausgeführt wird,
- der bei Eintritt definierter Bedingungen automatisch operiert (Wenn-dann-Regel),
- dessen Ausführung manipulationssicher ist aufgrund kryptographisch abgesicherter Dezentralität
- und dessen Verhalten deterministisch, also unveränderlich und vorhersehbar, erfolgt.

65 Anknüpfend an diese Elemente wird in dieser Untersuchung folgende Definition zugrunde gelegt: Smart Contracts sind auf der Blockchain basierende Computerprogramme, die beim Eintritt bestimmter Bedingungen selbstausführend, manipulationssicher und deterministisch vorprogrammierte Funktionen ausführen.

66 Bei näherer Betrachtung zeigt sich jedoch, dass der Begriff Smart Contract potenziell irreführend ist. Zum einen suggeriert das Attribut ‹smart› eine Form künstlicher Intelligenz, die Smart Contracts jedoch nicht aufweisen, da sie keine autonome Entscheidungsfindung vornehmen, sondern strikt deterministisch vorgegebenen Regeln folgen. Zum anderen handelt es sich nicht um ‹Verträge› im rechtlichen Sinn, sondern um technische Mechanismen zur automatisierten Ausführung vordefinierter Abläufe.[120]

67 In der Literatur wird deshalb teilweise zwischen Smart Contract Code und Smart Legal Contracts unterschieden. Ersterer bezeichnet den hier verwendeten technischen Begriff und meint die operative Ausführung eines Programms auf einem dezentralen Register. Letzterer umfasst Bestrebungen, Vertragsinhalte so in Programmcode zu übertragen, dass deren rechtlich relevante Elemente automatisiert durchgesetzt werden können.[121] Gegenstand der vorliegenden Untersuchung ist ausschliesslich der Smart Contract Code

118 MEIRICH, N 39.

119 Vgl. CLACK/BAKSHI/BRAINE, S. 2; MEYER/SCHUPPLI, S. 209; MÜLLER, Smart Contracts, S. 331.

120 Vgl. FAVROD-COUNE/BELET, S. 1107; FINCK, S. 7 f.; GUILLAUME, S. 42; MEYER/SCHUPPLI, S. 209; MÜLLER, Smart Contracts, S. 332; SIEGEL, S. 97; WEBER, Leistungsstörungen, N 1 f.

121 CLACK/BAKSHI/BRAINE, S. 2; DRUMMER/NEUMANN, S. 349.

im engeren technischen Sinn, der als Grundlage automatisierter Prozesse innerhalb dezentralisierter Finanzanwendungen dient.

C. Zusammenfassung

Smart Contracts erweitern die Einsatzmöglichkeiten der Blockchain grundlegend, indem sie deren Funktion nicht auf die blosse Erfassung und Übertragung digitaler Werte beschränken, sondern programmierbare Logik unmittelbar auf der Blockchain ausführbar machen. Während Bitcoin lediglich einfach strukturierte, fest einprogrammierte Bedingungen erlaubt, wurde Ethereum gezielt als Plattform für die Ausführung komplexer, Turing-vollständiger Programmcodes entwickelt. Die Ethereum Virtual Machine stellt hierfür eine dezentrale und deterministische Laufzeitumgebung bereit. 68

Das Konzept selbst geht auf NICK SZABO zurück, der in den 1990er-Jahren technische Mechanismen konzipierte, die vertragliche Verpflichtungen automatisiert durchsetzen können, wobei eine praktische Umsetzung erst mit der Blockchain-Architektur von Ethereum möglich wurde. Heute besteht weitgehend Einigkeit darüber, dass Smart Contracts als Computerprogramme zu verstehen sind, die auf der Blockchain gespeichert und ausgeführt werden und bei Eintritt bestimmter Bedingungen selbstausführend, manipulationssicher und deterministisch vorprogrammierte Funktionen auslösen. Diese Begriffsmerkmale decken sich mit der in dieser Arbeit zugrunde gelegten Definition. 69

Die Bezeichnung ‹Smart Contracts› ist technisch wie rechtlich missverständlich. Massgeblich ist daher ein funktionales Verständnis als deterministischer Smart-Contract-Code, der automatisierte Abläufe innerhalb blockchainbasierter Finanzanwendungen ausführt. 70

III. Dezentralisierte Finanzanwendungen

A. Begriff und Merkmale

Die Möglichkeit, über Smart Contracts automatisierte und bedingungsabhängige Transaktionen auf einer Blockchain auszuführen, hat zur Entstehung zahlreicher Anwendungen geführt, welche zentrale Funktionen des traditionellen Finanzwesens (TradFi) in digitaler Form abbilden.[122] Grundlage bilden öffentliche, zugangsfreie Blockchains wie Ethereum, deren Smart-Contract-Funktionalität die direkte Integration komplexer Finanzlogiken auf Protokollebene ermöglicht. Solche blockchainbasierten Finanzanwendungen erlauben 71

122 Zu Smart Contracts vgl. vorne N 52 ff.

etwa den Transfer von Vermögenswerten, die Kreditvergabe oder den Tausch von Token, ohne dass zentrale Intermediäre eingeschaltet werden müssen.[123]

72 Innerhalb dieses breiten Spektrums hat sich mit Decentralized Finance ein Teilbereich herausgebildet, der Finanzdienstleistungen gezielt offen, intermediärsfrei und selbstverwaltet organisiert.[124] Der Begriff ‹Decentralized Finance› bezeichnet in diesem Zusammenhang einen dynamischen Bereich an der Schnittstelle von Blockchain-Technologie, digitalen Vermögenswerten und Finanzdienstleistungen. Ziel der zugrunde liegenden Protokolle ist es, zentrale Finanzintermediäre durch dezentrale Strukturen zu ersetzen und Finanzdienstleistungen direkt auf Basis von Smart Contracts über öffentliche, zugangsfreie Blockchains bereitzustellen.[125]

73 Eine allgemein anerkannte Definition des DeFi-Begriffs fehlt bislang.[126] In einem weiten Verständnis lässt sich DeFi als blockchainbasierte Finanzinfrastruktur oder als Kategorie dezentralisierter blockchainbasierter Anwendungen (DApps) auffassen.[127] SCHÄR beschreibt DeFi als blockchainbasiertes Ökosystem, das Smart Contracts zur Kreation finanzieller Protokolle in einer zugänglichen, transparenten, zusammensetzbaren und mehrheitlich selbstverwaltenden Art nutzt.[128] Nach ANDREOTTI umfasst Decentralized Finance «Dienstleistungen, die bisher typischerweise von Finanzintermediären erbracht worden sind, in einer dezentralen Art und Weise auf der Grundlage offener Computerprotokolle».[129] Der Bundesrat versteht darunter «ein alternatives Finanzökosystem, in dem Nutzer auf Basis der DLT Finanzdienstleistungen dezentral und unabhängig von Finanzinstituten und den regulatorischen Strukturen, die um das traditionelle Bankwesen herum aufgebaut wurden, nutzen können».[130] Die OECD wiederum beschreibt DeFi als die Replikation verschiedener Aktivitäten des traditionellen Finanzsystems in einer offenen, dezentralen, genehmigungsfreien und autonomen Weise.[131] Schliesslich definiert MEIRICH DeFi als eine «Smart Contract-basierte Infrastruktur zur intermediärslosen und automatisierten Inanspruchnahme von Finanz-

123 Vgl. vorne N 57.

124 Vgl. OECD, DeFi, S. 6; MAURENBRECHER/LEISINGER, Teil 1, S. 648.

125 M.w.H. ANDREOTTI, S. 75 ff.; EBA/ESMA, S. 7; MAURENBRECHER/LEISINGER, Teil 1, S. 648 ff.

126 BOŠKIĆ/HEPP, S. 211; HUMBEL, S. 10; MAURENBRECHER/LEISINGER, Teil 1, S. 648; MEIRICH, N 265; ZETZSCHE/ARNER/BUCKLEY, S. 173.

127 Vgl. ANDREOTTI, S. 178; HUMBEL, S. 10; SCHÄR, S. 154; WEF, DeFi, S. 6.

128 SCHÄR, S. 153; vgl. MEIRICH, N 255.

129 ANDREOTTI, S. 77.

130 Bundesrat, Digital Finance, S. 8.

131 Vgl. OECD, DeFi, S. 16.

dienstleistungen auf einer öffentlichen und zugangsfreien Blockchain […], die den Nutzern die alleinige Verwaltung ihrer virtuellen Vermögenswerte belässt».[132]

74 Die hierfür erforderliche Dezentralität zeigt sich in drei Dimensionen, die sich an einer in der technischen und regulatorischen Fachliteratur[133] verbreiteten Differenzierung orientieren und teilweise Überlegungen von BUTERIN[134] aufgreifen: Erstens betrifft dies die architektonische Dezentralität, verstanden als die Speicherung und Ausführung des Protokolls auf einer öffentlichen Blockchain, die von einer Vielzahl unabhängiger Netzwerkteilnehmer getragen wird. Zweitens ist die funktionale Dezentralität massgeblich, bei der die Nutzer die alleinige Kontrolle über ihre Vermögenswerte behalten. Drittens stellt die administrative Dezentralität sicher, dass keine einzelne Entität in der Lage ist, unilateral Änderungen an den Smart Contracts vorzunehmen oder die Protokollparameter zu steuern.[135]

75 Gerade die Ebene der administrativen Dezentralität erweist sich als massgeblich für die Einordnung einer Finanzanwendung als tatsächlich – das heisst idealtypisch – dezentral im engeren Sinne. Bei solchen idealtypisch dezentralen Systemen erfolgt die Interaktion ausschliesslich über unveränderlich programmierte Smart Contracts, wobei die Nutzer durch die alleinige Kontrolle ihrer privaten Schlüssel uneingeschränkte Verfügungsmacht über ihre digitalen Vermögenswerte behalten.[136] Anders stellt sich die Situation bei sogenannten administrierten Protokollen dar: Ist die Steuerungsarchitektur eines Smart Contracts derart ausgestaltet, dass einzelne Personen oder Personengruppen befugt sind, in dessen Ablauf einzugreifen, widerspricht dies dem Grundgedanken einer vollständig dezentralen Anwendung. In derartigen Fällen existieren häufig sogenannte Admin Keys, die privilegierten Akteuren tiefgreifende Eingriffe ermöglichen, etwa durch Änderungen am Quellcode, Anpassungen von Protokollparametern oder Zugriff auf im Smart Contract gesperrte Tokenbestände.[137]

76 Die begriffliche Unschärfe dessen, was unter ‹Dezentralität› zu verstehen ist, führt dazu, dass zahlreiche Anwendungen unter dem Etikett ‹DeFi›

132 MEIRICH, N 270.

133 ANDREOTTI, S. 77 f.; Financial Stability Board, S. 5 ff.; GOGEL et al., DeFi, S. 3 ff.; HUMBEL, S. 10; OECD, S. 16 ff.; WEF, DeFi. S. 7 ff.

134 BUTERIN, Decentralization.

135 Vgl. zum Ganzen ANDREOTTI, S. 77 f.; Financial Stability Board, S. 5 ff.; GOGEL et al., DeFi, S. 3 f.; HUMBEL, S. 10; MEIRICH, N 272; OECD, DeFi, S. 18; WEF, DeFi, S. 7.

136 MEIRICH, N 286 ff.; WEF, DeFi, S. 30.

137 MEIRICH, N 289 ff.; vgl. Financial Stability Board, S. 6; OECD, DeFi, S. 18; vgl. auch EJPD, NRA, S. 23; GAFI, VASP, S. 27.

firmieren, obwohl sie den Anforderungen eines enger gefassten (das heisst idealtypischen) DeFi-Verständnisses nicht genügen.[138] Ein grosser Teil dieser Systeme weist zwar formale Merkmale einer dezentralen Architektur auf, namentlich den Betrieb auf öffentlichen Blockchains, bleibt jedoch faktisch durch einzelne Akteure oder Instanzen administrierbar bzw. beeinflussbar. Streng genommen handelt es sich bei der überwiegenden Mehrzahl solcher Systeme nicht um ‹dezentrale›, sondern um ‹dezentralisierte› Anwendungen, also Protokolle, die technisch auf Verteilung ausgelegt sind, tatsächlich aber weiterhin über zentrale Steuerungs- oder Eingriffsmechanismen verfügen.

77 Da vollumfängliche Dezentralität im praktischen Betrieb gegenwärtig kaum realisiert wird, verwendet diese Arbeit systematisch den Begriff der ‹dezentralisierten Finanzanwendung›. Damit erfasst werden Protokolle, die auf öffentlichen Blockchains betrieben werden (architektonische Dezentralität) und den Nutzenden durch ein non-custodial Design die Kontrolle über ihre Vermögenswerte belassen (funktionale Dezentralität), auch wenn im Hintergrund weiterhin administrative Eingriffs- oder Steuerungsmöglichkeiten bestehen können.

78 Der Begriff der ‹dezentralisierten Finanzanwendung› dient somit als übergeordnete Bezeichnung für Systeme, die zwar technisch auf Verteilung ausgelegt sind und ohne klassische Intermediäre operieren, jedoch nicht die Anforderungen einer idealtypisch vollständig dezentralen Architektur erfüllen. Als ‹idealtypisch dezentral› werden in dieser Arbeit solche Systeme verstanden, bei denen die Interaktion ausschliesslich über unveränderlich programmierte Smart Contracts erfolgt und keine einseitigen Administrationsrechte oder privilegierte Steuerungszugänge bestehen.

79 Vor diesem begrifflichen Hintergrund werden die Bezeichnungen ‹Anwendung›, ‹Protokoll› und ‹Plattform› im Folgenden synonym verwendet, da sie jeweils dasselbe technische Konstrukt bezeichnen: Smart-Contract-basierte Systeme zur automatisierten Inanspruchnahme von Finanzdienstleistungen auf öffentlichen Blockchains.

B. Kryptowerte

80 Dezentralisierte Finanzanwendungen basieren technisch darauf, dass Werte nicht in Form physischer oder buchgeldähnlicher Einheiten übertragen werden, sondern ausschliesslich als digitale Einheiten, die auf einer Blockchain

138 Man spricht auch von CeFi, Fake-DeFi oder Decentralized in Name Only (vgl. ANKER-SØRENSEN/ZETZSCHE, S. 13; OECD, Lesson, S. 6; SCHULER/CLOOTS/SCHÄR, S. 214); Deutsche Bundesbank, S. 33, beschreibt eine reine Dezentralisation als ein Konstrukt theoretischer Natur.

geführt werden.[139] In der Praxis hat sich hierfür eine Vielzahl von Begriffen etabliert, die je nach technischer Ausgestaltung oder wirtschaftlicher Funktion unterschiedliche Akzente setzen. Für die vorliegende Untersuchung ist deshalb ein einheitliches und klar konturiertes Begriffsverständnis erforderlich.

Als ‹Kryptowährungen› (teilweise auch ‹virtuelle Währungen› genannt) 81
werden gemeinhin digitale Werte wie Bitcoin oder Ether verstanden, die primär als Zahlungsmittel dienen und direkt aus dem jeweiligen Blockchain-Protokoll hervorgehen.[140] Sie werden auch als ‹Coins› oder ‹native Token› bezeichnet, da sie integraler Bestandteil der jeweiligen Blockchain sind und zur Ausführung von Transaktionen oder zur Nutzung von Protokollfunktionen benötigt werden.[141] Darüber hinaus existieren zahlreiche weitere digitale Einheiten, die nicht durch das Grundprotokoll selbst entstehen, sondern durch Smart Contracts ausgegeben werden. Solche Token können ganz unterschiedliche Funktionen erfüllen: Sie können Tauschmittel, Anlageobjekte, Stimmrechte oder Zugangsberechtigungen verkörpern oder als Sicherheiten innerhalb dezentralisierter Finanzanwendungen dienen.[142] Technisch unterscheiden sie sich von Kryptowährungen vor allem dadurch, dass sie nicht ‹nativ› in der Blockchain angelegt sind, sondern programmatisch auf ihr erzeugt werden.[143]

Sowohl die FINMA in ihrer geldwäschereirechtlichen Aufsichtspraxis 82
als auch die GAFI in ihren internationalen Standards fassen sämtliche der genannten digitalen Einheiten unter den Sammelbegriffen der ‹virtuellen Vermögenswerte›, ‹kryptobasierten Vermögenswerte› oder ‹Krypto-Assets› zusammen.[144] Dieser umfasst sämtliche digital gespeicherten Werte, die wirtschaftlich verwertbar sind, übertragen werden können und als Zahlungsmittel, Investitionsobjekt oder Tauschgut dienen.[145] Für die vorliegende Arbeit wird der funktionale Sammelbegriff ‹Kryptowerte› verwendet. Er erfasst sowohl Kryptowährungen als auch sämtliche Arten von Token und entspricht damit inhaltlich dem Begriff der ‹virtuellen Vermögenswerte›. Beide Begriffe werden im Rahmen der Untersuchung synonym verwendet.[146]

139 Vgl. NOSER/INFANGER/LÜDI, N 12.01, 12.41 ff.

140 EFD, Erläuterungen, S. 23 f.; ANDREOTTI, S. 147 f.; MEIRICH, N 1309; LEHMANN, S. 193.

141 Vgl. Bundesrat, DLT, S. 36; ANDREOTTI, S. 147 f.; LEHMANN, S. 194; STILLER/RODRIGUES/NEZHADSISTANI, N 2.79.

142 Vgl. FINMA, Wegleitung, S. 3 ff.; SCHÄRLI, N 9.11 ff.; STILLER/RODRIGUES/NEZHADSISTANI, N 2.92 ff.

143 Vgl. Bundesrat, DLT, S. 36; STILLER/RODRIGUES/NEZHADSISTANI, N 2.80.

144 Vgl. FINMA, Vermögenswerte, S. 1 f.; GAFI, Indicators, S. 3 ff.; GAFI, Standards, S. 140; GAFI, VASP, S. 7 ff.

145 GAFI, Standards, S. 140.

146 Vgl. auch LEHMANN, S. 194.

83 Diese begriffliche Klärung ist vor allem deshalb erforderlich, weil dezentralisierte Finanzanwendungen nicht nur mit einem bestimmten Typ digitaler Einheiten operieren, sondern mit der Gesamtheit der auf einer Blockchain zirkulierenden Kryptowerte.[147] Für die strafrechtliche Analyse kommt es daher weniger auf die formale Klassifikation als Kryptowährung, Token oder virtueller Vermögenswert an als auf die technische Struktur der digitalen Einheiten und ihre Bewegungs-, Umwandlungs- und Verschleierungsmöglichkeiten innerhalb dezentraler Protokolle. Auf dieser Grundlage knüpfen die nachfolgenden Ausführungen an und untersuchen, wie Kryptowerte im Rahmen dezentralisierter Anwendungen typischerweise eingesetzt werden und welche Handlungen in geldwäschereirechtlicher Hinsicht relevant werden können.

C. Typologie dezentralisierter Finanzanwendungen

84 Auf Grundlage des zuvor entwickelten Begriffsverständnisses folgt eine systematische Darstellung ausgewählter Typen dezentralisierter Finanzanwendungen.[148] Berücksichtigt werden dabei solche Ausprägungen, die im heutigen DeFi-Ökosystem eine besondere praktische Bedeutung aufweisen und zur Übertragung, Umwandlung oder Umlagerung kryptobasierter Vermögenswerte eingesetzt werden.[149] Im Zentrum der Darstellung stehen dezentralisierte Handelsplattformen und Kryptomixer, da sie für die weiteren strafrechtlichen und geldwäschereirechtlichen Analysen von besonderer Bedeutung sind und deshalb vertieft behandelt werden. Weitere, im DeFi-Ökosystem verbreitete Anwendungstypen werden indes in zusammenfassender Form dargestellt.

1. Dezentralisierte Handelsplattformen

85 Dezentralisierte Handelsplattformen sind blockchainbasierte Anwendungen, die es Nutzern ermöglichen, unmittelbar und ohne Einschaltung zentraler Intermediäre Kryptovermögenswerte zu tauschen.[150] Innerhalb dieses Anwendungsbereichs existieren unterschiedliche technische Ausprägungen, die sich sowohl in ihrer Funktionsweise als auch im Grad der tatsächlichen Dezentralisierung unterscheiden.

86 Zur begrifflichen Einordnung ist zunächst zu klären, was nicht unter dezentralisierten Handelsplattformen zu verstehen ist: Bei custodial Handels-

147 Vgl. NOSER/INFANGER/LÜDI, N 12.41 ff.

148 Vgl. vorne N 71 ff.

149 Vgl. auch Botschaft DLT, S. 28; KGGT, NRA 2024, S. 17 ff.; KGGT, NRA 2018, S. 36 ff.; OECD, DeFi, S. 22 ff.; MEIRICH, N 366.

150 M.w.H. ANDREOTTI, S. 178, 340 f.; HUMBEL/ECKERT, S. 11; LIN, S. 58.

plattformen übernehmen die Betreiberinnen die Verwahrung der Kryptovermögenswerte ihrer Kunden. Die Vermögenswerte bzw. die zugehörigen Private Keys werden in zentralen Datenbanken gespeichert, sodass die Kunden die Kontrolle über ihre Kryptowerte vollständig abgeben.[151] Auch das Orderbuch und die Matching Engine sind zentralisiert und werden vom Plattformbetreiber auf eigenen Servern verwaltet. Der Eigentumswechsel an den Vermögenswerten wird lediglich in den internen Systemen der Plattform verzeichnet, nicht jedoch auf einer Blockchain (off-chain).[152] Custodial Handelsplattformen wie etwa Coinbase sind zudem meist an das traditionelle Bankensystem angebunden, was den Erwerb von Kryptovermögenswerten mittels Fiatwährungen erleichtert.[153] Solche Anwendungen stellen damit keine dezentralisierten Handelsplattformen im hier verwendeten Sinn dar, da Transaktionen und Vermögensverwaltung weiterhin zentral kontrolliert werden und Smart Contracts nicht als intermediärsfreie Abwicklungsmechanismen fungieren.

87 Demgegenüber beruhen Smart-Contract-basierte Handelsplattformen auf der Nutzung von Smart Contracts – typischerweise auf öffentlichen Blockchains wie Ethereum –, welche zentrale Handelsfunktionen wie die temporäre Bindung bzw. Bereitstellung von Vermögenswerten, die Führung eines Orderbuchs sowie das Order Matching zwischen Verkäufern und Käufern programmatisch abbilden. Der Tausch der Vermögenswerte wird dabei vollständig auf der Blockchain (das heisst on-chain) vollzogen und direkt durch den Smart Contract ausgeführt.[154]

88 Eine besondere Ausprägung stellen Liquiditätspool-basierte Handelsplattformen dar. Sie verzichten auf ein klassisches Orderbuch und nutzen stattdessen automatisierte Liquiditätspools, in die Nutzer Vermögenswerte einbringen und für den Handel zur Verfügung stellen.[155] Der Handel findet nicht zwischen zwei direkt gegenüberstehenden Marktteilnehmern statt, sondern gegen den Pool, dessen Preisbildung durch im Smart Contract hinterlegte mathematische Formeln gesteuert wird.[156]

151 Botschaft DLT, S. 28; ANDREOTTI, S. 185 f.; GOGEL et al., DeFi, S. 10.

152 Botschaft DLT, S. 28; ANDREOTTI, S. 187; HABERBECK, S. 314 f.

153 ANDREOTTI, S. 187.

154 Vgl. ANDREOTTI, S. 200; HUMBEL/ECKERT, S. 13; vgl. auch Botschaft DLT, S. 146 f.

155 Vgl. ANDREOTTI, S. 207; GOGEL et al., DeFi, S. 10; HUMBEL/ECKERT, S. 15; MEIRICH, N 391 ff.; WEF, DeFi, S. 10.

156 Vgl. BERGAULT et al., S. 2 ff.; ANDREOTTI, S. 208 f.; MEIRICH, N 392.

2. Kryptomixer

89 Öffentliche Blockchains speichern sämtliche Transaktionen dauerhaft und für jedermann einsehbar.[157] Nutzer treten dabei nicht unter ihrem Realnamen, sondern unter Wallet-Adressen auf, was als Pseudonymität bezeichnet wird.[158] Gleichwohl bleiben Transaktionspfade technisch vollständig nachvollziehbar, sodass sich Herkunft und Bewegung von Kryptowerten auch ohne Kenntnis der dahinterstehenden Personen rekonstruieren lassen.[159] Vermögenswerte mit nachweislich deliktischer Herkunft (Tainted Coins) verlieren dadurch ihre Fungibilität[160] und werden in der Praxis von Börsen, Zahlungsdienstleistern oder anderen Marktteilnehmern unter Umständen nicht mehr akzeptiert.[161]

90 Kryptomixer setzen an dieser strukturellen Transparenz an. Es handelt sich um Anwendungen, die darauf ausgelegt sind, die Rückverfolgbarkeit von Kryptovermögenswerten zu erschweren, indem sie die Verbindung zwischen der ursprünglichen Herkunft und der späteren Verwendung der Token aufbrechen. Ziel ist es, Vermögenswerte so in den Verkehr zurückzuführen, dass kein Rückschluss auf ihre Transaktionshistorie gezogen werden kann.[162]

91 Obwohl Kryptomixer in der Praxis häufig zur Verschleierung deliktischer Gelder eingesetzt werden, können sie auch legitime Zwecke erfüllen, etwa den Schutz finanzieller Privatsphäre in Staaten ohne effektiven Datenschutz, die Wahrung sensibler Geschäftsbeziehungen oder die Verhinderung der Offenlegung von Zahlungsflüssen bei Lohn- oder Spendenzahlungen.[163]

92 Technisch lassen sich zwei Grundformen unterscheiden: custodial und non-custodial Mixer.[164] Custodial Mixer sind zentral betriebene Dienste, bei denen eine Betreiberin als Intermediärin fungiert. Nutzer transferieren ihre

157 Vgl. Botschaft DLT, S. 26; BERENTSEN/SCHÄR, S. 117 ff.; MEISSER, S. 80; OSWALD, S. 21.

158 Vgl. Botschaft DLT, S. 26; Financial Stability Board, S. 32; MEYER, Token, N 178; OECD, DeFi, S. 11.

159 MEIRICH, N 1538; SIEGEL, S. 82; vgl. auch BERENTSEN/SCHÄR, S. 129.

160 Fungibilität bedeutet, dass einzelne Einheiten eines Vermögenswerts frei gegeneinander austauschbar sind, ohne dass es auf ihre konkrete Identität ankommt. Kryptowährungen wie Bitcoin oder Ether sind technisch gesehen vollständig fungibel, das heisst, jeder Token ist gleichwertig mit jedem anderen. Bei Tainted Coins ist diese Eigenschaft eingeschränkt, obwohl sie technisch unverändert bleiben. Die verringerte Fungibilität resultiert ausschliesslich aus ihrer rückverfolgbaren Transaktionshistorie, die eine Verbindung zu kriminellen Aktivitäten erkennen lässt (vgl. ANDREOTTI, S. 285 sowie zur Abgrenzung von fungiblen und nicht fungiblen Token S. 149).

161 Vgl. ANDREOTTI, S. 285.

162 Vgl. Botschaft DLT, S. 26 f.; ANDREOTTI, S. 285; DUPUIS/GLEASON, S. 66; VAHRENHOLT DE LUCENA, S. 202.

163 Vgl. MEIRICH, N 451; Elliptic, S. 23.

164 NADLER/SCHÄR, Tornado Cash, S. 124.

Token an eine von der Betreiberin kontrollierte Adresse und übermitteln die Zieladresse. Häufig geschieht dies über einen separaten Kommunikationskanal mittels verschlüsselter Nachrichten.[165] Anschliessend koordiniert die Betreiberin die Auszahlung entweder manuell oder mittels Software. Während dieses Prozesses verfügt sie über die vollständige Kontrolle über die eingezahlten Vermögenswerte. Hierbei kann sie die Gelder in Sammelkonten halten oder auf interne Wallets verteilen und dadurch die Auszahlung zeitlich, betragsmässig oder strukturell gestalten und somit die Herkunftszuordnung zusätzlich erschweren.[166]

Ein prominentes Beispiel für einen custodial Mixer war ‹ChipMixer›. Die 93
Anwendung wandelte eingezahlte Bitcoins in standardisierte Stückelungen (Chips) um, die ausschliesslich in der internen Systembuchhaltung geführt wurden und damit nicht in der Blockchain erschienen.[167] Nutzer erhielten private Schlüssel zu diesen Guthaben und konnten sie später an neue Adressen auszahlen lassen, wodurch anhand der öffentlich einsehbaren Blockchain-Daten keine Verbindung zur ursprünglichen Einzahlung mehr herstellbar war.[168] Auch der jüngst abgeschaltete Dienst ‹cryptomixer.io›, dessen Server 2025 im Kanton Zürich beschlagnahmt wurden, ist ein Beispiel für einen zentral betriebenen Mixer, welcher ein erhebliches Transaktionsvolumen aufwies. Nach Erkenntnissen der Ermittlungsbehörden wurden über die Plattform seit 2016 mehr als eine Milliarde Franken in Bitcoin gewaschen.[169]

Im Gegensatz dazu funktionieren non-custodial Mixer ohne zentrale 94
Verwahrstelle. Nutzer interagieren direkt mit einem öffentlich zugänglichen Smart Contract und zahlen dort eine standardisierte Menge an Kryptowährung ein.[170] Einzahlungen verschiedener Nutzer werden im Protokoll gesammelt, sodass sich eine gemeinsame Menge an Vermögenswerten bildet.[171] Später

165 Vgl. VAN WEGBERG/OERLEMANS/VAN DEVENTER, S. 423.

166 Vgl. GRZYWOTZ/KÖHLER/RÜCKERT, S. 755; HAUSER-SPÜHLER, S. 25; NADLER/SCHÄR, Tornado Cash, S. 123.

167 PAKKI et al., S. 36; vgl. Europol, One of the darkweb's largest cryptocurrency laundromats washed out.

168 PAKKI et al., S. 36.

169 COVIELLO/MÄDER/BAUMGARTNER. Es ist zu beachten, dass sich Kryptomixer als solche technisch nicht ‹abschalten› lassen. Bei blockchainbasierten Anwendungen betrifft eine behördliche Intervention grundsätzlich nicht den zugrunde liegenden Protokollcode oder bereits deployte Smart Contracts, sondern lediglich die peripheren Zugangspunkte. In der Praxis werden insbesondere Webinterfaces, Serverinfrastruktur, Domainnamen oder sonstige zentrale Komponenten des Dienstes stillgelegt oder beschlagnahmt. Die zugrunde liegende Funktionalität besteht jedoch weiter und kann über alternative Zugangswege erneut nutzbar gemacht werden.

170 NADLER/SCHÄR, Tornado Cash, S. 124.

171 Vgl. NIEDERNHUBER, § 16 N 102.

kann jede berechtigte Person einen gleich hohen Betrag an eine neu gewählte Adresse auszahlen lassen, ohne dass sich anhand der Blockchain ohne Weiteres rekonstruieren lässt, welche Einzahlung welcher Auszahlung entspricht.[172] Durch diesen Prozess entsteht ein sogenanntes Anonymitätsset: Je mehr Nutzer sich gleichzeitig am Mixer beteiligen, desto schwieriger wird es, einzelne Transaktionen miteinander zu verknüpfen.[173] Ein typisches Beispiel für einen non-custodial Mixer ist das ethereumbasierte Protokoll ‹Tornado Cash›.[174] Charakteristisch ist dabei der Einsatz kryptographischer Nachweise, welche es berechtigten Nutzern erlauben, eine Auszahlung zu veranlassen, ohne die eigene Identität oder die ursprüngliche Einzahlung offenlegen zu müssen.[175]

3. Weitere Typen

95 Neben dezentralisierten Handelsplattformen und Kryptomixern existiert eine Vielzahl weiterer Finanzanwendungen, die auf Smart Contracts beruhen und im DeFi-Ökosystem weit verbreitet sind. Gemeinsam ist diesen Anwendungen, dass sie Kryptowerte automatisiert verwalten, umschichten oder zeitweise binden, ohne dass eine zentrale Vermittlungsstelle eingeschaltet ist. Für die vorliegende Untersuchung stehen diese Anwendungstypen nicht im Zentrum und werden daher überblicksartig dargestellt.

96 Zu solchen Anwendungen zählen Kreditvergabeprotokolle, welche es Nutzern ermöglichen, Kryptowerte verzinslich zu verleihen oder gegen Hinterlegung von Sicherheiten Kredite aufzunehmen.[176] Die Abwicklung erfolgt über Smart Contracts, welche die Einzahlung der Vermögenswerte, die Berechnung von Zinsen sowie die Überwachung der hinterlegten Sicherheiten automatisiert steuern.[177] Sinkt der Wert der Sicherheiten unter eine vorgegebene Schwelle, kann der Smart Contract selbständig eine Verwertung auslösen. Die Funktionsweise ähnelt damit klassischen Kreditbeziehungen, erfolgt jedoch vollständig auf Protokollebene.

97 Eine weitere Gruppe bilden Mechanismen zur Erzielung automatisierter Erträge, namentlich Staking, Liquidity Mining und Yield Farming. In all diesen Fällen stellen Nutzer ihre Kryptowerte einem Protokoll zeitweise zur Verfügung, indem sie diese in einem Smart Contract hinterlegen.[178] Als Gegenleistung erhalten sie regelmässige Vergütungen, etwa in Form von Zinsen, Trans-

172 Vgl. NIEDERNHUBER, § 16 N 102; NADLER/SCHÄR, Tornado Cash, S. 123.
173 M.w.W. ANDREOTTI, S. 284.
174 Vgl. NADLER/SCHÄR, Tornado Cash, S. 124; NIEDERNHUBER, § 16 N 106.
175 NADLER/SCHÄR, Tornado Cash, S. 123; vgl. ANDREOTTI, S. 283.
176 EBA/ESMA, S. 39; EUBOF, S. 25; GOGEL et al., DeFi, S. 12; MEIRICH, N 399.
177 EBA/ESMA, S. 39; Financial Stability Board, S. 14; MEIRICH, N 409.
178 Vgl. MAURENBRECHER/LEISINGER, Teil 2, S. 708 f.; OECD, DeFi, S. 17.

aktionsgebühren oder zusätzlichen Token.[179] Während Staking primär der technischen Absicherung bestimmter Blockchains dient und Liquidity Mining an den Handel von Kryptowerten anknüpft, beschreibt Yield Farming eine Kombination verschiedener solcher Mechanismen zur Optimierung von Erträgen.[180]

Schliesslich dienen Cross-Chain-Technologien der Verbindung voneinander unabhängiger Blockchains.[181] Sie ermöglichen es, Kryptowerte, die auf einer bestimmten Blockchain ausgegeben wurden, in anderen Blockchain-Ökosystemen nutzbar zu machen.[182] Technisch geschieht dies regelmässig dadurch, dass die ursprünglichen Token auf der Ausgangsblockchain gesperrt und auf der Zielblockchain entsprechende Ersatz-Token erzeugt werden.[183] Cross-Chain-Bridges schaffen damit Interoperabilität zwischen ansonsten isolierten Systemen und erweitern die Einsatzmöglichkeiten von Kryptowerten über einzelne Blockchains hinaus.[184] 98

D. Zusammenfassung

Dezentralisierte Finanzanwendungen bezeichnen technologische Infrastrukturen, die zentrale Funktionen des traditionellen Finanzwesens unter Einsatz von Smart Contracts auf öffentlichen, zugangsfreien Blockchains abbilden. Unter dem Schlagwort ‹Decentralized Finance› hat sich dabei ein Bereich herausgebildet, der Finanzdienstleistungen gezielt intermediärsfrei und selbstverwaltet organisiert. Mangels einheitlicher Definition wird DeFi in der Literatur unterschiedlich weit gefasst. Übereinstimmend knüpfen die Definitionsansätze jedoch an eine auf öffentlichen Blockchains ausgeführte Protokollarchitektur an, setzen die alleinige Verfügungsmacht der Nutzer über ihre Vermögenswerte voraus und verneinen einseitige administrative Eingriffsmöglichkeiten. In der Praxis weisen zahlreiche unter dem Label ‹DeFi› firmierende Protokolle zwar dezentrale Strukturelemente auf, ohne aber die Anforderungen einer vollständigen Dezentralisierung durchgehend zu erfüllen. Die Bezeichnung ‹dezentralisierte Finanzanwendung› entspricht der tatsächlichen Ausgestaltung regelmässig eher als der Begriff ‹dezentral›, der eine vollumfängliche Dezentralisierung nahelegt. 99

179 Vgl. MEIRICH, N 428; ANDREOTTI/ZIMMERMANN/PRANTL, Fn. 17; GOGOL et al., S. 2.

180 FINMA, Staking, S. 3; Financial Stability Board, S. 15; GOGEL et al., DeFi, S. 1f.; MEIRICH, N 394, 415, 425; OECD, DeFi, S. 9.

181 Vgl. LI/WU/CUI, S. 149; GABBIADINI/GOBBI/RUBERA, S. 6; LEE et al., S. 2.

182 Vgl. AKARTUNA/MADELIN, S. 22; ANDREOTTI, S. 231; EBA/ESMA, S. 19, 68; Financial Stability Board, S. 9; GABBIADINI/GOBBI/RUBERA, S. 6.

183 Vgl. AKARTUNA/MADELIN, S. 22; EBA/ESMA, S. 68; Financial Stability Board, S. 9; LEE et al., S. 4; MEIRICH, N 439; VERMANDE.

184 Vgl. LI/WU/CUI, S. 149; MEIRICH, N 439; OU et al., S. 2.

100 Für das Verständnis dieser Anwendungen ist zentral, wie Werte innerhalb solcher Systeme technisch repräsentiert werden. Dezentralisierte Finanzanwendungen operieren nicht mit physischen oder buchgeldähnlichen Einheiten, sondern mit Kryptowerten, einem funktionalen Sammelbegriff, der sowohl Kryptowährungen (native Token bzw. Coins) als auch sämtliche durch Smart Contracts ausgegebenen Token umfasst.

101 Auf dieser Grundlage lassen sich verschiedene Typen dezentralisierter Finanzanwendungen unterscheiden. Von besonderer praktischer und strafrechtlicher Relevanz sind dabei dezentralisierte Handelsplattformen und Kryptomixer. Erstere ermöglichen den unmittelbaren Tausch von Kryptowerten über Smart Contracts, teils unter Einsatz automatisierter Liquiditätspools und algorithmischer Preisbildungsmechanismen. Kryptomixer zielen derweil auf die Erschwerung der Rückverfolgbarkeit von Kryptowerte-Transaktionen ab, indem sie die Verbindung zwischen Ein- und Auszahlung technisch aufbrechen. Aufgrund ihrer besonderen Bedeutung für Herkunftsverschleierung und Layering-Strategien stehen diese beiden Anwendungstypen im Zentrum der nachfolgenden Untersuchung.

102 Daneben existiert eine Vielzahl weiterer, im DeFi-Ökosystem verbreiteter Anwendungstypen, die in dieser Arbeit lediglich überblicksartig dargestellt wurden. Gemeinsam ist diesen Anwendungen, dass sie Kryptowerte automatisiert verwalten, binden oder umschichten und damit zusätzliche technische Möglichkeiten für Vermögensbewegungen schaffen.

IV. Akteure im Umfeld von dezentralisierten Anwendungen

103 Dezentralisierte Finanzanwendungen funktionieren nicht durch ein abstraktes Zusammenspiel der Blockchain, sondern durch das koordinierte Wirken verschiedener, klar voneinander abgrenzbarer Komponenten. Dieses Gefüge wird technisch durch Smart Contracts, organisatorisch durch die Betreiberin und praktisch-anwendungsbezogen durch die Nutzer geprägt. Die jeweiligen Rollen ergeben sich aus der Architektur der Anwendung und bestimmen, wer welchen Einfluss auf Funktionsweise, Nutzungsmöglichkeiten und Veränderungen des Systems hat.

104 Smart Contracts stellen das technische Fundament der Anwendung dar. Sie enthalten die programmatische Logik, nach der Transaktionen und sonstige systeminterne Operationen deterministisch ausgeführt werden.[185] Die Betreiberin sorgt für das Bereitstellen und die Aufrechterhaltung dieser Infrastruktur. Sie bringt den relevanten Code in die Blockchain ein (Deployment) und

185 Vgl. vorne N 52 ff.

verfügt – je nach Ausgestaltung – über administrativ-technische Steuerungsmöglichkeiten, etwa zur Anpassung von Parametern oder zur Durchführung von Updates.[186] Die Nutzer wiederum interagieren in der Rolle der Endanwender mit dem Protokoll, indem sie über Wallets Transaktionen an Smart Contracts auslösen und dadurch die vordefinierten Abläufe in Gang setzen, ohne dabei typischerweise unmittelbaren Einfluss auf die Struktur oder Weiterentwicklung des Systems auszuüben.[187]

Vor diesem Hintergrund untersucht das Kapitel die drei Komponenten 105
getrennt: zunächst die technische und strafrechtsdogmatische Einordnung von Smart Contracts, danach den funktionalen Begriff der Betreiberin und abschliessend die Rolle der Nutzer als Endanwender.

A. Smart Contracts

1. Autonomie und Automation

In den strafrechtlichen Handlungstheorien wird Handeln durchgehend als 106
vom menschlichen Willen gesteuertes Wirken begriffen, wie bspw. im Rahmen der finalen Handlungslehre als zielgerichtete (menschliche) Steuerung eines Kausalverlaufs.[188] Autonome technische Systeme stellen dieses Verständnis jedoch in Frage, weil sie aufgrund ihrer Unvorhersehbarkeit und fehlenden menschlichen Steuerung die finale Kausalbestimmung unterlaufen und sich damit der klassischen Zurechnungslogik entziehen. Deterministische technische Systeme gelten demgegenüber als vollständig steuerbare Werkzeuge, deren Wirken dem Menschen als ‹verlängerter Arm› zugerechnet wird.[189] In diesem Zusammenhang widmet sich die jüngere Literatur vermehrt der Frage, ob autonomen technischen Systemen ein strafrechtlich relevantes ‹Handeln› und damit eine potenzielle Subjektqualität zukommen kann.[190]

Einen einheitlichen Begriff ‹autonomer Systeme› gibt es bislang weder in 107
der Rechtswissenschaft noch in den technischen Disziplinen.[191] Im Allgemeinen wird unter Autonomie die Fähigkeit zur ‹Selbstgesetzlichkeit›, ‹Selbständigkeit› oder ‹Selbstbestimmung› verstanden.[192]

186 Vgl. WEF, DeFi, S. 23; vgl. auch OECD, DeFi, S. 21 f.

187 Vgl. STILLER/RODRIGUES/NEZHADSISTAN, N 2.68; MEYER/SCHUPPLI, S. 207.

188 SIMMLER, S. 143 f.; zur finalen Handlungslehre vgl. WELZEL, S. 40; DONATSCH/GODENZI/TAG, S. 96; STRATENWERTH/BOMMER, § 7 N 5; TRECHSEL et al., S. 84 f.

189 Vgl. SIMMLER, S. 144 ff.; vgl. auch VAN DEN HOVEN VAN GENDEREN, N 21, 25; SEHER, S. 46.

190 Vgl. z.B. GLESS/SILVERMAN/WEIGEND, S. 412; HILGENDORF, S. 114; LOHMANN, KI, S. 105; SEHER, S. 60; SIMMLER/MARKWALDER, S. 20 ff.

191 GORDON/LUTZ, S. 54; WILDHABER/LOHMANN, S. 136.

192 SIMMLER, S. 63 m.V.a. BRADSHAW et al., S. 18 f.; VAGIA/TRANSETH/FJERDINGEN, S. 191.

108 Ein technisches System gilt insofern als autonom, wenn es seine Funktionsweise zumindest teilweise selbst kontrolliert und ohne menschliche Intervention agieren kann.[193] Autonomie wird dabei nicht als binäre Eigenschaft verstanden, sondern als graduell abgestufte Fähigkeit, wobei der Grad technischer Eigenständigkeit variieren kann.[194] Von diesem Verständnis zu unterscheiden ist die Automation, welche die Fähigkeit beschreibt, eine ursprünglich menschliche Tätigkeit eigenständig zu übernehmen und ohne kontinuierliche menschliche Kontrolle auszuführen.[195] Der Automationsgrad bestimmt somit, in welchem Umfang der Mensch bei der konkreten Ausführung die Kontrolle behält. Hierbei kann er von manuell über teilautomatisiert bis hin zu vollständig automatisiert reichen.[196]

109 Zur Systematisierung technischer Autonomie wurden verschiedene Klassifikationsansätze entwickelt. Eine dreistufige Typologie stammt etwa von GLESS/WEIGEND.[197] Sie unterscheiden geschlossene Systeme mit vollständig vorgegebenen Datenverarbeitungsroutinen, geöffnete Systeme, die externe Daten nach vordefinierten Regeln verarbeiten, und intelligente Systeme, die grosse Datenmengen interpretieren und daraufhin eigenständig reagieren können.[198]

110 Ein differenzierterer Ansatz wird von SIMMLER/FRISCHKNECHT vorgeschlagen, der auf vier Merkmalen technischer Autonomie (Intransparenz, Indetermination, Adaptierbarkeit und Offenheit) beruht und zwischen fünf Autonomiestufen unterscheidet.[199] Intransparenz beschreibt die fehlende Nachvollziehbarkeit der Funktionsweise eines Systems, bei der die Schritte vom Input zum Output für Nutzer oder Beobachter nicht vollständig ersichtlich sind.[200] Indetermination liegt vor, wenn ein System auf denselben Input unterschiedliche Outputs erzeugen kann. Diese Nichtvorhersehbarkeit signalisiert einen höheren Grad an Eigenständigkeit, da das System nicht strikt auf

193 LOHMANN, Maschinenerklärung, N 31; BIERMANN, S. 236 f.; FOERSTER, S. 421; SOSNITZA, S. 765; SPECHT/HEROLD, S. 41; vgl. auch SIMMLER, S. 63.

194 LOHMANN, Maschinenerklärung, S. 19; SIMMLER, S. 64; vgl. BRADSHAW et al., S. 18 f.; vgl. auch LOH, Ethik, S. 79; MÜNCH, S. 37 f.; VAGIA/TRANSETH/FJERDINGEN, S. 191.

195 Vgl. PARASURAMAN/SHERIDAN/WICKENS, S. 287; VAGIA/TRANSETH/FJERDINGEN, S. 191; vgl. auch LOHMANN, Maschinenerklärung, N 31.

196 Vgl. ENDSLEY, S. 1388 ff.; FLEMISCH et al., S. 7; PARASURAMAN/SHERIDAN/WICKENS, S. 287; VAGIA/TRANSETH/FJERDINGEN, S. 192 ff.

197 Vgl. GLESS/WEIGEND, S. 562 f.

198 Vgl. zum Ganzen GLESS/WEIGEND, S. 562 f.; ähnliche Abgrenzungen machen auch DECKER, S. 24; DRITTENBASS, N 43; GORDON/LUTZ, S. 54 ff.; LOH, Roboterethik, S. 33; WAGNER/LUYKEN, S. 167 f., 170 f.; WIDMER LÜCHINGER, S. 6.

199 SIMMLER/FRISCHKNECHT, S. 239 ff.; SIMMLER/WEDER/FRISCHKNECHT, S. 81 ff.

200 SIMMLER/FRISCHKNECHT, S. 244.

vordefinierte Reaktionsmuster beschränkt ist, sondern situationsbezogen unterschiedliche Ergebnisse produzieren kann.[201] Die dritte Dimension, Adaptierbarkeit, bezeichnet die Fähigkeit eines Systems, aus Daten oder Erfahrungen zu lernen und daraufhin seine Verhaltensweise zu modifizieren. Ein solches System reagiert nicht nur auf externe Reize, sondern entwickelt über die Zeit ein verändertes Antwortverhalten, ohne dass menschliches Eingreifen erforderlich wäre.[202] Schliesslich meint Interaktivität bzw. Offenheit die Möglichkeit eines Systems, über seinen ursprünglichen Input hinauszugehen, indem es externe Datenquellen nutzt oder mit anderen Systemen kooperiert.[203]

Innerhalb des von SIMMLER/FRISCHKNECHT entwickelten Modells lässt 111
sich der Grad technischer Autonomie anhand von fünf aufeinander aufbauenden Stufen beschreiben. Das Spektrum reicht von vollständig transparenten und determinierten Systemen, bei denen identische Eingaben stets zu identischen Ergebnissen führen und weder Lernfähigkeit noch Offenheit bestehen, bis hin zu hochautonomen, dynamisch mit externen Daten verknüpften Systemen, deren Verhalten sich fortlaufend weiterentwickelt und sich menschlicher Kontrolle weitgehend entzieht.[204] Zwischen diesen beiden Polen finden sich Systeme, deren Funktionsweise zunehmend an Nachvollziehbarkeit und Vorhersehbarkeit verliert. Dazu zählen zunächst deterministische, jedoch teilweise intransparente Systeme, sodann solche, bei denen identische Inputs nicht mehr zwingend zu identischen Outputs führen und deren Verhalten nur noch eingeschränkt rekonstruierbar ist, sowie schliesslich lernfähige Systeme, die ihr Verhalten aufgrund maschineller Lernprozesse adaptiv anpassen. Mit jeder Stufe nimmt die Transparenz ab und die Möglichkeit eigenständiger Reaktionen jenseits ursprünglich definierter Vorgaben zu.[205]

2. Technische Einordnung von Smart Contracts

Gemäss der aufgearbeiteten Definition handelt es sich bei Smart Contracts um 112
auf der Blockchain ausgeführte Computerprogramme, die beim Eintritt bestimmter Bedingungen selbstausführend, manipulationssicher und deterministisch vordefinierte Funktionen auslösen.[206] Bereits daraus ergibt sich, dass es sich um hochgradig automatisierte, nicht aber autonome Systeme handelt.

201 Vgl. MÜLLER-HENGSTENBERG/KIRN, S. 61; LOH, Ethik, S. 81; LOH/LOH, S. 40.

202 Vgl. ALONSO/MONDRAGÓN, S. 1 ff.; SARTOR/OMICINI, S. 49; SIMMLER/FRISCHKNECHT, S. 244.

203 SIMMLER/FRISCHKNECHT, S. 243.

204 SIMMLER/FRISCHKNECHT, S. 245 f.

205 SIMMLER/FRISCHKNECHT, S. 245 f.

206 Vgl. vorne N 57 ff.

Diese Einordnung wird durch die Taxonomien von GLESS/WEIGEND sowie SIMMLER/FRISCHKNECHT gestützt.

113 Das von GLESS/WEIGEND vorgeschlagene dreistufige Klassifikationsmodell verortet Smart Contracts eindeutig auf der untersten Stufe:[207] Sie entsprechen geschlossenen Systemen, bei denen sowohl die Datenaufnahme als auch die Verarbeitung abschliessend festgelegt sind. Externe Faktoren haben auf ihre Funktionsweise keinen Einfluss und ihre Operationen sind vollständig determiniert.

114 Auch unter Anwendung der von SIMMLER/FRISCHKNECHT entwickelten Kriterien technischer Autonomie zeigt sich ein geringer Eigenständigkeitsgrad.[208] So sind sie vollständig transparent, weil ihr Quellcode öffentlich einsehbar ist und sämtliche Verarbeitungsschritte vom Input bis zum Output rekonstruiert werden können. Ebenso fehlt es an jeglicher Indetermination, da identische Eingaben ausnahmslos zu identischen Ergebnissen führen und weder Zufallselemente noch kontextabhängige oder externe Variablen berücksichtigt werden, die abweichende Resultate hervorrufen könnten. Eine Adaptierbarkeit ist auch nicht gegeben. Smart Contracts verfügen über keine Lernfähigkeit, passen ihr Verhalten nicht an und verändern ihren Code nicht selbständig. Sie stellen vielmehr in sich geschlossene Programme mit fest umrissenem Funktionsumfang dar, deren Interaktionsmöglichkeiten strikt auf das ursprünglich programmierte Regelwerk beschränkt bleiben. In der Gesamtschau sind Smart Contracts damit vollständig transparent, determiniert, nicht adaptiv sowie nicht offen und folglich auf der untersten Stufe technischer Autonomie einzuordnen.

115 Eine weitere klare Abgrenzung ergibt sich im Vergleich zu verkörperten technischen Systemen wie Robotern. Smart Contracts verfügen weder über Sensorik noch über physische Aktoren oder eine Interaktion mit der realen Umwelt. Ihre Wirkung entfalten sie ausschliesslich auf der Datenebene innerhalb digitaler Infrastrukturen.

116 Daraus folgt, dass Smart Contracts deterministische Systeme darstellen, die starren ‹Wenn-dann›-Logiken folgen und nur ausführen, was zuvor programmatisch festgelegt wurde.[209] Aufgrund dieser fehlenden Eigenständigkeit kommt ihnen keine autonome Wirkung zu. In der Literatur herrscht weitgehend Einigkeit darüber, dass deterministische technische Systeme nicht als strafrechtliche Handlungssubjekte in Betracht gezogen werden können, sondern als Werkzeuge menschlicher Steuerung fungieren.[210]

207 Vgl. vorne N 109.

208 Vgl. vorne N 110 f.

209 Vgl. LOHMANN, Maschinenerklärung, N 14.

210 Vgl. VAN DEN HOVEN VAN GENDEREN, N 21, 25; SEHER, S. 46; SIMMLER, S. 151.

B. Betreiberschaft

Die nachfolgenden Ausführungen befassen sich mit der Frage, was unter dem ‹Betreiben› dezentralisierter Finanzanwendungen zu verstehen ist. Ausgangspunkt bildet der typische Lebenszyklus solcher Systeme, der von der Entwicklung über das Deployment bis hin zum Betrieb im engeren Sinne reicht. Auf dieser Grundlage wird ein funktionaler Betreiberbegriff entwickelt, der sowohl idealtypisch dezentral konzipierte Anwendungen als auch Protokolle mit zentralisierenden Elementen zu erfassen vermag. 117

1. Lebenszyklus von Finanzanwendungen

Dezentralisierte Finanzanwendungen wie Handelsplattformen oder Kryptomixer können in ihrer konkreten Ausgestaltung erheblich variieren, folgen jedoch in der Regel einem vergleichbaren Grundmuster. Typischerweise lassen sich drei Phasen unterscheiden: Entwicklung, Deployment und Betrieb im engeren Sinne, deren konkrete Ausprägung je nach Projekt unterschiedlich sein kann.[211] 118

In der Entwicklungsphase erfolgen die technische Konzeption und die Programmierung durch ein Entwicklerteam. Im Zentrum steht dabei die Erstellung der zugrunde liegenden Smart Contracts.[212] Bei einem Teil der Anwendungen werden die Smart Contracts mitsamt lesbarem Quellcode öffentlich zugänglich gemacht (wie z.B. über Plattformen wie ‹GitHub›)[213], um Transparenz zu gewährleisten und unabhängige Prüfungen durch Dritte zu ermöglichen. Andere Projekte veröffentlichen den Code nur teilweise oder überhaupt nicht; dort ist für die Nutzer nach der Veröffentlichung lediglich der auf der Blockchain gespeicherte maschinenlesbare Bytecode einsehbar.[214] 119

Nach Abschluss der Entwicklung werden die Smart Contracts im Rahmen des Deployments auf der Ziel-Blockchain veröffentlicht und damit on-chain für sämtliche Nutzer zugänglich gemacht.[215] Abhängig von der Architektur sind sie anschliessend grundsätzlich nicht mehr ohne Weiteres veränderbar. Gleichwohl enthalten die meisten Anwendungen technische Mechanismen, die eine spätere Modifizierung ermöglichen.[216] 120

211 Vgl. WEF, DeFi, S. 23; vgl. auch OECD, DeFi, S. 21 f.

212 M.w.H. ANTONOPOULOS/WOOD, S. 128 ff.; HUMBEL, S. 23; MAURENBRECHER/LEISINGER, Teil 2, S. 715.

213 GitHub ist eine webbasierte Plattform zur Versionsverwaltung und kollaborativen Softwareentwicklung (vgl. MANTZ, § 32.6 N 1).

214 MEIRICH, N 134; vgl. ZHOU et al., S. 1373.

215 Vgl. HUMBEL, S. 23; JACQUEMART, N 545; MAURENBRECHER/LEISINGER, Teil 2, S. 715.

216 Vgl. MEIRICH, N 179, 218 f.; ANTONOPOULOS/WOOD, S. 129; SALEHI/CLARK/MANNAN, S. 2 ff.

121 An das Deployment schliesst sich die Betriebsphase im engeren Sinne an. In dieser Phase werden Aufgaben wie die fortlaufende technische Pflege (etwa Bugfixes oder Weiterentwicklungen, sofern die Architektur entsprechende Modifikationen zulässt), die Bereitstellung bzw. das Hosting eines graphischen Benutzerinterfaces (bspw. einer Weboberfläche zur Interaktion mit den Smart Contracts) sowie die Festlegung betrieblicher Parameter (etwa Gebührenhöhen oder Routing-Mechanismen) durch ein fortbestehendes Kernteam wahrgenommen.[217] In der Praxis handelt es sich dabei regelmässig um dieselben Personen oder Gruppen, die bereits für die Entwicklung und das Deployment verantwortlich waren.[218]

122 Zwar streben einzelne Projekte eine spätere Überführung der Entscheidungsbefugnisse in eine kollektive Verwaltungsform wie eine sogenannte Dezentrale Autonome Organisation (DAO) an.[219] In der Realität bleibt eine solche Governance-Struktur jedoch häufig formell oder nur begrenzt wirksam, während wesentliche Funktionen weiterhin durch wenige Kernakteure bestimmt werden.[220]

2. Betreiben

123 Der Begriff der ‹Betreiberin› findet sich in zahlreichen Rechtsgebieten im Zusammenhang mit technischen Anlagen oder Infrastrukturen wie bspw. im Eisenbahngesetz (z.B. Art. 2 lit. a EBG; «Infrastrukturbetreiberinnen»), im Kernenergiegesetz (z.B. Art. 12 Abs. 1 KEG; «Kernanlage betreiben»), im Informationsschutzgesetz (z.B. Art. 74 ISG; «Betreiberinnen kritischer Infrastrukturen»), im Fernmeldegesetz (z.B. Art. 32a FMG; «Betreiben von Fernmeldeanlagen»), im Umweltschutzgesetz (z.B. Art. 32a^{sexies} USG; «Betreiber elektronischer Plattformen») oder im Finanzmarktinfrastrukturgesetz (z.B. Art. 112 Abs. 1 lit. b FinfraG; «Betreiber eines organisierten Handelssystems»). Gemeinsam ist diesen Verwendungen, dass die Betreibereigenschaft typischerweise eine tatsächliche, auf eine gewisse Dauer angelegte Kontrolle bzw. eine

217 HUMBEL, S. 23.

218 Vgl. MAURENBRECHER/LEISINGER, Teil 2, S. 715.

219 Eine DAO verfolgt den Zweck, gemeinsame Ressourcen oder Projekte ohne zentrale Instanz kollektiv zu verwalten (vgl. RIVA, S. 602 ff.; GOGEL et al., DAO, S. 6 ff.; GUILLAUME, S. 46 ff.; MEYER, DAO, S. 322; PASQUIER/BÄRTSCHI, S. 200 ff.). Sie kann definiert werden als eine blockchainbasierte Entität, die kollektiv von ihren Mitgliedern gesteuert wird. Governance-Rechte werden typischerweise in Form von Token ausgeübt, wobei über Mittelverwendung und andere wesentliche Entscheidungen online abgestimmt wird (GUILLAUME/RIVA, S. 206; vgl. auch HASSAN / DE FILIPPI, S. 2; BUTERIN, Terminology; MIENERT, S. 52; WEBER, DAO, N 2).

220 Vgl. OECD, DeFi, S. 21 f.; FRITSCH/MÜLLER/WATTENHOFER, S. 6 f.; NADLER/SCHÄR, Decentralized Finance, S. 34; TAMAI/KASAHARA, passim.

Entscheidungs- und Verantwortungskompetenz über die betreffende Infrastruktur voraussetzt.[221]

Die Bestimmung der Betreiberin gestaltet sich im Kontext dezentralisierter Finanzanwendungen besonders anspruchsvoll. Ihrem idealtypischen Selbstverständnis nach sollen diese Systeme gerade ohne eine kontrollierende Instanz auskommen. So interagieren Nutzer unmittelbar mit dem Code, ohne dass ein Intermediär zwischengeschaltet ist. Dieses Idealbild wird in der Realität jedoch häufig nicht eingelöst. Vielmehr lässt sich bei einem Grossteil der Anwendungen eine faktisch steuernde Instanz identifizieren.[222] 124

Vor diesem Hintergrund ist für die vorliegende Analyse ein funktionaler Betreiberbegriff zugrunde zu legen, der auch auf idealtypisch dezentral konzipierte Finanzanwendungen anwendbar ist. In einem weiten Verständnis erfasst das Betreiben nicht nur das Betreiben im engeren Sinne, das heisst die laufende technische und organisatorische Kontrolle, sondern auch die initiale Bereitstellung der Anwendung, namentlich durch das Deployment der relevanten Smart Contracts. Die Betreibertätigkeit im engeren Sinn gliedert sich dabei in zwei zentrale Komponenten, das Backend und das Frontend. Das Backend bezeichnet den technischen Kernbereich, der im Hintergrund die Funktionsweise des Protokolls steuert und insbesondere die Logik der Smart Contracts umfasst. Das Frontend bildet wiederum die sichtbare Benutzeroberfläche, über welche die Nutzer mit der Anwendung interagieren (z.B. über eine Weboberfläche).[223] 125

Auf der Backend-Ebene bedeutet ‹Betreiben› primär die administrative Kontrolle über die zugrunde liegenden Smart Contracts. Darunter fällt insbesondere die Fähigkeit, nachträgliche Veränderungen vorzunehmen oder operative Parameter zu konfigurieren.[224] Von besonderer Bedeutung ist dabei die häufig eingesetzte Proxy-Architektur, die es ermöglicht, trotz der grundsätzlichen Unveränderlichkeit von Smart Contracts nachträgliche Anpassungen vorzunehmen.[225] In diesem Modell interagieren die Nutzer stets mit demselben Proxy Contract, der sowohl die Adresse als auch den gespeicherten Zustand (z.B. Guthabenstände) bewahrt.[226] Die eigentliche Geschäftslogik ist dagegen in einem separaten Logic Contract hinterlegt, auf den der Proxy 126

221 Vgl. auch HAAS, S. 32; CONSTANTIN, N 675.

222 Vgl. vorne N 76; ANKER-SØRENSEN/ZETZSCHE, S. 13; OECD, Lesson, S. 6; SCHULER/CLOOTS/SCHÄR, S. 214.

223 Vgl. ANTONOPOULOS/WOOD, S. 268 ff.; MEIRICH, N 75.

224 Vgl. MEIRICH, N 179 ff.; vgl. auch SALEHI/CLARK/MANNAN, S. 2 ff.

225 Vgl. MEIRICH, N 198 ff.; BLOCHER, N 49.

226 Vgl. MEIRICH, N 199.

verweist. Soll eine Anwendung aktualisiert oder erweitert werden, genügt es, den Logic Contract auszutauschen, während der Proxy und damit auch die gespeicherten Daten unverändert bleiben.[227] Für die Nutzer erscheint dies wie ein ‹Update›, ohne dass sie ihr Interaktionsverhalten anpassen müssen. In einzelnen Anwendungen besteht zudem die Möglichkeit einer vollständigen Deaktivierung, etwa über einen sogenannten Kill Switch, der die weitere Nutzung technisch unterbindet.[228]

127 Auf der Frontend-Ebene umfasst das Betreiben dagegen die Aufrechterhaltung eines Webinterfaces, das als graphische Benutzeroberfläche den Zugang zur Anwendung vermittelt.[229] Fortgeschrittene Nutzer können auch ohne ein graphisches Webinterface direkt mit den Smart Contracts interagieren. Dies erfolgt etwa über Wallets, die das Ausführen einzelner Contract-Funktionen erlauben, über Blockchain-Explorer, die neben der Anzeige von Transaktionen auch ein einfaches Contract-Interface bereitstellen, oder über spezielle Programme, mit denen sich Transaktionen direkt an einen Blockchain-Knoten senden lassen.[230]

128 Die Frage, wer eine dezentralisierte Finanzanwendung betreibt (im engeren Sinne), knüpft unmittelbar an die vorstehend dargestellten administrativen Kontrollmechanismen an. Die konkrete Administration der zugrunde liegenden Smart Contracts kann dabei in unterschiedlicher technischer Form ausgestaltet sein. Im einfachsten Fall erfolgt sie über einen externen Account (Externally Owned Account), der durch einen einzelnen Private Key gesteuert wird und exklusiven Zugriff auf die Protokollfunktionen gewährt.[231] Alternativ kann die Kontrolle über eine sogenannte Multisignatur-Struktur (Multisig) erfolgen, bei der Änderungen nur mit der Signatur mehrerer vordefinierter Schlüsselparteien möglich sind.[232] Schliesslich existiert mit einer DAO eine Form kollektiv organisierter Governance, bei der über Modifikationen mittels tokenbasierter Abstimmungen entschieden wird.[233]

227 Vgl. MEIRICH, N 199.

228 Vgl. zum Ganzen MEIRICH, N 179 ff.; vgl. auch IVANOV/GUO/YAN, S. 1 ff.; OpenZeppelin; PALLADINO.

229 Vgl. ANTONOPOULOS/WOOD, S. 269 f.; BOŠKIĆ/HEPP, S. 213; CURCHOD/PASQUIER, S. 248; EBA/ESMA, S. 12 f.; GAFI, VASP, S. 26 f.; MEIRICH, N 76; NOSER/INFANGER/LÜDI, N 12.04; OECD, DeFi, S. 61; WEF, DeFi, S. 6.

230 Vgl. MEIRICH, N 1350 ff.; MAURENBRECHER/LEISINGER, Teil 1, S. 651.

231 M.w.H. MEIRICH, N 72, 148 ff.; ANTONOPOULOS/WOOD, S. 26; MEYER, Token, N 85.

232 M.w.H. MEIRICH, N 152 ff.; ANTONOPOULOS/WOOD, S. 124 f.; OECD, DeFi, S. 60; WEF, DeFi, S. 9.

233 M.w.H. MEIRICH, N 157 ff.; GOGEL et al., DAO, S. 4 ff.; GOGEL et al., Toolkit, S. 4 ff.; GYR, DAO, N 7 ff.; KLAAS, S. 162 f.

Zusammenfassend wird im Rahmen dieser Untersuchung der Begriff der Betreiberin einem weiten Begriffsverständnis zugeführt. Betreiberin ist jene Akteurin, die das Deployment der Smart Contracts – das heisst die Veröffentlichung des Codes – vornimmt und resp. oder über effektive Steuerungsmöglichkeiten sowohl im Backend (z.B. durch Admin Keys, Upgrade-Funktionalitäten oder Protokollparameter) als auch, sofern vorhanden, im Frontend (z.B. durch den Betrieb oder die Kontrolle des Webinterfaces) verfügt und dadurch die Anwendung faktisch kontrollieren oder konfigurieren kann. Bei idealtypisch dezentralen Anwendungen erschöpft sich das Betreiben hingegen im Deployment, weil nach der Veröffentlichung der Smart Contracts weder technische Eingriffs- noch nachträgliche Steuerungsmöglichkeiten bestehen und der weitere Ablauf ausschliesslich durch den unveränderlichen Programmcode bestimmt wird. 129

C. Nutzer

Als ‹Nutzer› wird im technischen Kontext jene Person verstanden, die eine Technologie situativ aktiv anwendet.[234] Im Bereich digitaler Anwendungen beschreibt der Nutzerbegriff also typischerweise Individuen, die Endverbraucher von Softwareprodukten oder technischen Diensten sind, ohne deren technischen Betrieb direkt steuern oder verändern zu können.[235] Übertragen auf dezentralisierte Finanzanwendungen sind ‹Nutzer› vorliegend Personen, die mittels digitaler Wallets Transaktionen an die Adresse eines Smart Contracts senden, welche dann dessen Funktionen entsprechend dem kodierten Ablauf auslösen.[236] Ihre Rolle ist hierbei auf die Nutzung definierter Protokollfunktionen beschränkt, ohne dass ihnen Möglichkeiten der Modifikation oder Steuerung des zugrundeliegenden Codes offenstehen.[237] 130

Die Interaktion mit dezentralisierten Protokollen erfolgt aus Nutzerperspektive über eine digitale Wallet, die als Schnittstelle zur Blockchain dient. Dabei handelt es sich in der Regel um einen sogenannten Externally Owned Account, also einen durch einen privaten kryptographischen Schlüssel kontrollierten Account, mit dem Transaktionen signiert und ausgeführt werden können.[238] Eine vorgängige Registrierung oder Identitätsverifikation ist bei 131

234 Vgl. SIMMLER, S. 147; vgl. auch DMA-BONGARTZ/KIRK, Art. 2 N 99 ff.

235 Vgl. z.B. DICKMANN, N 390; HK TTDSG-SCHNEIDER, § 25 N 18 f.; vgl. auch GÖHSL/ZIMMER, N 78.

236 Vgl. STILLER/RODRIGUES/NEZHADSISTAN, N 2.68; MEYER/SCHUPPLI, S. 207.

237 Vgl. ANTONOPOULOS/WOOD, S. 80; MEYER/SCHUPPLI, S. 205.

238 M.w.H. ANTONOPOULOS/WOOD, S. 26; MEIRICH, N 78 ff.; MEYER, Token, N 85.

den meisten Anwendungen nicht erforderlich. Der Zugang ist typischerweise offen ausgestaltet, sodass jede Person mit Internetzugang und einer kompatiblen Wallet auf die Funktionen zugreifen kann.[239]

132 Die eigentliche Interaktion mit den Smart Contracts erfolgt entweder über ein graphisches Webinterface oder direkt, etwa durch das Ausführen von Transaktionen mithilfe geeigneter Werkzeuge wie Kommandozeilenprogrammen, spezieller Browser für dezentrale Anwendungen oder erweiterter Funktionen von Blockchain-Explorern.[240] In beiden Fällen ist der Nutzer auf die Funktionen beschränkt, die durch den zugrundeliegenden Code vorgesehen sind. Eine Veränderung der Protokollstruktur oder des Funktionsumfangs ist auf Nutzerebene grundsätzlich nicht möglich.

133 Je nach Anwendungstyp fällt die Rolle des Nutzers unterschiedlich aus. Bei Handelsplattformen nehmen Nutzer entweder als Handelnde (durch Token-Tausch) oder als Liquiditätsanbieter teil, indem sie ihre Vermögenswerte einem Pool zur Verfügung stellen.[241] Bei Kryptowährungsmixern beschränkt sich die Nutzerhandlung auf die Auslösung einer Einzahlung in den Smart Contract sowie auf eine spätere, eigenständig initiierte Abrufhandlung, durch welche die automatisierte Auszahlung an eine neue Adresse erfolgt.[242]

134 Charakteristisch für die Nutzerstellung ist ferner das Fehlen klassischer Identifikationsmechanismen. Die Interaktion erfolgt regelmässig über pseudonyme Wallet-Adressen, die öffentlich sichtbar sind, jedoch keinen direkten Rückschluss auf die reale Identität zulassen.[243] Diese Pseudonymität ist funktionaler Bestandteil der meisten dezentralisierten Protokolle, insbesondere im Bereich von Mixern, wo der Schutz der Privatsphäre, ob berechtigt oder missbräuchlich motiviert, eine wesentliche Rolle spielt.[244]

135 Zusammenfassend lässt sich festhalten, dass Nutzer dezentralisierter Finanzanwendungen innerhalb eines durch Smart Contracts determinierten und in seinem Funktionsumfang abschliessend festgelegten Systems agieren. Sie initiieren Transaktionen, verfügen jedoch typischerweise über keinerlei darüber hinausgehende Kontroll- oder Entscheidungskompetenzen.

239 Vgl. RUTISHAUSER/RUBLI/WEBER, S. 15; BOŠKIĆ/HEPP, S. 212; NOSER/INFANGER/LÜDI, N 12.03; STILLER/RODRIGUES/NEZHADSISTAN, N 2.68.

240 Vgl. SCHÄR, S. 156; BOŠKIĆ/HEPP, S. 213; Financial Stability Board, S. 5.

241 Vgl. vorne N 87 f.; m.w.H. ANDREOTTI, S. 178, 340 f.; HUMBEL/ECKERT, S. 11; LIN, S. 58.

242 Vgl. vorne N 89 ff.; Botschaft DLT, S. 26 f.; ANDREOTTI, S. 285; DUPUIS/GLEASON, S. 66; VAHRENHOLT DE LUCENA, S. 202.

243 Vgl. Botschaft DLT, S. 19; EBA/ESMA, S. 10; KGGT, NRA 2018, S. 2; MEIRICH, N 135 ff.; OSWALD, S. 20 f.

244 Vgl. vorne N 90.

D. Zusammenfassung

Dezentralisierte Finanzanwendungen beruhen auf dem Zusammenspiel dreier zentraler Akteursgruppen: Smart Contracts als technisches Fundament, der Betreiberin mit administrativen Steuerungsbefugnissen sowie der Nutzer als Endanwendern. 136

Smart Contracts sind deterministische, selbstausführende Programme, deren Zweck, Struktur und Funktionsumfang vollständig durch menschliche Vorgaben bestimmt werden. Sie verfügen über keine eigene Entscheidungs- oder Anpassungsfähigkeit, sondern folgen starren ‹Wenn-dann-Logiken› und entfalten ihre Wirkung ausschliesslich innerhalb digitaler Infrastrukturen. Als rein deterministische Systeme sind sie als Werkzeuge menschlicher Steuerung zu qualifizieren. 137

Die Betreiberin stellt im Rahmen des Deployments den relevanten Code auf der Blockchain bereit und sorgt für die Funktionsfähigkeit der Anwendung. Je nach technischer Ausgestaltung verfügt sie über administrative Eingriffsmöglichkeiten im Backend – etwa zur Anpassung von Protokollparametern, zur Durchführung von Code-Updates oder zum Pausieren einzelner Funktionen – sowie im Frontend durch Betrieb und Gestaltung des Webinterfaces. Diese Steuerungsbefugnisse können über einen Admin Key, Multisignatur-Strukturen oder kollektive Governance-Modelle wie eine DAO ausgeübt werden. Als Betreiberin gilt jene Person oder Personengruppe, die den Code in die Blockchain einbringt und bzw. oder über fortlaufende Steuerungsmöglichkeiten im Backend sowie im Frontend faktisch Kontrolle über die Anwendung ausübt. Bei idealtypisch dezentralen Anwendungen erschöpft sich die Betreibereigenschaft im Deployment. 138

Die Nutzer schliesslich interagieren mit der Anwendung in der Rolle von Endanwendern. Sie initiieren Transaktionen, etwa durch den Tausch von Token auf einer Handelsplattform oder die Nutzung eines Mixers zur Verschleierung von Transaktionsketten, ohne über die zugrunde liegende Infrastruktur bestimmen zu können. Ihr Handeln bleibt auf die im Code vorgesehenen Funktionen beschränkt. Regelmässig agieren sie pseudonym, identifiziert lediglich über ihre Wallet-Adressen. Insgesamt bewegen sich Nutzer damit innerhalb eines technisch vorstrukturierten, durch die Betreiberin bereitgestellten und über Smart Contracts als Werkzeuge vermittelten Systems. 139

Kapitel 2: Geldwäschereihandlungen von Nutzern dezentralisierter Finanzanwendungen

140 Im ersten Kapitel des Grundlagenteils wurden die technologischen und begrifflichen Ausgangspunkte geklärt. Bevor sich die Untersuchung der eigentlichen Kernfrage – der Strafbarkeit der Betreiberinnen, deren Anwendungen von Nutzern zu Geldwäschereizwecken eingesetzt werden – zuwendet, richtet sich dieses zweite, den Grundlagenteil abschliessende Kapitel zunächst auf die Nutzerseite. Es untersucht, wie dezentralisierte Finanzanwendungen durch Nutzer zur Verschleierung deliktischer Vermögenswerte eingesetzt werden. Gegenstand ist damit nicht eine umfassende Strafbarkeitsanalyse der Nutzer, sondern die Rekonstruktion jener Vereitelungshandlungen, die sich in der Praxis durch das Interagieren der Nutzer mit von Betreiberinnen bereitgestellten Smart Contracts vollziehen und die Grundlage für die spätere Verantwortlichkeitsprüfung der Betreiberinnen bilden.

141 Der Aufbau des Kapitels folgt dieser Zielsetzung. Zunächst wird unter dem Titel ‹Phänomen› die kriminologische und praktische Relevanz der Geldwäscherei mit Kryptowerten aufgezeigt, die Einbettung in das klassische Drei-Phasen-Modell (Placement, Layering, Integration) erläutert und dargelegt, in welchen Deliktskonstellationen Kryptowerte typischerweise als Tatobjekt oder Transaktionsmedium auftreten. Daran anschliessend werden die spezifischen *modi operandi* der Herkunftsverschleierung im Blockchain-Kontext herausgearbeitet (I.). Im zweiten Teil erfolgt eine rechtliche Verdichtung dieses Befunds, indem die tatbestandliche Eignung der identifizierten Verhaltensweisen zur Einziehungsvereitelung im Sinne von Art. 305bis Ziff. 1 StGB an den von Lehre und Rechtsprechung entwickelten Grundsätzen geprüft wird (II.).

I. Phänomen

A. Einführung und Relevanz

142 Die Geldwäscherei umfasst eine Vielzahl von Verhaltensweisen, die darauf gerichtet sind, die Existenz, die illegale Herkunft oder die unrechtmässige Verwendung von Vermögenswerten zu verschleiern und diese in der Folge als

rechtmässig erscheinen zu lassen.[245] Dieses grundlegende kriminologische Verständnis, das sich in Anlehnung an die Definition der President's Commission on Organized Crime herausgebildet hat, ist auch in der schweizerischen Lehre weitgehend anerkannt.[246]

143 Im Zentrum des Phänomens steht die systematische Tarnung bzw. Verschleierung deliktisch erlangter Vermögenswerte mit dem Ziel, diese dem Zugriff der Strafverfolgungsbehörden zu entziehen und sie für die Täter weiterhin wirtschaftlich nutzbar zu halten.[247]

144 Die typischen Abläufe der Geldwäscherei lassen sich nach dem in der Literatur etablierten Drei-Phasen-Modell beschreiben.[248] Ausgangspunkt bildet die sogenannte Placement-Phase, in der deliktisch erlangte Vermögenswerte erstmals in den legalen Wirtschaftskreislauf überführt werden, etwa durch die Einschleusung über Finanzintermediäre.[249] Daran knüpft das Layering an, das durch die Verschleierung der Herkunft geprägt ist und regelmässig über komplexe Transaktionsketten, grenzüberschreitende Verschiebungen oder den Einsatz verschachtelter Strukturen erfolgt.[250] Den Abschluss bildet die Integrationsphase, in welcher die zuvor verschleierten Vermögenswerte wieder in den offenen Wirtschaftskreislauf zurückgeführt und den Tätern scheinbar legitim zur Verfügung gestellt werden.[251]

145 Während dieses Modell die klassischen Abläufe im traditionellen Finanzsystem beschreibt, haben sich die Rahmenbedingungen der Geldwäscherei durch die zunehmende Verbreitung virtueller Vermögenswerte erweitert.[252] Die wachsende Bedeutung von Kryptowerten ist dabei nicht per se ein Indikator

245 «Money laundering is a process by which one conceals the existence, illegal source or illegal application of income, and then disguises that income to make it appear legitimate» (President's Commission on Organized Crime USA, S. 7; vgl. DONATSCH/THOMMEN/WOHLERS, S. 491; FUCHS, N 19; PK StGB-PIETH/SCHULTZE, Art. 305bis N 2).

246 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 14; BERNASCONI, S. 20; DONATSCH/THOMMEN/WOHLERS, S. 491; GRABER, S. 55; BSK StGB II-PIETH, Art. 305bis N 7; PK StGB-PIETH/SCHULTZE, Art. 305bis N 2.

247 DONATSCH/THOMMEN/WOHLERS, S. 491 m.V.a. Botschaft StGB 1989, S. 1066; vgl. PK StGB-PIETH/SCHULTZE, Art. 305bis N 3.

248 BSK StGB II-PIETH, Art. 305bis N 7; vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 15; DONATSCH/THOMMEN/WOHLERS, S. 492; FUCHS, N 21; GIANNINI, S. 21 ff.; OFK StGB-ISENRING, Art. 305bis N 2; PK StGB-PIETH/SCHULTZE, Art. 305bis N 4.

249 Vgl. FUCHS, N 21; BSK StGB II-PIETH, Art. 305bis N 10; PK StGB-PIETH/SCHULTZE, Art. 305bis N 4.

250 Vgl. FUCHS, N 21; BSK StGB II-PIETH, Art. 305bis N 10; PK StGB-PIETH/SCHULTZE, Art. 305bis N 4.

251 DONATSCH/THOMMEN/WOHLERS, S. 492; FUCHS, N 21; vgl. GRABER, S. 57; HAUSER-SPÜHLER, N 166.

252 Vgl. auch Botschaft DLT, S. 142.

für ein erhöhtes Geldwäschereirisiko; sie schafft jedoch ein zusätzliches Transaktionsfeld, in dem entsprechende Handlungen auftreten können. So belief sich die Marktkapitalisierung von Kryptowerten im Jahr 2018 auf rund USD 455 Milliarden, stieg 2021 auf ein vorläufiges Hoch von etwa USD 2,8 Billionen und erreichte im Dezember 2024 mit rund USD 3,7 Billionen ihren bisherigen Höchststand.[253] Parallel dazu erhöhte sich auch die Zahl der Nutzer virtueller Vermögenswerte. Schätzungen zufolge stieg sie zwischen 2018 und 2020 von rund 35 Millionen auf über 100 Millionen, ehe im Jahr 2024 die Marke von 600 Millionen überschritten wurde.[254]

146 Diese strukturelle Ausweitung des Transaktionsfeldes schlägt sich auch in der Aufsichtspraxis nieder. Hinweise auf eine zunehmende Relevanz virtueller Vermögenswerte im Kontext der Geldwäscherei finden sich insbesondere in den Entwicklungen der nationalen und internationalen Verdachtsmeldungen.[255] Während im Jahr 2020 noch 5,8 % aller bei der Meldestelle für Geldwäscherei der Schweiz (MROS) eingegangenen Meldungen einen Bezug zu virtuellen Vermögenswerten aufwiesen, hatte sich dieser Anteil im Jahr 2022 mit 13,8 % mehr als verdoppelt. In den Folgejahren verblieb der Wert auf einem hohen Niveau und betrug 9,5 % im Jahr 2023 sowie 11,9 % im Jahr 2024.[256] Diese Tendenz widerspiegelt sich auch auf internationaler Ebene. So verzeichneten sowohl die deutsche Financial Intelligence Unit (Zentralstelle für Finanztransaktionsuntersuchungen) als auch die FIUs der Niederlande, Estlands und Liechtensteins seit dem Jahr 2020 einen signifikanten Anstieg an Meldungen im Zusammenhang mit Kryptowerten und schrieben diesem Bereich daher ein erhöhtes Risiko für Geldwäschereiaktivitäten zu.[257]

B. Modi operandi der Herkunftsverschleierung

1. ‹Tatort› Blockchain

147 Sowohl im klassischen Bargeld- und Buchgeldkreislauf als auch im Bereich der Kryptowerte erfolgen geldwäschereirelevante Handlungen mit dem Ziel, inkriminierte Vermögenswerte von ihrem deliktischen Ursprung zu lösen,

253 Vgl. KGGT, NRA 2024, S. 47 m.V.a. CoinMarketCap, Crypto Market Overview; ESMA, S. 4.

254 Vgl. BLANDIN et al., S. 12; KGGT, NRA 2024, S. 47; Crypto.com, Global Cryptocurrency Owners Grow to 659 Million Through 2024; MATSUOKA/HACKETT/LAZZARIN. So verzeichnete etwa die Kryptobörse Coinbase bereits im Jahr 2021 rund 56 Millionen registrierte Nutzer; bis 2024 stieg diese Zahl auf über 100 Millionen an (vgl. CURRY; KGGT, NRA 2024, S. 47).

255 KGGT, NRA 2024, S. 64.

256 Vgl. MROS, Jahresbericht, S. 16, 24.

257 Vgl. FIU Deutschland, 2022, S. 35 f.; FIU Deutschland, 2021, S. 48; FIU Estland, S. 20 ff.; FIU Niederlande 2021, S. 7, 27; FIU Liechtenstein, S. 5.

um sie anschliessend im legalen Wirtschaftskreislauf wiederverwenden zu können.[258]

Dass Kryptowerte zunehmend Gegenstand geldwäschereirelevanter Aktivitäten sind, lässt sich – neben der zuvor dargestellten wachsenden Akzeptanz und Nutzung – insbesondere mit ihrer technisch bedingten Pseudonymität erklären.[259] Transaktionen sind auf öffentlichen Blockchains nicht mit überprüfbaren Identitäten verknüpft, sondern werden Adressen zugeordnet, die kryptographisch generiert sind und keinen unmittelbaren Personenbezug aufweisen.[260] Zwar sind sämtliche Transaktionsdaten, wie Sender- und Empfängeradressen sowie der transferierte Betrag, auf der Blockchain öffentlich einsehbar; die Zuordnung zu wirtschaftlich berechtigten Personen bleibt jedoch grundsätzlich verborgen.[261] Darüber hinaus können Kryptowerte weltweit innert Sekunden und ohne geographische oder institutionelle Hürden direkt zwischen zwei Parteien übertragen werden.[262] 148

Das Blockchain-Ökosystem ist dabei in zweierlei Hinsicht in geldwäscherelevante Handlungen eingebunden. Zum einen ermöglicht es die Verschleierung sich bereits auf der Blockchain (on-chain) befindlicher deliktischer Vermögenswerte. Zum anderen dient es als Instrument zur Herkunfts-verschleierung, indem deliktisch erlangtes Fiatgeld durch Konvertierung in Kryptowerte in das Blockchain-System überführt wird.[263] 149

Bei der ersten Konstellation liegen die kriminell erlangten Vermögenswerte bereits in Form von Kryptowerten vor.[264] Dies ist bspw. der Fall, wenn infolge eines Hackerangriffs auf eine Handelsplattform Token entwendet werden (sogenanntes On-chain-Delikt) oder wenn bei einem Drogengeschäft im Darknet die Bezahlung direkt in Bitcoin erfolgt.[265] Da öffentliche Blockchains grundsätzlich transparent sind und jede Transaktion dauerhaft nachvollziehbar bleibt, hinterlassen solche Vermögensflüsse eine dokumentierte 150

258 Vgl. DONATSCH/THOMMEN/WOHLERS, S. 491; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 11 f.; MOLO/BRUNONE, S. 302.

259 Vgl. vorne N 2; Botschaft DLT, S. 143; FINMA, Jahresbericht, S. 32; Europol, Spotlight, S. 10, 19; KGGT, NRA 2018, S. 21; MEIRICH, N 492.

260 Vgl. Botschaft DLT, S. 19; KGGT, NRA 2018, S. 2; MEIRICH, N 135 ff.; OSWALD, S. 20 f.

261 Vgl. Botschaft DLT, S. 22, 25, 144; KGGT, NRA 2024, S. 84; KGGT, NRA 2018, S. 21.

262 Vgl. Europol, Spotlight, S. 19; FINMA, Jahresbericht, S. 32; KGGT, NRA 2018, S. 22; MEIRICH, N 493.

263 Vgl. KGGT, NRA 2024, S. 52 ff.; KGGT, NRA 2018, S. 21 ff.; Financial Crime Academy; GABBIADINI/GOBBI/RUBERA, S. 13.

264 Vgl. KGGT, NRA 2024, S. 57; KGGT, NRA 2018, S. 26 f.; Financial Crime Academy; GABBIADINI/GOBBI/RUBERA, S. 13.

265 Vgl. FELBER.

Transaktionsspur.[266] Diese Rückverfolgbarkeit kann dazu führen, dass bestimmte Token, die mit einer Straftat verknüpft sind (Tainted Coins), von Börsen, Dienstleistern oder anderen Marktteilnehmern nicht mehr akzeptiert werden. Die betroffenen Werte verlieren damit faktisch ihre Fungibilität, also ihre Eigenschaft, beliebig gegen andere gleichartige Token getauscht zu werden. Um ihre Verwertbarkeit wiederherzustellen sowie einer allfälligen strafrechtlichen Verfolgung zu entgehen, besteht aus Sicht der Täter ein erhebliches Interesse, die Transaktionshistorie gezielt zu verschleiern und die deliktische Herkunft der Vermögenswerte unkenntlich zu machen.[267]

151 Die zweite Konstellation betrifft Fälle, in denen Vermögenswerte zunächst ausserhalb der Blockchain (off-chain), z.B. in Form von Bargeld oder Buchgeld, deliktisch erlangt wurden und anschliessend in Kryptowerte konvertiert werden.[268] Je nach Art des verwendeten Konvertierungsmechanismus unterscheiden sich auch die Verschleierungsstrategien. Wird ein nicht regulierter oder identifikationsfreier Zugang (bspw. über einen Kryptoautomaten unterhalb der Meldegrenze)[269] genutzt, beginnt die Verschleierung bereits mit der Platzierung, indem die Gelder in ein System überführt werden, das keine direkte Verknüpfung zur realen Identität mehr zulässt. Erfolgt die Umwandlung hingegen über eine identifikationspflichtige Börse oder einen regulierten Broker, entsteht ein dokumentierter Bezug zwischen den eingesetzten Fiatgeldern und einer konkreten Person. Diese Transaktion begründet gewissermassen einen neuen Paper-Trail. In solchen Fällen deckt sich das Verschleierungsinteresse weitgehend mit jenem der ersten Konstellation. Ziel ist es, durch nachgelagerte Transaktionen auf der Blockchain die Rückverfolgbarkeit der Vermögenswerte zu unterbrechen und die Verbindung zur eigenen Identität zu kappen.

2. Deliktische Herkunft von Kryptowerten

152 In ihren Risikoanalysen von 2018 und 2024 gelangt die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) zum Ergebnis, dass virtuelle Vermögenswerte ein

266 Vgl. vorne N 21.

267 Vgl. NADLER/SCHÄR, Tornado Cash, S. 123; KGGT, NRA 2024; KGGT, NRA 2018, S. 26.

268 KGGT, NRA 2024, S. 57. Im Bericht von 2018 wurde hierfür noch der Ausdruck ‹Waschen illegal erworbener Krypto-Assets› verwendet (vgl. KGGT, NRA 2018, S. 30); Financial Crime Academy; GABBIADINI/GOBBI/RUBERA, S. 13; vgl. auch Urteil des BstGer RR.2022.45 vom 20. Dezember 2022.

269 Seit dem 1. Januar 2021 gilt gemäss Art. 51a Abs. 1 GwV-FINMA eine Identifizierungspflicht ab CHF 1'000 pro Transaktion. Die Regelung zielt darauf ab, anonymen Missbrauch zu verhindern, nachdem solche Automaten nachweislich für Geldwäscherei, insbesondere im Drogenhandel, genutzt wurden (vgl. FINMA, Teilrevision, S. 15 f.).

erhöhtes geldwäschereirelevantes Risiko aufweisen.[270] Auch andere nationale Behörden verweisen in ihren Lagebeurteilungen auf eine Zunahme entsprechender Risiken im Zusammenhang mit Kryptowerten.[271]

153 In der Praxis zeigt sich diese Risikoeinschätzung anhand der vielfältigen Einsatzformen virtueller Vermögenswerte im Rahmen unterschiedlicher Deliktsphänomene. So dienen sie bei Ransomware-Angriffen regelmässig als Lösegeldmittel, indem Kriminelle die Daten eines Systems verschlüsseln und Zahlungen in Kryptowährung für deren Freigabe verlangen.[272] Auch bei betrügerischen Machenschaften wie Scams stehen virtuelle Vermögenswerte im Fokus, z.B. bei Anlagebetrug oder gefälschten Initial Coin Offerings (ICOs), bei denen Opfer zur Überweisung digitaler Vermögenswerte verleitet werden.[273] Darüber hinaus werden sie zunehmend als Zahlungsmittel für illegale Güter und Dienstleistungen eingesetzt, wie bspw. im klassischen Drogenhandel oder beim anonymisierten Onlinehandel im Darknet.[274] Schliesslich kommen Kryptowerte auch im Zusammenhang mit der Terrorismusfinanzierung zum Einsatz.[275]

154 Quantitative Einschätzungen zur deliktsbezogenen Nutzung von virtuellen Vermögenswerten beruhen nahezu ausschliesslich auf Auswertungen spezialisierter Blockchainanalyse-Unternehmen.[276] Laut dem ‹Crypto Crime Report› von Chainalysis belief sich das weltweite Volumen an Kryptowerten, das im Jahr 2024 an als deliktisch klassifizierte Adressen gesendet wurde, auf rund USD 41 Milliarden – ein deutlicher Anstieg gegenüber USD 11 Milliarden im Jahr 2020.[277] Der Anteil illegaler Transaktionen am gesamten sich auf der Blockchain befindlichen Transaktionsvolumen wurde für die Jahre 2020 bis 2024 mit Werten zwischen rund 0,12 % und 0,7 % beziffert.[278]

270 Vgl. KGGT, NRA 2018, S. 4, 31, 36, 47; KGGT, NRA 2024, S. 47 ff.

271 Bundesrat, DLT, S. 143; Bundesrat, Virtuelle Währungen, S. 20 f.; FINMA, Vermögenswerte, S. 2; FINMA, Risikomonitor, S. 15, 19; JUTZI/ABBÜHL, N 673 ff.; vgl. auch MEIRICH, N 492; STENGEL/PAYDAR, N 18.01.

272 KGGT, NRA 2024, S. 53 f.; KGGT, NRA 2018, S. 26; Chainalysis, 2025, S. 10 ff.; COLLINS, S. 16; U.S. Department of the Treasury, S. 18 ff. Ransomware-Angriffe nehmen weltweit zu und betreffen inzwischen auch systemrelevante Infrastrukturen und grosse Finanzinstitutionen. Die Lösegeldforderungen erfolgen dabei fast ausschliesslich in Kryptowährungen (vgl. GAFI, Ransomware, S. 9; KGGT, NRA 2024, S. 53; BAUMGARTNER).

273 KGGT, NRA 2024, S. 70; KGGT, NRA 2018, S. 30; Chainalysis, 2025, S. 54 ff.; COLLINS, S. 13; U.S. Department of the Treasury, S. 21 ff.; vgl. auch MÜLLER, Initial Coin Offering.

274 KGGT, NRA 2024, S. 54; KGGT, NRA 2018, S. 28 f.; Chainalysis, 2025, S. 23 ff.; COLLINS, S. 18; FOLEY/KARLSEN/PUTNIŅŠ, S. 1798 ff.; U.S. Department of the Treasury, S. 23 f.

275 KGGT, NRA 2018, S. 27 f.; Chainalysis, 2025, S. 105 ff.

276 KGGT, NRA 2024, S. 55; vgl. CARLISLE, S. 83.

277 Vgl. Chainalysis, 2025, S. 2.

278 Vgl. Chainalysis, 2025, S. 4. Unter Transaktionsvolumen wird die Gesamtsumme der wirtschaftlich relevanten Transfers auf der Blockchain verstanden, wobei nur Trans-

155 Obwohl diese Analysen in weitem Umfang rezipiert werden, vermögen sie aufgrund ihrer methodischen Voraussetzungen nur in beschränktem Umfang verlässliche Aussagen zu tragen:

156 Die dem Bericht zugrunde liegende Erhebungsmethodik stützt sich auf den Indikator ‹total cryptocurrency value received by illicit addresses›, wobei solche Adressen als ‹illicit› eingestuft werden, die nachweislich im Zusammenhang mit strafbaren Aktivitäten stehen.[279] Der Report unterscheidet dabei verschiedene Deliktsphänomene hinsichtlich des kriminellen Ursprungs der Gelder, die unter den Begriff ‹Crypto Crime› gefasst werden. Darunter befinden sich insbesondere Ransomware, Malware, Scams, Terrorismusfinanzierung, Diebstahl sowie Transaktionen im Zusammenhang mit Darknet-Märkten.[280]

157 Eine abschliessende Begriffsbestimmung von ‹Crypto Crime› liegt jedoch nicht vor. Zumindest wird klargestellt, dass sich die Erhebungen primär auf ‹cryptocurrency-native crime› beziehen, also auf Delikte, bei denen Kryptowerte integraler Bestandteil der Tatausführung sind. Nicht erfasst sind demnach ‹non-cryptocurrency-native crimes›, etwa klassische Off-chain-Delikte wie der Drogenhandel, bei denen virtuelle Vermögenswerte lediglich als Zahlungsmittel verwendet werden, deren Transaktionen aber auf der Blockchain keine erkennbare Verbindung zu einer Straftat aufweisen.[281]

158 Ebenfalls nicht berücksichtigt werden Gelder, die an Adressen gesendet wurden, die (noch) nicht als verdächtig klassifiziert sind, etwa im Zusammenhang mit Transaktionen extremistischer Gruppen, betrügerischen Kryptoplattformen ohne rechtskräftige Verurteilung oder möglichen Marktmanipulationen. Diese Einschränkungen begründen sich teils durch Beweisprobleme, teils durch Rechtsunsicherheiten oder methodische Limitationen der Analyseverfahren.[282]

159 Die Einschätzungen zum Anteil von Vermögenswerten mit bekannter deliktischer Herkunft divergieren stark: So wurde dieser Anteil je nach Quelle mit 3,5 % (2022)[283] oder sogar bis zu 23 % (2017)[284] des gesamten Blockchain-Handelsvolumens beziffert. Diese erheblichen Unterschiede lassen sich unter

aktionen zwischen voneinander unabhängigen Akteuren berücksichtigt werden. Nicht erfasst werden interne Abläufe wie Wechselgeld, Transaktionen zwischen eigenen Wallets oder rein technische Vorgänge (Chainalysis, 2025, S. 5).

279 STÜRMER, S. 292; JIMENEZ, passim.

280 Vgl. Chainalysis, 2025, S. 2.

281 Vgl. KGGT, NRA 2024, S. 55; vgl. auch Chainalysis, 2025, S. 3; COLLINS, S. 18; MARRINAN, passim.

282 Vgl. Chainalysis, 2025, S. 4.

283 Vgl. CipherTrace, S. 4.

284 Vgl. FOLEY/KARLSEN/PUTNIŅŠ, S. 1800.

anderem auf die unterschiedlichen methodischen Ansätze und Klassifikationen in der Transaktionsanalyse zurückführen. Hinzu kommt, dass deliktische Handlungen, die ausserhalb der Blockchain (off-chain) stattfinden, in diesen Erhebungen regelmässig unberücksichtigt bleiben; sei es mangels verlässlicher Datengrundlagen oder aufgrund ihrer schwer erfassbaren Natur. Insofern ist in diesem Bereich von einer erheblichen Dunkelziffer auszugehen.[285]

Zusammenfassend ist hervorzuheben, dass die genannten Analysen nur 160
vor dem Hintergrund ihrer methodischen und inhaltlichen Begrenzungen zu betrachten sind. Die von Chainalysis und anderen Blockchainanalyse-Unternehmen publizierten Zahlen bilden nicht das deliktische Gesamtgeschehen ab, sondern erfassen lediglich solche Adressen, die anhand öffentlich zugänglicher Informationen und heuristischer Verfahren mit hinreichender Sicherheit einem deliktischen Kontext zugeordnet werden konnten. Methodische Beschränkungen – insbesondere nicht identifizierte oder falsch klassifizierte Adressen, rechtsunsichere Kategorisierungen sowie divergierende Erhebungsansätze der Anbieter – begrenzen zudem die Vergleichbarkeit der Resultate. Der wissenschaftliche Aussagegehalt dieser Daten liegt daher primär in der Identifikation struktureller Entwicklungen und relativer Trends, nicht jedoch in der exakten Quantifizierung des deliktischen Gesamtvolumens.[286]

Vor diesem Hintergrund ist ungeachtet der genannten Unsicherheiten 161
im internationalen Diskurs unbestritten, dass deliktische Verwendungen – sowohl off-chain als auch on-chain – angesichts der zunehmenden Verbreitung, der grenzüberschreitenden Verfügbarkeit und der pseudonymen Struktur von virtuellen Vermögenswerten deutlich an Bedeutung gewonnen haben.[287]

3. Drei-Phasen-Modell

Wie bereits dargelegt, kann die Blockchain sowohl zur Verschleierung bereits 162
on-chain befindlicher deliktischer Vermögenswerte als auch zur Einbringung kriminell erlangter Fiatgelder in das kryptobasierte Ökosystem genutzt werden.[288] Die Bedeutung dieses Phänomens zeigt sich auch in der quantitativen Dimension: Für das Jahr 2022 wird das Volumen der auf der Blockchain gewaschenen Kryptowerte auf rund USD 31,5 Milliarden geschätzt.[289]

285 Vgl. KGGT, NRA 2024, S. 58; COLLINS, S. 18; MARRINAN.

286 Vgl. KGGT, NRA 2024, S. 55.

287 KGGT, NRA 2024, S. 55; vgl. Europol, Spotlight, S. 11 ff.; GAFI, Indicators, S. 15; U.S. Department of the Treasury, S. 16 ff.

288 Vgl. vorne N 149 ff.

289 Chainalysis, 2024, S. 24; vgl. vorne N 154 ff. zur begrenzten Aussagekraft der von Blockchainanalyse-Unternehmen verwendeten Datengrundlagen die methodenkritische

163 Beide Konstellationen lassen sich mit gewissen Besonderheiten dem klassischen Drei-Phasen-Modell der Geldwäscherei zuordnen. Liegen die deliktischen Vermögenswerte bereits in Form von Kryptowerten vor, z.B. infolge eines Hacks oder als Zahlungsmittel beim Erwerb illegaler Güter, entfällt die klassische Placement-Phase weitgehend.[290] In Fällen, in denen kriminell erlangtes Fiatgeld zunächst ausserhalb der Blockchain vorliegt, kann der Placement-Phase besondere Bedeutung zukommen: Die Konvertierung in virtuelle Vermögenswerte führt die Gelder in ein pseudonymes und grenzüberschreitendes Transaktionssystem über, was je nach Ausgestaltung bereits gewisse Verschleierungseffekte zeitigen kann und in jedem Fall den Zugang zu Strukturen eröffnet, innerhalb derer nachgelagerte Verschleierungsstrategien typischerweise umgesetzt werden.[291]

164 Im Zentrum beider Szenarien steht sodann die Layering-Phase. Die auf der Blockchain grundsätzlich nachvollziehbaren Transaktionsspuren sollen gezielt durch technologische Mittel verschleiert werden. Hierzu werden die Vermögenswerte über verschiedene Protokolle weitergeleitet, in andere Token umgewandelt oder durch mehrstufige Transaktionsketten in ihrer Herkunft unkenntlich gemacht. Ziel ist es, die Nachverfolgbarkeit zu erschweren und die Verbindung zur ursprünglichen Straftat zu verwischen.[292]

165 Eine besondere Rolle in diesem Prozess kommt dezentralisierten Finanzanwendungen zu. Wie im vorangegangenen Kapitel ausgeführt, funktionieren diese Systeme ohne zentrale Intermediäre, erlauben einen pseudonymen Zugang ohne Identifikationspflicht und wickeln Transaktionen automatisiert über Smart Contracts ab.[293] Die Nutzer treten dabei nicht mit einer natürlichen Person in Kontakt, sondern interagieren über ihre Wallets unmittelbar mit den Smart Contracts der Anwendung.[294]

166 Diese strukturellen Merkmale machen sie besonders anfällig für missbräuchliche Verwendungen im Rahmen des Layerings. Entsprechend hält der schweizerische Risikobericht fest, dass im Jahr 2022 ungefähr die Hälfte der bei Hacks entwendeten Kryptowerte (insgesamt rund CHF 1,5 Milliarden)

Einordnung oben, insbesondere zu Erfassungsumfang, Klassifikationsansätzen und den daraus resultierenden Unsicherheiten.

290 UNODC.

291 Vgl. OSWALD, S. 32.

292 Vgl. KGGT, NRA 2024, S. 83; U.S. Department of the Treasury, S. 16 ff.; Europol, Spotlight, S. 9 f.; MEIRICH, N 492 ff.

293 Vgl. vorne N 71 ff.; KGGT, NRA 2024, S. 48 f.; Chainalysis, 2022, S. 10 ff.; GABBIADINI/GOBBI/RUBERA, S. 12.

294 Vgl. vorne N 71 ff.

nicht über zentralisierte Plattformen, sondern über dezentralisierte Protokolle gewaschen wurden.[295]

In der Layering-Phase zeigen sich vielfältige Nutzungsformen dezentralisierter Finanzanwendungen, die auf eine gezielte Verschleierung der Transaktionshistorie ausgerichtet sind.[296] Besonders häufig genannt werden dabei Kryptomixer, bei denen durch Aufspaltung, Neuverteilung und anschliessende Reaggregation von Tokenbeträgen die Verbindung zwischen Ein- und Auszahlung verwischt wird, sodass Rückschlüsse auf die Herkunft der Mittel kaum mehr möglich sind.[297] 167

Daneben kommen auch Cross-Chain-Bridges zum Einsatz, deren Funktion im technischen Transfer von Vermögenswerten zwischen unterschiedlichen Blockchains liegt.[298] Durch den mehrfachen Wechsel von Vermögenswerten zwischen verschiedenen Chains (sogenanntes Chain-Hopping) kann die Spur der Werte durch technische Inkompatibilitäten der Chains gezielt unterbrochen werden.[299] 168

Dezentralisierte Handelsplattformen wiederum ermöglichen den Tausch von Token ohne zentrale Instanz und können daher ebenfalls Teil solcher Verschleierungsstrategien sein.[300] Auch klassische dezentralisierte Finanzprotokolle wie Staking, Liquidity Mining, Yield Farming sowie Lending- und Borrowing-Dienste lassen sich grundsätzlich in Layering-Strategien einbinden. Dabei werden Vermögenswerte etwa in Pools hinterlegt, in neue Tokenformen überführt, innerhalb renditeoptimierter Strategien umgeschichtet oder als Sicherheiten verwendet, um neue Mittel zu generieren.[301] 169

Die Integration erfolgt schliesslich durch die Rückführung der bereinigten Vermögenswerte in den legalen Wirtschaftskreislauf, wie bspw. durch den Umtausch in Fiatgeld, durch den Erwerb realer Güter oder durch ihre Weiterverwendung innerhalb des dezentralisierten Finanzsystems.[302] In beiden Konstellationen besteht das Ziel darin, die deliktisch kontaminierten Vermögenswerte in eine ökonomisch nutzbare Form zu überführen. 170

295 Vgl. KGGT, NRA 2024, S. 49 m.V.a. Chainalysis, 2022, S. 74.

296 Chainalysis, 2024, S. 25.

297 Botschaft DLT, S. 26 f.; KGGT, NRA 2024, S. 103; Europol, Spotlight, S. 10; U.S. Department of the Treasury, S. 17; CipherTrace, S. 12; COLLINS, S. 15; GABBIADINI/GOBBI/RUBERA, S. 15 f.; zur Funktionsweise vgl. vorne N 89 ff.

298 Vgl. vorne N 98.

299 BENSON/TURKSEN/ADAMYK, S. 88 ff.; GABBIADINI/GOBBI/RUBERA, S. 17; vgl. KGGT, NRA 2024, S. 103; U.S. Department of the Treasury, S. 16 f.

300 U.S. Department of the Treasury, S. 16 f.; DUPUIS/GLEASON, S. 69; GABBIADINI/GOBBI/RUBERA, S. 17 f.

301 Chainalysis, 2024, S. 25; EBA/ESMA, S. 49; U.S. Department of the Treasury, S. 17.

302 Vgl. vorne N 149 ff.

171 Die dargestellten Mechanismen finden auch in der schweizerischen Praxis Niederschlag. So wurden im Jahr 2025 im Rahmen einer internationalen Ermittlungsoperation die Server eines seit 2016 betriebenen Kryptomixers im Kanton Zürich beschlagnahmt, über den weltweit erhebliche Mengen deliktisch erlangter Kryptowährungen verschleiert worden sein sollen.[303] In einem weiteren Fall stellte ein Strafverfahren gegen einen in der Schweiz agierenden Drogendealer zwischen 2018 und 2022 fest, dass die erzielten Kryptowerte systematisch über verschiedene Wallet-Strukturen und Protokolle weitergeleitet wurden, um die Transaktionshistorie gezielt zu verwischen.[304] Schliesslich zeigen auch Ransomware-Fälle mit Schweizer Bezug, dass die in Kryptowährungen geleisteten Lösegeldzahlungen regelmässig Ausgangspunkt für nachgelagerte Layering-Strategien auf der Blockchain bilden.[305]

II. Geldwäschereirelevante Nutzungsmuster im Umgang mit dezentralisierten Protokollen

172 Die vorangehenden Ausführungen haben aufgezeigt, in welchen Konstellationen Kryptowerte deliktisch erlangt werden, welche Rolle sie in unterschiedlichen Deliktsphänomenen spielen und wie sie sich in das klassische Drei-Phasen-Modell der Geldwäscherei einfügen. Zudem wurde herausgearbeitet, dass dezentralisierte Finanzanwendungen im Rahmen der Layering-Phase eine zentrale Funktion für die Herkunftsverschleierung übernehmen.

173 Der nachfolgende Abschnitt knüpft daran an und untersucht aus rechtlicher Perspektive, unter welchen Voraussetzungen das Interagieren der Nutzer mit solchen Protokollen als tatbestandsrelevante Verschleierungshandlung im Sinne von Art. 305bis Ziff. 1 StGB zu qualifizieren ist. Im Vordergrund steht dabei nicht eine umfassende Analyse der Nutzerstrafbarkeit, sondern die dogmatische Einordnung jener Nutzungsmuster, die für die im Zentrum der Untersuchung stehende Frage der Strafbarkeit der Betreiberinnen bedeutsam sind. Anhand der Beispiele dezentralisierter Handelsplattformen und Kryptomixer wird illustriert, inwiefern die von den Betreiberinnen bereitgestellten Anwendungen objektiv zur Einziehungsvereitelung im Sinne von Art. 305bis Ziff. 1 StGB eingesetzt werden können.

174 Zunächst werden die dogmatischen Grundlagen von Art. 305bis Ziff. 1 StGB und die Anforderungen an eine tatbestandsmässige Vereitelungshandlung dargestellt. Anschliessend werden anhand der Beispiele dezentralisierter

303 COVIELLO/MÄDER/BAUMGARTNER.

304 Vgl. FELBER.

305 Vgl. HUWILER.

Handelsplattformen und Kryptomixer jene Nutzungsmuster analysiert, in denen die bereitgestellten Anwendungen objektiv zur Herkunftsverschleierung eingesetzt werden können. Abschliessend wird die Frage beleuchtet, inwiefern auch die Konvertierung deliktisch erlangter Fiatgelder in Kryptowerte geldwäschereirelevant sein kann.

A. Tatbestandliche Grundlagen von Art. 305bis Ziff. 1 StGB

Der Geldwäschereitatbestand nach Art. 305bis Ziff. 1 StGB erfordert eine Handlung, die geeignet ist, die Ermittlung der Herkunft, die Auffindung oder die Einziehung von Vermögenswerten zu vereiteln, die, wie der Täter weiss oder annehmen muss, aus einem Verbrechen oder qualifizierten Steuervergehen herrühren. Gemäss der ständigen Rechtsprechung ist der Täterkreis unbeschränkt und erfasst auch den Vortäter.[306] 175

Aus den Materialien geht nicht eindeutig hervor, welches Rechtsgut der Gesetzgeber schützen wollte.[307] In Betracht kommen die Rechtspflege, das durch die Vortat betroffene Individualrechtsgut des Vermögens, der Schutz der Gesellschaft vor organisierter Kriminalität sowie der Ruf des schweizerischen Finanzplatzes.[308] Ein Teil der Lehre und die jüngere Rechtsprechung des Bundesgerichts sehen als primär geschütztes Rechtsgut die Durchsetzung des inländischen und ausländischen staatlichen Einziehungsanspruchs. Ergänzend wird in Fällen, in denen die einzuziehenden Vermögenswerte aus Vermögensdelikten herrühren, auch das Interesse der durch die Vortat individuell geschädigten Person als mitgeschütztes Rechtsgut anerkannt.[309] 176

Gegenstand einer Geldwäschereihandlung können sämtliche Vermögenswerte sein, die aus einem Verbrechen oder qualifizierten Steuerdelikt stammen. Der Vermögensbegriff wird in Rechtsprechung und Lehre weit gefasst und umfasst alle Güter mit wirtschaftlichem Wert, die zumindest 177

306 Vgl. BGE 149 IV 248 E. 6.2; 144 IV 172 E. 7.2; 132 IV 132 E. 6.3.1; Urteil des BGer 6B_691/2022 vom 17. Oktober 2022 E. 4.1; a.M. KV/KO StGB-ackermann/zehnder, Art. 305bis N 228 ff.; CR CP II-cassani/villard, Art. 305bis N 14; egger tanner, S. 21 ff.; BSK StGB II-pieth, Art. 305bis N 2.

307 KV/KO StGB-ackermann/zehnder, Art. 305bis N 94; vgl. auch Botschaft StGB 1989, S. 1081.

308 KV/KO StGB-ackermann/zehnder, Art. 305bis N 92; vgl. CR CP II-cassani/villard, Art. 305bis N 10 f.; donatsch/thommen/wohlers, S. 493 f.; PK StGB-pieth/schultze, Art. 305bis N 6.

309 Vgl. BGE 146 IV 211 E. 4.2.1; 145 IV 335 E. 3.1; 129 IV 322 E. 2.2.4; gl.M. CR CP II-cassani/villard, Art. 305bis N 10; AK StGB-graf, Art. 305bis N 1; OFK StGB-isenring, Art. 305bis N 4 ff.; HK StGB-wohlers, Art. 305bis N 1; krit. KV/KO StGB-ackermann/zehnder, Art. 305bis N 97.

hypothetisch einziehbar sind.[310] Darunter fallen auch virtuelle Vermögenswerte, deren Funktion als Tausch- und Zahlungsmittel ihre Qualifikation als taugliches Tatobjekt im Sinne dieser Norm nahelegt – ein Verständnis, das auch vom Gesetzgeber geteilt wird.[311]

178 Die Tathandlung muss sich eignen, die Ermittlung der Herkunft, die Auffindung oder die Einziehung zu vereiteln. Nach herrschender Lehre und Rechtsprechung kommt der Auffindungs- und Herkunftsermittlungsvereitelung allerdings keine eigenständige Bedeutung zu, da beide Aspekte in der Einziehungsvereitelung aufgehen.[312]

179 Bei der Geldwäscherei handelt es sich um ein abstraktes Gefährdungsdelikt bzw. Eignungsdelikt. Tatbestandsmässig ist also bereits ein Verhalten, das geeignet ist, das geschützte Rechtsgut, das heisst die Einziehungsinteressen der Rechtspflege, typischerweise zu gefährden.[313] Ein tatsächlicher Vereitelungserfolg oder eine konkrete Gefährdung sind hingegen nicht erforderlich.[314] Massgebend ist, ob das «Verhalten jedenfalls in der überwiegenden Zahl der Fälle tatsächlich gefährlich ist, das heisst zumindest die Möglichkeit einer Rechtsgutsverletzung begründet» ist.[315] Es muss sich dabei weder um eine unausweichliche noch um eine besonders hohe Gefahr handeln.[316] Nach der Rechtsprechung des Bundesgerichts ist bereits eine Handlung tatbestandsmässig, welche die Zugriffsmöglichkeiten der Strafverfolgungsbehörden auf deliktisch erlangte Vermögenswerte erschwert.[317] Der Geldwäschereitatbestand

310 Vgl. Botschaft StGB 1989, S. 1082; ACKERMANN et al., S. 223; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 334; BSK StGB II-PIETH, Art. 305bis N 9; DONATSCH/THOMMEN/WOHLERS, S. 495; AK StGB-GRAF, Art. 305bis N 7; STRATENWERTH/BOMMER, BT II, § 57 N 26; HK StGB-WOHLERS, Art. 305bis N 3.

311 Vgl. Bundesrat, Virtuelle Währungen, S. 7, 11; STENGEL/PAYDAR, N 18.07, 18.10; MOLO/DRZALIC, S. 42; vgl. auch Botschaft StGB 1989, S. 1082; MOLO/BRUNONE, S. 301; zur Einziehbarkeit von Kryptowährungen TSCHUDI, N 20.04 ff.; MOLO/DRZALIC, S. 47 f.; RONC/SCHUPPLI, S. 532; SIMMLER/SELMAN/BURGERMEISTER, passim; zum deutschen Recht STÜRMER, S. 300.

312 M.w.H. BSK StGB II-PIETH, Art. 305bis N 37; vgl. BGE 129 IV 238 E. 3.3; 126 IV 255 E. 3a; 119 IV 242 E. 1; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 390; CR CP II-CASSANI/VILLARD, Art. 305bis N 34; GIANNINI, S. 74; GRABER, S. 139.

313 Vgl. Botschaft StGB 1989, S. 1083; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 106 f.; DONATSCH/THOMMEN/WOHLERS, S. 502; EGGER TANNER, S. 121; GRABER, S. 133; PK StGB-PIETH/SCHULTZE, Art. 305bis N 17, 30.

314 Vgl. BGE 136 IV 188 E. 6.1; 127 IV 20 E. 3a; 119 IV 59 E. 2e; Urteil des BGer 6B_295/2022 vom 15. September 2022 E. 1.2; Botschaft StGB 1989, S. 1083; CR CP II-CASSANI/VILLARD, Art. 305bis N 10; DONATSCH/THOMMEN/WOHLERS, S. 502.

315 FRISTER, § 3 N 29.

316 ACKERMANN, Eignungsdelikt, S. 4.

317 Vgl. BGE 145 IV 335 E. 3.1; Urteil des BGer 6B_1013/2020 vom 12. März 2024 E. 2.2; Urteil des BGer 6B_97/2019 vom 6. November 2019 E. 2.2; Urteil des BGer 6B_295/2019 vom 8. August 2019 E. 1.4; Urteil des BGer 6B_1208/2018 vom 6. August 2019 E. 3.1.

erfasst daher nicht nur den letzten, unmittelbar zur endgültigen Vereitelung führenden Schritt, sondern auch vorgelagerte Verhaltensweisen, die das Einziehungsinteresse gefährden, wie z.B. durch eine gezielte Verzögerung des staatlichen Zugriffs auf deliktisch erlangte Vermögenswerte.[318]

Die Beurteilung, welche Verhaltensweisen typischerweise geeignet sind, 180
die Einziehung zu vereiteln, hat der Gesetzgeber der Rechtsprechung überlassen.[319] Zur Strukturierung der bislang entwickelten Kasuistik hat ACKERMANN ein überzeugendes System gebildet, das geldwäschereirelevante Handlungen in fünf Fallgruppen unterteilt: die Schaffung von persönlicher, örtlicher und sachlicher Distanz sowie Verheimlichungs- und Manipulations-handlungen.[320] Die Herstellung persönlicher Distanz bezweckt, den Rückschluss vom Verbrechenserlös auf die wirtschaftlich berechtigte Person zu erschweren.[321] Dies erfolgt etwa durch Bareinzahlungen auf Konten von Strohpersonen, durch Zwischenschaltung von Berufsgeheimnisträgern oder durch die Einbringung der Werte in Trusts oder Stiftungen, während der Täter im Hintergrund die tatsächliche Kontrolle behält.[322] Örtliche Distanz beruht demgegenüber auf der geografischen Verlagerung der Vermögenswerte, typischerweise durch Überweisungen ins Ausland oder Transfers auf ausländische Wallets oder Konten.[323] Die Herstellung zeitlicher Distanz besteht darin, den Einsatz der Vermögenswerte hinauszuschieben, etwa durch das bewusste Zurückhalten oder Verstecken der Beute, bis der erste Ermittlungsdruck abgeklungen ist.[324] Von sachlicher Distanz spricht man, wenn der Wertträger gezielt verändert

318 ACKERMANN, Eignungsdelikt, S. 5.

319 Vgl. Botschaft StGB 1989, S. 1083; krit. STRATENWERTH/BOMMER, BT II, § 57 N 31; GIANNINI, S. 73 f.; GRABER, S. 131 ff.; BSK StGB II-PIETH, Art. 305bis N 38; PK StGB-PIETH/SCHULTZE, Art. 305bis N 17; VEST, Geldwäscherei, S. 55.

320 Vgl. ACKERMANN, Wirtschaftsstrafrecht, § 15 N 50 ff.; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 413 ff.; gl.M. GIANNINI, S. 73; LENGAUER/RUCKSTUHL, N 519; BSK StGB II-PIETH, Art. 305bis N 42; SUTER/REMUND, S. 58.

321 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 416; BOURQUIN, S. 192; KERN, Geldwäschereibekämpfung, S. 82; LENGAUER/RUCKSTUHL, N 519; ROTH, Kunsthandel, S. 53; SUTER/REMUND, S. 58.

322 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 416 ff.; vgl. BGE 127 IV 20 E. 3b; 124 IV 274 E. 4; 119 IV 242 E. 1; Urteil des BstGer SSK.2020.21 vom 15. Dezember 2021 E. 2.4.6.2; Urteil des BstGer SK.2020.40 vom 15. November 2021 E. 4.1.3.2; DONATSCH/THOMMEN/WOHLERS, S. 503; EGGER TANNER, S. 129 f.; KERN, Geldwäschereibekämpfung, S. 82; BSK StGB II-PIETH, Art. 305bis N 48.

323 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 454 ff.; BOURQUAIN, S. 196; KERN, Geldwäschereibekämpfung, S. 82; LENGAUER/RUCKSTUHL, N 519; ROTH, Kunsthandel, S. 53; SUTER/REMUND, S. 58; vgl. auch BGE 144 IV 172 E. 7.2.2; 127 IV 20 E. 3b; Urteil des BstGer SK.2020.21 vom 15. Dezember 2021 E. 2.4.6.2; Urteil des BstGer SK.2020.40 vom 15. November 2021 E. 4.1.3.2.

324 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 483 ff.; BOURQUAIN, S. 198 f.; KERN, Geldwäschereibekämpfung, S. 82; LENGAUER/RUCKSTUHL, N 519; ROTH, Kunsthandel,

wird, um Rückschlüsse auf seine Herkunft zu erschweren.[325] Dies kann durch den Umtausch von Bargeld in anderes Bargeld, in Buchgeld, in Fremdwährungen oder in andere Vermögenswerte erfolgen.[326] Ergänzend umfasst die Gruppe der Verheimlichungs- und Manipulationshandlungen sämtliche Verhaltensweisen, die unmittelbar auf die Verschleierung der Herkunft, der Verfügungsmacht oder der Bewegungen der Vermögenswerte gerichtet sind, etwa durch Vernichtung oder Fälschung von Unterlagen, die Umgehung von Identifikationspflichten oder den Einsatz falscher Identitäten.[327]

B. Nutzungsmuster bei der Verschleierung deliktischer Kryptowerte

181 Ausgehend von den zuvor dargestellten Phänomenlagen und den tatbestandlichen Grundlagen von Art. 305bis StGB stellt sich die Frage, in welchen typischen Konstellationen bereits auf der Blockchain zirkulierende deliktische Kryptowerte verschleiert werden. Im Folgenden werden jene Nutzungsmuster in den Blick genommen, bei denen die Interaktion der Nutzer mit dezentralisierten Anwendungen – namentlich mit Handelsplattformen und Kryptomixern – objektiv zu einer Herkunftsverschleierung führen und damit die Einziehung im Sinne von Art. 305bis Ziff. 1 StGB typischerweise zu vereiteln vermögen.

1. Dezentralisierte Handelsplattformen

182 Dezentralisierte Handelsplattformen ermöglichen den unmittelbaren Tausch von Kryptowerten zwischen Nutzern, ohne Beteiligung einer zentralen Vermittlungsinstanz.[328] Ein verbreitetes Modell beruht auf sogenannten Liquiditätspools: Nutzer hinterlegen Tokenpaare – etwa Ether und USD Coin – in einem Smart Contract, aus dessen Verhältnis sich der Preis algorithmisch

S. 53; SUTER/REMUND, S. 58; vgl. auch Urteil des BstGer SK.2020.21 vom 15. Dezember 2021 E. 2.4.6.2; Urteil des BstGer SK.2020.40 vom 15. November 2021 E. 4.1.3.2.

325 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 491 ff.; BOURQUAIN, S. 194 f.; KERN, Geldwäschereibekämpfung, S. 82; LENGAUER/RUCKSTUHL, N 519; BSK StGB II-PIETH, Art. 305bis N 47; ROTH, Kunsthandel, S. 53; SUTER/REMUND, S. 58.

326 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 492 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 35; PK StGB-PIETH/SCHULTZE, Art. 305bis N 18; vgl. auch BGE 145 IV 335 E. 3.1; 122 IV 211 E. 2c; Urteil des BGer 6B_124/2016 vom 11. November 2016 E. 5.1.

327 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 558 ff.; GIANNINI, S. 77; KERN, Geldwäschereibekämpfung, S. 82; PAJAROLA, N 510; SUTER/REMUND, S. 58; vgl. auch Urteil des BGer 6B_45/2021 vom 27. April 2022 E. 4.4.2; Urteil des BstGer SK.2019.77 vom 26. Juni 2020 E. 3.7.2.2.

328 Vgl. vorne N 85.

bestimmt. Der Pool stellt dadurch fortlaufend Liquidität bereit, ohne dass für jede Transaktion ein direktes Gegenüber erforderlich wäre.[329]

In der Praxis nutzen Täter dezentralisierte Handelsplattformen häufig als ersten Schritt zur Verschleierung deliktisch belasteter Vermögenswerte. Die dabei erhaltenen Token werden oft mehrfach und über verschiedene Plattformen hinweg gewechselt. Häufig erfolgt der Tausch gezielt in sogenannte native Token, also Vermögenswerte, die keiner zentralen Kontrollinstanz unterstehen und somit nicht eingefroren werden können.[330] Um die Rückverfolgung zusätzlich zu erschweren, werden die Werte in kleinere Einheiten aufgeteilt und über unterschiedliche Tokenpaare verteilt.[331] 183

Objektiv tatbestandsmässig im Sinne von Art. 305bis Ziff. 1 StGB ist eine Handlung dann, wenn sie den Zugriff der Strafbehörden auf die aus einem Verbrechen stammenden Vermögenswerte typischerweise zu behindern vermag.[332] Nach herrschender Lehre und Rechtsprechung liegt diese Eignung nicht bereits dann vor, wenn der Paper-Trail bloss verlängert oder begründet wird, sondern wenn zusätzliche Verschleierungshandlungen hinzutreten, bspw. durch eine Täuschung über die wirtschaftliche Berechtigung.[333] Vor diesem Hintergrund gelten einfache Inlandüberweisungen zwischen Konten desselben Berechtigten regelmässig nicht als tatbestandsmässig.[334] Entsprechend ist auch der einfache 1:1-Tausch deliktisch belasteter Kryptowerte über einen Smart Contract zu beurteilen. Eine derartige Transaktion führt zwar zum Austausch des ursprünglich belasteten Tokens gegen einen anderen, lässt jedoch sowohl die wirtschaftlich berechtigte Wallet-Adresse als auch 184

329 Vgl. vorne N 87; ANDREOTTI, S. 207; GOGEL et al., DeFi, S. 10; HUMBEL/ECKERT, S. 15; MEIRICH, N 391 ff.; WEF, DeFi, S. 10.

330 BENSON/TURKSEN/ADAMYK, S. 87; SIDORENKO, S. 826 f.; vgl. vorne N 81.

331 SIDORENKO, S. 826 f.

332 Vgl. BGE 145 IV 335 E. 3.1; Urteil des BGer 6B_1013/2020 vom 12. März 2024 E. 2.2; Urteil des BGer 6B_97/2019 vom 6. November 2019 E. 2.2; Urteil des BGer 6B_295/2019 vom 8. August 2019 E. 1.4; Urteil des BGer 6B_1208/2018 vom 6. August 2019 E. 3.1.

333 Vgl. BGE 127 IV 20 E. 3; 124 IV 274 E. 4a; Urteil des BGer 6B_88/2009 vom 29. Oktober 2009 E. 4.3; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 406 ff.; EGGER TANNER, S. 125; OFK StGB-ISENRING, Art. 305bis N 49, 16; BSK StGB II-PIETH, Art. 305bis N 43 f.

334 Vgl. BGE 124 IV 274 E. 4a; Urteil des BGer 6B_1201/2019 vom 1. Mai 2020 E. 3.4; Urteil des BGer 6B_217/2013 vom 28. Juli 2014 E. 3.4; Urteil des BGer 6B_1013/2010 vom 17. Mai 2011 E. 5.2; Urteil des BGer 6B_88/2009 vom 29. Oktober 2009 E. 4.3; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 407; DONATSCH/THOMMEN/WOHLERS, S. 503; EGGER TANNER, S. 126; CR CP II-CASSANI/VILLARD, Art. 305bis N 35. Auch bei Auslandsüberweisungen weicht die neuere Rechtsprechung des Bundesgerichts vom Erfordernis eines Unterbrechens des Paper-Trails ab (vgl. BGE 144 IV 172 E. 7.2.2; frühere Rechtsprechung: Urteil des BGer 6B_1013/2010 vom 17. Mai 2011 E. 5.2; Urteil des BGer 6B_88/2009 vom 29. Oktober 2009 E. 4.3; Urteil des BstGer SK.2015.55 vom 28. Oktober 2016 E. 3.1.2).

den Wert des Vermögensgegenstandes unverändert. Zudem bleibt die Transaktionsspur auf der Blockchain nachvollziehbar. Eine solche Handlung ist somit noch nicht tatbestandsmässig im Sinne von Art. 305bis Ziff. 1 StGB.

185 Davon abzugrenzen sind Konstellationen, in denen die Papierspur zwar erhalten bleibt, jedoch zusätzliche Kaschierungshandlungen hinzutreten, welche als tatbestandsmässige Vereitelungshandlung gelten.[335] Ein klassisches Beispiel bildet das sogenannte Structuring. Dabei werden deliktisch erlangte Vermögenswerte bewusst in zahlreiche kleinere Teilbeträge aufgespalten, um gesetzliche Schwellenwerte zu umgehen und automatisierte Kontroll- oder Meldeprozesse zu unterlaufen, wie dies etwa bei Bargeldeinzahlungen im traditionellen Finanzsystem vorkommt.[336] Ein vergleichbares Vorgehen zeigt sich auch im Zusammenhang mit dezentralisierten Handelsplattformen. Hierbei werden deliktisch belastete Kryptowerte in zahlreiche kleinere Transaktionen aufgespalten und über verschiedene Tokenpaare getauscht. Da auf einer Plattform jeder Swap eine eigenständige, in sich abgeschlossene Transaktion darstellt, entsteht durch diese Strukturierung eine Vielzahl isolierter Transaktionsspuren. Der ursprüngliche Zusammenhang zwischen den deliktischen Eingangsvermögenswerten und den resultierenden Token wird dadurch aufgelöst, sodass kein durchgehender, unmittelbar nachvollziehbarer Transaktionsfluss mehr erkennbar ist. Zwar bleibt die Papierspur auf der Blockchain formal bestehen, weil sämtliche Transaktionen öffentlich dokumentiert und technisch rekonstruierbar sind; die gezielte Aufteilung in viele unabhängige Einzelschritte erschwert jedoch die forensische Nachverfolgung.

186 Eine weitere Kaschierungshandlung liegt vor, wenn ein und derselbe Betrag mehrfach hintereinander über verschiedene Tokenpaare getauscht wird. Durch diese Abfolge von Swaps, teils über wenig gehandelte oder nur schwer rückverfolgbare Token, entsteht eine lange und technisch komplexe Transaktionskette. Zwar bleibt jede Einzeltransaktion für sich betrachtet nachvollziehbar, doch wird es für Strafverfolgungsbehörden zunehmend schwieriger, den Zusammenhang zur ursprünglichen deliktischen Quelle herzustellen. Dies gilt insbesondere, wenn bei jeder Tauschstation neue Adressen, Smart Contracts oder dezentralisierte Handelsplätze involviert sind. Auch aus ökonomischer Sicht erscheinen die beschriebenen Verhaltensmuster wenig plausibel. Die Vielzahl einzelner Transaktionen verursacht nicht nur kumulativ

335 Vgl. BGE 144 IV 172 E. 7.2.2; 122 IV 211 E. 2b; 119 IV 59 E. 2d; vgl. auch AK StGB-GRAF, Art. 305bis N 13 ff.

336 Vgl. BGE 119 IV 242 E. 1e; Urteil des BGer 6B_321/2010 vom 25. August 2010 E. 4.1; Urteil OG (ZH) SB130239-O/U/cs vom 22. August 2014 E. 6.4; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 524.

beträchtliche Gebühren, sondern bringt regelmässig auch Verluste durch ungünstige Wechselkurse oder sogenannte Slippage mit sich.

Die Vorgehensweisen des Structuring sowie der mehrfachen Token-Swaps 187
erinnern in ihrer Ausgestaltung an die vom Bundesgericht entwickelten Konstellationen geldwäschereitypischer Vorkehren im klassischen Finanzsystem. Ein Verschleierungsverdacht ergibt sich danach insbesondere dann, wenn Vermögenswerte über komplexe, fragmentierte Transaktionen unter Einbezug zahlreicher Akteure und Staaten verschoben werden.[337]

Ein weiterer Beweggrund für die Nutzung von Handelsplattformen liegt 188
in der Vermeidung von Einfrierungen sogenannter freezable Token, also insbesondere zentral emittierter Stablecoins wie Tether oder USD Coin, deren Smart Contracts eine technische Kontrollmöglichkeit durch die Herausgeber vorsehen.[338] Diese können auf Anweisung Adressen sperren und damit den Zugriff auf entsprechende Token unterbinden, was bspw. nach dem KuCoin-Hack oder dem Angriff auf PolyNetwork umgesetzt wurde.[339]

Um einem solchen Einfrieren zuvorzukommen, tauschen Täter belastete 189
Vermögenswerte häufig unmittelbar nach dem Delikt über dezentralisierte Handelsplattformen in unfreezable Token wie Ether, die keiner zentralen Kontrollinstanz unterstehen.[340] Da Kryptowerte grundsätzlich ein effektives Mittel zur Sicherstellung darstellen, führt die bewusste Verlagerung in nicht kontrollierbare Tokenformen dazu, dass diese Möglichkeit entfällt.

Die tatbestandsrelevante Gefährdung des Einziehungsinteresses liegt 190
bei der Interaktion mit Handelsplattformen nicht in einer Unterbrechung des Paper-Trails, sondern in der Komplexitätssteigerung der Transaktionsspur. Es handelt sich um zusätzliche Kaschierungshandlungen, die auf eine Erschwerung der Rückverfolgung ausgerichtet sind. Während ein einfacher Token-Tausch allein noch nicht als tatbestandsmässig zu qualifizieren ist, stellt die Kombination mit Techniken wie Structuring, wiederholtem Swapping oder dem gezielten Wechsel in unfreezable Assets eine Geldwäschereihandlung dar, da sie der bewussten Erschwerung der forensischen Nachvollziehbarkeit dient.[341]

337 Vgl. BGE 129 II 97 E. 3.3; Urteil des BGer 1B_394/2021 vom 16. Juni 2022 E. 3.4; Urteil des BGer 1B_339/2017 vom 5. Januar 2018 E. 2.5; Urteil des BGer 1B_713/2012 vom 21. Mai 2013 E. 3.4.2; MOLO/DRZALIC, S. 45; PK StGB-PIETH/SCHULTZE, Art. 305bis N 18; HK StGB-WOHLERS, Art. 305bis N 21.

338 Vgl. MAUCHLE, Registrierungsvereinbarung, S. 692 f.; ANDREOTTI, S. 583; MEIRICH, Fn. 442.

339 AKARTUNA; KMIELIAUSKAS.

340 Vgl. AKARTUNA.

341 A.M. ANDREOTTI, S. 361.

2. Kryptomixer

191 Kryptomixer, auch bekannt als Tumbler, sind Programme, die speziell dafür konzipiert sind, die unmittelbare Verbindung zwischen Einzahlungs- und Auszahlungsadressen auf der Blockchain zu überwinden.[342] Bei den auf Smart Contracts basierenden non-custodial Kryptomixern zahlen Nutzer eine standardisierte Menge an Kryptowährung in einen öffentlich zugänglichen Smart Contract ein.[343] Dort werden die Einzahlungen verschiedener Personen gebündelt und als gemeinsamer Vermögenspool verwaltet. Die berechtigten Nutzer können zu einem späteren Zeitpunkt denselben Betrag an eine neu gewählte Adresse auszahlen lassen.[344] Auf der Blockchain ist dabei nicht mehr ersichtlich, welche Einzahlung welcher Auszahlung zuzuordnen ist.

192 Hintergrund dieser Technologie ist die transparente Struktur öffentlicher Blockchains. Auch nach einem Transfer bleibt die Transaktionshistorie eines Tokens dauerhaft einsehbar.[345] Wird ein Kryptovermögenswert mit einer Straftat in Verbindung gebracht, verliert er faktisch seine Fungibilität, da viele Börsen und Dienstleister solche deliktischen Kryptowerte (Tainted Coins) ablehnen.[346] Kryptomixer setzen gezielt an dieser Problematik an, indem sie die Verbindung zwischen Herkunft und Weiterverwendung der Token aufheben und dadurch eine erneute Identifizierung erschweren.

193 Eine Verhaltensweise gilt im Sinne von Art. 305bis Ziff. 1 StGB typischerweise als geeignet, die Einziehung zu vereiteln, wenn sie zur Unterbrechung der sogenannten Papierspur führt.[347] Bei Kryptomixern erfolgt dies durch das Zusammenspiel mehrerer technischer Mechanismen. Sämtliche Einzahlungen erfolgen zunächst in standardisierter Höhe, beispielsweise exakt 1 Ether, und fliessen anschliessend in einen gemeinsamen Smart Contract, in welchem die Vermögenswerte nicht mehr individuell, sondern als kollektiver Pool verwaltet werden.[348] Bereits diese Vermischung der eingebrachten Vermögenswerte mit jenen anderer Nutzer erschwert die individuelle Zuordnung der Gelder und stellt eine zusätzliche Kaschierungshandlung dar. Einerseits

342 Vgl. Botschaft DLT, S. 26 f.; DUPUIS/GLEASON, S. 66; VAHRENHOLT DE LUCENA, S. 202; zur Funktionsweise von Kryptomixer vgl. vorne N 89.

343 Vgl. NADLER/SCHÄR, Tornado Cash, S. 123.

344 Vgl. NIEDERNHUBER, § 16 N 102; NADLER/SCHÄR, Tornado Cash, S. 123.

345 Vgl. vorne N 22.

346 Vgl. ANDREOTTI, S. 285; vorne N 89.

347 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 409; EGGER TANNER, S. 125; AK StGB-GRAF, Art. 305bis N 14; OFK StGB-ISENRING, Art. 305bis N 14; BSK StGB II-PIETH, Art. 305bis N 43 f., 47.

348 Vgl. SIDORENKO, S. 828.

verlieren die ursprünglichen Vermögenswerte durch die Zusammenführung mit weiteren Mitteln ihre individuelle Identifizierbarkeit, wodurch eine sachliche Distanz geschaffen wird. Andererseits wird die Zuordnung der Vermögenswerte zu einer bestimmten wirtschaftlich berechtigten Person erschwert, womit zugleich persönliche Distanz erzeugt wird.[349] Die spätere Auszahlung erfolgt zeitlich entkoppelt und an eine neue Adresse, die bisher in keinem Zusammenhang mit der Einzahlung stand. Der Anspruch auf Auszahlung wird dabei nicht über eine erkennbare Adressverbindung, sondern mittels eines kryptographischen Nachweises geltend gemacht, der die Identität der einzahlenden Adresse technisch nicht offenlegt. Dadurch wird die persönliche Distanz zusätzlich verstärkt. Gleichzeitig erschwert die zeitliche Entkopplung zwischen Ein- und Auszahlung die Rekonstruktion chronologischer Zusammenhänge.[350] In ihrer Kombination führen diese Elemente dazu, dass sich Ein- und Auszahlungen auf der Blockchain nicht mehr als zusammengehörige Vorgänge erkennen lassen. Der ursprüngliche Paper-Trail wird dadurch unterbrochen und die Rückverfolgung der Vermögenswerte erheblich erschwert.[351]

194 Die technischen Mechanismen von Kryptomixern entfalten ihre (geldwäscherei-)tatbestandsrelevante Wirkung also, indem sie mehrere Arten von Distanzen gleichzeitig erzeugen.[352] Während das Pooling der Vermögenswerte deren individuelle Identifizierbarkeit aufhebt und die Zuordnung zur wirtschaftlich berechtigten Person erschwert, verhindert die zeitlich entkoppelte Auszahlung an neue Adressen die Rekonstruktion eines durchgehenden Transaktionsverlaufs. Die Kombination dieser Effekte führt zur Unterbrechung der Papierspur und begründet die Eignung des Mischvorgangs, die Einziehung der Vermögenswerte zu vereiteln.

C. Nutzungsmuster bei der Konvertierung von Fiatgeld in Kryptowerte

195 Während sich die vorangehenden Ausführungen mit der Nutzung dezentralisierter Anwendungen zur Verschleierung bereits innerhalb des Blockchain-Systems zirkulierender deliktischer Vermögenswerte befassten, betrifft die nachfolgende Konstellation die Überführung kriminell erlangter Bargeld- oder Buchgeldbeträge in virtuelle Vermögenswerte.[353] In diesen Fällen stellt sich die Frage, inwiefern schon die Art des Zugangs zum Blockchain-System oder

349 Vgl. REGGIANI, S. 119.
350 Vgl. REGGIANI, S. 119.
351 Vgl. SIDORENKO, S. 828.
352 Vgl. vorne N 89.
353 Vgl. vorne N 149.

die daran anschliessenden Transaktionen geldwäschereirelevante Verschleierungshandlungen im Sinne von Art. 305bis Ziff. 1 StGB begründen können.

196 Dabei ist zu unterscheiden, über welchen Zugang die Umwandlung vorgenommen wird. Erfolgt die Konvertierung über eine identifikationspflichtige Börse oder einen regulierten Broker, entsteht ein dokumentierter Bezug zwischen dem eingesetzten Fiatgeld und einer konkreten Person. Diese Transaktion begründet einen neuen Paper-Trail – und stellt für sich allein noch keine tatbestandsmässige Geldwäschereihandlung nach Art. 305bis Ziff. 1 StGB dar.[354] Vergleichbar sind hier Fälle, in denen der Geldwäscher Bargeld auf sein eigenes Bankkonto einzahlt.[355]

197 Das Verschleierungsinteresse des Täters richtet sich hier vielmehr auf die nachgelagerten Vorgänge innerhalb des Blockchain-Ökosystems. Durch den Rückgriff auf Anwendungen wie Handelsplattformen oder Kryptomixer soll die Verbindung zur realen Identität im Nachhinein unkenntlich gemacht werden. Die geldwäschereirelevante Handlung liegt damit, gleich wie bei der ersten Konstellation, in der gezielten Unterbrechung der Transaktionsspur und der Entkopplung von Herkunft und wirtschaftlicher Berechtigung durch die Nutzung von dezentralisierten Finanzprotokollen.[356]

198 Anders verhält es sich, wenn der Täter zur Konvertierung auf einen nicht regulierten oder identifikationsfreien Fiat On-Ramp zurückgreift, wie bspw. auf einen Kryptoautomaten.[357] Zwar wird dabei grundsätzlich eine Transaktionsspur erzeugt, diese ist jedoch nicht mit jener bei Buchgeldtransaktionen vergleichbar. Es treten vielmehr typische Kaschierungsmechanismen hinzu. Durch den Transfer des Fiatgeldes auf eine Wallet-Adresse, die lediglich einem Pseudonym zugeordnet ist, entsteht eine persönliche Distanz zur realen Identität des Täters. Bereits mit der Platzierung in das Blockchain-System wird somit eine Entkopplung von der tatsächlichen Person bewirkt. Zudem verändert sich der Wertträger (aus Bargeld wird ein digitaler Vermögenswert), der sich unmittelbar weiterverwenden oder weiter transferieren lässt, wodurch zusätzlich eine sachliche Distanz geschaffen wird.

199 Sowohl das Bundesstrafgericht als auch das Obergericht des Kantons Bern haben in Fällen, in denen deliktische Gelder über Kryptoautomaten in

354 Vgl. BGE 127 IV 20 E. 3; 124 IV 274 E. 4a; Urteil des BGer 6B_88/2009 vom 29. Oktober 2009 E. 4.3; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 406 ff.; EGGER TANNER, S. 125; OFK StGB-ISENRING, Art. 305bis N 49, 16; BSK StGB II-PIETH, Art. 305bis N 43 f.

355 Vgl. BGE 127 IV 20 E. 3; 124 IV 274 E. 4a; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 493; DONATSCH/THOMMEN/WOHLERS, S. 503; PK StGB-PIETH/SCHULTZE, Art. 305bis N 18; HK StGB-WOHLERS, Art. 305bis N 22.

356 Vgl. vorne N 181.

357 Vgl. auch LAGISTORFER/GÜDEL.

das Blockchain-System eingebracht wurden, das Vorliegen einer Geldwäschereihandlung bejaht.[358]

Innerhalb dieser zweiten Konstellation ist daher zu differenzieren, ob der Zugriff auf die Blockchain über identifizierende oder anonymisierte Kanäle erfolgt. Eine tatbestandsmässige Geldwäschereihandlung nach Art. 305bis Ziff. 1 StGB liegt jedenfalls dann vor, wenn die Überführung in das Blockchain-System ohne oder unter nur rudimentären Identifizierungsmassnahmen erfolgt. 200

III. Zusammenfassung

Kryptowerte haben sich innert kurzer Zeit zu einem global etablierten Transaktions- und Vermögensmedium entwickelt. Ihre technischen Eigenheiten – insbesondere die dezentrale Architektur, die grenzüberschreitende Verfügbarkeit und die pseudonyme Ausgestaltung von Transaktionen – eröffnen legitime Nutzungsmöglichkeiten, schaffen aber zugleich spezifische Risiken für die Herkunftsverschleierung. Eine zentrale Rolle kommt dabei dezentralisierten Finanzanwendungen zu, die Wertübertragungen und -umwandlungen ohne zentrale Intermediäre ermöglichen und damit auch als Instrumente zur Erschwerung staatlicher Zugriffsmöglichkeiten dienen können. 201

Auf Grundlage der zuvor skizzierten kriminologischen Ausgangslage, wonach Kryptowerte in unterschiedlichen Deliktskontexten eingesetzt werden – etwa bei Ransomware, Betrugsschemata, Diebstählen digitaler Vermögenswerte, Zahlungen im Darknet, im klassischen Drogenhandel oder Terrorismusfinanzierung –, lassen sich geldwäschereirelevante Abläufe im Kern zwei Grundkonstellationen des klassischen Drei-Phasen-Modells zuordnen. Entweder werden sich bereits auf der Chain befindende deliktische Vermögenswerte verschleiert oder ausserhalb der Blockchain erlangte Gelder werden in Kryptowerte überführt. Während in der ersten Konstellation das Layering im Vordergrund steht, kommt in der zweiten der Art des Zugangs zum Blockchain-System besondere Bedeutung zu. 202

358 Vgl. Urteil des BGer 6B_584/2024 vom 27. November 2024 E. 3.2. Im Urteil des OG (BE) SK 23 90 vom 16. Februar 2024 E. 17.2.1 wurde argumentiert, dass durch die Einzahlung an den Bitcoin-Automaten jeweils eine erhebliche sachliche und räumliche Distanz geschaffen wurde und dass infolgedessen «der Nachweis der wirtschaftlichen Berechtigung an den Vermögenswerten unterlaufen werde, zumal Kryptowährungen sehr schnell weiterüberwiesen werden können». Hierbei ist anzufügen, dass das Gericht die Schaffung räumlicher Distanz nicht bereits in der Einzahlung am Bitcoin-Automaten selbst sah, sondern diese erst auf die nachfolgende Weiterleitung der Wallet-Zugangsdaten ins Ausland zurückführte.

203 Aus rechtlicher Sicht ist nicht jede Interaktion mit dezentralisierten Anwendungen tatbestandsmässig. Art. 305bis Ziff. 1 StGB erfasst nur jene Handlungen, die über die blosse Verlängerung des Paper-Trails hinausgehen und typischerweise geeignet sind, die Einziehung zu vereiteln. Ein einfacher 1:1-Tausch über einen Smart Contract, der weder den wirtschaftlich Berechtigten noch den Wertträger verändert, erreicht diese Schwelle regelmässig nicht. Tatbestandsrelevanz entsteht erst durch zusätzliche Kaschierungshandlungen – z.B. durch die Aufspaltung von Vermögenswerten in zahlreiche Transaktionen (Structuring), wiederholte Token-Swaps über mehrere Paare hinweg oder den gezielten Wechsel in unfreezable Token, die einer behördlichen Sicherstellung entzogen sind.

204 Bei Kryptomixern knüpft die tatbestandsmässige Eignung bereits an den Kernmechanismus an. Die Kombination aus standardisierten Einzahlungsbeträgen, Pooling der Vermögenswerte, zeitlich entkoppelter Auszahlung und Nutzung kryptographischer Beweise zur Geltendmachung des Auszahlungsanspruchs durchtrennt die Papierspur und erzeugt gleichzeitig sachliche, persönliche und zeitliche Distanz.

205 Schliesslich zeigt die Analyse der Konvertierung von Fiatgeld, dass die Geldwäschereirelevanz massgeblich von der Art des Zugangs zum Blockchain-System abhängt: Während identifikationspflichtige Börsen einen neuen Paper-Trail schaffen und für sich genommen noch keine Verschleierung darstellen, begründet die Nutzung nicht regulierter, pseudonymer Fiat On-Ramps – etwa Kryptoautomaten – bereits in der Platzierungsphase persönliche und sachliche Distanz und erfüllt nach der Rechtsprechung regelmässig den Tatbestand von Art. 305bis Ziff. 1 StGB.

206 Insgesamt verdeutlicht das Kapitel, dass geldwäschereirelevante Handlungen im Umgang mit Kryptowerten typischerweise an den Stellen ansetzen, an denen dezentralisierte Anwendungen den Bruch von Identitäts-, Wert- oder Chronologieketten ermöglichen. Für die spätere Beurteilung der Betreiberstrafbarkeit ist daher entscheidend, welche dieser objektiven Verschleierungsmechanismen durch die von Betreiberinnen bereitgestellten Strukturen ermöglicht werden.

Teil 2: Betreiberverantwortlichkeit für Geldwäscherei

Nachdem die technischen und juristischen Grundlagen im ersten Teil der Arbeit aufgearbeitet wurden, widmet sich der zweite Teil nun der eigentlichen Forschungsfrage, ob Betreiberinnen dezentralisierter Finanzanwendungen für Geldwäschereihandlungen ihrer Nutzer nach Art. 305bis StGB strafrechtlich zur Verantwortung gezogen werden können. Zunächst wird untersucht, ob eine Begehensstrafbarkeit in Betracht kommt. Im Fokus steht dabei die Qualifikation des Bereitstellens bzw. Deployments einer Anwendung als tatbestandsrelevantes Tun sowie die Einordnung des Verhaltens als Täterschaft oder Teilnahme (Kap. 1). Daran anschliessend wird geprüft, ob sich Betreiberinnen auch durch Unterlassen strafbar machen können (Kap. 2). Behandelt werden hierfür die Voraussetzungen unechter Unterlassungsdelikte im Kontext automatisierter und pseudonym genutzter Finanzsysteme, namentlich das Bestehen einer Garantenstellung, die hypothetische Kausalität, die Tatmacht und die subjektive Tatseite. Abschliessend befasst sich der letzte Teil dieser Untersuchung mit dem Vorliegen von Qualifikationstatbeständen im Sinne von Art. 305bis Ziff. 2 StGB, mit möglichen Konkurrenzverhältnissen sowie mit den Anknüpfungspunkten einer schweizerischen Strafhoheit (Kap. 3). 207

Kapitel 1: Begehensstrafbarkeit nach Art. 305bis StGB

Im nachfolgenden Kapitel wird zunächst dargestellt, welches Rechtsgut durch den Geldwäschereitatbestand geschützt wird, ob Kryptowerte als taugliche Objekte der Geldwäscherei in Betracht kommen und welche Vortaten im Zusammenhang mit dezentralisierten Finanzprotokollen in Frage kommen (I.). Darauf aufbauend wird untersucht, an welches aktive Handeln der Betreiberin angeknüpft werden kann und ob sie hierdurch als unmittelbare Täterin oder aufgrund von Zurechnung als Mittäterin in Betracht kommt (II.). Abschliessend werden die Voraussetzungen und Grenzen einer Strafbarkeit wegen Teilnahmehandlungen in Form der Anstiftung und Gehilfenschaft analysiert (III.). 208

I. Rechtsgut, Geldwäschereiobjekt und Vortat

209 Wie bereits im ersten Teil dieser Arbeit dargelegt, schützt der Geldwäschereitatbestand nach Art. 305bis StGB gemäss der Rechtsprechung sowie einem Teil der Lehre grundsätzlich das staatliche Einziehungsinteresse bzw. die Rechtspflege.[359] Bei Vermögensdelikten als Vortaten wird zudem gemäss der bundesgerichtlichen Rechtsprechung auch das Vermögen der durch die Vortat individuell Geschädigten geschützt.[360]

210 Tatobjekt der Geldwäscherei können alle Vermögenswerte sein, die aus einem tatbestandsmässigen und rechtswidrigen Verbrechen im Sinne von Art. 10 Abs. 2 StGB oder aus qualifizierten Steuervergehen herrühren.[361] Der Verbrechensbegriff ist dabei im technischen Sinne zu verstehen. Er erfasst ungeachtet des geschützten Rechtsguts sämtliche Delikte, für welche das Gesetz abstrakt eine Freiheitsstrafe von mehr als drei Jahren androht.[362]

211 Vom Tatbestand erfasst werden sämtliche Vermögenswerte, welche einen wirtschaftlichen Wert aufweisen und hypothetisch einziehbar sind.[363] Kryptowerte, die dezentralisierten Finanzanwendungen mit dem Zweck der Geldwäscherei zugeführt werden, stellen ein taugliches Tatobjekt in diesem Sinne dar, zumal sie in der Praxis als Tausch- und Zahlungsmittel fungieren.[364] Typischerweise rühren sie aus Verbrechen her, bei denen entweder bereits virtuelle Vermögenswerte verwendet wurden (on-chain), oder aus solchen,

359 Vgl. vorne N 176; BGE 146 IV 211 E. 4.2.1; 145 IV 335 E. 3.1; 129 IV 322 E. 2.2.4; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 92; CR CP II-CASSANI/VILLARD, Art. 305bis N 10 f.; DONATSCH/THOMMEN/WOHLERS, S. 493 f.; PK StGB-PIETH/SCHULTZE, Art. 305bis N 6.

360 Vgl. BGE 146 IV 211 E. 4.2.1; 145 IV 335 E. 3.1; 129 IV 322 E. 2.2.4; gl.M. CR CP II-CASSANI/VILLARD, Art. 305bis N 10; AK StGB-GRAF, Art. 305bis N 1; OFK StGB-ISENRING, Art. 305bis N 9; HK StGB-WOHLERS, Art. 305bis N 1; krit. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 97.

361 Vgl. Botschaft StGB 1989, S. 1082; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 245 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 17; DONATSCH/THOMMEN/WOHLERS, S. 495; GRABER, S. 128; BSK StGB II-PIETH, Art. 305bis N 9 ff.; AK StGB-GRAF, Art. 305bis N 5; OFK StGB-ISENRING, Art. 305bis N 30; STRATENWERTH/BOMMER, BT II, § 57 N 27.

362 Vgl. Botschaft StGB 1989, S. 1082; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 248; CR CP II-CASSANI/VILLARD, Art. 305bis N 17; DONATSCH/THOMMEN/WOHLERS, S. 495; EGGER TANNER, S. 38; PK StGB-PIETH/SCHULTZE, Art. 305bis N 10.

363 Vgl. Botschaft StGB 1989, S. 1082; ACKERMANN et al., S. 223; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 334; DONATSCH/THOMMEN/WOHLERS, S. 495; AK StGB-GRAF, Art. 305bis N 7; BSK StGB II-PIETH, Art. 305bis N 9; STRATENWERTH/BOMMER, BT II, § 57 N 26; HK StGB-WOHLERS, Art. 305bis N 3.

364 Vgl. vorne N 177; Bundesrat, Virtuelle Währungen, S. 7, 11; MOLO/DRZALIC, S. 42; STENGEL/PAYDAR, N 18.07, 18.10; vgl. auch Botschaft StGB 1989, S. 1082; MOLO/BRUNONE, S. 301.

bei denen der deliktische Ertrag zunächst in Fiatwährungen bestand und erst nachträglich in Kryptowerte überführt wurde (off-chain).[365] Verbrechen, die in diesem Zusammenhang von besonderer Relevanz sind, ergeben sich in erster Linie aus Deliktsphänomenen wie Hacking, Ransomware, Scams, Handel mit illegalen Gütern oder Dienstleistungen oder Terrorismusfinanzierung.[366]

212 Klassischerweise bilden, vorbehaltlich der geringfügigen Vermögensdelikte (Art. 172ter StGB), Vermögensdelikte die typischen verbrecherischen Vortaten der Geldwäscherei. Eine zentrale Rolle nehmen insbesondere im Zusammenhang mit Hacking-, Ransomware- und Scam-Konstellationen verschiedene Cyberdelikte[367] wie namentlich die unbefugte Datenbeschaffung (Art. 143 Abs. 1 StGB), das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143 Abs. 1 StGB), die qualifizierte Datenbeschädigung (Art. 144bis Ziff. 1 Abs. 1 und Ziff. 2 Abs. 2 StGB) sowie der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 143 Abs. 1 und 2 StGB) ein. Darüber hinaus kommen aber auch der Betrug (Art. 146 Abs. 1 und 2 StGB) oder die Erpressung (Art. 156 StGB), z.B. im Zusammenhang mit einer Ransomware-Lösegeldforderung, in Betracht.[368] Schliesslich sind auch Straftatbestände relevant, die im Kontext des Handels mit illegalen Gütern und Dienstleistungen über das Darknet stehen, namentlich Verstösse gegen das Betäubungsmittelgesetz gemäss Art. 19 Abs. 2 BetmG.[369] Ebenfalls von Bedeutung ist der Tatbestand der Terrorismusfinanzierung (Art. 260ter Abs. 1 lit. b bzw. Art. 260quinquies StGB).[370]

213 Unerheblich ist indes, ob die Vortat im In- oder Ausland begangen wurde, sofern sie nach dem Recht des Tatorts strafbar ist und in der Schweiz als taugliche Vortat gilt.[371]

365 Vgl. vorne N 149; KGGT, NRA 2024, S. 52 ff.; KGGT, NRA 2018, S. 21 ff.; Financial Crime Academy; GABBIADINI/GOBBI/RUBERA, S. 13.

366 Vgl. vorne N 152 ff.; KGGT, NRA 2024, S. 53 ff.; KGGT, NRA 2018, S. 26 ff.; Chainalysis, 2025, S. 10 ff.; COLLINS, S. 13 ff.; U.S. Department of the Treasury, S. 18 ff.

367 Zum Begriff Bundeskriminalamt Deutschland, S. i; GYARMATI, S. 87; vgl. auch STÜRMER, S. 291.

368 Vgl. BENHAMOU/WANG, S. 82; GERMANN/WICKI-BIRCHLER, Fn. 39.

369 Vgl. auch KGGT, NRA 2024, S. 54; KGGT, NRA 2018, S. 28 f.; Chainalysis, 2025, S. 23 ff.; COLLINS, S. 18; FOLEY/KARLSEN/PUTNIŅŠ, S. 1798 ff.; U.S. Department of the Treasury, S. 23 f.

370 Vgl. auch KGGT, NRA 2018, S. 27 f.; Chainalysis, 2025, S. 105 ff.

371 Vgl. Urteil des BGer 6B_341/2019 vom 21. Februar 2020 E. 1.3.1; DONATSCH/THOMMEN/WOHLERS, S. 497 f.; BSK StGB II-PIETH, Art. 305bis N 67; PK StGB-PIETH/SCHULTZE, Art. 305bis N 28.

II. Täterschaft

A. Tun durch Bereitstellen einer Infrastruktur

214 Ausgangspunkt der weiteren Analyse ist die Frage, welches Verhalten der Betreiberin als tatbestandsrelevantes aktives Tun im Sinne von Art. 305bis StGB qualifiziert werden kann. Zu prüfen ist daher, ob ein allfälliger strafrechtlicher Anknüpfungspunkt im Deployment der Finanzanwendung beziehungsweise der Smart Contracts zu sehen ist oder ob das spätere Betreiben (im engeren Sinne) der Anwendung als aktives Handeln in Betracht kommt.

215 Nach dem in der schweizerischen Doktrin geltenden Subsidiaritätsprinzip knüpft das Strafrecht primär an ein aktives Handeln an; ein Unterlassen kommt nur dann in Betracht, wenn kein tatbestandsrelevantes Tun vorliegt.[372] Für das Vorliegen einer aktiven Handlung können im vorliegenden Kontext einerseits das initiale Bereitstellen der Finanzanwendung beziehungsweise der Smart Contracts im Sinne des Deployments[373] sowie grundsätzlich das überdauernde Betreiben (im engeren Sinne)[374], das heisst die administrative Kontrolle bzw. Verwaltung über die Anwendung, einschlägig sein.

216 Dabei ist zu berücksichtigen, dass dezentralisierte Finanzanwendungen einerseits vollautomatisiert funktionieren und andererseits als für jedermann frei zugängliche Infrastruktur ausgestaltet sind.[375] Nutzer interagieren direkt mit den Smart Contracts, sodass die Betreiberin bei der Nutzung der Anwendung regelmässig nicht aktiv tätig wird. Eine Anknüpfung an ein ‹Betreiben› scheidet daher als tatbestandsrelevantes Tun aus, weil sich die Smart-Contract-Prozesse vollständig selbsttätig vollziehen und die Rolle der Betreiberin faktisch auf ein passives Bereitstellen reduziert bleibt.[376] Ein aktives Handeln wäre nur dann denkbar, wenn die Betreiberin die Nutzer prüfen oder freischalten müsste,[377] was bei den vorliegend interessierenden offen zugänglichen

372 BGE 129 IV 119 E. 2.2; 122 IV 145 E. 2; 122 IV 17 E. 2b/aa; Urteil des BGer 6B_1148/2018 vom 6. Dezember 2018 E. 2.3.1; DONATSCH/GODENZI/TAG, S. 311; FLACHSMANN, S. 20; GETH, N 275; GRAVEN/STRÄULI, S. 78; KILLIAS/KUHN/DONGOIS, S. 64; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 53; STRATENWERTH/BOMMER, AT I, § 14 N 2; TRECHSEL et al., S. 252.

373 Vgl. vorne N 120.

374 Vgl. vorne N 121.

375 Vgl. vorne N 71 f.

376 Vgl. BGE 121 IV 109 E. 3b; vgl. zum deutschen Recht CEFFINATO, Internetplattformbetreiber, S. 407; EQUEY, N 360; GRECO, S. 440; Netzwerkkriminalität, S. 67; ZÖLLER, Strafbarkeit, S. 85; anders aber BACHMANN/ARSLAN, S. 243; ROSENTHAL, N 18 f.

377 Vgl. CECCINATO, S. 404; BÄCHER, S. 149; WÜST, S. 68 betreffend Betreiberinnen von Darknetplattformen; vgl. auch LG Karlsruhe 4 KLs 608 Js 19580/17 vom 19. Dezember 2018, BeckRS 2018, 40013, N 312 ff.; für eine vergleichbare Argumentation im Zusammenhang mit dem Bereitstellen von Mailboxen RIKLIN, Mailbox, S. 108.

Anwendungen gerade nicht der Fall ist.[378] Als einziges potenziell relevantes Tun verbleibt somit das Deployment des Smart-Contract-Codes, das heisst das anfängliche Zurverfügungstellen der Finanzanwendung, welche anschliessend von den Nutzern als Tatwerkzeug für deliktische Zwecke missbraucht werden kann.[379]

B. Unmittelbare Täterschaft

In einem nächsten Schritt ist zu klären, ob bereits das Deployment bzw. die Bereitstellung einer dezentralisierten Finanzanwendung per se durch die Betreiberin den objektiven Tatbestand der Geldwäscherei im Sinne von Art. 305bis Ziff. 1 StGB erfüllen kann. 217

Der Geldwäschereitatbestand nach Art. 305bis Ziff. 1 StGB erfasst Handlungen, die geeignet sind, die Ermittlung der Herkunft, die Auffindung oder die Einziehung von Vermögenswerten zu vereiteln. Nach herrschender Lehre und Rechtsprechung kommt jedoch der Vereitelung der Herkunftsermittlung und der Auffindung keine eigenständige Bedeutung zu, da beide in der Vereitelung der Einziehung aufgehen.[380] 218

Als abstraktes Gefährdungsdelikt ist bereits eine Handlung tatbestandsmässig, die typischerweise geeignet ist, die Einziehungsinteressen der Strafverfolgung abstrakt zu gefährden.[381] Es ist weder erforderlich, dass ein Vereitelungserfolg eingetreten ist, noch dass die Einziehungsbemühungen der Behörden konkret gefährdet sind.[382] Es genügt, wenn eine Handlung erfahrungsgemäss die Möglichkeit einer Rechtsgutsverletzung (konkret: der Vereitelung der Einziehung) begründet.[383] Die bundesgerichtliche Rechtsprechung qualifiziert bereits ein Verhalten als tatbestandsmässig, das geeignet ist, den behördlichen Zugriff auf aus einem Verbrechen stammende Vermögenswerte zu behindern.[384] 219

378 Vgl. vorne N 71 ff.

379 Vgl. CECCINATO, S. 405.

380 M.w.H. BSK StGB II-PIETH, Art. 305bis N 37; vgl. BGE 129 IV 238 E. 3.3; 126 IV 255 E. 3a; 119 IV 242 E. 1; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 390; CR CP II-CASSANI/VILLARD, Art. 305bis N 34; GIANNINI, S. 74; GRABER, S. 139.

381 Vgl. Botschaft StGB 1989, S. 1083; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 106 f.; DONATSCH/THOMMEN/WOHLERS, S. 502; EGGER TANNER, S. 121; GRABER, S. 133; PK StGB-PIETH/SCHULTZE, Art. 305bis N 17, 30.

382 Vgl. vorne N 181; Botschaft StGB 1989, S. 1083; BGE 136 IV 188 E. 6.1; 127 IV 20 E. 3a; 119 IV 59 E. 2e; Urteil des BGer 6B_295/2022 vom 15. September 2022 E. 1.2; CR CP II-CASSANI/VILLARD, Art. 305bis N 10; DONATSCH/THOMMEN/WOHLERS, S. 502.

383 FRISTER, § 3 N 29.

384 Vgl. BGE 145 IV 335 E. 3.1; Urteil des BGer 6B_1013/2020 vom 12. März 2024 E. 2.2; Urteil des BGer 6B_97/2019 vom 6. November 2019 E. 2.2; Urteil des BGer 6B_295/2019 vom 8. August 2019 E. 1.4; Urteil des BGer 6B_1208/2018 vom 6. August 2019 E. 3.1.

220 Zur Strukturierung typischer Tathandlungen unterscheidet ACKERMANN zwischen Handlungen zur Schaffung persönlicher, örtlicher, zeitlicher oder sachlicher Distanz sowie Verheimlichungs- und Manipulationshandlungen.[385] Alle genannten Verhaltensweisen verfolgen das Ziel, die deliktische Herkunft der Vermögenswerte zu verschleiern und deren behördliche Rückverfolgung zu erschweren.[386]

221 Das blosse Bereitstellen einer öffentlich zugänglichen technischen Infrastruktur erfüllt diese Voraussetzungen jedoch nicht. Es fehlt sowohl an einem konkreten Bezug zu einer deliktischen Herkunft einzelner Vermögenswerte als auch an einem Verhalten, das typischerweise auf die Verschleierung oder Entziehung von Zugriffsmöglichkeiten zielt. Die potenzielle Gefährdung der Einziehungsinteressen entsteht erst durch das Handeln der Nutzer, sei es durch konkrete Interaktionen mit dem Smart Contract oder durch Transaktionen, die in die klassischen Fallgruppen geldwäschereirelevanter Handlungen einzuordnen sind. Ohne dieses Zusammenwirken tritt die für den Tatbestand erforderliche Eignung zur Vereitelung nicht zutage. Das Deployment allein begründet daher keine unmittelbare Täterschaft nach Art. 305bis Ziff. 1 StGB.[387]

C. Mittäterschaft

222 Wie bereits gezeigt, kann die blosse Bereitstellung der Finanzanwendungsinfrastruktur durch die Betreiberin keine selbständige Verwirklichung des Geldwäschereitatbestands begründen. In einem nächsten Schritt ist daher zu prüfen, ob eine Strafbarkeit der Betreiberin aufgrund der Zurechnung von Nutzerhandlungen im Sinne einer Mittäterschaft in Betracht kommt.

1. (Mit-)Tatherrschaft

223 Ob ein Tatbeitrag als Teilnehmer oder Mittäter geleistet wurde, beurteilt sich gemäss der ständigen Rechtsprechung des Bundesgerichts und der herrschenden Lehre nach der Tatherrschaftstheorie.[388] Mittäter ist, «wer bei der Entschliessung, Planung oder Ausführung eines Delikts vorsätzlich und in massgebender Weise mit anderen Tätern zusammenwirkt, sodass er als Haupt-

385 Vgl. vorne N 180; ACKERMANN, Wirtschaftsstrafrecht, § 15 N 50 ff.; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 413 ff.; zustimmend GIANNINI, S. 73; LENGAUER/RUCKSTUHL, N 519; BSK StGB II-PIETH, Art. 305bis N 42; SUTER/REMUND, S. 58.

386 Vgl. vorne N 177; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 413 ff.

387 Anders aber GRECO, S. 440, der eine mögliche unmittelbare Täterschaft der Betreiberinnen von Kryptomixern bejaht.

388 DONATSCH/GODENZI/TAG, S. 187; AK StGB-NYDEGGER, Vor Art. 24 ff. N 5; TRECHSEL et al., S. 208; vgl. BGE 133 IV 76 E. 2.7; 130 IV 58 E. 9.2.1; 126 IV 84 E. 2c/aa; Urteil des BGer 6B_1206/2018 vom 17. Mai 2019 E. 2.3.3; STRATENWERTH/BOMMER, AT I, § 13 N 59.

beteiligter dasteht».[389] Erforderlich für das Vorliegen der Mittäterschaft ist, ob (Mit-)Tatherrschaft besteht resp. ob eine Mitwirkung in «massgebender» Weise vorliegt.[390] Im Sinne der funktionellen Tatherrschaft verlangt das Bundesgericht zudem, dass «der Tatbeitrag nach den Umständen des konkreten Falles und dem Tatplan für die Ausführung des Delikts so wesentlich ist, dass sie mit ihm steht oder fällt».[391]

Sofern Tatherrschaft besteht, bejahen ein Teil der Lehre sowie die Rechtsprechung Mittäterschaft auch bei Tatbeiträgen im Vorbereitungsstadium der Tat sowie bei Tatbeiträgen, welche die Ausführung der Tat erleichtern.[392] Dies ist der Fall, wenn sie nach dem Gesamtplan «im Ausführungsstadium eine unerlässliche Voraussetzung für die Verwirklichung des angestrebten Erfolges bilden».[393] Die Annahme von Tatherrschaft knüpft bei vorbereitenden Tatbeiträgen daran an, dass diese zumindest in die Ausführungsphase (wesentlich) weiterwirken müssen,[394] das heisst, dass «der Beteiligte weiterhin das Geschehen verfolgen muss in einer Weise, die für die Ausführenden mitbestimmend ist»,[395] oder er «kraft seiner Beziehung zu den Ausführenden aber weiterhin einen tragenden Einfluss ausübt».[396] In der Rechtsprechung wurde Mittäterschaft trotz fehlender Mitwirkung im Ausführungsstadium namentlich bejaht, wenn eine Person an Planung und Organisation einer Straftat beteiligt war oder sonst eine leitende Funktion innehatte, durch welche Beteiligte im Ausführungsstadium gelenkt wurden.[397] Gleiches gilt bei 224

389 BGE 133 IV 76 E. 3.2.1; 130 IV 58 E. 9.2.1; 125 IV 134 E. 3a; 120 IV 265 E. 2c/aa; 118 IV 227 E. 5d/aa; vgl. DONATSCH/GODENZI/TAG, S. 178; BSK StGB I-FORSTER, Vor Art. 24 N 9; STRATENWERTH/BOMMER, AT I, § 13 N 59; CR CPI I-STRÄULI, Intro aux art. 24-27 N 97 f.

390 Vgl. DONATSCH/GODENZI/TAG, S. 178; BSK StGB I-FORSTER, Vor Art. 24 N 9; AK StGB-NYDEGGER, Vor Art. 24 ff. N 18; STRATENWERTH/BOMMER, AT I, § 13 N 59; CR CP I-STRÄULI, Intro aux art. 24-27 N 97 f.; vgl. auch BGE 133 IV 76 E. 2.7; 118 IV 397 E. 2b; 108 IV 88 E. I.1b.

391 STRATENWERTH/BOMMER, AT I, § 13 N 61; DONATSCH/GODENZI/TAG, S. 178; BSK StGB I-FORSTER, Vor Art. 24 N 9; GRAVEN/STRÄULI, S. 290; TRECHSEL et al., S. 208.; vgl. BGE 135 IV 152 E. 2.3.1; 133 IV 76 E. 2.7; 130 IV 58 E. 9.2.1; 126 IV 84 E. 2c/aa; 125 IV 134 E. 3a; 120 IV 265 E. 2c/aa.

392 BGE 133 IV 76 E. 2.7; 108 IV 88 E. I.2a; 101 IV 306 E. 8b; 88 IV 53 E. 4; DONATSCH/GODENZI/TAG, S. 184; BSK StGB I-FORSTER, Vor Art. 24 N 9; STRATENWERTH/BOMMER, AT I, § 13 N 61; PK StGB-TRECHSEL/GETH, Vor Art. 24 N 18; TRECHSEL et al., S. 210; HK StGB-WOHLERS, Vor Art. 24 ff. N 18; a.M. GETH, N 423; CR CP I-STRÄULI, Intro aux art. 24-27 N 97.

393 STRATENWERTH/BOMMER, AT I, § 13 N 61 f.; vgl. BGE 130 IV 58 E. 9.2.1; 120 IV 265 E. 2c; 118 IV 397 E. 2; 118 IV 227 E. 5d; PK StGB-TRECHSEL/GETH, Vor Art. 24 N 18; VEST et al., AT, S. 194 f.; a.M. CR CP I-STRÄULI, Intro aux Art. 24-27 N 97.

394 STRATENWERTH/BOMMER, AT I, § 13 N 61.

395 PK StGB-TRECHSEL/GETH, Vor Art. 24 N 18.

396 BGE 143 IV 361 E. 4.10; 120 IV 265 E. 2c/aa; vgl. TRECHSEL et al., S. 210.

397 STRATENWERTH/BOMMER, AT I, § 13 N 62; BSK StGB I-FORSTER, Vor Art. 24 N 9; PK StGB-TRECHSEL/GETH, Vor Art. 24 N 18; vgl. BGE 98 IV 255 E. 5; 91 IV 218 E. 2; 85 IV 130 E. 3; 81 IV 60 E. 2.

Finanzierung[398] oder wenn ein Delikt im Rahmen betrieblicher Organisationen ohne Weisungen nicht begangen worden wäre.[399]

225 Abzulehnen ist eine kategorische Bejahung der (Mit-)Tatherrschaft bei Tatbeiträgen im Vorbereitungsstadium, die conditio sine qua non zur Tat sind.[400] Ein solches Erfordernis würde bedeuten, dass Tatherrschaft bejaht wird, wenn es ohne den Tatbeitrag nicht zur Tat gekommen wäre.[401] Hierbei ist jedoch anzuführen, dass bspw. mit dem Bereitstellen des Tatwerkzeugs erst die Bedingungen der Deliktsbegehung geschaffen werden, die vollständige Deliktsausgestaltung jedoch der tatausführenden Person überlassen wird.[402] Ebenso wenig Tatherrschaft begründend ist das Interesse am Erfolg (z.B. durch anteilsmässige Beteiligung an der Tatbeute) der Tat.[403]

226 Im Kontext von dezentralisierten Protokollen ist das Bereitstellen der Finanzanwendung bzw. das Deployment der Smart Contracts dem tatbestandsrelevanten Verhalten des Nutzers (der Interaktion mit den Smart Contracts) zeitlich vorgelagert. Im weiteren Verlauf greift die Betreiberin nicht mehr in das Geschehen ein, da sie aufgrund der automatisierten Funktionsweise der Plattform weder Freischaltungen oder vorgelagerte Prüfungen vornimmt noch an der Ausführung der eigentlichen Zwecktätigkeit, etwa dem Austausch von Vermögenswerten, beteiligt ist. Ihr Beitrag beschränkt sich damit auf das Vorbereitungsstadium der Tat.[404]

227 Dieser Tatbeitrag ist zwar conditio sine qua non für die Deliktsausführung des Nutzers mittels der Smart Contracts, da ohne das Deployment der Smart Contracts kein Zugriff auf die Infrastruktur und damit keine Ausführung der Geldwäschereihandlung möglich gewesen wäre. Dass der Beitrag die Deliktsbegehung ermöglicht, genügt jedoch – zumindest in der Vorbereitungsphase

398 Vgl. BGE 70 IV 101 E. 2; vgl. auch BGE 80 IV 258 E. I.2.

399 Vgl. BGE 120 IV 24 E. 2d; 96 IV 169 E. I; 77 IV 88 E. 1.

400 Vgl. Urteil des BGer 6B_42/2016 vom 26. Mai 2016 E. 3.1; Urteil des OG (SO) STBER.2023.61 vom 12. März 2024 E. 3.1.6; Urteil des OG (SO) STBER.2017.61 vom 18. April 2018 E. 2.1; Urteil des OG (BE) SK 22 512 vom 21. April 2016 E. 15.3.

401 Vgl. STRATENWERTH/BOMMER, AT I, § 13 N 61; m.w.H. zur Conditio-sine-qua-non-Formel RIEDO, N 2184 ff.; anstatt vieler BGE 143 IV 330 E. 2.5; 130 IV 58 E. 9.1.1; 109 IV 94 E. 3; Urteil des BGer 6B_1002/2021 vom 3. Oktober 2022 E. 3.3.1; DONATSCH/GODENZI/TAG, S. 106; GETH, N 101; AK StGB-GRAF, Art. 12 N 33; BSK StGB I-NIGGLI/MAEDER, Art. 12 N 90.

402 BOMMER, ZBJV 2008, S. 854; STRATENWERTH/BOMMER, AT I, § 13 N 61; m.w.V. NYDEGGER, S. 91.

403 Urteil des BGer 6B_452/2023 vom 20. Oktober 2023 E. 3.4; m.V.a. HK StGB-WOHLERS, Vor Art. 24 ff. N 19; VEST et al., AT, S. 196; zumindest als Indiz für eine Tatherrschaft verstehend vgl. DONATSCH/GODENZI/TAG, S. 178.

404 Ähnlich auch im Kontext von Plattformbetreibern im Darknet BÄCHER, S. 150; CEFFINATO, Internetplattformbetreiber, S. 408; GRECO, S. 440 f.; WEBER, Darknet, S. 132 f.; WÜST, S. 87 f.

des Delikts – nicht für die Annahme von Tatherrschaft. Hinzutreten müsste vielmehr, dass das Bereitstellen der Finanzanwendung in der Ausführungsphase weiterwirkt beziehungsweise einen tragenden Einfluss auf die Interaktion des Nutzers mit der Anwendung ausübt.[405]

228 Der Tatbeitrag der Betreiberin erschöpft sich jedoch im Bereitstellen der Finanzanwendung. Die Reduktion auf dieses Zurverfügungstellen des Werkzeugs für den Nutzer, welcher anschliessend die eigentliche Geldwäschereihandlung damit durchführt, kann nicht als unerlässlich oder weiterwirkend gewertet werden. Die Betreiberin eröffnet dem Nutzer zwar den Weg zur Deliktsbegehung; sie hat im Moment des Zurverfügungstellens jedoch keinerlei Vorstellung oder Einflussnahme hinsichtlich der Deliktsausgestaltung, namentlich der Identität des Nutzers, des Zeitpunkts der Inanspruchnahme, der Art und Höhe der transferierten Vermögenswerte oder sonstiger damit im Zusammenhang stehender Tatumstände.[406] Insofern hält die Betreiberin mit dem zeitlich vorgelagerten Zurverfügungstellen der Infrastruktur nicht als Organisatorin durch vorausgehende Planung die Fäden der Tatherrschaft in der Hand.[407] Auch der Umstand, dass der Betreiberin im Zuge der Nutzung automatisch eine Gebühr zufliesst, vermag daran nichts zu ändern, da hierdurch kein unerlässlicher oder fortwirkender Einfluss auf die Ausgestaltung oder Durchführung der deliktischen Handlung begründet wird.

229 Eine Tatherrschaft kann daher durch das Bereitstellen der Finanzanwendung nicht begründet werden. Ein anschauliches Beispiel im Analogen ergibt sich aus der Überlassung eines Tatmittels, etwa dem Ausleihen einer Leiter, die anschliessend für einen Einbruchdiebstahl verwendet wird. Auch hier schafft der Beteiligte zwar die Möglichkeit der Tat, wirkt aber nicht am weiteren Verlauf in einer Weise mit, welche Tatherrschaft vermitteln würde.[408]

2. Gemeinsamer Tatentschluss

230 Schliesslich scheitert eine Mittäterschaft nicht nur am Fehlen einer Tatherrschaft der Betreiberin, sondern auch am fehlenden, gemeinsam getragenen, ausdrücklichen oder konkludenten Tatentschluss.[409] Eine hierfür erforderliche

405 Vgl. BÄCHER, S. 150; STRATENWERTH/BOMMER, AT I, § 13 N 61; PK StGB-TRECHSEL/GETH, Vor Art. 24 N 18; TRECHSEL et al., S. 210.

406 Vgl. BÄCHER, S. 150; JAKOBS, S. 621; abweichend im Kontext von custodial Kryptomixern REGGIANI, S. 123 ff.

407 Vgl. BÄCHER, S. 151; WÜST, S. 88.

408 Vgl. STRATENWERTH/BOMMER, AT I, § 13 N 61; BOMMER, ZBJV 2008, S. 144; NYDEGGER, S. 91.

409 BGE 143 IV 361 E. 4.10; 135 IV 152 E. 2.3.1; 125 IV 134 E. 3a; 118 IV 227 E. 5d/aa; DONATSCH/GODENZI/TAG, S. 178 f.; AK StGB-NYDEGGER, Vor Art. 24 ff. N 17; STRATENWERTH/BOMMER, § 13 N 54; PK StGB-TRECHSEL/GETH, Vor Art 24 N 13.

wechselseitige Kommunikationsmöglichkeit besteht nicht, da der Nutzer ausschliesslich mit dem Smart Contract interagiert und keine unmittelbare Abstimmung mit der Betreiberin stattfindet. Aufgrund der weitgehenden Automatisierung der Abläufe entfällt auch eine spätere Einwirkung oder Koordination zwischen Betreiberschaft und Nutzer. Der Tatbeitrag der Betreiberin liegt zeitlich deutlich vor der konkreten Nutzung durch den einzelnen Nutzer und erschöpft sich in der passiven Ermöglichung technischer Abläufe. Ein Zueigenmachen des konkreten Vorsatzes des Nutzers durch die Betreiberinnen ist unter diesen Umständen ausgeschlossen.[410] Unerheblich ist in diesem Zusammenhang, dass sich Betreiberinnen und Nutzer nicht persönlich kennen.[411] Entscheidend bleibt das Fehlen eines auf eine bestimmte Tat gerichteten, gemeinschaftlich getragenen Willensentschlusses im Sinne einer arbeitsteiligen Begehung.[412]

D. Zwischenfazit

231 Die vorangehende Prüfung galt der Frage, ob das Verhalten der Betreiberin im Zusammenhang mit der Bereitstellung der dezentralisierten Finanzanwendung die Voraussetzungen einer täterschaftlichen Geldwäschereibegehung erfüllt. Zwar lässt sich im initialen Deployment der Smart Contracts bzw. der technischen Infrastruktur ein aktives Tun erkennen, welches den Nutzern die Möglichkeit eröffnet, diese für Geldwäschereihandlungen einzusetzen. Aufgrund der vollautomatisierten Funktionsweise blockchainbasierter Finanzanwendungen und der öffentlichen Zugänglichkeit ohne vorgelagerte Nutzerinteraktion fehlt es jedoch im laufenden Betrieb an weiteren, auf eine konkrete Tat bezogenen Handlungselementen. Das fortgesetzte Betreiben im engeren Sinne der Anwendung erschöpft sich typischerweise in passiver technischer Verfügbarkeit und stellt kein tatbestandsrelevantes Handeln dar.

232 Hinsichtlich einer unmittelbaren Täterschaft genügt das Bereitstellen einer allgemein zugänglichen Infrastruktur nicht, um den objektiven Tatbestand der Geldwäscherei zu erfüllen. Es fehlt sowohl am spezifischen Bezug zu aus Straftaten stammenden Vermögenswerten als auch an einem Verhalten, das auf die Verschleierung oder Entziehung behördlicher Zugriffsmöglichkeiten

410 Zur sukzessiven Mittäterschaft BGE 130 IV 58 E. 9.2.1; 120 IV 265 E. 2c/aa; 118 IV 227 E. 5d/aa; BSK StGB I-FORSTER, Vor Art. 24 N 1; DONATSCH/GODENZI/TAG, S. 179; GETH, N 417; AK StGB-NYDEGGER, Vor Art. 24 ff. N 17; STRATENWERTH/BOMMER, § 13 N 54; PK StGB-TRECHSEL/GETH, Vor Art 24 N 13.

411 Vgl. BÄCHER, S. 151 f.; Tübinger Kommentar StGB-WEISSER, § 25 N 94; WÜST, S. 87.

412 Vgl. BÄCHER, S. 151 f.; CEFFINATO, S. 408; GRECO, S. 440 f.; SAFFERLING/RÜCKERT, S. 10; WEBER, Darknet, S. 139 ff.; WÜST, S. 87.

gerichtet ist. Die tatbestandliche Eignung zur Vereitelung im Sinne von Art. 305bis StGB entsteht erst durch die Nutzungshandlungen der Anwender.

Auch eine Zurechnung im Rahmen der Mittäterschaft scheidet aus. Das einmalige Zurverfügungstellen der Infrastruktur liegt zeitlich vor der Tatausführung und wirkt nicht in diese hinein. Es fehlt somit an einer fortwirkenden Einflussnahme oder einer organisatorischen Steuerung auf die eigentliche Deliktsbegehung. Ebenso wenig ist ein gemeinsamer Tatentschluss ersichtlich, da zwischen Betreiberin und Nutzern keine kommunikative Abstimmung erfolgt und die Deliktsgestaltung vollständig in der Sphäre der Nutzer verbleibt. Selbst wenn der Tatbeitrag der Betreiberin eine notwendige Bedingung für die Begehung darstellt, genügt dies nach der herrschenden Tatherrschaftslehre nicht, um Mittäterschaft zu begründen. 233

Zusammenfassend ist festzuhalten, dass das blosse Tun in Form des Bereitstellens einer dezentralisierten Finanzanwendung zwar die Möglichkeit zur Deliktsbegehung eröffnet, jedoch weder die Voraussetzungen unmittelbarer Täterschaft noch diejenigen der Mittäterschaft erfüllt. 234

III. Teilnahme

Nachdem eine unmittelbare Täterschaft oder Mittäterschaft der Betreiberin mangels tatbestandsmässigen Handelns in eigener Person resp. mangels (Mit-) Tatherrschaft ausscheidet, ist im Folgenden zu prüfen, ob eine Verantwortlichkeit wegen Teilnahme durch Bereitstellen der dezentralisierten Finanzanwendung in Betracht fällt.[413] In Frage kommen dabei zum einen eine Anstiftung im Sinne von Art. 24 Abs. 1 StGB, sofern die Betreiberin durch das Bereitstellen der Finanzanwendung den Nutzer zur Begehung einer Geldwäschereihandlung bestimmt. Zum anderen ist zu untersuchen, ob eine Gehilfenschaft nach Art. 25 StGB vorliegt, indem dem Nutzer ein technisches Tatwerkzeug zur Verfügung gestellt wird, das die Ausführung der Geldwäschereihandlung ermöglicht. 235

A. Anstiftung

Im objektiven Sinne erfordert die Anstiftung nach Art. 24 Abs. 1 StGB zunächst, dass der Anstifter den Haupttäter zu einem Verbrechen oder Vergehen bestimmt.[414] Die Anstiftung muss hierbei bei einem anderen den Entschluss zu 236

413 Vgl. vorne N 208 zu den Ausführungen zum strafrechtlich relevanten Verhalten des Bereitstellens als Tun.

414 BGE 144 IV 265 E. 2.3.2; 128 IV 11 E. 2a; 127 IV 122 E. 2b/aa; 124 IV 34 E. 2c; 116 IV 1 E. 3c; Urteil des BGer 6B_828/2015 vom 5. November 2015 E. 2.1; DONATSCH/GODENZI/TAG, S. 158;

einer bestimmten rechtswidrigen Tat hervorrufen.[415] Als Anstiftungsmittel fallen grundsätzlich jegliche motivierende Verhaltensweisen (also auch bspw. blosse Bitten, Anregungen oder konkludente Aufforderungen) in Betracht, welche eine kausal unmittelbare psychische oder intellektuelle Einflussnahme auf die Willensbildung des Haupttäters herbeiführen.[416] Eine Einschränkung gemäss herrschender Lehre und Rechtsprechung erfährt das Tatmittel jedoch durch das Erfordernis, dass zwischen dem Anstifter und dem Angestifteten ein psychischer Kontakt oder eine kommunikative Beeinflussung stattgefunden hat.[417] Insofern nicht ausreichend ist eine lediglich äussere Herbeiführung einer Situation, in der sich der Täter zu einem Delikt entschliesst.[418]

237 Das Bereitstellen einer Finanzanwendung kann eine tatanreizende Situation schaffen, indem eine Infrastruktur mit Funktionen bereitgestellt wird, die Geldwäschereihandlungen technisch erleichtern oder attraktiver erscheinen lassen können. Gleichwohl genügt eine solche rein faktische Ermöglichung deliktischer Handlungen nicht, um den Tatbestand der Anstiftung im Sinne von Art. 24 Abs. 1 StGB zu erfüllen. Die Bereitstellung einer Finanzanwendung erfolgt typischerweise ohne individuelle Absprache, ohne Interaktion und ohne zielgerichtete Einflussnahme im Hinblick auf eine konkrete Straftat. Das blosse Schaffen einer tatanreizenden Sachlage durch das Zurverfügungstellen einer solchen Infrastruktur ohne spezifische Einwirkung auf den Nutzer bleibt daher hinter den Anforderungen von Lehre und Rechtsprechung an ein Bestimmen zurück.[419]

BSK StGB I-FORSTER, Art. 24 N 12; HURTADO POZO/GODEL, N 571; AK StGB-NYDEGGER, Art. 24 N 1; STRATENWERTH/BOMMER, AT I, § 13 N 98; CR CP I-STRÄULI, Art. 24 N 22.

415 Urteil des BGer 6B_828/2015 vom 5. November 2015 E. 2.1; DONATSCH/GODENZI/TAG, S. 158; BSK StGB I-FORSTER, Art. 24 N 12; AK StGB-NYDEGGER, Art. 24 N 1; STRATENWERTH/BOMMER, AT I, § 13 N 98.

416 BGE 128 IV 11 E. 2a; 127 IV 122 E. 2b/aa; Urteil des BGer 6B_1194/2019 vom 27. April 2020 E. 2.1; Urteil des BGer 6B_17/2016 vom 18. Juli 2017 E. 2.4.2; GRAVEN/STRÄULI, S. 299; AK StGB-NYDEGGER, Art. 24 N 2; HK StGB-WOHLERS, Art. 24 N 5.

417 STRATENWERTH/BOMMER, AT I, § 13 N 101; vgl. BGE 127 IV 122 E. 2b/aa; 128 IV 11 E. 2a; Urteil des BGer 6B_598/2009 vom 23. November 2009 E. 5.2; Urteil des BGer 6S.448/2004 vom 3. Oktober 2005 E. 4.2.1; DONATSCH/TAG/GODENZI, S. 160; GETH, N 435; NYDEGGER, S. 262 ff.; CR CP I-STRÄULI, Art. 24 N 22; HK StGB-WOHLERS, Art. 24 N 5.

418 128 IV 11 E. 2a; 127 IV 122 E. 2b/aa; Urteil des BGer 6B_828/2015 vom 5. November 2015 E. 2.2; Urteil des BGer 6B_920/2013 vom 18. Mai 2015 E. 8.1; Urteil des BGer 6B_591/2013 vom 22. Oktober 2014 E. 5.1.1; BOMMER, Anstiftung, S. 34; DONATSCH/TAG/GODENZI, S. 160 f.; STRATENWERTH/BOMMER, AT I, § 13 N 101; CR CP I-STRÄULI, Art. 24 N 22; HK StGB-WOHLERS, Art. 24 N 6.

419 Eine ähnliche Argumentation findet sich bei der Beurteilung der Anstiftung durch das Bereitstellen von Darknet-Plattformen. Im deutschen Recht wird dies mangels ausdrücklicher oder konkludenter Kommunikation zwischen Plattformbetreiber und Nutzer einhellig abgelehnt (vgl. BACHMANN/ARSLAN, S. 243; BÄCHER, S. 159 f.; WEBER, Darknet, S. 143 ff.; WÜST, S. 132 ff.).

B. Gehilfenschaft

1. Objektiver Beihilfetatbestand

Als Hilfeleistung gilt nach ständiger Rechtsprechung des Bundesgerichts «jeder kausale Beitrag, der die Tat fördert, sodass sich diese ohne Mitwirkung des Gehilfen anders abgespielt hätte. Nicht erforderlich ist, dass es ohne die Hilfeleistung nicht zur Tat gekommen wäre».[420] Im Sinne der Rechtsprechung braucht der Gehilfe die Tat lediglich gefördert zu haben, das heisst, er muss die Erfolgschancen, wie bspw. durch das Überlassen des Gehilfen eines Werkzeuges für den Haupttäter, der tatbestandserfüllenden Handlung erhöhen.[421] 238

Schwierigkeiten in der Abgrenzung zwischen Täterschaft und Teilnahme im Kontext der Geldwäscherei ergeben sich in Anbetracht der weiten Umschreibung der Tathandlung der Geldwäscherei, da bereits jegliche Verhaltensweisen, welche den Zugriff der Strafverfolgungsorgane auf die kontaminierten Vermögenswerte gefährden, als tatbestandsmässig erfasst werden.[422] Dies führt dazu, dass sich der Anwendungsbereich der Gehilfenschaft verkleinert und sonst typischerweise Art. 25 StGB zugeordnete Verhaltensweisen als (mit-)täterschaftlich aufgefasst werden.[423] Nach GRABER ist Gehilfenschaft in Konstellationen anzunehmen, in denen der Gehilfe keinen unmittelbaren Kontakt zu den zu waschenden Vermögenswerten hat. So würde etwa das Zurverfügungstellen eines Fahrzeugs für den Geldtransport als Hilfeleistung qualifiziert werden.[424] Dieses Abgrenzungskriterium erweist sich im Kontext virtueller Vermögenswerte jedoch als wenig trennscharf. Dies wird bereits daran deutlich, dass GRABER selbst die Frage aufwirft, ob das blosse Zurverfügungstellen eines Bankkontos für Finanztransaktionen eine Geldwäschereihandlung darstellt.[425] Insofern ist für die Annahme von Täterschaft vielmehr darauf abzustellen, ob die Handlung geeignet ist, die Einziehung zu vereiteln, auch wenn in einer Gesamtbetrachtung «die Handlung gewichtsmässig 239

420 BGE 149 IV 75, E. 3.2.3; 137 IV 153 E. 1.8; 121 IV 109 E. 3a; 120 IV 265 E. 2c/aa; DONATSCH/GODENZI/TAG, S. 158 f.; GETH, N 428; STRATENWERTH/BOMMER, AT I, § 13 N 62; PK StGB-TRECHSEL/GETH, Art. 25 N 6.

421 Vgl. BGE 137 IV 153 E. 1.8; 129 IV 124 E. 3.2; 121 IV 109 E. 3a; 120 IV 265 E. 2c/aa; 119 IV 289 E. 2c/aa; 117 IV 186 E. 3; BSK StGB I-FORSTER, Art. 25 N 8; STRATENWERTH/BOMMER, AT I, § 13 N 62, 118; CR CP I-STRÄULI, Art. 25 N 22.

422 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 769; DONATSCH/THOMMEN/WOHLERS, S. 508 f.; EGGER TANNER, S. 254; GRABER, S. 174; AK StGB-GRAF, Art. 305bis N 14; PK StGB-PIETH/SCHULTZE, Art. 305bis N 31; vgl. auch BGE 122 IV 211 E. 2.

423 EGGER TANNER, S. 254; GRABER, S. 174 spricht gar von einer Annäherung an das Konzept der Einheitstäterschaft.

424 GRABER, S. 174.

425 GRABER, S. 174; ablehnend auch KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 770; EGGER TANNER, S. 254.

lediglich eine Hilfeleistung darstellt».[426] In der Literatur werden etwa das Zurverfügungstellen von Bankkonten oder Transportmitteln als typische Beihilfehandlungen genannt, wobei jedoch dann von Täterschaft ausgegangen wird, wenn neben dem Überlassen zusätzliche geldwäschereirelevante Handlungen hinzutreten.[427]

240 Die natürliche Kausalität zwischen dem Zurverfügungstellen der Plattform und der Nutzung dieser zu Geldwäschereihandlungen wurde bereits dargelegt.[428] Ebenso konnte eine unmittelbare Täterschaft oder Mittäterschaft verneint werden, da die blosse Bereitstellung der Plattform noch keine konkrete Gefährdung des Einziehungsinteresses bewirkt. Erst das gezielte Interagieren des Nutzers mit der Smart-Contract-Infrastruktur in einer bestimmten Weise begründet eine tatbestandliche Geldwäschereihandlung.[429]

241 Mit dem Deployment, das heisst mit dem Bereitstellen der Smart-Contract-Infrastruktur auf der Blockchain, schafft die Betreiberin eine automatisierte, öffentlich zugängliche Umgebung, die es Nutzern erlaubt, Vermögenswerte zu transferieren, zu konvertieren oder in Pools einzuspeisen, wobei die Abwicklung ohne zentrale Kontrollinstanz erfolgt. Durch dieses Zurverfügungstellen konstituiert die Betreiberin eine technische Grundlage, auf die Nutzer eigenständig zugreifen und die sie zur Durchführung von Vereitelungshandlungen verwenden können. Ein allfällig bereitgestelltes Webinterface senkt zudem die Zugangshürden erheblich und erleichtert die Nutzung auch für technisch weniger versierte Personen. In der Gesamtschau wird damit eine strukturierte, funktionale Möglichkeit zur tatbestandlichen Umsetzung von Geldwäschereihandlungen geschaffen. Die Betreiberin stellt ein Werkzeug bereit, das die Durchführung der Haupttat durch den Nutzer fördert. Entsprechende Konstellationen sind aus der analogen Welt bekannt, etwa wenn einer Drittperson durch das Zurverfügungstellen einer Leiter die funktionale Möglichkeit zur Durchführung eines Einbruchsdiebstahls eröffnet wird.[430]

426 EGGER TANNER, S. 254; gl.M. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 770.

427 EGGER TANNER, S. 254; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 773; anders jedoch im Urteil des BG (ZH) DG960343.U vom 12. Dezember 1996 S. 344, wo Täterschaft angenommen wurde.

428 Vgl. vorne N 227. Auf eine vertiefte Auseinandersetzung mit dem umstrittenen Erfordernis der Kausalität der Gehilfenhandlung wird vorliegend verzichtet, da sich diese Frage im gegebenen Zusammenhang nicht stellt.

429 Vgl. vorne N 221.

430 Vgl. STRATENWERTH/BOMMER, AT I, § 13 N 61; BOMMER, ZBJV 2008, S. 863; NYDEGGER, S. 91.

2. Harmlose Gehilfenschaft

a) Überblick

Umstritten ist der Umgang mit Hilfeleistungen in der Form von äusserlich neutralen Handlungen und berufstypischen Dienstleistungen.[431] Diese umfassen Verhaltensweisen, «die der Ausführende jedem anderen in der Lage des Täters gegenüber vorgenommen hätte, weil er mit der Handlung, im vorhinein (auch), tat- und täterunabhängige eigene, rechtlich als solche nicht missbilligte Zwecke verfolgt».[432] In der Praxis betreffen die einschlägigen Fallkonstellationen vor allem den Vertrieb an sich erlaubter, aber deliktisch verwendbarer Gegenstände sowie die Erbringung äusserlich neutraler Dienstleistungen wie bspw. im Bereich der Massenkommunikation.[433] 242

Vergleichbare Konstellationen können sich auch bei der Bereitstellung technischer Infrastrukturen ergeben, die grundsätzlich legitimen Zwecken dienen, jedoch missbräuchlich verwendet werden können. Strukturelle Ähnlichkeiten zeigen sich dabei insbesondere bei Dienstleistungen, die ohne individuelle Nutzerselektion oder konkrete Tatnähe allgemein zugänglich sind und gleichwohl die Begehung von Straftaten faktisch erleichtern können. In diese Kategorie fällt auch die Bereitstellung dezentralisierter Finanzanwendungen, bei denen ein technisches System den Zugang zu einer grundsätzlich legitimen Dienstleistung eröffnet, die durch einzelne Nutzer zur Begehung von Geldwäschereidelikten missbraucht werden kann.[434] 243

Ein Teil der Lehre versucht, solche Konstellationen bereits auf objektiver Ebene einzuschränken, indem auf die dogmatischen Figuren des unerlaubten Risikos, der Sozialadäquanz oder der Solidarisierung des Gehilfen mit dem Täter zurückgegriffen wird.[435] So wollen STRATENWERTH/BOMMER strafrechtlich relevante Hilfeleistungen nur dort bejahen, «wo eine im Allgemeinen unverfängliche Handlung unter den gegebenen Umständen allein den Sinn haben kann, zur Begehung eines Delikts beizutragen und der Gehilfe sich 244

431 Zum Meinungsstand BSK StGB I-FORSTER, Art. 25 N 30 ff.; FORSTER, FS Schmid, S. 129 ff.; DONATSCH/GODENZI/TAG, S. 168 ff.; PK StGB-TRECHSEL/GETH, Art. 25 N 7.

432 Zum deutschen Recht WOHLLEBEN, S. 4; vgl. LK StGB-SCHÜNEMANN/GRECO, StGB, § 27 N 17.

433 STRATENWERTH/BOMMER, AT I, § 13 N 120; WOHLERS, S. 425 ff.; vgl. BGE 121 IV 109; 119 IV 294; 114 IV 112; 111 IV 32; 109 IV 147.

434 Vgl. LK StGB-SCHÜNEMANN/GRECO, StGB, § 27 N 17; Urteil des BGH 5 StR 624/99 vom 1. August 2000.

435 BSK StGB I-FORSTER, Art. 25 N 30; DONATSCH/GODENZI/TAG, S. 159; GETH/LEU, S. 30; CR CP I-STRÄULI, Art. 25 N 25; PK StGB-TRECHSEL/PIETH, Art. 25 N 7; vgl. HASSEMER, S. 41 ff.; RIKLIN, AT I, § 18 N 34; SCHILD TRAPPE, S. 186 ff.; SCHUMANN, S. 56 ff.; STRATENWERTH/BOMMER, AT I, § 13 N 120; WOHLERS, S. 435 ff.

dessen bewusst ist».[436] Schliesslich sind sich auch die Vertreter der objektiven Modelle uneinig, nach welchen Kriterien das erlaubte Risiko oder die Sozialadäquanz zu bestimmen sind.[437]

245 Andere Ansätze wiederum stellen bei der Prüfung der Strafbarkeit bei Fällen dieser Art primär auf den subjektiven Tatbestand, insbesondere auf das Wissenselement des Teilnehmers, ab.[438]

246 Einen differenzierten Zugang bietet FORSTER mit dem sogenannten ‹zielobjektivierten Beihilfetatbestand›, der objektive Elemente in ein überwiegend subjektives Modell integriert.[439] Zunächst verlangt dieser Ansatz, dass die deliktische Verwendung der Handlung für den Leistungserbringer naheliegend und erkennbar ist (Wissens- und Gefährdungskriterium).[440] Dabei ist zu berücksichtigen, wie alltäglich bzw. harmlos die fragliche Leistung erscheint und ob gesetzliche Sorgfaltspflichten bestehen.[441] Sodann ist entscheidend, ob der Beitrag nach dem sogenannten Zielkriterium für den Teilnehmer nur im Zusammenhang mit dem deliktischen Zweck sinnvoll erscheint.[442] Erst auf dieser Grundlage stellt sich die Frage nach dem Willen, wobei es für die Strafbarkeit genügt, dass der Teilnehmer den deliktischen Erfolg zumindest in Kauf nimmt.[443]

247 WOHLERS identifiziert drei zentrale Fallgruppen, in denen eine strafrechtliche Verantwortlichkeit für das Anschlussverhalten Dritter in Betracht kommt.[444] Erstens sind dies Konstellationen, in denen der Handelnde spezifische Sorgfaltsnormen verletzt, die gerade dem Zweck dienen, deliktisches Verhalten Dritter zu verhindern. Zweitens erfasst er Fälle eines kollusiven Zusammenwirkens, wo Mittäterschaft jedoch ausgeschlossen wird. Drittens

436 STRATENWERTH/BOMMER, AT I, § 13 N 120.

437 GETH/LEU, S. 30; vgl. STRATENWERTH/BOMMER, AT I, § 13 N 120; SCHILD TRAPPE, S. 182 ff.; WOHLERS, S. 429.

438 Vgl. BGE 121 IV 109 E. 3; 119 IV 289 E. 2c/cc; 117 IV 186 E. 4c; 111 IV 32 E. 3; BSK StGB I-FORSTER, Art. 25 N 30 ff.; DONATSCH/GODENZI/TAG, S. 170; GETH, N 430; GETH/LEU, S. 30; CR CP I-STRÄULI, Art. 25 N 26; PK StGB-TRECHSEL/PIETH, Art. 25 N 7.

439 Vgl. Urteil des AGe (BS) SB.2014.14 vom 6. Februar 2015 E. 2.1; BSK StGB I-FORSTER, Art. 25 N 37; FORSTER, FS Schmid, S. 130 ff.

440 BSK StGB I-FORSTER, Art. 25 N 37; vgl. GETH/LEU, S. 34.

441 BSK StGB I-FORSTER, Art. 25 N 38.

442 BSK StGB I-FORSTER, Art. 25 N 40; FORSTER, FS Schmid, S. 137; GETH/LEU, S. 35; CR CP I-STRÄULI, Art. 25 N 26; WOHLERS, S. 437; zum deutschen Recht ROXIN, S. 513.

443 BSK StGB I-FORSTER, Art. 25 N 43 f. Nicht überzeugend ist es hingegen, bei eventualvorsätzlicher Gehilfenschaft im Rahmen neutraler Handlungen mit naheliegender deliktischer Verwendung kategorisch von Straflosigkeit auszugehen (vgl. ROXIN, S. 516; GETH/LEU, S. 35; MOOS, S. 499).

444 WOHLERS, S. 435.

bezieht er jene Konstellationen ein, in denen der Handelnde ein Risiko für ein fremdes Rechtsgut geschaffen hat, das seiner Obhut untersteht und für dessen Integrität er rechtlich einzustehen hat.[445]

Im ‹Antilopenfleischfall› ist das Bundesgericht vom alleinigen Abstellen auf den subjektiven Tatbestand abgewichen.[446] Unter Hinweis auf ROXIN hat es zusätzlich das Erfordernis des deliktischen Sinnbezugs geprüft,[447] wonach «[der Tatbeitrag] für den Täter einzig im Hinblick auf die Haupttat sinnvoll ist».[448] So sieht es dann keinen Grund für eine Einschränkung der Strafbarkeit, wenn der Teilnehmer aufgrund der Umstände weiss, dass der Abnehmer die bezogene Ware oder Dienstleistung praktisch nur illegal verwenden kann.[449] 248

b) Deliktischer Sinnbezug

Konkret stellt sich im vorliegenden Zusammenhang die Frage, ob das Zurverfügungstellen von dezentralisierten Finanzanwendungen wie Kryptomixern oder Handelsplattformen durch die Betreiberin lediglich im Hinblick auf Geldwäschereihandlungen der Nutzer als sinnvoll erscheint.[450] Dieser Ansatz verdient grundsätzlich Zustimmung, da es ein sachgerechtes Korrektiv zur Ausuferung der Gehilfenstrafbarkeit bietet, um nicht jede beliebige äusserlich unverfängliche kausale Verhaltensweise als strafbare Hilfeleistung zu qualifizieren. 249

Dezentralisierte Anwendungen zeichnen sich dadurch aus, dass sie in ihrer Grundkonzeption auf technische Offenheit und funktionale Vielseitigkeit angelegt sind. Zwar können diese Systeme von Nutzern zur Verschleierung deliktischer Vermögensherkunft eingesetzt werden, sie dienen jedoch zugleich auch einer Vielzahl legitimer Zwecke. So ermöglichen dezentralisierte 250

445 Zum Ganzen WOHLERS, S. 435 ff.

446 Im ‹Antilopenfleischfall› hatten Führungsverantwortliche eines Importunternehmens in den 1980er-Jahren rund 450 Tonnen afrikanisches Antilopenfleisch in die Schweiz eingeführt. Der weitaus überwiegende Teil wurde in der Folge von Zwischenhändlern unter falscher Deklaration (z.B. als Reh oder Hirsch) in den Handel gebracht. Das Bundesgericht befasste sich mit der Frage, ob den Importeuren wegen dieser Weiterverwendung eine Gehilfenschaft zum Betrug vorzuwerfen sei (vgl. BGE 119 IV 289).

447 Vgl. ROXIN, S. 513; LK StGB-SCHÜNEMANN/GRECO, StGB, § 27 N 18; vgl. auch FORSTER, FS Schmid, S. 137; GETH/LEU, S. 35; CR CP I-STRÄULI, Art. 25 N 26; WOHLERS, S. 437.

448 GETH/LEU, S. 30; vgl. BGE 119 IV 289 E. 2c/cc; offengelassen jedoch in BGE 121 IV 109; vgl. auch Urteil des OG (AG) SST.2022.15 vom 9. Juni 2022 E. 5.1.1; Urteil des AGe (BS) SB.2014.14 vom 6. Februar 2015 E. 2.1; Urteil des OG (ZH) SB130066 vom 19. August 1998 E. 3.2.

449 GETH/LEU, S. 30; vgl. BGE 119 IV 289 E. 2c/cc; vgl. auch BGE 121 IV 109.

450 Vgl. BGE 119 IV 289 E. 2c/cc; BSK StGB I-FORSTER, Art. 25 N 43; FORSTER, FS Schmid, S. 137; GETH/LEU, S. 35; CR CP I-STRÄULI, Art. 25 N 26; WOHLERS, S. 437; vgl. auch in der deutschen Doktrin ROXIN, S. 513; LK StGB-SCHÜNEMANN/GRECO, StGB, § 27 N 18.

Handelsplattformen den unmittelbaren Handel von Token zwischen Nutzerkonten, ohne auf zentrale Vermittler angewiesen zu sein. Sie erfüllen legitime Funktionen wie bspw. die Ermöglichung eines offenen Marktzugangs unabhängig von geographischer Lage oder regulatorischem Status, die Vermeidung von Verwahrrisiken bei zentralisierten Börsen sowie den diskriminierungsfreien Zugang zu Kapitalmärkten.[451] Anders verhält es sich bei Kryptomixern. Deren zentrale Funktion besteht darin, Transaktionszusammenhänge aufzubrechen und die Rückverfolgbarkeit von Vermögenswerten auf öffentlichen Blockchains zu erschweren. Zwar kann eine solche Anonymisierung auch legitimen Zwecken dienen, etwa dem Schutz geschäftlicher Diskretion, der Trennung privater und öffentlicher Zahlungsströme oder dem Schutz sensibler personenbezogener Informationen. Gleichwohl bleibt die Verschleierung von Herkunfts- und Zuordnungszusammenhängen der eigentliche technische Zweck dieser Anwendungen. Damit weisen Kryptomixer einen deutlich engeren Bezug zu geldwäschereirelevanten Handlungen auf als andere Arten dezentralisierter Finanzanwendungen.[452]

251 Die Tatsache, dass eine Anwendung missbrauchsanfällig ist oder faktisch auch für Geldwäschereizwecke verwendet wird, genügt für die Annahme eines deliktischen Sinnbezugs nicht. Dieser verlangt eine objektive Zweckausrichtung auf die Haupttat, das heisst eine technische, kommunikative oder faktische Struktur, die erkennen lässt, dass das Angebot nahezu ausschliesslich auf deliktische Nutzung angelegt ist. Eine solche Konstellation liegt etwa bei Infrastrukturen im Darknet vor, die einzig der Abwicklung illegaler Transaktionen dienen und keine anderweitige Funktionslogik aufweisen.[453] Ein vergleichbares Beispiel wäre ein dezentralisiertes Finanzprotokoll, das programmatisch an einen Darknet-Marktplatz angebunden ist – etwa durch Schnittstellen, die ausschliesslich den Ein- und Ausfluss von Vermögenswerten zwischen dem Protokoll und der entsprechenden Deliktsplattform ermöglichen. Eine solche Architektur liesse sich funktional einzig durch die Abwicklung illegaler Transaktionen rechtfertigen und wäre damit objektiv auf die Haupttat ausgerichtet.

252 Ausserhalb dieser Ausnahme bleibt die Sinnhaftigkeit des Deployments typischer dezentralisierter Finanzanwendungen mehrdeutig. Selbst bei Kenntnis des möglichen Missbrauchs erscheint der Tatbeitrag der Betreiberin nicht

451 Vgl. vorne N 85 ff.; ANDREOTTI, S. 240 ff.; MEIRICH, N 385 ff.

452 Vgl. vorne N 91; NADLER/SCHÄR, Tornado Cash, S. 122 f.; ANDREOTTI, S. 283 ff.; MEIRICH, N 499.

453 Anstatt vieler BÄCHER, S. 170 ff.; BACHMANN/ARSLAN, S. 243; GRECO, S. 441; HAAS, S. 100 ff.; SAFFERLING/RÜCKERT, S. 10 f.; WEBER, Darknet, S. 154 f.; WÜST, S. 139 f.; ZÖLLER, Strafbarkeit, S. 86; vgl. auch LG Karlsruhe 4 KLs 608 Js 19580/17 vom 19. Dezember 2018 N 430 ff.

ausschliesslich im Lichte einer Unterstützung geldwäschereirelevanter Handlungen erklärbar. Es fehlt damit an der funktionalen Einbettung der Handlung in den deliktischen Gesamtzusammenhang, wie sie der deliktische Sinnbezug voraussetzt.

Im Ergebnis lässt sich festhalten, dass das Kriterium des deliktischen Sinnbezugs im konkreten Kontext nicht erfüllt ist. Die Bereitstellung der betreffenden Plattformen erfolgt im Rahmen einer generischen Infrastrukturleistung, die typischerweise auch (und nicht bloss beiläufig) legalen Zwecken zugänglich ist. Anders zu beurteilen wäre hingegen eine Konstellation, in der ein Kryptomixer technisch und funktional an einen Darknet-Marktplatz angebunden ist und damit von vornherein ausschliesslich der Abwicklung illegaler Transaktionen dient. Eine Strafbarkeit nach Art. 25 StGB scheidet insofern aus, als das Bereitstellen der Anwendung nicht sinnvoll nur im Hinblick auf die geldwäschereirelevanten Handlungen der Nutzer erklärbar ist. 253

c) Vorsatz bezüglich der Hilfeleistung

Im subjektiven Tatbestand ist erforderlich, dass der Gehilfe vorsätzlich handelt, mithin die Förderung der Haupttat zumindest für möglich hält und diese in Kauf nimmt.[454] Aus dem blossen Bewusstsein um die Möglichkeit einer Förderung der Tat darf nicht ohne Weiteres auf deren Inkaufnahme geschlossen werden.[455] Ein solcher Schluss vom Wissen auf Willen ist gemäss ständiger bundesgerichtlicher Rechtsprechung jedoch dann zulässig, «wenn sich dem Täter der Erfolg seines Verhaltens als so wahrscheinlich aufdrängte, dass sein Verhalten vernünftigerweise nur als Inkaufnahme dieses Erfolges ausgelegt werden kann».[456] Diese Beurteilung richtet sich unter anderem nach der Schwere der Sorgfaltspflichtverletzung, dem Risiko der Tatbestandsverwirklichung sowie nach Beweggrund und Art der Tathandlung.[457] 254

An die subjektiven Merkmale werden geringere Anforderungen gestellt, wenn im Sinne des Wissens- und Gefährdungskriteriums eine deliktische Verwendung der Ware bzw. der Dienstleistung den Umständen nach so wie 255

454 BGE 132 IV 49 E. 1.1; 128 IV 53 E. 5f/cc; 121 IV 109 E. 3a; 117 IV 186 E. 3; 113 IV 108 E. 1; Urteil des BGer 6B_836/2015 vom 28. April 2016 E. 1.3; DONATSCH/GODENZI/TAG, S. 172 f.; BSK StGB I-FORSTER, Art. 25 N 3; GETH, N 433; STRATENWERTH/BOMMER, AT I, § 13 N 121; CR CP I-STRÄULI, Art. 25 N 30; PK StGB-TRECHSEL/GETH, Art. 25 N 10; TRECHSEL et al., S. 231.

455 BGE 135 IV 12, E. 2.3.2; BGE 133 IV 9 E. 4.1; Urteil des BGer 6B_775/2011 vom 4. Juni 2012 E. 2.4.1; AK StGB-ABO YOUSSEF, Art. 12 N 9; HK StGB-WOHLERS, Art. 12 N 8.

456 Vgl. BGE 147 IV 439 E. 7.3.1; 138 V 74 E. 8.4.1; 137 IV 1 E. 4.2.3; 133 IV 222 E. 5.3; BSK StGB I-NIGGLI/MÄDER, Art. 12 N 53.

457 BGE 147 IV 439 E. 7.3.1; 135 IV 12 E. 2.3.2; 134 IV 29 E. 3; 133 IV 9 E. 4.1; 131 IV 1 E. 2.2; 130 IV 58, E. 8; Urteil des BGer 6B_1084/2023 vom 29. November 2023 E. 1.2.2; DONATSCH/GODENZI/TAG, S. 125; AK StGB-ABO YOUSSEF, Art. 12 N 9; STRATENWERTH/BOMMER, AT I, § 9 N 107; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 12 N 15.

aus der Beteiligtensicht naheliegend erscheint.[458] Hierzu sind auch allfällige gesetzliche Sorgfaltspflichten im Zusammenhang mit der Leistung mitzuberücksichtigen.[459]

256 Vorliegend stellt sich somit die Frage, ob sich für die Betreiberin sowie unter Berücksichtigung der objektiven Umstände die deliktische Verwendung der bereitgestellten Finanzanwendung zur Geldwäscherei als naheliegend aufdrängt. Zudem ist zu prüfen, ob sie daran anknüpfend für möglich hält und in Kauf nimmt, dass ihr Tatbeitrag – die Bereitstellung der Infrastruktur – die Geldwäschereihandlung des Nutzers fördert.

257 Zunächst ist festzuhalten, dass bei sämtlichen Arten dezentralisierter Finanzanwendungen ein erhöhtes Geldwäschereipotenzial bereits aus zwei strukturellen Merkmalen resultiert: zum einen aus der öffentlichen Zugänglichkeit, indem Nutzer ohne zentrale Registrierung direkt mit dem auf der Blockchain gespeicherten Smart Contract interagieren und zum anderen aus der Pseudonymität der Beteiligten, welche typischerweise ausschliesslich mittels Wallet-Adressen auftreten, ohne dass eine Identitätsprüfung auf Protokollebene erfolgt.[460]

258 Ob eine deliktische Verwendung eines blockchainbasierten Protokolls aus den Umständen heraus sowie aus Sicht der Betreiberin als naheliegend erscheint, ist im Hinblick auf die technische Ausrichtung der Anwendung und unter Einbezug allfälliger geldwäschereirechtlicher Sorgfaltspflichten zu beurteilen. Hierbei ist im Einzelfall zu überprüfen, ob die Betreiberin der dezentralisierten Finanzanwendung dem Geldwäschereigesetz unterstellt ist.[461] Sofern eine Unterstellung vorliegt, ist weiter zu prüfen, ob das Protokoll geldwäschereirechtliche Sorgfaltspflichten oder Meldepflichten – insbesondere die Abklärungspflichten nach Art. 5 GwG, die Meldepflicht nach Art. 9 GwG sowie die Vermögenssperre nach Art. 10 GwG – technisch implementiert hat.[462]

259 Im Hinblick auf die technische Ausrichtung drängt sich im Fall von Kryptomixern eine deliktische Zweckverwendung bereits deshalb als naheliegend auf, weil ihre Funktionsweise gezielt auf die Erzeugung von Anonymität und die Verschleierung des Transaktionspfads ausgelegt ist.[463] Der Zweck dieser

458 BSK StGB I-FORSTER, Art. 25 N 38; FORSTER, FS Schmid, S. 136; GETH/LEU, S. 34.

459 BSK StGB I-FORSTER, Art. 25 N 38; GETH/LEU, S. 34 f.; WOHLERS, S. 436 f.

460 Vgl. Botschaft DLT, S. 143; FINMA, Jahresbericht, S. 32; Europol, Spotlight, S. 10, 19; KGGT, NRA 2018, S. 21; BOŠKIĆ/HEPP, S. 212; MEIRICH, N 492; NOSER/INFANGER/LÜDI, N 12.03; RUTISHAUSER/RUBLI/WEBER, S. 15; STILLER/RODRIGUES/NEZHADSISTAN, N 2.68.

461 Zur vertieften Unterstellungsanalyse unter das Geldwäschereigesetz vgl. hinten N 307 ff.

462 Vgl. Urteil des BGer 6B_1362/2020 vom 20. Juni 2022 E. 15.2.4; Urteil des BGer 6S.56/2007 vom 30. März 2007 E. 3.1; ACKERMANN/ZEHNDER, Dogmatik, S. 49; BOURQUIN, S. 251; CASSANI/VILLARD, N 6.94; CR CP II-CASSANI/VILLARD, Art. 305bis N 42; STRASSER, S. 158.

463 Vgl. vorne N 89.

Systeme besteht gerade nicht im wirtschaftlichen Nutzen im engeren Sinn, sondern in der Umgehung der Transparenz, die der Blockchain typischerweise inhärent ist; ein Umstand, der sowohl objektiv als auch aus Betreibersicht deutlich eine deliktische Verwendung nahelegt.

Bei dezentralisierten Börsen erscheint eine deliktische Verwendung den 260
technischen Umständen nach sowie aus Sicht der Betreiberin nicht als naheliegend. Zwar ist es technisch möglich, solche Plattformen zur Verschleierung des Transaktionsursprungs zu nutzen (z.B. durch wiederholte Token-Swaps), doch steht die legitime Nutzung zum dezentralen Austausch von Vermögenswerten im Vordergrund.[464] Die Anwendungen sind nicht auf Anonymisierung ausgelegt, sondern auf den offenen und transparenten Austausch von Vermögenswerten zwischen Nutzern. Transaktionen werden protokolloffen abgewickelt, sodass die Interaktion der Nutzer gerade nicht auf die Verschleierung, sondern auf die öffentliche Handelbarkeit von Token ausgerichtet ist. Infolgedessen ist das Gefährdungspotenzial dieser Systeme strukturell deutlich geringer einzuschätzen.

Die Frage, ob die Betreiberin die Förderung der geldwäschereirelevanten 261
Handlung des Nutzers erkennt und in Kauf nimmt, knüpft an die vorstehenden Überlegungen zum Kriterium der naheliegenden deliktischen Verwendung an. Sie hängt neben dem anwendungsimmanenten Anonymisierungs- und Gefährdungspotenzial auch davon ab, ob geldwäschereirechtliche Sorgfalts- und Meldepflichten beachtet werden. Das Vorsatzerfordernis im Hinblick auf die Förderung von Geldwäschereihandlungen ist folglich in Abhängigkeit von der strukturellen technischen Ausgestaltung der jeweiligen Anwendung zu beurteilen. Bei Kryptomixern legt bereits ihre technische Konzeption, die gezielt auf Anonymisierung und die Durchbrechung der Rückverfolgbarkeit ausgerichtet ist, eine deliktische Verwendung nahe. Aus Sicht der Betreiberin ist daher regelmässig davon auszugehen, dass eine Nutzung zu geldwäschereirelevanten Zwecken erkannt und zumindest in Kauf genommen wird. Demgegenüber fehlt es bei dezentralisierten Handelsplattformen an einer vergleichbaren strukturellen Ausrichtung auf Verschleierung, sodass das blosse Bereitstellen der Infrastruktur für sich allein weder auf ein entsprechendes Gefährdungsbewusstsein noch auf eine Inkaufnahme der Förderung schliessen lässt. Für das Vorliegen der subjektiven Merkmale ist dabei nicht allein das Anonymisierungs- und Gefährdungspotenzial massgebend, sondern – sofern eine Unterstellung unter das Geldwäschereigesetz besteht – auch, ob die sich aus der Struktur ergebenden Sorgfalts- und Meldepflichten technisch umgesetzt wurden. Je stärker eine Anwendung funktional auf Herkunftsvereitelung

464 Vgl. vorne N 85 ff.

angelegt ist und je geringer die implementierten Sicherungsmechanismen ausfallen, desto eher ist der erforderliche Vorsatz zu bejahen.

d) Vorsatz bezüglich der Bestimmtheit der Haupttat

262 Der Gehilfe muss Vorsatz bezüglich einer bestimmt gearteten Haupttat aufweisen.[465] Nach herrschender Lehre und Rechtsprechung muss er nicht sämtliche Einzelheiten der Haupttat wie Person des Täters oder die genauen Modalitäten der Tatausführung kennen.[466] Er muss jedoch den wesentlichen Geschehensablauf voraussehen können, das heisst die wesentlichen Merkmale des vom Täter zu verwirklichenden strafbaren Tuns erkennen.[467] Ein völlig unbestimmter, lediglich allgemein gehaltener Vorsatz, wonach das eigene Verhalten einem Dritten irgendwie Hilfe zu einer Deliktsbegehung leisten könnte, genügt hingegen nicht.[468]

263 Gerade im Kontext der Bereitstellung dezentralisierter Finanzanwendungen zeigt sich die fehlende Bestimmtheit der Haupttat als entscheidendes Problem. Ein Gehilfenvorsatz wäre nur dann zu bejahen, wenn die Betreiberin zumindest in groben Zügen die wesentlichen Merkmale der vom Nutzer begangenen Geldwäschereihandlung vorhersehen könnte. Dies erweist sich regelmässig als problematisch, weil die Nutzung solcher Anwendungen anonym, zeitlich unbestimmt und inhaltlich offen erfolgt und oftmals erst lange nach dem Deployment der Infrastruktur stattfindet. Die Betreiberin weiss typischerweise weder, wer die Nutzer sind, noch wann oder wie sie die Anwendung verwenden werden. Es fehlt damit regelmässig an der für den Gehilfenvorsatz erforderlichen konkreten Vorstellbarkeit einer bestimmt gearteten Haupttat.

264 Eine vergleichbare Fragestellung wird in der deutschen Literatur insbesondere im Zusammenhang mit der strafrechtlichen Verantwortlichkeit bei Darknet-Marktplätzen diskutiert. Auch deren Betreiberinnen stellen im Kern eine automatisierte Infrastruktur bereit. Teilweise wird in der deutschen Rechtsprechung und Lehre argumentiert, dass das Erfordernis der Bestimmtheit

465 DONATSCH/GODENZI/TAG, S. 172 f.; AK StGB-NYDEGGER, Art. 25 N 9; CR CP I- STRATENWERTH/BOMMER, AT I, § 13 N 121 f.; STRÄULI, Art 25 N 33; PK StGB-TRECHSEL/GETH, Art. 25 N 10; TRECHSEL et al., S. 231.

466 BSK StGB I-FORSTER, Art. 25 N 19; vgl. Urteil des BGer 6B_808/2010 vom 17. Juni 2011 E. 3.6.2; CR CP I-STRÄULI, Art. 25 N 7 f.

467 BGE 132 IV 49 E. 1.1; 128 IV 53 E. 5f/cc; 121 IV 109 E. 3a; Urteil des BGer 6B_836/2015 vom 28. April 2016 E. 1.3; DONATSCH/GODENZI/TAG, S. 172 f.; GRAVEN/STRÄULI, S. 300; STRATENWERTH/BOMMER, AT I, § 13 N 121; CR CP I-STRÄULI, Art 25 N 7.

468 BGE 117 IV 186 E. 3; Urteil des BGer 6B_808/2010 vom 17. Mai 2011 E. 3.6.2; Urteil des OG (BE) SK 19 315 vom 8. Januar 2020 E. 14.2; AK StGB-GRAF, Art. 25 N 9; ähnlich auch DONATSCH/GODENZI/TAG, S. 173.

nur dann erfüllt ist, wenn die Betreiberin durch die Ausgestaltung ihrer Plattform (bspw. durch detaillierte Angebotskategorien) zumindest die wesentliche Unrechtskategorie der Haupttat erfasst und damit eine hinreichend konkrete Vorstellung von den zu erwartenden Delikten besitzt.[469]

265 In der schweizerischen Lehre und Rechtsprechung stellt sich die Problematik in ähnlicher Form bei Access- und Hosting-Providern sowie im ‹Telekiosk-Entscheid›[470] des Bundesgerichts. In Letzterem wurde eventualvorsätzliche Gehilfenschaft bejaht, da der Beschwerdeführer nachweislich Kenntnis von konkreten, regelmässig begangenen Delikten hatte, auf behördliche Hinweise nicht reagierte und die Dienstleistung bewusst zur Gewinnerzielung weiter anbot.[471]

266 Auch im Kontext von Access- und Hosting-Providern wird in der Literatur weitgehend einhellig verlangt, dass für die Erfüllung des Wissenselements konkrete Hinweise von Strafverfolgungsbehörden vorliegen müssen. Derweil werden Hinweise von Privaten (z.B. Nutzern) oder aus der Presse in der Regel nicht als ausreichend erachtet.[472]

267 Dezentralisierte Finanzanwendungen wie Kryptomixer oder Handelsplattformen nehmen hinsichtlich der Bestimmtheit der Haupttat eine Zwischenstellung zwischen Darknet-Plattformen und Access- bzw. Hosting-Providern ein. Während ihre technische Ausgestaltung spezifische Transaktionsformen ermöglicht und damit tendenziell eine höhere Vorhersehbarkeit bestimmter Unrechtskategorien schaffen kann, erfolgt die Nutzung, ähnlich wie bei Infrastrukturprovidern, anonym, zeitlich unbestimmt und ohne inhaltliche Kontrolle durch die Betreiberin. Aus der zu Darknet-Plattformen entwickelten Argumentation lässt sich ableiten, dass die Bestimmtheit steigen kann, wenn die Funktionsarchitektur faktisch eine klar umrissene Angebotskategorie schafft. Zudem folgt aus der Rechtsprechung, namentlich dem ‹Telekiosk-Entscheid› sowie der Literatur zu Access- und Hosting-Providern, dass qualifizierte behördliche Hinweise ausreichen können, um das Erfordernis der Bestimmtheit der Haupttat zu erfüllen.[473]

469 Vgl. LG Karlsruhe Urteil 4 KLs 608 JS 19580/17 vom 19. Dezember 2018; BÄCHER, S. 180 f.; BACHMANN/ARSLAN, S. 244; GRECO, S. 446; WÜST, S. 144; ZÖLLER, Handelsplattformen, S. 285.

470 BGE 121 IV 109 E. 3c.

471 Vgl. BGE 121 IV 109 E. 3c; EQUEY, N 255.

472 Vgl. zum Ganzen Bundesamt für Justiz, Internet, S. 844 f.; EJPD, Internet, S. 5 ff.; EJPD, Netzwerkkriminalität, S. 66; EQUEY, N 255, 360 f.

473 Vgl. BGE 121 IV 109 E. 3c; Bundesamt für Justiz, Internet, S. 844 f.; EJPD, Internet, S. 5 ff.; EJPD, Netzwerkkriminalität, S. 66; EQUEY, N 255.

268 Bei Kryptomixern ist der Grad der Bestimmtheit tendenziell am höchsten. Die technische Ausgestaltung ist auf die Verschleierung von Transaktionszusammenhängen angelegt, wodurch die Betreiberin regelmässig die wesentlichen Merkmale einer potenziellen Haupttat, hier im Sinne einer Geldwäschereihandlung, in groben Zügen vorhersehen kann. Dies entspricht strukturell dem Argument im Zusammenhang mit Darknet-Marktplätzen, wonach die Schaffung klar definierter Angebotskategorien den Vorsatz hinsichtlich einer bestimmt gearteten Haupttat stützen kann. Zudem ist auch hier das Argument aus der Rechtsprechung zu Access- und Hosting-Providern übertragbar, wonach behördliche Hinweise geeignet sind, die erforderliche Bestimmtheit der Haupttat herzustellen.

269 Am Beispiel vom Kryptomixer ‹Tornado Cash› zeigt sich, dass Betreiberinnen von solchen Protokollen regelmässig über hinreichend konkrete Anhaltspunkte zur deliktischen Nutzung verfügen. Aus der Anklage gegen die Betreiber Roman Storm und Roman Semenov ergibt sich, dass die Betreiber über gesicherte Kommunikationskanäle detaillierte Kenntnisse zu einer Reihe von Hackerangriffen besassen, deren Erträge über die Plattform verschleiert wurden. Ihnen war unter anderem bekannt, dass die nordkoreanische Lazarus-Gruppe mutmasslich rund USD 455 Millionen in Ether über ‹Tornado Cash› transferierte und ein erheblicher Teil der Transaktionsvolumina (nach Ermittlungsangaben bis zu 90 %) aus illegalen Quellen stammte.[474]

270 Einen vergleichbaren, wenngleich technisch anders gelagerten Fall stellt der Kryptomixer Helix dar. Hier programmierte der Betreiber eine technische Schnittstelle, über die Darknet-Märkte den Mixer direkt in ihre Auszahlungsprozesse integrieren konnten.[475] Diese Ausrichtung der Funktionsarchitektur auf einen spezifischen deliktischen Kontext (die Abwicklung von Auszahlungen aus Darknet-Märkten) begründete eine Bestimmtheit der potenziellen Haupttaten.

271 Bei dezentralisierten Börsen ist die Konkretisierung der Haupttat in der Regel geringer als bei Kryptomixern. Zwar können auch hier deliktische Transaktionen erfolgen, doch sind diese Anwendungen technisch nicht ausschliesslich auf Verschleierung ausgelegt, sondern erfüllen primär andere Funktionen. Handelsplattformen dienen dem direkten Tausch von Kryptowerten innerhalb einer Blockchain. Aufgrund dieser breiteren Nutzungsmöglichkeiten fehlt es häufig an einem spezifischen deliktischen Kontext, der den Vorsatz hinsichtlich einer bestimmt gearteten Haupttat begründen würde. Zwar wird

474 Vgl. zum Ganzen United States of America v. Roman Storm and Roman Semenov, Indictment 23 Cr. 430 vom 23. August 2023.

475 Vgl. U.S. Attorney's Office District of Columbia, Operator of Helix Darknet Cryptocurrency 'Mixer' Sentenced in Money Laundering Conspiracy Involving Hundreds of Millions of Dollars.

in der Rechtsprechung zu Access- und Hosting-Providern teilweise angenommen, dass qualifizierte behördliche Hinweise geeignet sein können, die Bestimmtheit der Haupttat herzustellen. Die Übertragbarkeit dieser Grundsätze auf Betreiberinnen dezentralisierter Finanzanwendungen ist jedoch kritisch zu beurteilen. Zum einen beziehen sich solche Hinweise regelmässig auf einzelne, konkret gemeldete Sachverhalte und erlauben keine Verallgemeinerung auf zukünftige, zeitlich und personell unbestimmte Nutzungen. Zum anderen setzt der Gehilfenvorsatz voraus, dass die Kenntnis der Haupttat im Zeitpunkt einer tatbestandsmässigen Unterstützungshandlung besteht. Liegen behördliche Hinweise erst nach dem Deployment vor, vermögen sie für sich allein keinen Vorsatz hinsichtlich dieser Handlung zu begründen.

Insgesamt zeigt sich, dass das Erfordernis der Bestimmtheit umso eher 272
erfüllt ist, je stärker die Funktionsarchitektur auf einen spezifischen deliktischen Kontext ausgerichtet ist. Fehlen solche Anhaltspunkte, tritt regelmässig die strukturelle Unbestimmtheit in den Vordergrund und steht der Annahme von Gehilfenvorsatz entgegen.

3. Beihilfe am Versuch

Die Strafbarkeit der Gehilfenschaft setzt voraus, dass zumindest eine rechts- 273
widrige und versuchte Haupttat vorliegt. Bleibt die Haupttat im Versuchsstadium stecken, ist der Tatbeitrag als Beihilfe zum Versuch zu qualifizieren.[476] Der Gehilfe untersteht in diesem Fall lediglich der Strafdrohung der versuchten Haupttat (vgl. Art. 25 StGB).[477] Nicht strafbar ist hingegen die versuchte Gehilfenschaft selbst.[478]

Im Kontext der Geldwäscherei als abstraktes Gefährdungsdelikt ist der 274
Raum für Versuchskonstellationen ohnehin eng bemessen. Bereits ein Verhalten, das typischerweise zur Vereitelung der Einziehung geeignet ist, erfüllt den Tatbestand, weshalb ein vollendeter tauglicher Versuch daher dogmatisch ausgeschlossen ist.[479] Erforderlich für einen strafbaren Versuch nach Art. 22 StGB im Sinne der Schwellentheorie ist eine Tätigkeit, «die nach dem Plan des Täters den letzten entscheidenden Schritt auf dem Weg zur Tatbestandsverwirklichung darstellt, von dem es in der Regel kein Zurück mehr gibt, es sei denn äussere Umstände erschwerten oder verunmöglichten

476 BSK StGB I-FORSTER, Art. 25 N 52; STRATENWERTH/BOMMER, AT I, § 13 N 126; CR CP I-STRÄULI, Art. 25 N 44.

477 BSK StGB I-FORSTER, Art. 25 N 62; CR CP I-STRÄULI, Art. 25 N 44; TRECHSEL et al., S. 233.

478 BGE 130 IV 131 E. 2.4; Urteil des BGer 6B_894/2009 vom 19. Januar 2010 E. 1.2.1; DONATSCH/GODENZI/TAG, S. 173; BSK StGB I-FORSTER, Art. 25 N 52; GRAVEN/STRÄULI, S. 312.

479 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 660, 745; GRABER, S. 166, 169; vgl. DONATSCH/THOMMEN/WOHLERS, S. 508; EGGER TANNER, S. 245; PK StGB-PIETH/SCHULTZE, Art. 305bis N 30; vgl. auch DONATSCH/GODENZI/TAG, S. 146.

es, diese Absicht weiterzuverfolgen».[480] Zudem muss das Verhalten in örtlicher und zeitlicher Hinsicht tatnah sein.[481]

275 Eine versuchte Geldwäscherei kann im vorliegenden Zusammenhang etwa vorliegen, wenn der Nutzer eine Transaktion, die der Herkunftsverschleierung dienen soll, bereits signiert und zur Ausführung an das Netzwerk übermittelt hat, diese aber aufgrund technischer Umstände (z.B. fehlender Bestätigung oder eines Smart-Contract-Fehlers) nicht in die Blockchain gelangt. Die Versuchsschwelle kann ebenso überschritten sein, wenn der Nutzer mittels einer dezentralisierten Anwendung einen Swap, einen Transfer oder eine spezifische Smart-Contract-Interaktion auslöst, die objektiv geeignet wäre, die Rückverfolgbarkeit der Vermögenswerte zu erschweren, die Transaktion jedoch im letzten Ausführungsschritt scheitert (z.B. Revert, unzureichende Liquidität, externe Abbrüche).[482] Bezogen darauf würde die Bereitstellung der Finanzanwendung durch die Betreiberin in diesen Fällen den Gehilfenbeitrag zur versuchten Geldwäscherei des Nutzers darstellen.

276 Demgegenüber ist die Versuchsschwelle noch nicht erreicht, wenn der Nutzer lediglich vorbereitende Schritte setzt, etwa indem er eine neue Wallet einrichtet, die Benutzeroberfläche der Anwendung öffnet oder darin navigiert, Transaktionsvorschauen berechnet, eine neue Adresse generiert, eine mögliche Transaktionskette plant oder lediglich die Verbindung zur Anwendung herstellt. Solange es zu keiner verbindlichen Interaktion mit einer Smart-Contract-Funktion kommt, die nach seinem Plan unmittelbar der Verschleierung dienen soll, verbleibt sein Verhalten im Bereich der straflosen Vorbereitung.

C. Zwischenfazit

277 Im Ergebnis zeigt die Analyse, dass das blosse Tun in Form des Bereitstellens einer dezentralisierten Finanzanwendung zwar eine technische Grundlage schafft, auf der Nutzer eigenständig geldwäschereirelevante Handlungen ausführen können, dieses Verhalten jedoch in der Regel nicht die Anforderungen an eine strafbare Teilnahmehandlung erfüllt.

278 Hinsichtlich der Anstiftung fehlt es am erforderlichen psychischen oder intellektuellen Einfluss auf die Willensbildung eines konkreten Haupttäters.

480 Anstatt vieler BGE 131 IV 100 E. 7.2.1; 120 IV 113 E. 1b; 119 IV 250 E. 3c; DONATSCH/GODENZI/TAG, S. 142; AK StGB-DEMARMELS/VONWIL, Art. 22 N 4; BSK StGB I-NIGGLI/MÄDER, Art. 22 N 10.

481 BGE 131 IV 100 E. 7.2.1; Urteil des BGer 7B_6/2023 vom 28. November 2023 E. 3.1.3; Urteil des BGer 6B_28/2023 vom 30. Januar 2023 E. 3.3.2; DONATSCH/GODENZI/TAG, S. 142; AK StGB-DEMARMELS/VONWIL, Art. 22 N 4; BSK StGB I-NIGGLI/MÄDER, Art. 22 N 18.

482 Vgl. auch KV/KO StGB-KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 747.

Das Bereitstellen der Infrastruktur erfolgt typischerweise ohne individuelle Ansprache, ohne Interaktion und ohne Ausrichtung auf eine bestimmte Straftat. Das Schaffen einer allgemein zugänglichen Nutzungsmöglichkeit stellt daher kein Bestimmen im Sinne von Art. 24 Abs. 1 StGB dar.

279 Auch im Rahmen der Gehilfenschaft genügt die Bereitstellung allein nicht, um regelmässig eine Strafbarkeit nach Art. 25 StGB zu begründen. Zwar liegt in der Bereitstellung eines dezentralisierten Protokolls ein kausaler Tatbeitrag im Sinne des Zurverfügungstellens eines Werkzeugs zur Geldwäschereihandlung des Nutzers. Ungeachtet des Anwendungstyps stellt sich jedoch das Problem der harmlosen Gehilfenschaft, da Finanzanwendungen nicht ausschliesslich zu deliktischen Zwecken bestimmt sind, sondern selbst bei Kryptomixern auch legal verwendet werden können. Eine Ausnahme besteht nur in Konstellationen, in denen die Funktionsarchitektur des Protokolls programmatisch auf deliktische Nutzung angelegt ist, etwa wenn eine Schnittstelle ausschliesslich der Anbindung an einen Darknet-Marktplatz dient und so die Abwicklung strafbarer Transaktionen strukturell vorzeichnet.

280 Auf subjektiver Ebene konzentrieren sich die Schwierigkeiten auf zwei Problemfelder: Erstens kann der Vorsatz hinsichtlich der Förderung der Haupttat nur dann bejaht werden, wenn sich die deliktische Nutzung der bereitgestellten Anwendung für die Betreiberin klar aufdrängt. Dies ist bei Kryptomixern aufgrund ihrer auf Verschleierung ausgerichteten Funktionsarchitektur regelmässig der Fall, bei dezentralisierten Handelsplattformen hingegen nur bei besonderen konkreten Anhaltspunkten, insbesondere wenn zugleich jegliche geldwäschereirechtlichen Sorgfaltspflichten missachtet wurden. Zweitens scheitert der Vorsatz hinsichtlich der Haupttat an der fehlenden Bestimmtheit der Haupttat. Die anonyme, zeitlich und inhaltlich offene Nutzung erschwert es der Betreiberin, die wesentlichen Merkmale einer bestimmten Geldwäschereihandlung vorherzusehen. Eine Ausnahme kann bestehen, wenn die Funktionsarchitektur (z.B. wie bei Kryptomixern durch technische Anbindungen an einschlägige Darknet-Markplätze) einen klar umrissenen deliktischen Kontext schafft.

IV. Fazit

281 Dieses Kapitel ging der Frage nach, ob und unter welchen Voraussetzungen Betreiberinnen dezentralisierter Finanzanwendungen durch deren Bereitstellen wegen Geldwäscherei nach Art. 305bis StGB strafrechtlich verantwortlich gemacht werden können, wenn Nutzer ihre Protokolle für Geldwäschereihandlungen verwenden.

282 Tatbestandsrelevantes Verhalten lässt sich – jenseits blosser Passivität – primär im Deployment der Smart-Contract-Infrastruktur verorten. Das anschliessende Betreiben (im engeren Sinn) vollautomatisierter, offen zugänglicher Protokolle erschöpft sich regelmässig in technischer Verfügbarkeit ohne auf eine konkrete Tat bezogene Handlungselemente. Vor diesem Hintergrund trägt die blosse Bereitstellung einer generischen Infrastruktur eine unmittelbare Täterschaft grundsätzlich nicht. So besteht weder beim Deployment ein spezifischer Bezug zu deliktisch kontaminierten Vermögenswerten, noch zeigt sich eine auf Vereitelung ausgerichtete Verschleierungs- oder Manipulationskomponente. Die tatbestandliche Eignung zur Vereitelung entsteht erst durch die Nutzungshandlungen der Anwender.

283 Eine Zurechnung über Mittäterschaft scheitert regelmässig an fehlender (Mit-)Tatherrschaft und am gemeinsamen Tatentschluss. Der vorgelagerte Tatbeitrag wirkt nicht in die Ausführung hinein und es fehlt an fortlaufender organisatorischer Steuerung wie auch an kommunikativer Abstimmung mit späteren Haupttätern. Selbst wenn das Deployment conditio sine qua non späterer Taten ist, genügt dies hinsichtlich der dargelegten Gründe nicht.

284 Auch eine Anstiftung durch die Betreiberin ist zu verneinen. Das Erfordernis eines psychischen oder intellektuellen Einflusses (Bestimmen) auf die Willensbildung eines konkreten Haupttäters wird durch das Offenhalten eines technischen Angebots nicht ersetzt. Die Bereitstellung erfolgt typischerweise ohne individuelle Adressierung, ohne Interaktion und ohne Ausrichtung auf eine bestimmte Straftat.

285 Im Rahmen der Gehilfenschaft kann das Bereitstellen einer Finanzanwendung zwar als fördernder Tatbeitrag in Betracht fallen, indem der Nutzer ein technisches Werkzeug zur Durchführung seiner Geldwäschereihandlung erhält. In aller Regel fehlt es jedoch am deliktischen Sinnbezug, da dezentralisierte Anwendungen grundsätzlich für legale Zwecke konzipiert sind, wie etwa zum Schutz der Privatsphäre oder zum Austausch von Vermögenswerten. Zudem erfordert der Teilnehmervorsatz, dass sich die Betreiberin die Geldwäschereihandlung des Nutzers in ihren wesentlichen Zügen vorstellen konnte. Die anonyme, zeitlich und inhaltlich offene Nutzung macht es indessen regelmässig unmöglich, den konkreten Ablauf einer Geldwäschereihandlung vorausschauend zu erfassen.

286 Zusammenfassend kommt eine Beihilfe in Form der Bereitstellung dezentralisierter Finanzanwendungen nur in einem engen Anwendungsbereich in Betracht. Sie setzt voraus, dass das Protokoll durch seine Funktionsarchitektur faktisch auf deliktische Nutzungen ausgerichtet ist, die eine deliktische Nutzung der Anwendung hinreichend konkret vorhersehbar machen.

Kapitel 2: Strafbarkeit durch Unterlassen

Das vorhergehende Kapitel hat die Frage behandelt, ob sich Betreiberinnen für das Bereitstellen der Finanzanwendung durch ein Tun strafbar machen können. Die Analyse hat ergeben, dass eine strafrechtliche Verantwortlichkeit aufgrund aktiven Handelns nur im Ausnahmefall in Betracht kommt, nämlich bei Anwendungen, deren Funktionsarchitektur eindeutig auf einen deliktischen Kontext zugeschnitten ist. Hiervon betroffen ist lediglich ein marginaler Anteil an Protokollen, insbesondere solche, die technisch unmittelbar mit Vermögenswerten aus Darknet-Marktplätzen verknüpft sind, wie z.B. Kryptomixer mit entsprechender Ausrichtung. 287

Für die grosse Mehrheit dezentralisierter Protokolle lässt sich eine Strafbarkeit der Betreiberinnen aufgrund eines Tuns nicht begründen. Das nachfolgende Kapitel widmet sich deshalb der Frage, ob sich Betreiberinnen dezentralisierter Finanzanwendungen wegen Geldwäscherei durch Unterlassen nach Art. 305bis i.V.m. Art. 11 StGB strafbar machen können, wenn Nutzer die Protokolle für Geldwäschereihandlungen einsetzen. 288

Zur Beantwortung dieser Frage wird zunächst geklärt, unter welchen Voraussetzungen Geldwäscherei als Tätigkeitsdelikt überhaupt durch Unterlassen begangen werden kann und ob im vorliegenden Kontext von einer täterschaftlichen Unterlassung oder einer Gehilfenschaft durch Unterlassen auszugehen ist (I.). Darauf aufbauend wird untersucht, ob Betreiberinnen eine Garantenstellung trifft, aus der sich eine qualifizierte Handlungspflicht zur Verhinderung geldwäschereirelevanter Vorgänge ergeben kann (II.). Anschliessend werden die weiteren objektiven Voraussetzungen der unechten Unterlassung – insbesondere hypothetische Kausalität, Tatmacht und die Gleichwertigkeit von Tun und Unterlassen – geprüft (III.). Der letzte Abschnitt befasst sich sodann mit dem subjektiven Tatbestand (IV.). 289

I. Täterschaftliche Geldwäscherei durch Unterlassen

Im Gegensatz zu Begehungsdelikten, bei denen ein bestimmter Erfolg oder eine bestimmte Gefährdung durch aktives Tun herbeigeführt wird, betreffen Unterlassungsdelikte Fälle, in denen dem Täter vorgeworfen wird, eine Verletzung oder Gefährdung eines strafrechtlich geschützten Rechtsguts nicht verhindert zu haben, obwohl er deren Eintritt durch pflichtgemässes Handeln 290

hätte abwenden können.[483] Unterlassungsdelikte lassen sich in echte und unechte Unterlassungsdelikte unterteilen. Echte Unterlassungsdelikte beruhen bereits auf einem im Straftatbestand umschriebenen Gebot zum Tätigwerden und knüpfen ausdrücklich an das Unterlassen einer bestimmten Handlung an. Unechte Unterlassungsdelikte hingegen liegen vor, wenn der tatbestandsmässige Unrechtserfolg durch pflichtwidriges Untätigbleiben verwirklicht wird.[484]

291 Vorliegend könnte eine Betreiberin den Geldwäschereitatbestand durch eine Unterlassung erfüllen, indem der Nutzer die von ihr bereitgestellte Finanzanwendung zu Geldwäschereizwecken missbraucht und sie dies trotz bestehender Rechtspflichten nicht verhindert.

292 Damit stellen sich zwei zentrale Problemkreise: Zum einen ist zu klären, ob schlichte Tätigkeitsdelikte beziehungsweise abstrakte Gefährdungsdelikte wie die Geldwäscherei überhaupt durch Unterlassen begangen werden können. Zum anderen bedarf es einer Auseinandersetzung mit den Fällen, in denen ein Dritter (der Nutzer) durch aktives Tun eine Straftat begeht und diejenige Person, der eine Garantenpflicht obliegt, hier die Betreiberin, untätig bleibt.

A. Begehung durch Unterlassen bei Tätigkeitsdelikten

293 Ein Teil der Lehre vertritt die Auffassung, dass eine Begehung durch Unterlassen ausschliesslich bei Erfolgsdelikten möglich sei.[485] NIGGLI/MUSKENS sehen in der Unterlassung eines schlichten Tätigkeitsdelikts einen logischen Widerspruch. So lasse sich Unterlassen als Nichtvornahme einer Handlung mit dem Konzept eines schlichten Tätigkeitsdelikts, bei dem bereits die blosse Vornahme einer bestimmten Handlung tatbestandsmässig sei, nicht in Einklang bringen. Während beim Erfolgsdelikt trotz Ausbleibens der Tathandlung der Erfolg als Anknüpfungspunkt für die Strafbarkeit dienen könne, fehle es beim schlichten Tätigkeitsdelikt gerade an einem solchen Bezugspunkt, wenn die Tathandlung nicht ausgeführt wurde.[486]

483 Vgl. BGE 150 IV 389 E. 4.3; 148 IV 39 E. 2.3.2; 141 IV 249 E. 1.1; DONATSCH/GODENZI/TAG, S. 309; CR CP I-CASSANI/VILLARD, Art. 11 N 14; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 41 f.; STRATENWERTH/BOMMER, AT I, § 14 N 1.

484 Vgl. BGE 148 IV 39 E. 2.3.2; 141 IV 249 E. 1.1; Urteil des BGer 6B_230/2022 vom 25. Oktober 2023 E. 3.3; CR CP I-CASSANI/VILLARD, Art. 11 N 1 f.; DONATSCH/GODENZI/TAG, S. 310; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 3 f.; RIKLIN, § 9 N 30 ff.; m.w.H. GRUBMILLER, S. 64 ff., 221 ff.

485 BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 40 ff.; NIGGLI/MUSKENS, S. 18 ff.; RIKLIN, § 19 N 4; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2; vgl. auch DONATSCH/TAG/GODENZI, S. 322.

486 Vgl. BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 43.

Ein anderer Teil der Lehre sowie die jüngere Rechtsprechung des Bundesgerichts halten indessen dafür, dass auch schlichte Tätigkeitsdelikte durch Unterlassen begangen werden können.[487] GRAF weist darauf hin, dass der Gesetzeswortlaut die Unterlassensstrafbarkeit nicht auf Erfolgsdelikte beschränke, sondern er allgemein jedes Verbrechen oder Vergehen erfasse, sofern eine Pflicht zum Tätigwerden bestand und das Untätigbleiben dem Unrecht einer aktiven Tatbegehung gleichkomme. Der Vorwurf richte sich dabei nicht auf die Verletzung des tatbestandlich geforderten positiven Handelns, sondern auf das Unterlassen der gebotenen Gegenhandlung, welche spiegelbildlich zu diesem Verhalten zu verstehen sei.[488] 294

Unter den Befürwortern betonen STRATENWERTH/BOMMER, dass nicht die dogmatische Einordnung der nicht verhinderten Straftat als Erfolgs- oder Tätigkeitsdelikt (bzw. Verletzungs- oder Gefährdungsdelikt) entscheidend sei, sondern ob der jeweilige Tatbestand nach Wortlaut und Sinngehalt Unterlassungen mitumfasst.[489] Dieser Gedanke findet sich auch in der neueren bundesgerichtlichen Rechtsprechung wieder, welche bspw. für die Urkundenfälschung (Art. 251 StGB) die Begehung durch Unterlassen ausgeschlossen hat.[490] 295

Nach TRECHSEL/FATEH-MOGHADAM handelt es sich bei unechten Unterlassungsdelikten stets um Erfolgsdelikte: Der Täter wird bestraft, weil er nicht in einen bestehenden Kausalablauf eingreift, um einen ‹Erfolg› zu verhindern.[491] Unter ‹Erfolg› verstehen die Autoren den Begriff nicht im engen, tatbestandsmässigen Sinn,[492] sondern allgemein als Verletzung oder Gefährdung eines Rechtsguts, welche auch durch die Straftat eines Dritten herbeigeführt werden. In diesem Fall bildet die fremde Straftat den Unterlassungserfolg.[493] 296

487 Vgl. Botschaft StGB 1998, S. 2001; BGE 136 IV 188 E. 6.2; 125 IV 139 E. 3b; Urteil des BGer 6B_489/2012 vom 10. Juni 2013 E. 2.4; Urteil des BGer 6B_969/2009 vom 25. Januar 2010 E. 1; CR CP I-CASSANI/VILLARD, Art. 11 N 17 ff.; AK StGB-GRAF, Art. 11 N 3; RIEDO, Fn. 2008; SCHILD TRAPPE, S. 9; STRATENWERTH/BOMMER, § 14 N 36; TRECHSEL et al., S. 247; WIPRÄCHTIGER, S. 412.

488 AK StGB-GRAF, Art. 11 N 3; ähnlich auch CR CP I-CASSANI/VILLARD, Art. 11 N 17 ff.

489 STRATENWERTH/BOMMER, § 14 N 36; CR CP I-CASSANI/VILLARD, Art. 11 N 18 f.

490 Vgl. Urteil des BGer 6B_844/2011 vom 18. Juni 2012 E. 3.1.1; Urteil des BGer 6B_711/2012 vom 17. Mai 2013 E. 2.4; vgl. auch BGE 136 IV 188 E. 6.1; 128 IV 117 E. 7; 127 IV 20 E. 3; Urteil des BGer 6B_729/2010 vom 8. Dezember 2011 E. 4.3; Urteil des BGer 4A_603/2020 vom 16. November 2022 E. 4.4.

491 PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2; gl.M. DONATSCH/GODENZI/TAG, S. 322; TRECHSEL et al., S. 247.

492 Erfolg im engeren Sinne ist als eine Veränderung in der Aussenwelt zu verstehen, die dem Täter zurechenbar ist und zu den Tatbestandsmerkmalen gehört (vgl. DONATSCH/GODENZI/TAG, S. 104 f.; GRUBMILLER, S. 186 ff.; TRECHSEL et al., S. 98 f.).

493 PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2.

297 In ähnlicher Weise argumentieren NIGGLI/MUSKENS, indem sie betonen, dass eine Veränderung der Aussenwelt im Sinne eines ‹Erfolgs› nicht nur im tatbestandsmässigen Erfolg eines Erfolgsdelikts bestehen kann, sondern auch in der Begehung einer Straftat durch eine andere Person.[494] DONATSCH/GODENZI/TAG halten hierzu fest: «Geht es um die Pflicht, Straftaten anderer Personen zu verhindern, so tritt an die Stelle des Erfolgs im Sinne einer Rechtsgüterverletzung die Vornahme der darauf angelegten Handlung eines Dritten».[495]

298 Im Kontext der Geldwäscherei durch Unterlassen folgt auch die Doktrin sowie das Bundesgericht dieser Linie, indem sie die Tatbegehung der Geldwäscherei durch einen Dritten als Erfolg (im weiteren Sinne) des Unterlassungsdelikts begreifen.[496] Dem Erfolg gleichzusetzen ist die als Aussenwirkung in Erscheinung tretende Deliktsbegehung des Dritten, welche nicht durch den Unterlassungstäter verhindert wurde. Daraus folgt, dass im Rahmen der weiteren Strafbarkeitsprüfung auch die Kausalität zwischen dem pflichtwidrigen Untätigbleiben des Garanten und der deliktischen Handlung des Dritten nachzuweisen ist.[497]

B. Täterschaft und Teilnahme

299 Im Kontext der Strafbarkeit durch Unterlassen, wenn Delikte von Dritten trotz bestehender Handlungspflichten nicht verhindert werden, besteht – wie bereits dargelegt – Einigkeit darüber, dass bei Untätigkeit der verpflichteten Person eine täterschaftliche Unterlassung in Betracht fällt.[498] Umstritten bleibt hingegen, wie diese von einer Gehilfenschaft durch Unterlassen abzugrenzen ist.[499]

494 BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 41; allerdings widersprechen sie sich durch die kategorische Ablehnung der Begehung von schlichten Tätigkeitsdelikten durch unechtes Unterlassen in diesem Punkt (BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 43; vgl. auch CR CP I-CASSANI/VILLARD, Art. 11 N 18).

495 DONATSCH/GODENZI/TAG, S. 338; so auch CR CP I-CASSANI/VILLARD, Art. 11 N 18.

496 Vgl. BGE 136 IV 188 E. 6.2; BACHARACH, S. 225 f.; BOURQUIN, S. 218 f.; CR CP I-CASSANI/VILLARD, Art. 11 N 18; CR CP II-CASSANI/VILLARD, Art. 305bis N 39; CONRAD HARI, S. 369; VON ROTZ, S. 114.

497 Vgl. BACHARACH, S. 225 f.; BOURQUIN, S. 218 f.; CASSANI/VILLARD, N 6.87; CR CP II-CASSANI/VILLARD, Art. 305bis N 37; CONRAD HARI, S. 369; VON ROTZ, S. 114; a.M. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 611; vgl. auch Urteil des BGer 6B_908/2009 vom 3. November 2010 E. 7.

498 Vgl. vorne N 296 ff.; vgl. auch PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2; CR CP I-CASSANI/VILLARD, Art. 11 N 66; DONATSCH/TAG/GODENZI, S. 228; AK StGB-GRAF, Art. 11 N 5; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 41, 141; HK StGB-WOHLERS, Art. 11 N 7.

499 Vgl. STRATENWERTH/BOMMER, AT I, § 15 N 14; GETH, N 452; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2.

Die herrschende Lehre geht grundsätzlich davon aus, dass bei Tätigkeitsdelikten Täterschaft zu bejahen ist, wenn der Garant eine andere Person nicht von der Begehung einer Straftat abhält.[500] Von diesem Grundsatz wird allerdings in einzelnen Konstellationen abgewichen, in denen aushilfsweise auf die Teilnahmebestimmungen zurückgegriffen wird.[501] Dies betrifft namentlich Fälle, in denen der Garant nicht sämtliche subjektiven Tatbestandsmerkmale, etwa besondere Beweggründe oder die Eigenhändigkeit der Ausführung, erfüllt.[502] Ebenso wird bei Sonderdelikten trotz bestehender Garantenpflicht auf Gehilfenschaft erkannt, wenn die besondere Täterstellung fehlt.[503] Darüber hinaus bejaht STRÄULI eine Gehilfenschaft durch Unterlassen für Fälle, in denen der Garant die Verantwortung für die Überwachung einer Person trägt, die selbst als Gehilfe an einer Straftat beteiligt ist und es unterlässt, seiner Überwachungspflicht nachzukommen.[504] 300

Bemühungen, Täterschaft und Gehilfenschaft bei Unterlassen ausserhalb der aushilfsweisen Rückgriffkonstellationen auf die Teilnahme voneinander abzugrenzen, überzeugen nur bedingt.[505] Gerade im Anwendungsbereich des Geldwäschereitatbestands erweist sich die Unterscheidung zwischen Fällen, in denen das Unterlassen die Tat bloss fördert, und solchen, in denen bereits eine Gefährdung des Einziehungsinteresses vorliegt, als kaum trennscharf umsetzbar.[506] Folgerichtig erkennt die bundesgerichtliche Praxis auf Täterschaft statt auf Gehilfenschaft durch Unterlassen.[507] 301

500 BGE 105 IV 176 E. 4b; DONATSCH/TAG/GODENZI, S. 343 f.; GETH, N 452; AK StGB-GRAF, Art. 11 N 5; STRATENWERTH/BOMMER, AT I § 15 N 15; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2; a.M. BGE 121 IV 109 E. 3b; 118 IV 309 E. 2c; 113 IV 68 E. 4; Urteil des BGer 6B_489/2012 vom 10. Juni 2013 E. 3.1; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 41, 141 schliessen generell eine mögliche Täterschaft durch Unterlassen bei Tätigkeitsdelikten aus.

501 STRATENWERTH/BOMMER, AT I, § 15 N 16.

502 STRATENWERTH/BOMMER, AT I, § 15 N 15; DAN, N 471; DONATSCH/TAG/GODENZI, S. 344 f.; GETH N 453; AK StGB-GRAF, Art. 11 N 5; CR CP I-STRÄULI, Art. 25 N 49; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2; vgl. auch Urteil des BGer 6B_489/2012 vom 10. Juni 2013 E. 3.

503 DONATSCH/TAG/GODENZI, S. 344; DAN, N 472; AK StGB-GRAF, Art. 11 N 5; BSK StGB I-FORSTER, Art. 26 N 1; STRATENWERTH/BOMMER, AT I, § 15 N 15; CR CP I-STRÄULI, Art. 25 N 48 und Art. 26 CP N 13 f.

504 CR CP I-STRÄULI, Art. 25 N 50; vgl. DAN, N 474.

505 STRATENWERTH/BOMMER, AT I, § 15 N 16; GETH, N 452.

506 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 779.

507 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 779; vgl. BGE 136 IV 188 E. 6; Urteil des BGer 6B_879/2013 vom 18. November 2013 E. 1; Urteil des BStGer SK. 2010.10 vom 1. Juni 2010 E. 2; Urteil des OG (BE) SK 23 435 vom 14. August 2024 E. 11.1; vgl. auch CR CP II-CASSANI/VILLARD, Art. 305bis N 37 ff.; CASSANI/VILLARD, N 6.80 ff.; AK StGB-GRAF,

302 Im vorliegenden Kontext verwirklicht der Nutzer mittels der von der Betreiberin bereitgestellten Finanzanwendung die Geldwäschereihandlung nach Art. 305bis StGB. Dass der Tatbestand bei pflichtwidriger Untätigkeit auch durch Unterlassen erfüllt werden kann, wird in Rechtsprechung und Lehre weitgehend anerkannt.[508] Einschlägig ist jene Konstellation, in der – vorausgesetzt, eine Handlungspflicht besteht – die pflichtwidrige Untätigkeit in der Nichtverhinderung der aktiven Geldwäschereihandlung des Nutzers durch die Betreiberin liegt. In Übereinstimmung mit Rechtsprechung und Lehre wird sie in diesem Fall nicht als Teilnehmerin, sondern als Unterlassungstäterin eingeordnet. Dies ergibt sich zum einen daraus, dass bei der Geldwäscherei die für den aushilfsweisen Rückgriff auf die Teilnahme typischen Konstellationen, wie Sonderdelikte, besondere Beweggründe oder die Eigenhändigkeit des Delikts, nicht vorliegen. Zum anderen lässt sich eine dogmatisch tragfähige Differenzierung zwischen einem fördernden Beitrag im Sinne der Gehilfenschaft und einer täterschaftlichen Gefährdung des Einziehungsinteresses nicht ziehen.

C. Zwischenfazit

303 Zusammenfassend kann festgehalten werden, dass die Geldwäscherei nach Art. 305bis StGB auch durch (unechte) Unterlassung im Sinne von Art. 11 StGB begangen werden kann. Im vorliegenden Fall betrifft die Analyse einer möglichen Strafbarkeit durch Unterlassen die Konstellation der Nichtverhinderung von Delikten Dritter. Konkret geht es darum, dass Betreiberinnen dezentralisierter Finanzanwendungen strafbar sein können, wenn sie es unterlassen, Nutzer von Geldwäschereihandlungen mittels der jeweiligen Anwendung abzuhalten. Die Geldwäscherei des Nutzers ist der Betreiberin, welche zu ihrer Verhinderung verpflichtet ist, als täterschaftlich herbeigeführter Unterlassungserfolg vorzuwerfen. Die Qualifizierung als täterschaftliche Begehung durch Unterlassung ergibt sich daraus, dass ein aushilfsweiser Rückgriff auf die Teilnahmebestimmungen nicht in Betracht kommt und bereits die abstrakte Gefährdung des Rechtsguts des staatlichen Einziehungsinteresses den Geldwäschereitatbestand selbständig erfüllt, womit eine Einordnung als blosser Tatbeitrag als Teilnehmer ausser Betracht fällt.

Art. 305bis N 17 f.; BSK StGB II-PIETH, Art. 305bis N 57; PK StGB-PIETH/SCHULTZE, Art. 305bis N 20.

508 Vgl. Botschaft StGB 1989, S. 1083; BGE 136 IV 188 E. 6.1; 128 IV 117 E. 7; 127 IV 20 E. 3; Urteil des BGer 6B_729/2010 vom 8. Dezember 2011 E. 4.3; zustimmend auch KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 611, 631; CR CP I-CASSANI/VILLARD, Art. 11 N 18; DONATSCH/THOMMEN/WOHLERS, S. 509; PK StGB-PIETH/SCHULTZE, Art. 305bis N 20; HK StGB-WOHLERS, Art. 305bis N 19; a.M. BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 47.

II. Garantenstellung

Für die Strafbarkeit eines unechten Unterlassungsdelikts ist erforderlich, dass den Täter eine besondere Rechtspflicht trifft, eine drohende Verletzung oder Gefährdung des geschützten Rechtsguts abzuwenden.[509] Diese Garantenpflicht kann sich zum einen in der Form der Obhuts- oder Schutzgarantenpflicht manifestieren, die eine Verpflichtung zur Abwehr von bestimmten Rechtsgütern einzelner Personen begründet. Zum anderen kann sie als Sicherungs- oder Überwachungsgarantenpflicht auftreten, welche dazu verpflichtet, eine bestimmte Gefahrenquelle unter Kontrolle zu halten, um Beeinträchtigungen von unbestimmt vielen Rechtsgütern zu verhindern.[510] 304

Die Garantenstellung kann sich gemäss Art. 11 Abs. 2 StGB unter anderem aus Gesetz, Vertrag, freiwillig eingegangener Gefahrengemeinschaft oder aus der Schaffung einer Gefahr ergeben.[511] Darüber hinaus eröffnet die nicht abschliessende Natur der gesetzlichen Aufzählung weitere mögliche Entstehungsgründe wie etwa die Geschäftsherrenhaftung oder die Herrschaft über eine Gefahrenquelle. Jedoch können aus dem Grundsatz von Treu und Glauben abgeleitete sittliche oder moralische Gebote keine Garantenstellung begründen.[512] Entscheidend ist zudem, dass es sich bei der daraus abgeleiteten Garantenpflicht stets um eine qualifizierte Handlungspflicht handelt, die eine besondere Beziehung zwischen der verpflichteten Person und dem geschützten Rechtsgut voraussetzt.[513] 305

Nachfolgend wird untersucht, ob sich für Betreiberinnen dezentralisierter Finanzanwendungen aus dem Geldwäschereigesetz, aus Ingerenz, aus der Herrschaft über eine Gefahrenquelle oder aus der Geschäftsherrenhaftung 306

509 CR CP I-CASSANI/VILLARD, Art. 11 N 20 f.; DAN, N 188; DONATSCH/GODENZI/TAG, S. 322 ff.; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 7; STRATENWERTH/BOMMER, AT I, § 15 N 16; TRECHSEL et al., S. 254.

510 BGE 141 IV 249 E. 1.1; 134 IV 255 E. 4.2.1; 120 IV 98 E. 2c; 113 IV 68 E. 5b; CR CP I-CASSANI/VILLARD, Art. 11 N 21 f.; DONATSCH/GODENZI/TAG, S. 323 f.; HURTADO POZO/GODEL, N 826; KAUFMANN, S. 283.

511 CR CP I-CASSANI/VILLARD, Art. 11 N 23; DONATSCH/GODENZI/TAG, S. 324; HURTADO POZO/GODEL, N 826 ff.; STRATENWERTH/BOMMER, AT I, § 14 N 13 ff.; TRECHSEL et al., S. 255 ff.

512 Botschaft StGB 1998, S. 2002; BGE 123 IV 70 E. 2; 120 IV 98 E. 2c; 108 IV 3 E. 1b; Urteil des BGer 6B_274/2019 vom 28. Februar 2020 E. 2.4; DAN, N 195; DONATSCH/GODENZI/TAG, S. 325; GETH, N 295; AK StGB-GRAF, Art. 11 N 10 ff.; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 47; STRATENWERTH/BOMMER, AT I, § 14 N 27; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 7.

513 BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 67; CONRAD HARI, S. 365; AK StGB-GRAF, Art. 11 N 10; VON ROTZ, S. 74; HK StGB-WOHLERS, Art. 11 N 9; vgl. BGE 148 IV 39 E. 2.3.2; 141 IV 459 E. 4.2; 123 IV 70 E. 2; DONATSCH/GODENZI/TAG, S. 325.

eine Garantenstellung ergibt, die sie verpflichtet, eine Gefährdung des im Rahmen der Geldwäscherei geschützten Rechtsguts des staatlichen Einziehungsinteresses durch die deliktische Nutzung ihrer Anwendungen seitens der Nutzer zu verhindern.[514]

A. Geldwäschereigesetz

307 Eine mögliche Quelle einer Garantenstellung ist das Gesetz, wobei im Bereich der Geldwäscherei insbesondere das Geldwäschereigesetz (GwG) von Bedeutung ist.[515] Das Bundesgericht hat in seiner Rechtsprechung gestützt auf die darin verankerten Sorgfaltspflichten eine Garantenpflicht bejaht und damit die Grundlage für eine strafrechtliche Verantwortlichkeit der Finanzintermediäre durch Unterlassen geschaffen.[516] Diese Rechtsprechung hat eine anhaltende Debatte in der Literatur ausgelöst, die sich im Kern um die Frage dreht, ob Finanzintermediärinnen verpflichtet werden können, im Interesse der Rechtspflege tätig zu werden.[517] Im Mittelpunkt steht dabei insbesondere die Überlegung, ob die Meldepflicht nach Art. 9 GwG eine Garantenpflicht begründen kann.[518]

308 Losgelöst von dieser Debatte bedingt eine Garantenstellung aus dem Geldwäschereigesetz die Unterstellung der Betreiberinnen unter dessen persönlichen, sachlichen und örtlichen Geltungsbereich.[519] Im Folgenden werden diese drei Dimensionen im Kontext des Betreibens dezentralisierter Finanzanwendungen näher untersucht. Dabei ist zu berücksichtigen, dass das schweizerische Finanzmarktrecht einem technologieneutralen Regulierungsansatz folgt. Demzufolge gelten Rechtsnormen unabhängig von der dabei verwendeten Technologie – und damit auch für dezentralisierte Finanzanwendungen. Dies entspricht dem Leitprinzip ‹same business, same risks, same rules›,

514 Für Ausführungen zum Rechtsgut vgl. vorne N 176; BGE 145 IV 335 E. 3.1; 129 IV 322 E. 2.2.4; Urteil des BGer 6B_45/2021 vom 27. April 2022 E. 4.2; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 91 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 10; HK StGB-WOHLERS, Art. 305bis N 1.

515 Vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 630 ff.; AK StGB-GRAF, Art. 11 N 11; BSK StGB II-PIETH, Art. 305bis N 57.

516 Urteil des BGer 6B_729/2010 vom 8. Dezember 2011 E. 4.3; CR CP II-CASSANI/VILLARD, Art. 305bis N 39; PK StGB-PIETH/SCHULTZE, Art. 305bis N 20; vgl. BGE 136 IV 188 E. 6.2.1.

517 Anstatt vieler KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 630 ff.; BOMMER, ZBJV 2015, S. 351 f.; CONRAD HARI, S. 365 ff.; DONATSCH/THOMMEN/WOHLERS, S. 509; BSK StGB II-PIETH, Art. 305bis N 57; THOMMEN, S. 425 ff.; vgl. auch die ältere Lehre ARZT, S. 192; EGGER TANNER, S. 137; GRABER, S. 137.

518 Vgl. z.B. BOMMER, ZBJV 2015, S. 352; CONRAD HARI, S. 370; THOMMEN, S. 432 ff.

519 Vgl. SHK GwG-SCHÄREN, Art. 2 N 1 ff.; OFK GwG-WYSS, Art. 2 N 1 ff.; vgl. auch BAUMANN, N 47; NAGEL, Diss., N 151.

wonach Tätigkeiten mit vergleichbarem Risikoprofil denselben regulatorischen Anforderungen unterstellt werden.[520]

1. Persönlicher und sachlicher Geltungsbereich

Der persönliche Geltungsbereich des Geldwäschereigesetzes erfasst in Art. 2 Abs. 1 GwG sowohl Finanzintermediärinnen als auch Händlerinnen.[521] Der Begriff der Finanzintermediärin kann keiner allgemeingültigen Definition zugeführt werden,[522] einer systematischen Betrachtungsweise folgend erschliesst sich dieser jedoch aus den in Art. 2 Abs. 2 und 3 GwG umschriebenen natürlichen und juristischen Personen.[523] Während natürliche Personen direkt dem Geldwäschereigesetz unterstellt sind, obliegen bei juristischen Personen die Pflichten nicht deren Organen oder Mitarbeitenden, sondern der juristischen Person selbst.[524] Anders verhält es sich bei einfachen Gesellschaften, bei denen die Pflichten jedem Gesellschafter auferlegt sind, der eine finanzintermediäre Tätigkeit ausübt.[525] 309

Das Geldwäschereigesetz teilt Finanzintermediärinnen in zwei Kategorien ein: zum einen die prudenziell beaufsichtigten Finanzintermediärinnen nach Art. 2 Abs. 2 GwG und zum anderen die nicht prudenziell beaufsichtigten Finanzintermediärinnen nach Art. 2 Abs. 3 GwG.[526] Erstere werden in der Bestimmung ausdrücklich aufgezählt und unterliegen einer umfassenden (prudenziellen)[527] Finanzmarktaufsicht im Rahmen einer staatlichen Bewilligung.[528] Letztere stehen unter der Aufsicht einer Selbstregulierungsorgani- 310

520 Bundesrat, Digital Finance, S. 3, 12; Botschaft DLT, S. 239; FINMA, Jahresbericht, S. 20; FINMA, Leitlinien, N 5; vgl. auch GAFI, VASP, N 25.

521 BSK GwG-KILGUS/LOSINGER, Art. 1 N 17; OFK GwG-WYSS, Art. 2 N 7 ff. Da die Qualifikation als Händlerin an die Entgegennahme von Bargeld anknüpft, kommt sie im Zusammenhang mit Kryptowerten nicht in Betracht (vgl. BSK GwG-RAMELET, Art. 2 Abs. 1 lit. b N 17).

522 BOVET / HÉRITIER LACHAT, N 131; EICHHORN, N 42; NAGEL, Diss., N 183; SHK GwG-SCHÄREN, Art. 2 N 2.

523 Botschaft GwG 1996, S. 1116; BSK GwG-PEYER, Art. 2 Abs. 1 lit. a N 6; OFK GwG-WYSS, Art. 2 N 22.

524 DUARTE, § 31 N 8; NAGEL, Diss. N 194; BSK GwG-PEYER, Art. 2 Abs. 2 N 2; ROHR, S. 11.

525 NAGEL, Diss., N 194; BSK GwG-PEYER, Art. 2 Abs. 2 N 3; ROHR, S. 12; OFK GwG-WYSS, Art. 2 N 29.

526 BSK GwG-PEYER, Art. 2 Abs. 1 lit. a N 6; SHK GwG-SCHÄREN, Art. 2 N 2; ZYSSET/NAGEL, S. 143.

527 Prudenziell bezeichnet im finanzmarktrechtlichen Kontext eine Aufsicht, die (im Gegensatz zu absoluten Verboten oder einem Laisser-faire-Ansatz) durch Umsicht, Vernunft und Sachverstand gekennzeichnet und primär auf die Stabilität und Funktionsfähigkeit des Finanzmarkts ausgerichtet ist (EICHHORN, N 44; GYSI, N 54 ff.; NAGEL, Diss., N 10; vgl. BSK GwG-PEYER, Art. 2 Abs. 1 lit. a N 7 f.; vgl. auch BGE 143 II 162 E. 2.2; Urteil des BVGer B-7234/2015 vom 6. Dezember 2017 E. 2.2; BOVET / HÉRITIER LACHAT, N 128; SHK GwG-SCHÄREN, Art. 2 N 7).

528 NAGEL, Diss., N 217 ff.; BSK GwG-PEYER, Art. 2 Abs. 2 N 22 ff.; OFK GwG-WYSS, Art. 2 N 14.

sation (SRO).[529] Ihnen obliegt nach Art. 14 Abs. 1 GwG die Pflicht, sich einer solchen anzuschliessen.[530]

311 Der persönliche und sachliche Geltungsbereich für nicht-prudenzielle Finanzintermediärinnen ist in Art. 2 Abs. 3 GwG festgelegt. Erfasst werden natürliche und juristische Personen, die entweder eine Tätigkeit im Sinne der Generalklausel («Personen, die berufsmässig fremde Vermögenswerte annehmen oder aufbewahren oder helfen, sie anzulegen oder zu übertragen») oder eine Tätigkeit nach den Spezialtatbeständen Art. 2 Abs. 3 lit. a-g GwG ausüben.[531] Umstritten ist, ob diese als eigenständige Spezialtatbestände neben die Generalklausel treten oder ob sie lediglich deren Konkretisierung darstellen.[532] Die herrschende Lehre geht davon aus, dass sämtliche in den Spezialtatbeständen genannten Tätigkeiten nur dann unter das Geldwäschereigesetz fallen, wenn zugleich die Tatbestandsmerkmale der Generalklausel (Fremdheit der Vermögenswerte und Berufsmässigkeit) erfüllt sind.[533]

312 Bei prudenziellen Finanzintermediärinnen bestimmt sich der sachliche Geltungsbereich, im Gegensatz zu den in Art. 2 Abs. 3 GwG erfassten Finanzintermediärinnen, aufgrund eines bestimmten abschliessend aufgeführten regulatorischen Status (resp. Bewilligungsstatus).[534] Umstritten ist, ob die Bewilligungspflicht nach Art. 2 Abs. 2 GwG unabhängig von der konkret ausgeübten Tätigkeit das allein massgebende Kriterium für die Unterstellung unter den sachlichen Geltungsbereich bildet. Dies ist im Einklang mit der herrschenden Lehre abzulehnen: Aus teleologischer Sicht erfassen die Bestimmungen des Geldwäschereigesetzes nur Tätigkeiten, die ein typisches Geldwäschereirisiko aufweisen, weshalb vor diesem Hintergrund der Begriff der Finanzintermediation gemäss Art. 2 Abs. 3 GwG den sachlichen Geltungsbereich auch für die in Art. 2 Abs. 2 GwG genannten Finanzintermediäre einschränkend konturiert.[535]

529 NAGEL, Diss., N 221 ff.; BSK GwG-GRETER, Art. 2 Abs. 3 N 1.

530 BSK GwG-FRIGO/JAIN, Art. 14 N 9; OFK GwG-WYSS, Art. 14 N 7; vgl. SHK GwG-BRUNNHOFER/LEIMGRUBER, Art. 14 N 12. Das Betreiben einer GwG-pflichtigen Tätigkeit ohne Anschluss an eine SRO ist gemäss Art. 44 FINMAG i.V.m. Art. 14 GwG strafbar (vgl. Urteil des BGer 2C_303/2016 vom 24. November 2016 E. 3.3; JOSITSCH/VON ROTZ, S. 594; PAJAROLA, N 521).

531 BSK GwG-GRETER, Art. 2 Abs. 3 N 9 ff.; NAGEL, Diss., N 221 ff.

532 Zum Meinungsstand NAGEL, Diss., N 221 ff.; für eine Subsidiarität der Generalklausel vgl. z.B. CR LBA-BOVET/BACHARACH, Art. 2 N 75.

533 RIMLE, § 12 N 18; NAGEL, Diss., N 221 ff.; ROHR, S. 5; SHK GwG-SCHÄREN, Art. 2 N 55.

534 BSK GwG-PEYER, Art. 2 Abs. 2 N 8; SHK GwG-SCHÄREN, Art. 2 N 8.

535 SHK GwG-SCHÄREN, Art. 2 N 9; ANDREOTTI, S. 350 f.; NAGEL, Diss., N 198 ff.; BSK GwG-PEYER, Art. 2 Abs. 2 N 9.

Im Folgenden wird untersucht, inwiefern Betreiberinnen dezentralisierter Anwendungen unter den persönlichen und sachlichen Geltungsbereich des Geldwäschereigesetzes fallen – sei es durch eine finanzintermediäre Tätigkeit im Sinne der Generalklausel bzw. der Spezialtatbestände oder durch eine Einordnung als prudenziell beaufsichtigte Finanzintermediäre. Die Unterstellungsfragen müssen grundsätzlich im Einzelfall und im Hinblick auf die Art der Finanzanwendung durchgeführt werden. 313

a) Hilfe bei der Übertragung von virtuellen Vermögenswerten

Im Zusammenhang mit dezentralisierten Finanzanwendungen von grosser Bedeutung ist der Spezialtatbestand der Erbringung einer Dienstleistung für den Zahlungsverkehr nach Art. 2 Abs. 3 lit. b GwG, welcher durch Art. 4 Abs. 1 GwV eine Präzisierung erfährt.[536] Relevanz hat im Kontext von Kryptowerten vor allem Art. 4 Abs. 1 lit. b GwV, wonach eine Finanzintermediärin «hilft, virtuelle Währungen an eine Drittperson zu übertragen, sofern er [sie] mit der Vertragspartei eine dauernde Geschäftsbeziehung unterhält oder sofern er [sie] für die Vertragspartei Verfügungsmacht über virtuelle Währungen ausübt und er [sie] die Dienstleistung nicht ausschliesslich gegenüber angemessen beaufsichtigten Finanzintermediären erbringt».[537] 314

Der Tatbestand erfasst somit nicht nur die Unterstützung bei der Übertragung virtueller Währungen an eine Drittperson, sondern setzt zusätzlich entweder das Bestehen einer dauernden Geschäftsbeziehung mit der Vertragspartei oder die Ausübung von Verfügungsmacht über deren virtuelle Währungen voraus. 315

536 ANDREOTTI, S. 393 f.; MEIRICH, N 1297 ff.; vgl. EFD, Erläuterungen, S. 22; Bundesrat, DLT, S. 140; NAGEL, Diss., N 637 ff.

537 Diese Konkretisierung wurde im Zuge der Anpassung des Bundesrechts an Entwicklungen der Technik verteilter Register eingeführt. Zuvor wurden hinsichtlich der Erbringung von Dienstleistungen für den Zahlungsverkehr nur DLT-Konstellationen darunter subsumiert, bei denen der Dienstleister Verfügungsmacht über fremde Vermögenswerte hatte (vgl. FINMA-RS-11/1, N 58). Neben der Verfügungsmacht wurde der neue Tatbestand nun auch um eine zweite Tatbestandsvariante der dauernden Geschäftsbeziehung zwischen Dienstleister und Kunde erweitert (EFD, Erläuterungen, S. 4; GLARNER/GANZONI/HEPP, S. 1092 f.; MAURENBRECHER/LEISINGER, S. 711 f.; STENGEL/RUCKSTUHL, N 548, 573). Dies begründete der Gesetzgeber damit, dass angesichts der rasanten Entwicklung solcher Geschäftsmodelle und des unverhältnismässigen Abklärungsaufwands die Verfügungsmacht als alleiniges Abgrenzungskriterium zwischen unterstellten und nicht unterstellten Dienstleistungen als nicht mehr sachgerecht erachtet wird (EFD, Erläuterungen, S. 22; BOŠKIĆ/HEPP, S. 219; krit. ANDREOTTI, S. 394 ff.; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 15; GLARNER/GANZONI/HEPP, S. 1091 ff.; MEIRICH, N 1323 ff.; STENGEL/PAYDAR, N 18.50).

aa) Virtuelle Währungen

316 Das von der FINMA verwendete und mit den Materialien des Bundesrats weitgehend übereinstimmende Begriffsverständnis definiert virtuelle Währungen als «digitale Darstellung eines Wertes, welche im Internet handelbar ist und die Funktion von Geld übernimmt, ohne jedoch als gesetzliches Zahlungsmittel akzeptiert zu werden. Virtuelle Währungen haben eine eigene Denomination und sind – im Unterschied zu E-Geld – nicht durch ein gesetzliches Zahlungsmittel unterlegt. Sie existieren lediglich als digitaler Code und haben deswegen auch kein materialisiertes Gegenstück bspw. in Form von Münzen oder Noten. Jedoch können virtuelle Währungen als Zahlungsmittel für reale Güter und Dienstleistungen verwendet werden».[538]

317 Erfasst sind damit Kryptovermögenswerte, die eine Zahlungsmittelfunktion erfüllen, mithin sogenannte Zahlungs-Token (vgl. Art. 4 Abs. 1bis lit. c GwV).[539] Nicht unter diesen Begriff fallen Token, deren Ausgabe primär dem Zugang zu einer Blockchain-Anwendung ausserhalb des Finanzsektors dient, oder solche, die ausschliesslich innerhalb eines geschlossenen Systems und nur gegenüber dem Emittenten als Zahlungsmittel eingesetzt werden können (Zwei-Parteien-Konstellation).[540]

318 Für die hier relevanten dezentralisierten Finanzanwendungen ist die Einordnung in der Regel unproblematisch, da sie funktional überwiegend auf Zahlungs-Token wie Bitcoin oder Ether ausgerichtet sind und damit unter den Begriff der virtuellen Währungen im Sinne des Geldwäschereigesetzes fallen.[541]

bb) Hilfe zur Übertragung

319 Die Hilfe zur Übertragung an eine Drittperson ist weit auszulegen und erfasst jeden kausalen Beitrag der Finanzintermediärin, der die Übertragung virtueller Währungen an eine Drittperson ermöglicht oder erleichtert.[542] Erforderlich ist ein Abhängigkeitsverhältnis zwischen dem Nutzer und dem Dienst-

538 FINMA, Erläuterungsbericht, S. 11; Bundesrat, Virtuelle Währungen, S. 7 f.; vgl. ANDREOTTI, S. 385 f.; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 12; MEIRICH, N 1310; NAGEL, Zahlungsverkehr, S. 76.

539 ANDREOTTI, S. 386; GLARNER/GANZONI/HEPP, S. 1097; KUHN, S. 38; MEIRICH, N 1310; vgl. EFD, Erläuterungen, Fn. 13.

540 GLARNER/GANZONI/HEPP, S. 1097; ANDREOTTI, S. 386; m.w.H. zum Begriff des Zahlungs-Tokens Bundesrat, DLT, S. 89; FINMA, Wegleitung, S. 2 f.; NAGEL, Zahlungsverkehr, S. 78.

541 Vgl. MAURENBRECHER/LEISINGER, Teil 2, S. 711.

542 NAGEL, Zahlungsverkehr, S. 76, NAGEL, Diss., N 208; vgl. Bundesrat DLT, S. 23; BACHARACH, S. 287.

leister bzw. dessen Infrastruktur im Hinblick auf den Übertragungsvorgang.[543] Ein solches liegt insbesondere dann vor, wenn die Unterstützungsleistung des Dienstleisters aus Sicht eines durchschnittlichen, technisch wenig versierten Nutzers die Durchführung der Transaktion erleichtert.[544] Dies kann sich etwa darin zeigen, dass die Benutzung eines vom Dienstleister bereitgestellten Webinterfaces erforderlich ist, um virtuelle Währungen über dessen Infrastruktur zu transferieren. Ebenso kann eine Abhängigkeit entstehen, wenn die Erstellung eines Accounts oder eine Anmeldung Voraussetzung für den Zugang zur technischen Infrastruktur ist, um Übertragungen vornehmen zu können. Schliesslich ist auch die Bereitstellung von cloudbasierten Speicherlösungen für Private Keys relevant, sofern der Nutzer auf diese zurückgreifen muss, um seine Transaktionen durchzuführen.[545]

Bei dezentralisierten Finanzanwendungen übernehmen Smart Contracts 320
die Funktion, die Übertragung von Kryptowerten zwischen Nutzern automatisiert und technisch abgesichert abzuwickeln. Sie stellen damit eine Infrastruktur bereit, welche die Durchführung solcher Transaktionen in intermediärsfreier und standardisierter Form ermöglicht und deren Abwicklung für die Nutzer vereinfacht.[546] Dies zeigt sich exemplarisch bei Handelsplattformen, auf denen die Übertragung entweder unmittelbar zwischen den Wallets zweier Nutzer oder durch Umschichtung von Vermögenswerten innerhalb eines Liquiditätspools erfolgt. Ebenso erleichtern Kryptomixer die Durchführung von Transfers, indem sie Einzahlungen verschiedener Nutzer sammeln und standardisierte Auszahlungen an neu gewählte Adressen ermöglichen, wodurch die Verbindung zwischen Ein- und Auszahlung technisch aufgehoben wird. In beiden Fällen stellt das jeweilige Protokoll damit eine Unterstützung der Übertragung im Sinne von Art. 4 Abs. 1 lit. b GwV dar.[547]

BACHARACH legt jedoch zutreffend dar, dass der Begriff der ‹Hilfe› im 321
Kontext der geldwäschereirechtlichen Unterstellung eine tatsächliche Verhaltenskomponente erfordert. Die massgebliche ‹Aktivität› muss gegenwärtig und aktiv ausgeübt werden, nicht bloss initial kodiert oder in abstrakter Form bereitgestellt worden sein. Der blosse Quellcode, der Dritten offen zur Verfügung gestellt wird, ist einer Dienstleistung im Sinne der Geldwäschereiverordnung nicht gleichzusetzen, solange die Protokollfunktionen vollständig autonom und unveränderlich ausgeführt werden. Ob ein Verhalten in diesem

543 GLARNER/GANZONI/HEPP, S. 1100.

544 GLARNER/GANZONI/HEPP, S. 1100.

545 Vgl. zum Ganzen GLARNER/GANZONI/HEPP, S. 1100.

546 Botschaft DLT, S. 270 f.; ANDREOTTI, S. 397; MEIRICH, N 1303.

547 Vgl. MEIRICH, N 1304; STENGEL/PAYDAR, N 18.74.

Sinne vorliegt, beurteilt sich laut BACHARACH nicht anhand eines einzelnen Kriteriums, sondern im Rahmen eines faktischen Kontrollniveaus, das durch ein Bündel von Indizien bestimmt werden kann. Dazu zählen insbesondere das Erheben von Transaktionsgebühren, die Möglichkeit, den Smart Contract zu modifizieren, die Fähigkeit, Transaktionen auf den Krypto-Assets Dritter auszulösen, die Option, Funktionen des Smart Contracts auszusetzen oder zu unterbrechen, der betriebene zentrale Zugang über eine Benutzeroberfläche (Frontend) sowie das Fehlen dezentraler Governance-Mechanismen wie etwa Governance-Token. Je mehr dieser Elemente kumulativ vorliegen, desto eher kann von einem ‹aktiven› Verhalten der Betreiberschaft ausgegangen werden, das unter Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 GwV fällt.[548]

322 Für DeFi-Protokolle liegt eine ‹Hilfe zur Übertragung› nur dann vor, wenn die Betreiberschaft nicht lediglich den Smart Contract initial veröffentlicht, sondern gegenwärtig an der Ermöglichung oder Erleichterung des Transferprozesses mitwirkt. Dies setzt ein funktionales Einflussmoment voraus, etwa durch die Kontrolle eines Frontends, die Erhebung von Gebühren oder fortbestehende Administrations- bzw. Eingriffsrechte. Bei idealtypisch dezentral ausgestalteten Anwendungen, deren Protokoll autonom und unveränderlich ausgeführt wird und bei denen die Betreiberschaft weder über ein eigenes Frontend noch über Gebührenmechanismen oder sonstige administrative Eingriffs- und Steuerungsmöglichkeiten verfügt, fehlt es hingegen an einem solchen funktionalen Einflussmoment.

cc) Erste Tatbestandsvariante: Verfügungsmacht

323 Den Materialien zufolge liegt Verfügungsmacht vor, wenn die Finanzintermediärin Zugriff auf den Private Key des Nutzers hat.[549] Sofern dies nicht gegeben ist, erstreckt sich das Begriffsverständnis auch auf Dienstleister, welche «die Übertragung der virtuellen Währungen jedoch mittels Smart Contract ermöglichen und dabei die Aufträge bestätigen, freigeben oder sperren können oder anderweitig Kontrolle über den Smart Contract haben».[550] Nicht erfasst werden hingegen Dienstleister, die lediglich eine reine Vermittlungstätigkeit ausüben, das heisst Käufer und Verkäufer zusammenführen, ohne Zugriff auf Smart Contracts oder deren Ausführungsmöglichkeiten zu besitzen.[551]

548 Vgl. zum Ganzen BACHARACH, S. 332 ff.

549 Bundesrat, DLT, S. 146 f.; EFD, Erläuterungen, S. 22 f.

550 Bundesrat, DLT, S. 147; EFD, Erläuterungen, S. 22; vgl. BACHARACH, S. 336; NAGEL, Zahlungsverkehr, S. 76 f.

551 EFD, Erläuterungen, S. 23; Bundesrat, DLT, S. 147; Bundesrat, Virtuelle Währungen, S. 16; vgl. ANDREOTTI, S. 402 f.

Die herrschende Lehre folgt dem Grundgedanken der Materialien im Wesentlichen, präzisiert jedoch die Anforderungen.[552] Unbestritten liegt eine Verfügungsmacht vor, wenn die Betreiberin Zugriff auf den Private Key des Nutzers hat.[553] Darüber hinaus kann nicht jede beliebige Form der Kontrolle über einen Smart Contract als Verfügungsmacht qualifiziert werden. Erforderlich ist ein unmittelbarer Bezug zu den Aufträgen der Nutzer. Nur wenn die Plattformbetreiberin mittels Admin Keys oder vergleichbarer Mittel in der Lage ist, in den Transaktionsfluss einzugreifen, etwa eine Transaktion dauerhaft zu blockieren oder deren Ausführung von einer Bestätigung abhängig zu machen, liegt Verfügungsmacht im Sinne des Geldwäschereigesetzes vor.[554] Eine blosse Parametrisierung der Funktionsweise, bspw. durch Anpassung von Handelsgebühren, reicht derweil nicht aus.[555] Ebenso werden reine Vermittlungstätigkeiten ohne Einfluss auf den Zahlungsfluss grundsätzlich nicht erfasst.[556] 324

Für dezentralisierte Finanzanwendungen bedeutet dies, dass eine Verfügungsmacht nur besteht, wenn die Betreiberin über eine fortbestehende Interventions- oder Freigabekompetenz verfügt, die sich auf konkrete Übertragungsvorgänge auswirkt. Fehlt eine solche Einflussmöglichkeit und werden die Protokollfunktionen vollständig autonom sowie unveränderlich ausgeführt, wie bei idealtypisch dezentralen Anwendungen, kann eine Verfügungsmacht nicht bejaht werden. 325

dd) Zweite Tatbestandsvariante: dauernde Geschäftsbeziehung

Das Tatbestandselement der dauernden Geschäftsbeziehung gemäss Art. 4 Abs. 1 lit. b GwV setzt zunächst voraus, dass zwischen dem Finanzintermediär und dem Nutzer ein ausdrückliches oder stillschweigendes Vertragsverhältnis im Sinne von Art. 1 Abs. 1 OR besteht, das sich inhaltlich auf die Übertragung virtueller Währungen bezieht.[557] GLARNER/GANZONI/HEPP betonen, dass ein solches Vertragsverhältnis auch konkludent zustande kommen kann. 326

552 ANDREOTTI, S. 396 ff.; BACHARACH, S. 336 ff.; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 21; BOŠKIĆ/HEPP, S. 219 ff.; GLARNER/GANZONI/HEPP, S. 1097 ff.; MEIRICH, N 1311 ff.; NAGEL, Diss., N 638 f.; NAGEL, Zahlungsverkehr, S. 76 f.

553 ANDREOTTI, S. 402 f.; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 21; BOŠKIĆ/HEPP, S. 219 f.; GLARNER/GANZONI/HEPP, S. 1097 f.; MEIRICH, N 1312; NAGEL, Diss., N 638; NAGEL, Zahlungsverkehr, S. 76.

554 ANDREOTTI, S. 397; BACHARACH, S. 336; NAGEL, Zahlungsverkehr, S. 76; STENGEL/PAYDAR, N 18.70.

555 ANDREOTTI, S. 397.

556 ANDREOTTI, S. 402 ff.; MEIRICH, N 1315; MOLO/DRZALIC, S. 50; STENGEL/PAYDAR, N 18.70.

557 ANDREOTTI, S. 399; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 13; GLARNER/GANZONI/HEPP, S. 1101; vgl. MEIRICH, N 1337 ff., der die Frage des Vertragsverhältnisses detailliert unter Rückgriff auf die Konstruktionen des Mäkler- sowie des Softwarenutzungsvertrags prüft.

Indizien hierfür sind insbesondere, wenn die Nutzung der technischen Infrastruktur mit laufenden Dienstleistungen des Anbieters verbunden ist, wenn regelmässige Wartungen oder Aktualisierungen erforderlich sind, wenn Gebühren nicht bloss transaktionsbezogen, sondern in zeitlichen Intervallen erhoben werden, wenn zur Nutzung ein spezifisches Interface bereitgestellt werden muss oder wenn der Zugang eine Anmeldung beziehungsweise Kontoeröffnung voraussetzt.[558]

327 Über das Bestehen eines Vertragsverhältnisses hinaus ist erforderlich, dass dem Anbieter eine gewisse Einfluss- oder Kontrollmöglichkeit im Hinblick auf den Übertragungsvorgang zukommt.[559] Diese muss zwar hinter den Erfordernissen der Verfügungsmacht zurückbleiben, erfordert aber mehr als eine blosse Zurverfügungstellung von Infrastruktur ohne Eingriffsmöglichkeiten.[560] Damit scheiden grundsätzlich reine Vermittlungstätigkeiten ebenso wie vollständig autonome Systeme aus.[561] Relevanz kann hingegen insbesondere die Administrierbarkeit von Smart Contracts erlangen, sofern nicht unmittelbar in die Transaktion der Nutzer bzw. deren Aufträge eingegriffen werden kann.

328 Schliesslich setzt das Tatbestandsmerkmal eine gewisse Kontinuität voraus. Diese fehlt bei bloss einmaligen Tätigkeiten, wie sie etwa im Rahmen von Kassageschäften vorkommen.[562] Dauerhaftigkeit liegt demgegenüber gemäss MEIRICH dann vor, wenn der Betrieb einer dezentralisierten Anwendung von fortlaufenden Handlungen des Dienstleisters abhängig ist – etwa vom dauerhaften Unterhalt eines Interface oder von einer kontinuierlichen Administration zur Implementierung von Aktualisierungen und Konfigurationsanpassungen. Auch eine Serie aufeinanderfolgender Vertragsabschlüsse kann den Charakter einer dauernden Geschäftsbeziehung begründen. Gerade im DeFi-Bereich wird dieser Aspekt häufig dadurch verwirklicht, dass die Verbindung eines Wallets mit dem Interface einer Anwendung die fortgesetzte Nutzung des Protokolls erst ermöglicht und die Nutzer dadurch in eine wiederholte, auf Dauer angelegte Beziehung mit dem jeweiligen Anbieter treten.[563]

329 Für idealtypisch dezentrale Anwendungen gilt indessen: Werden Smart Contracts vollständig autonom und unveränderlich ausgeführt, besteht kein

558 GLARNER/GANZONI/HEPP, S. 1101.

559 GLARNER/GANZONI/HEPP, S. 1101 f.; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 16; NAGEL, Zahlungsverkehr, S. 77; MEIRICH, N 1358 ff.

560 BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 16; GLARNER/GANZONI/HEPP, S. 1101; MEIRICH, N 1358.

561 ANDREOTTI, S. 402 ff.; vgl. EFD, Erläuterungen, S. 23.

562 ANDREOTTI, S. 399; GLARNER/GANZONI/HEPP, S. 1101; MEIRICH, N 1367 ff.

563 MEIRICH, N 1372.

Frontend-Gatekeeping, keine Registrierungspflicht und keine laufende Betreiberintervention, fehlt es an einer fortgesetzten Dienstleistungsstruktur. In solchen Fällen ist das Tatbestandsmerkmal der dauernden Geschäftsbeziehung grundsätzlich zu verneinen.

ee) Berufsmässigkeit und Fremdheit der Vermögenswerte

Auch die Spezialtatbestände des Geldwäschereigesetzes setzen voraus, dass die allgemeinen Kriterien der Berufsmässigkeit und der Fremdheit der Vermögenswerte erfüllt sind.[564] Das Erfordernis der Berufsmässigkeit ist in Art. 7 Abs. 1 GwV näher konkretisiert und qualifiziert eine Tätigkeit als berufsmässig, wenn die Finanzintermediärin pro Kalenderjahr entweder einen Bruttoerlös von mehr als CHF 50'000 erzielt (lit. a), mit mehr als zwanzig Vertragsparteien Geschäftsbeziehungen aufnimmt oder mindestens zwanzig solche Beziehungen unterhält (lit. b), unbefristete Verfügungsmacht über fremde Vermögenswerte in einem Umfang von über CHF 5 Millionen hat (lit. c) oder Transaktionen in einem Gesamtvolumen von über CHF 2 Millionen durchführt (lit. d).[565] 330

Das Erfordernis der Fremdheit der Vermögenswerte bestimmt sich nach der rechtlichen Situation. Es liegt vor, wenn der Finanzintermediärin keine eigenen Rechtsansprüche, bspw. in Form von Eigentumsrechten, an den betreffenden Vermögenswerten zukommen.[566] 331

ff) Würdigung

Bei dezentralisierten Handelsplattformen zeigt sich, dass die Hilfe zur Übertragung regelmässig durch Smart Contracts erfolgt, die entweder den direkten Tausch zwischen den Wallets zweier Nutzer oder die Umschichtung von Beständen innerhalb eines Liquiditätspools ermöglichen.[567] Eine Verfügungsmacht liegt nur dann vor, wenn die Smart Contracts administrierbar sind und die Betreiberin in die Abwicklung eingreifen kann, etwa indem Transaktionen blockiert oder freigegeben werden.[568] In einer Vielzahl der Protokolle 332

564 Vgl. vorne N 311; RIMLE, § 12 N 18; NAGEL, Diss., N 221 ff.; ROHR, S. 5; SHK GwG-SCHÄREN, Art. 2 N 55.

565 Vgl. CR LBA-BOVET/BACHARACH, Art. 2 N 265; BSK GwG-GRETER, Art. 2 Abs. 3 N 41; MEIRICH, N 1079; NAGEL, Diss., N 210.

566 CR LBA-BOVET/BACHARACH, Art. 2 N 78; BSK GwG-GRETER, Art. 2 Abs. 3 N 28; NAGEL, Diss., N 203; ROHR, S. 8; SHK GwG-SCHÄREN, Art. 2 Abs. 3 N 75; OFK GwG-WYSS, Art. 2 N 26.

567 Vgl. Botschaft DLT, S. 270 f.; ANDREOTTI, S. 397; MEIRICH, N 1303.

568 Vgl. EFD, Erläuterungen, S. 22; Bundesrat, DLT, S. 147; ANDREOTTI, S. 397; BACHARACH, S. 336; NAGEL, Zahlungsverkehr, S. 76; STENGEL/PAYDAR, N 18.70.

fehlt ein solches unmittelbares Kontrollrecht.[569] Gleichwohl ist eine Unterstellung über die Tatbestandsvariante der dauernden Geschäftsbeziehung naheliegend, da Nutzer oft über ein von der Betreiberin unterhaltenes Interface Zugang erhalten, wiederholt mit demselben Wallet am Handel teilnehmen und für die Nutzung regelmässig Gebühren entrichten.[570]

333 Bei dezentralisierten Mixern gestaltet sich die Situation ähnlich. Der Kernmechanismus, die Bündelung von Ein- und Auszahlungen und die standardisierte Weiterleitung an neu gewählte Adressen, wird durch Smart Contracts ausgeführt.[571] Eine Verfügungsmacht im engeren Sinn ist hierbei in der Regel nicht gegeben, da die Betreiberin nicht in einzelne Transaktionen eingreifen kann.[572] Die geldwäschereirechtliche Relevanz ergibt sich vielmehr aus der dauernden Geschäftsbeziehung. Diese kann sich aus der wiederholten Nutzung der Dienste durch dieselben Wallets ergeben, ebenso aus der Abhängigkeit von einem kontinuierlichen Betrieb der Anwendung.[573] Der Unterhalt der Infrastruktur, etwa durch Updates oder Schutzvorkehrungen gegen Angriffe, ist für die Funktionsfähigkeit des Mixers unabdingbar. Daraus erwächst eine fortgesetzte Bindung der Nutzer an die Betreiberin, die das Merkmal der Dauerhaftigkeit erfüllt.[574]

334 Die Praxis verdeutlicht damit, dass das Tatbestandselement der Verfügungsmacht in dezentralisierten Umgebungen nur punktuell greift, während die Variante der dauernden Geschäftsbeziehung als ‹Auffangtatbestand› eine wesentliche Rolle spielt. Sie erfasst gerade jene Fälle, in denen keine unmittelbare Zugriffsmöglichkeit besteht, die Nutzer aber dennoch in ein auf Dauer angelegtes Vertrags- und Abhängigkeitsverhältnis mit der Betreiberin eingebunden sind. Sofern es sich jedoch um idealtypisch dezentrale Protokolle ohne jegliche Kontroll- und Einflussmöglichkeit handelt, etwa weil die Smart Contracts nicht modifizierbar sind und kein Zugriff auf Private Keys besteht, scheidet die Unterstellung unter die Tatbestandsvariante der dauernden Geschäftsbeziehung ebenfalls aus.[575]

335 Für beide Anwendungsfälle gilt schliesslich, dass neben den tatbestandsspezifischen Merkmalen auch die allgemeinen Voraussetzungen der Berufs-

569 ANDREOTTI, S. 402 f.

570 Vgl. EFD, Erläuterungen, S. 22; ANDREOTTI, S. 402 f.; GLARNER/GANZONI/HEPP, S. 1101.

571 Vgl. MEIRICH, N 1304; STENGEL/PAYDAR, N 18.74.

572 Vgl. NADLER/SCHÄR, Tornado Cash, S. 124; STENGEL/PAYDAR, N 18.74.

573 Vgl. GLARNER/GANZONI/HEPP, S. 1101.

574 Vgl. MEIRICH, N 1372.

575 Vgl. GLARNER/GANZONI/HEPP, S. 1101 f.; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 16; MEIRICH, N 1358 ff.

mässigkeit und der Fremdheit der Vermögenswerte erfüllt sein müssen.[576] Angesichts der regelmässigen Erhebung von Gebühren, der Vielzahl gleichartiger Nutzerbeziehungen und der beträchtlichen Transaktionsvolumina ist die Berufsmässigkeit in der Praxis bei DeFi-Protokollen in aller Regel gegeben (Art. 7 GwV).[577] Ebenso ist die Fremdheit der Vermögenswerte zu bejahen, da die Token rechtlich im Vermögen der Nutzer verbleiben und die Betreiberinnen lediglich technische Infrastrukturen zur Übertragung bereitstellen, ohne selbst Eigentumsrechte an den übertragenen Vermögenswerten zu erlangen.[578]

b) Geld- und Wertübertragung

Für dezentralisierte Finanzanwendungen kommt schliesslich auch der Tatbestand des Geld- und Wertübertragungsgeschäfts in Betracht (Art. 2 Abs. 2 lit. b i.V.m. Art. 4 Abs. 1 lit. d GwV).[579] Dieser ist definiert als der «Transfer von Vermögenswerten durch Entgegennahme von Bargeld, Edelmetallen, virtuellen Währungen, Schecks oder sonstigen Zahlungsmitteln» und entweder «Auszahlung einer entsprechenden Summe in Bargeld, Edelmetallen oder virtuellen Währungen» (lit. a) oder die «bargeldlose Übertragung oder Überweisung über ein Zahlungs- oder Abrechnungssystem» (lit. b).[580] 336

Das Merkmal der Entgegennahme setzt voraus, dass die Finanzintermediärin Verfügungsmacht über die Vermögenswerte erlangt.[581] Dies ist im Kontext dezentralisierter Anwendungen, wie bereits dargelegt, nur dann erfüllt, wenn der Dienstleister mittels Admin Keys oder vergleichbarer Mittel in den Transaktionsfluss eingreifen kann, etwa indem er Transaktionen blockiert oder deren Ausführung von einer Bestätigung abhängig macht.[582] Darüber hinaus verlangt der Tatbestand das Vorliegen eines Dreiparteienverhältnisses.[583] 337

576 Vgl. RIMLE, § 12 N 18; NAGEL, Diss., N 221 ff.; ROHR, S. 5; SHK GwG-SCHÄREN, Art. 2 N 55.

577 Vgl. MEIRICH, N 1281.

578 Vgl. CR LBA-BOVET/BACHARACH, Art. 2 N 78; BSK GwG-GRETER, Art. 2 Abs. 3 N 28; NAGEL, Diss., N 203; ROHR, S. 8; SHK GwG-SCHÄREN, Art. 2 Abs. 3 N 75; OFK GwG-WYSS, Art. 2 N 26.

579 EFD, Erläuterungen, S. 23; MEIRICH, N 1330; STENGEL/PAYDAR, N 18.63 ff.

580 Vgl. BACHARACH, S. 271; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 22; CR LBA-BOVET/BACHARACH, Art. 2 N 138; NAGEL, Zahlungsverkehr, S. 80.

581 STENGEL/PAYDAR, N 18.85; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 22; CR LBA-BOVET/BACHARACH, Art. 2 N 138; NAGEL, Zahlungsverkehr, S. 74, 80.

582 Vgl. vorne N 323 ff.; ANDREOTTI, S. 397; BACHARACH, S. 336; NAGEL, Zahlungsverkehr, S. 76; STENGEL/PAYDAR, N 18.70.

583 BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 26; CR LBA-BOVET/BACHARACH, Art. 2 N 156; STENGEL/PAYDAR, N 18.59; STENGEL/BIANCHI, N 30; NAGEL, Diss., N 642; NAGEL, Zahlungsverkehr, S. 80; MOLO/DRZALIC, S. 50.

338 Bei dezentralisierten Protokollen erweist sich bereits das Tatbestandsmerkmal der Entgegennahme als problematisch, da hierfür eine Verfügungsmacht der Betreiberin über die Vermögenswerte erforderlich wäre. Diese fehlt aber in der Regel, weil Smart Contracts ohne Eingriffsmöglichkeit der Betreiberinnen ausgeführt werden.[584]

339 Hinsichtlich des Dreiparteienverhältnisses ist bei P2P-Handelsplattformen von dessen Vorliegen auszugehen, da neben Sender und Empfänger stets auch die Betreiberin als vermittelnde Instanz in den Transaktionsablauf eingebunden ist. Schwieriger gestaltet sich die Beurteilung bei Mixern, da die Übertragungen zwar an neue Adressen erfolgen, es sich dabei aber häufig um dieselbe Person handeln kann. Aufgrund der mit der Pseudonymität verbundenen Intransparenz ist jedoch regelmässig nicht feststellbar, ob Sender und Empfänger identisch sind. Daher ist auch bei Mixern grundsätzlich von einem Dreiparteienverhältnis auszugehen.[585]

340 Zusammenfassend ist eine Unterstellung unter Art. 2 Abs. 2 lit. b i.V.m. Art. 4 Abs. 1 lit. d GwV nur bei solchen dezentralisierten Finanzanwendungen möglich, bei denen sowohl ein Dreiparteienverhältnis als auch fortbestehende Interventions- und Steuerungsrechte der Betreiberinnen bestehen, die sich auf konkrete Übertragungsvorgänge auswirken. Fehlt ein solches Einflussmoment – insbesondere bei idealtypisch dezentralen Anwendungen, deren Smart Contracts vollständig autonom und unveränderlich ausgeführt werden –, liegt weder eine Entgegennahme noch ein Dreiparteienverhältnis vor, sodass dieser Anwendungsbereich regelmässig nicht erfüllt ist.

c) Prudenzielle Finanzintermediäre

aa) Bank

341 Denkbar erscheint eine Unterstellung dezentralisierter Anwendungen unter das Geldwäschereigesetz gestützt auf die Einordnung als Bank im Sinne von Art. 1a oder Art. 1b BankG.[586] Erforderlich ist hierfür das Vorliegen einer gewerbsmässigen Entgegennahme von Publikumseinlagen, was grundsätzlich bereits dann erfüllt sein kann, wenn im Rahmen einer auf Dauer angelegten Geschäftstätigkeit fremde Mittel entgegengenommen werden.[587] Der Begriff ‹Publikumseinlagen› ist weit zu verstehen und erfasst prinzipiell, vorbehältlich

584 Vgl. vorne N 325.

585 Vgl. Bundesrat, Virtuelle Währungen, S. 15 f.; FINMA, Erläuterungsbericht, S. 12; BSK GwG-BACHELARD/HESS, Art. 2 Abs. 3 lit. b N 27.

586 ANDREOTTI, S. 462 ff.; NOSER/INFANGER/LÜDI, N 12.43 ff., vgl. Bundesrat, DLT, S. 91; EFD, Vernehmlassungsvorlage, S. 15; BACHARACH, S. 325.

587 SCHÖNKNECHT, Einlagebegriff, S. 301; MEIRICH, N 737; NOSER/INFANGER/LÜDI, N 12.43; vgl. EFD, Vernehmlassungsvorlage, S. 14.

der Ausnahmen gemäss Art. 5 Abs. 1 BankV, sämtliche Verbindlichkeiten mit Darlehens- oder Hinterlegungscharakter.[588] Auch Kryptowerte im Sinne von Zahlungs-Token können Einlagequalität aufweisen.[589] Dies erfordert einerseits das Bestehen eines Rückzahlungsanspruchs des Nutzers, der sich bei dezentralisierten Protokollen im Hinblick auf den Übertrag der Kryptowerte an den Smart Contract grundsätzlich implizit ergibt.[590] Darüber hinaus darf dem Nutzer keine uneingeschränkte Verfügungsmacht zukommen. Insbesondere darf er nicht allein mittels seines Private Keys Zugriff auf die Werte behalten.[591]

342 Schliesslich dürfen die Kryptowerte im Konkursfall nicht aussonderbar sein, das heisst, sie müssen in die Konkursmasse der Intermediärin fallen (vgl. Art. 242 ff. SchKG).[592] Ob eine Aussonderung möglich ist, richtet sich grundsätzlich gemäss Art. 242 Abs. 1 SchKG danach, ob die Konkursmasse Gewahrsam über die betreffende Sache innehat.[593] Im Kontext von Kryptowerten ist dies nicht der Fall, wenn der Kunde mittels seines Private Keys weiterhin Zugriff auf die fremdverwahrten Vermögenswerte hat, selbst wenn dem Verwahrer ein Mitgewahrsam zukommt.[594] Ergänzend ergibt sich ein Aussonderungsanspruch gemäss Art. 242a Abs. 2 SchKG, sofern sich der Gemeinschuldner verpflichtet hat, die kryptobasierten Vermögenswerte jederzeit bereitzuhalten, und diese entweder dem Dritten individuell (lit. a) oder einer Gemeinschaft zugeordnet wurden und klar ersichtlich ist, welcher Anteil des Gemeinschaftsvermögens dem Dritten zusteht (lit. b).[595]

343 Zwar kann bei dezentralisierten Finanzanwendungen eine Einordnung als Bank denkbar sein, ein Scheitern der Bewilligungspflicht ergibt sich allerdings in erster Linie aus dem Kriterium der Verfügungsmacht des Dienstleisters über die eingebrachten Vermögenswerte.[596] Bei der Interaktion mit

588 MEIRICH, N 736; ANDREOTTI, S. 463; BSK BankG-BAHAR/STUPP, Art. 1 N 11 ff.

589 Vgl. EFD, Erläuterungen, S. 17; MEIRICH, N 7423 ff.; NOSER/INFANGER/LÜDI, N 12.43.

590 MEIRICH, N 756 ff.; NOSER/INFANGER/LÜDI, N 12.43; vgl. Bundesrat, DLT, S. 91 EFD, Vernehmlassungsvorlage, S. 15; BACHARACH, S. 272; BSK GwG-PEYER, Art. 2 Abs. 2 N 26.

591 MEIRICH, N 789 ff.; NOSER/INFANGER/LÜDI, N 12.43; ANDREOTTI, S. 462; BACHARACH, S. 274 ff.; vgl. Bundesrat, DLT, S. 91 EFD, Vernehmlassungsvorlage, S. 15. Die Ausführungen, die hierzu vorne in N 323 ff. gemacht wurden, gelten analog.

592 Bundesrat, DLT, S. 97; EFD, Vernehmlassungsvorlage, S. 15; m.w.H. ANDREOTTI, S. 469 ff.; MEIRICH, N 825; NOSER/INFANGER/LÜDI, N 12.43.

593 Botschaft DLT, S. 264; ANDREOTTI, S. 469; MEIRICH, N 824; NOSER/INFANGER/LÜDI, N 12.43; vgl. BGE 110 III 87 E. 2a.

594 ANDREOTTI, S. 469 f.; MEIRICH, N 825.

595 Botschaft DLT, S. 292; ANDREOTTI, S. 472 f.; NOSER/INFANGER/LÜDI, N 12.43; MEIRICH, N 829 ff.; Bei sammelverwahrten (kryptobasierten) Depotwerten findet eine Absonderung gemäss Art. 16 Ziff. 1bis i.V.m. Art. 37d BankG unter den gleichen Voraussetzungen von Amtes wegen statt (vgl. Botschaft DLT, S. 303; ANDREOTTI, S. 474).

596 Vgl. vorne N 323 ff.

Smart Contracts verbleibt die Zugriffsmöglichkeit typischerweise beim Nutzer – sei es vollständig oder in Form eines geteilten Gewahrsams.[597] Ausschliessliche Verfügungsmacht kann der Intermediärin allerdings dann zukommen, wenn die Betreiberin der Finanzanwendung durch eine dauerhafte Verfügungsbeschränkung mittels Modifikationen an den Smart Contracts auf die Rückzahlungs-, Weiterleitungs- oder Abwicklungsfunktion einwirkt und den Mitgewahrsam des Nutzers aufheben kann.[598] Dies ist namentlich der Fall, wenn der Zugriff des Nutzers durch irreversible Übertragung oder Vernichtung der Token, durch das Einfrieren des Zugangs oder durch gezielte Neukonfiguration der Vertragslogik technisch oder wirtschaftlich dauerhaft ausgeschlossen wird, wodurch der Mitgewahrsam des Nutzers entfällt und die alleinige Verfügungsmacht der Betreiberin begründet wird.[599]

344 Gerade idealtypisch dezentrale Finanzanwendungen erfüllen diese Kriterien regelmässig nicht. Ihre Smart Contracts werden autonom und unveränderlich ausgeführt, Nutzer behalten die uneingeschränkte oder geteilte Kontrolle über ihre Vermögenswerte und die Betreiberin verfügt über keinerlei Interventions- oder Freigabekompetenz.

bb) Finanzmarktinfrastrukturen

345 Bei dezentralisierten Finanzanwendungen stellt sich (jedenfalls soweit sie den Handel mit tokenisierten Effekten oder anderen finanzmarktrechtlich erfassten Instrumenten ermöglichen) die Frage, ob sie gestützt auf eine Einordnung als DLT-Handelssystem gemäss Art. 73a FinfraG oder als Zentralverwahrerin in der Funktion eines Effektenabwicklungssystems gemäss Art. 61 Abs. 3 FinfraG dem Geldwäschereigesetz unterstehen (Art. 2 Abs. 2 lit. d^{bis} und d^{quater} GwG).[600]

346 Ein DLT-Handelssystem ist eine Einrichtung zum multilateralen Handel mit DLT-Effekten, das den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmern sowie Vertragsabschlüsse nach nichtdiskretionären Regeln ermöglicht.[601] Zusätzlich muss entweder eine Zulassung von Teilnehmern gemäss Art. 73c Abs. 1 lit. e FinfraG vorliegen (lit. a), eine zentrale Verwahrung der DLT-Effekten auf Grundlage einheitlicher Regeln und Verfahren erfolgen (lit. b) oder die Abrechnung und Abwicklung entsprechender

597 Vgl. ANDREOTTI, S. 476.

598 MEIRICH, N 821 f.

599 MEIRICH, N 821; vgl. ANDREOTTI, S. 477; NOSER/INFANGER/LÜDI, N 12.43.

600 Vgl. ANDREOTTI, S. 443 ff.; HUMBEL/ECKERT, S. 20; NOSER/INFANGER/LÜDI, N 12.65; MAURENBRECHER/LEISINGER, Teil 2, S. 711; vgl. auch Bundesrat, DLT, S. 112 f.

601 Botschaft DLT, S. 310 f.; ANDREOTTI, S. 436 MEIRICH, N 634; REMUND/MEIER, S. 350; WEBER, DLT, S. 452.

Geschäfte zentral organisiert sein (lit. c).[602] Als Effektenabwicklungssystem gilt eine Einrichtung, die basierend auf einheitlichen Regeln und Verfahren Geschäfte mit Effekten und anderen Finanzinstrumenten abrechnet und abwickelt (Art. 61 Abs. 3 FinfraG).[603]

Ungeachtet weiterer individueller Voraussetzungen[604] verlangen beide 347
Formen von Finanzmarktinfrastrukturen, dass es sich um eine ‹Einrichtung› handelt.[605] Den Materialien zufolge setzt dieser Begriff eine gewisse physische Präsenz sowie eine technische Infrastruktur für den Handel voraus.[606] In der Literatur wird ergänzend gefordert, dass zumindest ein Mindestmass an zentraler Organisation oder technischer Infrastruktur gegeben sein muss.[607]

Diese Anforderungen sind bei dezentralisierten Protokollen in aller Regel 348
nicht erfüllt. Es fehlt an einer physischen Präsenz, einer zentralen technischen Infrastruktur sowie einer organisatorisch einheitlich gesteuerten Plattformstruktur. Der Protokollbetrieb erfolgt automatisiert und verteilt, ohne dass eine zentrale Stelle den Handel, die Ausführung oder die Abwicklung koordiniert. Eine Einordnung als Einrichtung im Sinne von Art. 73a Abs. 1 und Art. 61 Abs. 3 FinfraG ist daher abzulehnen.[608]

2. Örtlicher Geltungsbereich

Dezentralisierte Finanzanwendungen operieren über global verteilte Netz- 349
werke und autonom ausgeführte Smart Contracts, sodass Transaktionen ohne territoriale Bindung abgewickelt werden. Zu bestimmen ist daher, welche Anknüpfungspunkte für die Eröffnung des örtlichen Geltungsbereichs des Geldwäschereigesetzes massgeblich sind.[609]

Das Geldwäschereigesetz ist dem Verwaltungsrecht zuzuordnen, womit 350
grundsätzlich die allgemeinen Regeln zum örtlichen Geltungsbereich nach dem Territorialitätsprinzip zur Anwendung gelangen.[610] Eine besondere

602 Botschaft DLT, S. 310 f.; ANDREOTTI, S. 436; MEIRICH, N 634; REMUND/MEIER, S. 350; WEBER, DLT, S. 452.

603 Bundesrat, DLT, S. 112; ANDREOTTI, S. 457; BSK FinfraG-SCHLEIFFER/SCHÄRLI, Art. 61 N 63.

604 Zum Vorliegen der einzelnen Tatbestandsmerkmalen vgl. ANDREOTTI, S. 436 ff., 458 ff.

605 Vgl. ANDREOTTI, S. 448 f., 459; BSK FinfraG-SCHLEIFFER/SCHÄRLI, Art. 61 N 66 ff.

606 Vgl. Botschaft BEHG 1993, S. 1396 ff.

607 Vgl. KRAMER/MEIER, Fn. 160; BSK FinfraG-BAHAR/STUPP, Art. 81 N 2; SK FinfraG-HESS/KALBERMATTER/WEISS VOIGT, Art. 81 N 30; zustimmend ANDREOTTI, S. 448 f.

608 Gl.M. ANDREOTTI, S. 449; WEBER, Aktiven, N 110.

609 Vgl. ANDREOTTI, S. 346; MAURENBRECHER/LEISINGER, Teil 2, S. 710; MEIRICH, N 663; NOSER/INFANGER/LÜDI, N 12.23.

610 HÄFELIN/MÜLLER/UHLMANN, N 308 ff.; CR LBA-CASSANI, Art. 1 N 18; BSK GwG-GRETER, Art. 2 Abs. 3 N 48; LUTHIGER, N 218; STENGEL/PAYDAR, N 18.33.

Ausprägung davon bildet das sogenannte Auswirkungsprinzip, das die Anwendung schweizerischen Verwaltungsrechts auf Auslandssachverhalte erlaubt, sofern sie sich «in einem ausreichenden Mass auf dem Territorium der Schweiz auswirken».[611]

351 Eine Konkretisierung des territorialen Geltungsbereichs der Geldwäschereiverordnung findet sich in Art. 2 Abs. 1 lit. a GwV.[612] Danach ist das Gesetz anwendbar, wenn eine finanzintermediäre Tätigkeit in der Schweiz ausgeübt wird oder von der Schweiz aus erfolgt. Dies gilt insbesondere, wenn die Finanzintermediärin entweder in der Schweiz ihren Wohnsitz hat oder im Handelsregister eingetragen ist, selbst wenn die Tätigkeit ausschliesslich im Ausland erfolgt.[613] Erfasst wird ebenso eine im Handelsregister eingetragene Zweigniederlassung (sogenannte formelle Zweigniederlassung im Sinne der Art. 113 ff. HRegV).[614]

352 Die Praxis der FINMA bezieht zudem faktische Zweigniederlassungen in den örtlichen Geltungsbereich ein.[615] Gemäss Bundesgericht fallen darunter «Geschäftsstellen von Firmen, die nach ausländischem Recht konstituiert sind und ihre Hauptniederlassung im Ausland haben, hier jedoch einer bewilligungspflichtigen Tätigkeit nachgehen, ohne formell eine Zweigniederlassung begründet zu haben».[616]

353 Eine faktische Zweigniederlassung setzt gemäss FINMA-Praxis einen Personenbezug auf schweizerischem Territorium voraus, etwa wenn die Finanzintermediärin «in der Schweiz Personen beschäftigt, die für ihn [sie] dauernd in der Schweiz oder von der Schweiz aus finanzintermediäre Geschäfte ausführen oder abschliessen oder ihn [sie] rechtlich zu solchen verpflichten können», oder wenn Personen «dem ausländischen Finanzintermediär dauernd

611 BGE 133 II 331 E. 6.1; 93 II 192 E. 3; vgl. auch BGE 138 II 346 E. 3.2. Dogmatisch bleibt allerdings umstritten, ob das Auswirkungsprinzip als eine spezielle Ausprägung des Territorialitätsprinzips oder als eine Ausnahme davon zu verstehen ist (ZYSSET/NAGEL, S. 141; vgl. HÄFELIN/MÜLLER/UHLMANN, N 311).

612 Die herrschende Lehre und die FINMA wenden die sich auf die Geldwäschereiverordnung beziehende Bestimmung zum räumlichen Geltungsbereich auch auf das Geldwäschereigesetz an (STENGEL/PAYDAR, N 18.34; vgl. ZYSSET/NAGEL, S. 144; CR LBA-CASSANI, Art. 1 N 19; BSK GwG-GRETER, Art. 2 Abs. 3 N 51; SHK GwG-SCHÄREN, Art. 2 N Fn. 59; vgl. auch FINMA-RS 11/1).

613 FINMA-RS-11/2, N 28.2; CR LBA-CASSANI, Art. 1 N 20; BSK GwG-GRETER, Art. 2 Abs. 3 N 48; MEIRICH, N 699; SHK GwG-SCHÄREN, Art. 2 N 67 f.; OFK GwG-WYSS, Art. 2 N 3; ZYSSET/NAGEL, S. 145.

614 FINMA-RS-11/2, N 28.2; BSK GwG-GRETER, Art. 2 Abs. 3 N 48; ZYSSET/NAGEL, S. 145.

615 FINMA-RS-11/2, N 28.3; MEIRICH, N 700; SHK GwG-SCHÄREN, Art. 2 N 69; OFK GwG-WYSS, Art. 2 N 3; ZYSSET/NAGEL, S. 145.

616 BGE 130 II 351 E. 5.1; RIMLE, § 1 N 108, 111; vgl. auch FINMA-RS-11/2, N 28.3; MEIRICH, N 700; SHK GwG-SCHÄREN, Art. 2 N 69; OFK GwG-WYSS, Art. 2 N 3; ZYSSET/NAGEL, S. 145.

helfen, in der Schweiz oder von der Schweiz aus wesentliche Bestandteile der finanzintermediären Tätigkeit auszuführen, etwa durch die Entgegennahme oder die Aushändigung von Vermögenswerten oder durch die Erbringung der finanzintermediären Dienstleistung».[617] Nicht erfasst werden hingegen rein grenzüberschreitende Tätigkeiten im Ausland ohne jegliche physische Präsenz in der Schweiz, wie dies bei reinen Online-Angeboten oder blossem Serverstandort in der Schweiz der Fall ist.[618]

354 Die räumliche Unterstellung dezentralisierter Finanzanwendungen unter das Geldwäschereigesetz erfordert nach diesem Verständnis eine physische Präsenz von gewisser Dauerhaftigkeit. Unproblematisch ist dies bei Anwendungen, die im Namen von Personen mit (Wohn-)Sitz bzw. Handelsregistereintrag in der Schweiz betrieben werden – ein in der Praxis jedoch seltener Ausnahmefall.[619]

355 Fehlt eine solche formelle Präsenz und ist eine Betreiberschaft nicht erkennbar, ist zwischen idealtypisch dezentralen Anwendungen und solchen mit zentralisierenden Elementen zu unterscheiden. Bei idealtypisch dezentralen Anwendungen, das heisst Konstrukten ohne jegliche Kontroll- oder Einflussmöglichkeiten und mit unveränderlichen Smart Contracts, erscheint eine physische Anknüpfung an das schweizerische Territorium höchstens mit Blick auf den Ort der initialen Bereitstellung der Smart Contracts denkbar.[620] Das Kriterium der Dauerhaftigkeit liesse sich dabei jedoch kaum bejahen, weshalb eine Eröffnung des räumlichen Geltungsbereichs grundsätzlich ausscheidet. Zudem fehlt es bei solchen Strukturen regelmässig bereits am persönlichen und sachlichen Anwendungsbereich des Geldwäschereigesetzes.[621]

356 Indessen können bei Anwendungen mit zentralisierenden Elementen Anknüpfungspunkte über Personen mit physischer Präsenz (insbesondere mit Wohnsitz) in der Schweiz entstehen. Dies betrifft insbesondere Personen mit Admin Keys oder sonstigen Eingriffsmöglichkeiten, deren Tätigkeit für das Funktionieren der Smart Contracts unerlässlich ist (etwa das Zurverfügungstellen von Hardware-Zugängen), oder Personen, die ein Interface betreiben.[622]

617 FINMA-RS-11/2, N 28.4; vgl. ZYSSET/NAGEL, S. 145; BSK GwG-GRETER, Art. 2 Abs. 3 N 48; MEIRICH, N 701; SHK GwG-SCHÄREN, Art. 2 N 70.

618 FINMA-RS-11/2, N 28.6; CR LBA-CASSANI, Art. 1 N 22; BSK GwG-GRETER, Art. 2 Abs. 3 N 49; MEIRICH, N 703; SHK GwG-SCHÄREN, Art. 2 N 70; ZYSSET/NAGEL, S. 146; vgl. auch EFD, Erläuterungen, S. 23.

619 Vgl. MAURENBRECHER/LEISINGER, Teil 2, S. 710; NOSER/INFANGER/LÜDI, N 12.22 f.

620 Vgl. auch MEIRICH, N 666.

621 Vgl. vorne N 309 ff.

622 Vgl. NOSER/INFANGER/LÜDI, N 12.33.

3. Zwischenfazit

357 Die Analyse des persönlichen und sachlichen Geltungsbereichs zeigt, dass eine Einordnung dezentralisierter Anwendungen als prudenziell beaufsichtigte Finanzintermediärinnen nach Art. 2 Abs. 2 GwG als Bank (lit. a) oder als DLT-Handelssystem (lit. d^{quater}) regelmässig ausscheidet. Weder die ausschliessliche Verfügungsmacht über die eingebrachten Vermögenswerte noch die Anforderungen an eine ‹Einrichtung› sind in der Praxis typischerweise erfüllt.

358 Demgegenüber kommt im Bereich der nicht-prudenziellen Finanzintermediärinnen dem Spezialtatbestand der Erbringung einer Dienstleistung für den Zahlungsverkehr nach Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. b GwV zentrale Bedeutung zu. Die Voraussetzung der virtuellen Vermögenswerte ist bei dezentralisierten Anwendungen unproblematisch gegeben, da diese typischerweise auf Zahlungs-Token wie Bitcoin oder Ether beruhen. Auch die ‹Hilfe zur Übertragung› ist zu bejahen, da Smart Contracts die Abwicklung von Transaktionen nicht nur ermöglichen, sondern für den durchschnittlichen Nutzer erheblich erleichtern. Hinsichtlich der Tatbestandsvarianten ist festzuhalten, dass eine Verfügungsmacht nur ausnahmsweise besteht, etwa wenn administrierbare Smart Contracts Eingriffe in den Transaktionsfluss erlauben. Weit häufiger rückt die Variante der dauernden Geschäftsbeziehung in den Vordergrund. Diese kann sich aus der fortgesetzten Nutzung der von Betreiberinnen unterhaltenen Interfaces, der Verbindung eines Wallets mit der Anwendung sowie aus der Entrichtung von Gebühren ergeben und begründet ein Vertragsverhältnis.

359 Auch das Geld- und Wertübertragungsgeschäft nach Art. 2 Abs. 2 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. d GwV knüpft an die Verfügungsmacht der Betreiberin an. Insoweit gelten die gleichen Überlegungen wie bei Art. 4 Abs. 1 lit. b GwV: Eine Verfügungsmacht ist zwar denkbar, liegt jedoch bei dezentralisierten Protokollen in aller Regel nicht vor. Damit ist eine Unterstellung zwar möglich, bleibt praktisch jedoch auf Ausnahmefälle beschränkt.

360 In diesem Zusammenhang ist ergänzend festzuhalten, dass idealtypisch dezentrale Anwendungen (verstanden als Systeme ohne jegliche Kontroll- oder Einflussmöglichkeiten auf die Vermögenswerte und mit unveränderlichen Smart Contracts) vom sachlichen wie persönlichen Geltungsbereich des Geldwäschereigesetzes regelmässig nicht erfasst werden.

361 Hinsichtlich des räumlichen Geltungsbereichs gilt, dass sich dezentralisierte Anwendungen in aller Regel einer formellen Niederlassung in der Schweiz entziehen. Für ihre Unterstellung ist daher in erster Linie auf die Figur der faktischen Zweigniederlassung nach FINMA-Praxis abzustellen, die einen Personenbezug auf schweizerischem Territorium voraussetzt. Bei

idealtypisch dezentralen Protokollen könnte zwar der Ort der initialen Bereitstellung als Anknüpfungspunkt in Betracht gezogen werden; das Erfordernis einer dauerhaften physischen Präsenz liesse sich damit jedoch kaum bejahen, sodass eine Unterstellung grundsätzlich auch in räumlicher Sicht ausscheidet. Wiederum können Anwendungen mit zentralisierenden Elementen (z.B. durch Betreiberinnen mit Admin Keys, durch sonstige Eingriffsmöglichkeiten oder durch den Betrieb eines Interface von der Schweiz aus) eine faktische Präsenz bspw. am Wohnsitz der Betreiberin begründen und damit in den örtlichen Geltungsbereich des Geldwäschereigesetzes fallen.

4. Qualifizierte Handlungspflichten des Geldwäschereigesetzes

Aus dem Gesetz erwachsende Rechtspflichten begründen nicht in jedem Fall eine Garantenstellung. Erforderlich ist vielmehr eine qualifizierte Pflicht zum Tätigwerden, die sich aus der besonderen Beziehung zwischen der verpflichteten Person und dem geschützten Rechtsgut oder der Gefahrenquelle ergibt.[623] In diesem Zusammenhang ist Teil einer breiteren Meinungsdebatte, ob die Sorgfaltspflichten des Geldwäschereigesetzes als Handlungspflichten im qualifizierten Sinne zu verstehen sind.[624] 362

a) Meinungsstand

Das Bundesgericht hat in seinem Leitentscheid eine Garantenstellung von Finanzintermediärinnen, gestützt auf Art. 6 (Abklärungspflicht) und Art. 9 GwG (Meldepflicht) sowie die Geldwäschereiverordnung-FINMA, bejaht.[625] Insofern kann sich eine Sicherungspflicht ergeben, wenn die Finanzintermediärin die Art und den Zweck einer Transaktion oder einer Geschäftsbeziehung bei Ungewöhnlichkeit oder bei Anhaltspunkten auf ein Verbrechen identifiziert sowie bei der Meldestelle für Geldwäscherei keine Meldung absetzt.[626] 363

623 AK StGB-GRAF, Art. 11 N 20; HK StGB-WOHLERS, Art. 11 N 10; vgl. BGE 148 IV 39 E. 2.3.2; 141 IV 249 E. 1.1; 140 IV 11 E. 2.4.2; Urteil des BGer 6B_1341/2018 vom 16. April 2019 E. 3.2; CR CP I-CASSANI/VILLARD, Art. 11 N 21, 30; EGGER TANNER, S. 133; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 71; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 7; vgl. auch Botschaft StGB 1998, S. 2002.

624 Anstatt vieler KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 630 ff.; BOURQUIN, S. 205 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 39; CONRAD HARI, S. 365; MUSKENS/NIGGLI, S. 16 ff.; BSK StGB II-PIETH, Art. 305bis N 57 f.; THOMMEN, S. 425 ff.

625 BGE 138 IV 188 E. 6.2.2; bestätigt in Urteil des BGer 6B_729/2010 vom 8. Dezember 2011 E. 4.3, Urteil des BGer 4A_603/2020 vom 16. November 2022 E. 4.4.

626 BGE 138 IV 188 E. 6.2.2; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 631; ACKERMANN/ZEHNDER, Dogmatik, S. 46; AK StGB-GRAF, Art. 305bis N 17.

364 Die herrschende Lehre schliesst sich dieser Rechtsprechung im Grundsatz inzwischen mehrheitlich an.[627] Allerdings betonen die Befürworter mit Hinweis auf zusätzliche Zurechnungsvoraussetzungen wie die hypothetische Kausalität oder den Vorsatz, dass nicht jede Pflichtverletzung automatisch eine Garantenstellung begründet.[628]

365 Derweil verneint ein anderer Teil der Lehre eine Garantenstellung von Finanzintermediärinnen gestützt auf das Geldwäschereigesetz.[629] DONATSCH/THOMMEN/WOHLERS argumentieren, dass Finanzintermediärinnen im Gegensatz zu Polizei- und Justizbeamten keine qualifizierte Pflicht auferlegt werden kann, zum Schutz des staatlichen Einziehungsinteresses tätig zu werden.[630] In ähnlicher Weise betont EGGER TANNER, dass Finanzintermediärinnen nicht für die Wahrung der Rechtspflege zuständig seien, sondern ihre Funktion im Erbringen von Finanzdienstleistungen liege.[631] Gleichermassen lehnt BOMMER die Qualifikation der Rechtspflicht ab, da Finanzintermediärinnen nicht dieselbe Verantwortung für die Rechtspflege bzw. die Durchsetzung des staatlichen Einziehungsanspruchs tragen wie dies bei institutionell zuständigen Akteuren, etwa der Staatsanwaltschaft, der Fall sei.[632]

366 Beanstandet wird insbesondere, dass das Bundesgericht die Meldepflicht nach Art. 9 GwG zur Begründung einer Garantenpflicht heranzieht und damit der Strafnorm von Art. 37 GwG (Verletzung der Meldepflicht) ihren eigenständigen Anwendungsbereich entzieht.[633]

627 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 630 ff.; ACKERMANN/ZEHNDER, Dogmatik, S. 46 ff.; BACHER, S. 235 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 39; DONATSCH/CAVALLO, S. 524; AK StGB-GRAF, Art. 305bis N 17 f.; HK StGB-ISENRING, Art. 305bis N 7 f.; KUNZ, S. 5 f.; MACALUSO/GARBARSKI, S. 1318 ff.; BSK StGB II-PIETH, Art. 305bis N 57; PK StGB-PIETH/SCHULTZE, Art. 305bis N 20.

628 CR CP II-CASSANI/VILLARD, Art. 305bis N 37; ACKERMANN/ZEHNDER, Dogmatik, S. 47 ff.; CONRAD HARI, S. 369; KUNZ, S. 4 f.; MACALUSO/GARBARSKI, S. 1321; vgl. auch Urteil des BGer 6B_908/2009 vom 3. November 2010 E. 7.1.2; CR CP I-CASSANI/VILLARD, Art. 11 N 19; BSK StGB II-PIETH, Art. 305bis N 57.

629 DONATSCH/THOMMEN/WOHLERS, S. 509.

630 BOMMER, ZBJV 2015, S. 352; CONRAD HARI, S. 361 ff.; DONATSCH/THOMMEN/WOHLERS, S. 509; EGGER TANNER, S. 137; THOMMEN, S. 430 ff.

631 EGGER TANNER, S. 137; vgl. CONRAD HARI, S. 366.

632 BOMMER, ZBJV 2015, S. 352.

633 BOMMER, ZBJV 2015, S. 352; CONRAD HARI, S. 367; THOMMEN, S. 432. Dieser Argumentation folgt auch das Bundesgericht im Falle der sozialversicherungsrechtlichen Meldepflichtverletzung: «Die genannten Strafbestimmungen in den Spezialgesetzen hätten keinen Sinn bzw. wären überflüssig, wenn man aus der Meldepflicht eine Garantenpflicht ableiten und die blosse Verletzung der Meldepflicht als Betrug qualifizieren wollte» (BGE 140 IV 11 E. 2.4.6; vgl. auch BGE 150 IV 389 E. 4.5 f.; 131 IV 83 E. 2.1.3; BOURQUIN, S. 212; VON ROTZ, S. 173).

b) Würdigung

Kritisch zu würdigen ist die Auffassung, dass Finanzintermediärinnen grundsätzlich keine qualifizierte Handlungspflicht gestützt auf das Geldwäschereigesetz zukommen kann. 367

Der Gesetzgeber sieht den Zweck des Geldwäschereigesetzes nicht nur in der Aufspürung und Einziehung krimineller Vermögenswerte, sondern auch in der Ermittlung und strafrechtlichen Verfolgung der dahinterstehenden Personen.[634] Diese Auffassung wird auch durch das Bundesgericht gestützt: «Das Geldwäschereigesetz soll in Ergänzung zu strafrechtlichen Bestimmungen [...] verhindern, dass Gelder verbrecherischen Ursprungs in den ordentlichen Geldkreislauf gelangen, und helfen, die für die Geldwäscherei verantwortlichen Personen zu ermitteln und strafrechtlich zu belangen [...]. Es dient der Bekämpfung der Geldwäscherei (Art. 305bis StGB) im Finanzsektor und regelt in diesem Zusammenhang die dazu notwendige Sicherstellung der Sorgfalt bei Finanzgeschäften (vgl. Titel des Gesetzes und Art. 1 GwG)».[635] 368

Im Hinblick darauf, dass das schweizerische Rechtssystem keine generelle Pflicht zur Anzeige strafbarer Handlungen kennt, kommt der Meldepflicht nach Art. 9 GwG eine besondere Bedeutung zu.[636] Als ausschlaggebend für die Einführung dieser Meldepflicht erachtete der Gesetzgeber wiederum die Zwecksetzung des Geldwäschereigesetzes.[637] 369

In Anbetracht des Zweckes des Geldwäschereigesetzes ist der bundesgerichtlichen Rechtsprechung beizupflichten, wonach die geldwäschereirechtlichen Pflichten der Finanzintermediärinnen als spezifische Sicherungspflichten zum Schutz des staatlichen Einziehungsinteresses zu qualifizieren sind, die über eine blosse ‹allgemeine Bürgerpflicht› hinausgehen und den Anforderungen an eine qualifizierte Handlungspflicht genügen.[638] 370

Die Sorgfalts- und Meldepflichten des Geldwäschereigesetzes sind vom Gesetzgeber ausdrücklich als paralleles und ergänzendes Instrumentarium zu den strafrechtlichen Bestimmungen ausgestaltet worden, um eine effektive 371

634 Botschaft GwG 1996, S. 1113; vgl. BOURQUIN, S. 211; KV/KO GwG-HUTZLER, Art. 9 N 3; BSK GwG-IVELL, Art. 9 N 4; SHK GwG-LUCHSINGER, Art. 9 N 6; REINLE, N 87 f.; OFK GwG-THELESKLAF, Art. 9 N 3; vgl. auch BGE 134 III 529 E. 4.2.

635 BGE 134 III 529 E. 4.2; vgl. BSK GwG-IVELL, Art. 9 N 4.

636 EGGER TANNER, S. 133; BOURQUIN, S. 211; KV/KO GwG-HUTZLER, Art. 9 N 3; SHK GwG-LUCHSINGER, Art. 9 N 6.

637 Botschaft GwG 1996, S. 1113; BOURQUIN, S. 212; KV/KO GwG-HUTZLER, Art. 9 N 3; BSK GwG-IVELL, Art. 9 N 4; SHK GwG-LUCHSINGER, Art. 9 N 6; OFK GwG-THELESKLAF, Art. 9 N 3.

638 Vgl. BGE 138 IV 188 E. 6.2.2; gl.M. ACKERMANN, Unterlassungsrisiken, S. 156 f.; BOURQUIN, S. 212 f.; CORBOZ, Art. 305bis N 23; vgl. auch CR CP II-CASSANI/VILLARD, Art. 305bis N 39.

Bekämpfung der Geldwäscherei zu gewährleisten.[639] Dem Einwand, die separate Strafnorm von Art. 37 GwG verliere ihren eigenständigen Anwendungsbereich, ist entgegenzuhalten, dass nicht jede Verletzung der Meldepflicht zugleich die Tatbestandsvoraussetzungen einer Unterlassungsstrafbarkeit nach Art. 305bis StGB erfüllt. Art. 37 GwG behält daher einen selbständigen Anwendungsbereich.[640]

372 Ferner ist zu beachten, dass die geldwäschereirechtlichen Sorgfaltspflichten sich unmittelbar an die (Kollektiv-)Person mit der Sondereigenschaft ‹Finanzintermediärin› richten.[641] In der Regel müssen diese Pflichten nach Art. 29 StGB über die Zurechnungsnorm auf Organe bzw. Vertreter oder Mitglieder übertragen werden.[642] Sofern natürliche Personen als Finanzintermediärinnen tätig sind, unterstehen sie unmittelbar den Bestimmungen des Geldwäschereigesetzes.[643]

5. Zwischenfazit

373 Ist das Geldwäschereigesetz sachlich, persönlich und räumlich anwendbar, kann sich eine Handlungspflicht für Finanzintermediärinnen aus den darin verankerten Sorgfaltspflichten ergeben. Eine qualifizierte Pflicht zum Tätigwerden folgt dabei aus dem gesetzgeberischen Zweck. So dient das Geldwäschereigesetz nicht nur der Lokalisierung deliktisch erlangter Vermögenswerte und der Sicherung ihrer Einziehung, sondern ebenso der Identifikation der hinter den Transaktionen stehenden Personen und deren strafrechtlicher Verfolgung. Damit obliegt den Finanzintermediärinnen eine spezifische Sicherungsfunktion zugunsten des staatlichen Einziehungsinteresses, die sie deutlich über eine blosse ‹allgemeine Bürgerpflicht› hinaushebt und die Anforderungen an eine qualifizierte Handlungspflicht erfüllt.

B. Garantenstellungen im Kontext von Gefahrenquellen

374 Die vorstehenden Ausführungen betreffen ausschliesslich Konstellationen, in denen die Betreiberin als Finanzintermediärin dem Geldwäschereigesetz untersteht. Eine solche Unterstellung lässt sich jedoch nicht für sämtliche

639 Botschaft GwG 1996, S. 1102; BOURQUIN, S. 212; VON ROTZ, S. 147.

640 Vgl. SHK GwG-HILF, Art. 37 N 38; a.M. BOMMER, ZBJV 2015, S. 352.

641 DUARTE, § 31 N 8; NAGEL, Diss. N 194; BSK GwG-PEYER, Art. 2 Abs. 2 N 2; ROHR, S. 11.

642 Urteil des BGer 4A_603/2020 vom 16. November 2022 E. 6.1; Urteil des BGer 2C_192/2019 vom 11. März 2020 E. 5.4.1; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis StGB N 641 f.; ACKERMANN/ZEHNDER, Dogmatik, S. 48; BOURQUIN, S. 213 f.; CONRAD HARI, S. 368; MÖCKLI/REBER, S. 159; ablehnend gegenüber der Zurechnung von Garantenpflichten, die dem Unternehmen obliegen, VON ROTZ, S. 174.

643 ROHR, S. 11; BSK GwG-PEYER, Art. 2 Abs. 2 N 2; vgl. NAGEL, Diss., N 192 ff.

Arten dezentralisierter Finanzanwendungen ohne Weiteres bejahen.[644] Insbesondere bei idealtypisch dezentral ausgestalteten Anwendungen oder bei Geschäftsmodellen ausserhalb des sachlichen Geltungsbereichs des Geldwäschereigesetzes fehlt es an einer entsprechenden gesetzlichen Handlungspflicht. Es ist daher zu prüfen, ob für Betreiberinnen dezentralisierter Finanzanwendungen eine solche aus Ingerenz, aus der Herrschaft über eine Gefahrenquelle oder aus Geschäftsherrenhaftung ergehen kann.

1. Ingerenz und Herrschaft über eine Gefahrenquelle

Eine Garantenstellung aus Ingerenz nach Art. 11 Abs. 2 lit. d StGB knüpft an den Grundsatz an, dass, wer eine Gefahr schafft oder vergrössert, verpflichtet ist, alle durch die Umstände gebotenen Massnahmen zu ergreifen, um die Realisierung der Gefahr zu vermeiden oder gegebenenfalls die Erhöhung der bereits verursachten Gefährdung zu verhindern.[645] Vor diesem Hintergrund könnte auch das Bereitstellen dezentralisierter Finanzanwendungen als Schaffung einer Gefahr verstanden werden. Die Anwendung eröffnet eine technische Möglichkeit zur Begehung von Delikten durch Dritte (Geldwäschereihandlungen durch die Nutzer) und begründet damit eine mögliche Gefährdung des staatlichen Einziehungsinteresses.[646] 375

In der Doktrin besteht Einigkeit darüber, dass nicht jede Gefahrschaffung eine Garantenstellung zu begründen vermag.[647] So setzt ein Teil der Lehre für die Entstehung einer Garantenstellung ein pflichtwidrig gefahrschaffendes Vorverhalten voraus.[648] Die herrschende Lehre und im Ergebnis auch das Bundesgericht stellen hingegen auf die Intensität der Gefahr selbst ab.[649] 376

644 Vgl. vorne N 307 ff.

645 BGE 134 IV 255 E. 4.2.2; 134 IV 193 E. 7.2; 116 IV 202 E. 2; CR CP I-CASSANI/VILLARD, Art. 11 N 41; DONATSCH/GODENZI/TAG, S. 332; MOREILLON, S. 252; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 92; TRECHSEL et al., S. 244 ff.; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 14.

646 Davon abzugrenzen ist die Frage, ob bereits durch das Gefahrschaffen, das heisst das Deployment des Codes, eine Strafbarkeit begründet wird (vgl. hierzu vorne N 208 ff.).

647 BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 95; GETH, N 291; GRUBMILLER, S. 138; STRATENWERTH/BOMMER, AT I, § 14 N 22.

648 GRUBMILLER, S. 144 ff.; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 14; TRECHSEL et al., S. 259 ff.

649 CR CP I-CASSANI/VILLARD, Art. 11 N 41; DAN, N 250; DONATSCH/GODENZI/TAG, S. 333; GETH, N 299; AK StGB-GRAF, Art. 11 N 14; MOREILLON, S. 257 f.; STRATENWERTH/BOMMER, AT I, § 14 N 24; VON ROTZ, S. 99; vgl. BGE 134 IV 255 E. 4.2.2; CAPRARA, S. 138 f. In der Literatur werden daneben auch das Adäquanzprinzip sowie die Eigenverantwortung als einschränkende Kriterien herangezogen (vgl. BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 96, 98; DONATSCH/GODENZI/TAG, S. 333; STRATENWERTH/BOMMER, AT I, § 14 N 22, 25; CR CP I-CASSANI/VILLARD, Art. 11 N 42; FLACHSMANN, S. 51 ff.; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 14).

377 Im Kontext von dezentralisierten Finanzanwendungen zeigt sich, dass das Deployment, verstanden als blosses Bereitstellen des Codes, weder pflichtwidrig erfolgt noch für sich genommen eine Gefahr von hinreichender Intensität für das staatliche Einziehungsinteresse zu begründen vermag.[650] Die dogmatisch einschlägige Figur liegt daher nicht in der Ingerenz, da nicht der einmalige Akt der Veröffentlichung des Programmcodes, sondern die durch die Anwendung selbst geschaffene und fortdauernd bestehende Risikolage prägend ist. Entscheidend ist daher nicht das punktuelle Vorverhalten der Entwicklerin oder Betreiberin; vielmehr zählt die tatsächliche Möglichkeit, über eine auf Dauer angelegte Gefahrenquelle zu verfügen und diese zu kontrollieren. In Betracht fällt vorliegend die Garantenstellung aus der Herrschaft über eine Gefahrenquelle, welche eine bislang wenig geklärte und gesetzlich nicht ausdrücklich geregelte Konstellation bildet.[651] Ihre Konturen verschwimmen in der Literatur teilweise mit jenen der Ingerenz, sodass bei einem weiten Gefahrschaffungsverständnis auch die Herrschaft über eine Gefahrenquelle unter diesen Tatbestand subsumiert wird.[652]

378 Die Herrschaft über eine Gefahrenquelle begründet eine Form der Zustandshaftung, die dem Grundsatz folgt, dass der «Eigentümer von Sachen, Anlagen, Maschinen usw.» verpflichtet ist, «die davon ausgehenden Gefahren zu kontrollieren und zu verhindern, dass aus ihnen Schädigungen fremder Rechtsgüter entstehen».[653] Leitend ist dabei der Gedanke, dass jene Person, die für einen bestimmten Lebensbereich Verantwortung trägt, auch die von diesem Bereich ausgehenden Gefahren abwenden muss.[654]

379 Der Entstehungsgrund der Garantenstellung aus der Herrschaft über eine Gefahrenquelle orientiert sich in der Lehre an den von DONATSCH/GODENZI/TAG formulierten Voraussetzungen.[655] Danach genügt für deren

650 Eine vergleichbare Problematik stellt sich bei digitalen Infrastrukturen wie Hosting-Providern, Content-Providern, Darknet-Handelsplattformen oder selbst einer Pinnwand eines Facebook-Kontos, die von Dritten bzw. Nutzern als Plattform zur Begehung von Straftaten genutzt werden (vgl. BGE 148 IV 188 E. 3.5.1; EQUEY, N 263; 363; FRANCEY, N 254; zum deutschen Recht BÄCHER, S. 317 ff.; CEFFINATO, Internetplattformbetreiber, S. 404 ff.; SIEBER, N 42 ff.; WEBER, S. 268; S. WÜST, S. 166 ff.).

651 CR CP I-CASSANI/VILLLARD, Art. 11 N 48; OFK StGB-DONATSCH/HEIMGARTNER, Art. 11 N 14; DONATSCH/GODENZI/TAG, S. 334 ff.; GRUBMILLER, S. 142; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 102; STRATENWERTH/BOMMER, AT I, § 14 N 29 ff.; VON ROTZ, S. 100.

652 Vgl. z.B. AK StGB-GRAF, Art. 11 N 14; TRECHSEL et al., S. 259 ff.; PK StGB-TRECHSEL/FATEHMOGHADAM, Art. 11 N 14.

653 STRATENWERTH/BOMMER, AT I, § 14 N 30 m.V.a. die deutsche Lehre Tübinger Kommentar StGB-BOSCH, § 13 N 43; JESCHECK/WEIGEND, S. 626 ff.; m.w.H. zu technischen Systemen als Gefahrenquellen SIMMLER, S. 227 ff.

654 STRATENWERTH/BOMMER, AT I, § 14 N 30; HURTADO POZO/GODEL, N 838; VON ROTZ, S. 100.

655 CAPRARA, S. 139; vgl. CR CP I-CASSANI/VILLLARD, Art. 11 N 48; DONATSCH/GODENZI/TAG, S. 334 f.; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 102; VON ROTZ, S. 100.

Entstehung weder die blosse Möglichkeit, über eine Gefahrenquelle zu herrschen, noch deren tatsächliche Ausübung. Erforderlich ist vielmehr, dass sich die betroffenen Dritten sowie die Allgemeinheit auf deren Eindämmung durch die verantwortliche Person verlassen dürfen.[656] Eine solche Erwartung wird in Rechtsprechung und Lehre primär bei Bergbahnunternehmen (z.B. der Sicherung von Skipisten) sowie bei Konzert- und Sportveranstaltern bejaht.[657]

Für dezentralisierte Finanzanwendungen fehlt es demgegenüber an einer 380
solchen vergleichbaren, gefestigten gesellschaftlichen Erwartungshaltung, wonach Betreiberinnen verpflichtet wären, Geldwäschereihandlungen durch Nutzer zu verhindern oder anzuzeigen. Anders als bei Bergbahnunternehmen oder Veranstaltern werden Betreiberinnen dezentralisierter Finanzanwendungen gesellschaftlich nicht als Personen wahrgenommen, denen die Verantwortung für die Verhinderung der durch die Nutzung der Anwendung ermöglichten Straftaten zukommt. Eine entsprechende Verkehrserwartung hat sich bislang weder in der gesellschaftlichen Wahrnehmung noch im rechtlichen Umgang mit solchen Anwendungen herausgebildet. Eine Begründung der Garantenstellung durch Herrschaft über eine Gefahrenquelle lässt sich folglich im Zusammenhang mit dezentralisierten Protokollen nach diesen in der schweizerischen Lehre vertretenen Voraussetzungen nicht herleiten.

In der deutschen Lehre und Rechtsprechung sowie gemäss SEELMANN 381
bildet die verantwortliche Stellung für Gefahren, die aus Räumlichkeiten ergehen, eine besondere Fallgruppe innerhalb der Garantenstellung aus Herrschaft über eine Gefahrenquelle.[658] Eine Garantenpflicht wird dort angenommen, wo Räume aufgrund ihrer besonderen Beschaffenheit oder Lage zur Begehung von Straftaten genutzt werden.[659] Die schweizerische Doktrin (mit Ausnahme von SEELMANN) steht diesem Ansatz jedoch überwiegend kritisch gegenüber.[660]

656 DONATSCH/GODENZI/TAG, S. 334 f.; CR CP I-CASSANI/VILLLARD, Art. 11 N 48; CAPRARA, S. 139; OFK StGB-DONATSCH/HEIMGARTNER, Art. 11 N 14; HEINE/TRUNIGER, S. 91; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 102; HK StGB-WOHLERS, Art. 11 N 16.

657 DONATSCH/GODENZI/TAG, S. 334; CR CP I-CASSANI/VILLLARD, Art. 11 N 48; CAPRARA, S. 139; ENGLER, Sportanlässe, S. 496 ff.; HEINE/TRUNIGER, S. 91 ff.; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 102; HK StGB-WOHLERS, Art. 11 N 16; vgl. BGE 141 IV 249 E. 1.4.1 f.; 125 IV 9 E. 2; 122 IV 193 E. 2a; 115 IV 189 E. 3; 111 IV 15 E. 1 f.; 109 IV 99 E. 1.

658 Vgl. z.B. aBSK StGB I-SEELMANN, Art. 11 N 53; vgl. auch STRATENWERTH/BOMMER, AT I, § 14 N 30.

659 Anstatt vieler Urteil des BGH 3 StR 34/82 vom 24. Februar 1982, NJW 22/1982, S. 1235 ff.; Tübinger Kommentar StGB-BOSCH, § 13 N 54; MüKo StGB-FREUND/ROSTALSKI, § 13 N 155 f.

660 Vgl. BGE 79 IV 145; aBSK StGB I-SEELMANN, Art. 11 N 53; MELE/PETERS, S. 393 mit Verweis auf die eigene Selbstverantwortung Dritter; MOREILLON, S. 276 f.; STRATENWERTH/BOMMER, AT I, § 14 N 30; vgl. auch BGE 81 IV 197 E. 2; HURTADO POZO/GODEL, N 836.

382 In diesem Zusammenhang lässt sich eine Parallele zu dezentralisierten Protokollen ziehen, da auch sie Dritten einen digitalen Handlungsraum eröffnen, der über die neutrale Bereitstellung hinaus für deliktische Zwecke instrumentalisiert werden kann.[661] In Anlehnung an die deutsche Lehre wäre eine Garantenstellung grundsätzlich denkbar und jedenfalls dort naheliegend, wo eine Anwendung gerade durch ihre besondere Beschaffenheit oder spezifischen Funktionen Geldwäschereihandlungen von Nutzern erleichtert. Mit Blick auf den hier interessierenden Geldwäschereitatbestand und das dadurch geschützte staatliche Einziehungsinteresse betrifft dies insbesondere Systeme, die Anonymisierungsmechanismen implementieren. So bündeln etwa Mixer Einzahlungen verschiedener Nutzer, verteilen diese automatisiert neu und lösen die Rückverfolgbarkeit von Transaktionen auf, was sie in besonderer Weise für missbräuchliche Verwendungen prädestiniert. Angesichts des – aus Gründen der Rechtsstaatlichkeit von Lehre und Rechtsprechung zu Recht eng bemessenen – Anwendungsbereichs dieser gesetzlich nicht ausdrücklich normierten Garantenstellung aus Herrschaft über eine Gefahrenquelle ist einer Ausdehnung ihres Anwendungsbereichs mit besonderer Zurückhaltung zu begegnen und ginge im vorliegenden Kontext zu weit.

2. Geschäftsherrenhaftung

383 Eine weitere mögliche Grundlage für die Annahme einer Garantenstellung bildet die Geschäftsherrenhaftung. Sie beruht auf der Überlegung, dass dem Inhaber oder Leiter eines Unternehmens Straftaten zugerechnet werden können, die im Rahmen des Betriebs verübt werden.[662] Damit handelt es sich um eine besondere Ausprägung der Herrschaft über eine Gefahrenquelle, die sich jedoch spezifisch im Unternehmenskontext entfaltet.[663] Als Gefahrenquellen kommen einerseits Personen in Betracht, sodass dem Geschäftsherrn kraft seiner Autoritätsstellung die Pflicht zukommt, deliktisches Verhalten von Untergebenen zu verhindern; andererseits können auch sachliche Gefahrenquellen in seinen Verantwortungsbereich fallen.[664]

661 Bei Handelsplattformen im Darknet vgl. BÄCHER, S. 320; CEFFINATO, Internetplattformbetreiber, S. 405 f.; SIEBER, N 56; WEBER, S. 275, die das Zurverfügungstellen von Speicherplatz mit dem Vermieten einzelner Wohnungen in einem Hochhaus vergleicht, wo ab einer gewissen Anzahl von Mietern davon auszugehen ist, dass einzelne Bewohner Straftaten begehen; so auch ZIESCHANG, S. 66.

662 DONATSCH/GODENZI/TAG, S. 334; CR CP I-CASSANI/VILLLARD, Art. 11 N 48; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 102; HK StGB-WOHLERS, Art. 11 N 16; vgl. BGE 96 IV 155 E. 4.

663 OFK StGB-DONATSCH/HEIMGARTNER, Art. 11 N 15; DONATSCH/GODENZI/TAG, S. 336; STRATENWERTH/BOMMER, AT I, § 14 N 31; TRECHSEL et al., S. 262.

664 SIMMLER, S. 233 f. m.V.a. EIDAM, S. 202.

Wie bereits ausgeführt, lassen sich dezentralisierte Finanzanwendungen als sachliche Gefahrenquellen begreifen, die Dritten die Begehung von Geldwäschereihandlungen ermöglichen.[665] Eine beherrschende Stellung des Betreibers könnte insofern angenommen werden, wenn er über wirksame Kontrollmechanismen verfügt und dadurch den Betrieb der Anwendung beeinflussen kann.[666] Die Qualifikation als Geschäftsherr setzt jedoch voraus, dass das Betreiben der Anwendung einem Geschäfts- oder Unternehmensbetrieb im Sinne der abschliessend enumerierten Unternehmensformen des schweizerischen Gesellschaftsrechts entspricht.[667] Jenseits einer gewählten gesetzlichen Rechtsform kommen vorliegend aufgrund ihrer Auffangfunktion das Einzelunternehmen[668] bei einer einzelnen Person oder eine einfache Gesellschaft bzw. Kollektivgesellschaft bei einer Personenmehrheit in Betracht.[669] 384

Fraglich ist allerdings, ob überhaupt der Weg über die Geschäftsherrenhaftung beschritten werden kann. Diese greift typischerweise in Konstellationen, in denen einer für einen Gefahrenbereich verantwortlichen Person Straftaten aufgrund ihrer autoritäts- und weisungsbegründeten Stellung zugerechnet werden, gerade weil ihr nicht unmittelbar eine Unterlassung vorgeworfen werden kann.[670] Eine solche Struktur ist bei dezentralisierten Finanzanwendungen regelmässig nicht gegeben. Der dezentralisierte Charakter der 385

665 Vgl. vorne N 378.

666 Vgl. vorne N 123 ff.

667 Für die Geschäftsherrenhaftung bietet sich als systematischer Anhaltspunkt der Unternehmensbegriff nach Art. 102 Abs. 4 StGB an, der ausdrücklich juristische Personen, Gesellschaften und Einzelunternehmen umfasst (vgl. auch FORSTER, S. 92, 97; GRAF, S. 362; HEINIGER, N 466; JEANNERET, S. 919; BSK StGB I-NIGGLI/GFELLER, Art. 102 N 370).

668 Bei Einzelunternehmen handelt es sich um ein durch eine natürliche Person in eigenem Namen und eigener Verantwortung betriebenes Unternehmen, welches kein eigenes Rechtsubjekt darstellt (vgl. BGE 74 II 224 E. 2; MEIER-HAYOZ/FORSTMOSTER/SETHE, § 26 N 3; BK OR-SEIFFERT, Art. 931 N 6).

669 Eine einfache Gesellschaft nach Art. 530 ff. OR ist die vertragliche Verbindung von zwei oder mehreren Personen zur Erreichung eines gemeinsamen Zweckes mit gemeinsamen Kräften oder Mitteln. Sie ist nach Art. 530 Abs. 2 OR subsidiär und kommt nur zur Anwendung, wenn keine andere Rechtsform einschlägig ist. Charakteristisch ist ihre weitgehend dispositive Ordnung mit nur wenigen Schutzvorschriften zugunsten der Beteiligten (BK OR-FELLMANN/MÜLLER, N 13; ZK OR-HANDSCHIN/VONZUN, Art. 530 N 3 ff.; BSK OR II-TRUNIGER/HANDSCHIN, Art. 530 N 13 f.). Der Einbezug nicht rechtsfähiger Personenverbindungen in den Unternehmensbegriff von Art. 102 Abs. 4 StGB ist in Rechtsprechung und Lehre anerkannt (vgl. CASSANI/VILLARD, N 3.56 ff.; BSK StGB I-NIGGLI/GFELLER, Art. 102 N 409 ff.; ROTH, Responsabilité, S. 368; RYSER, N 152; krit. BERTOSSA, S. 82 ff.; ENGLER, Diss., S. 26; FORSTER, S. 118; CR CP I-MACALUSO, Art. 102 N 15; BSK StGB I-NIGGLI/GFELLER, Art. 102 N 413; vgl. auch MEIER-HAYOZ/FORSTMOSTER/SETHE, § 12 N 18 ff.).

670 GRAF, S. 520.

Aufgabenverteilung sowie die Abwesenheit einer hierarchischen Organisations- und Befehlskette sprechen gegen die Annahme einer geschäftsherrentypischen Autoritätsstellung gegenüber handelnden Dritten. Bei Betreiberinnen dezentralisierter Finanzanwendungen besteht hingegen – soweit überhaupt – eine Verantwortlichkeit nicht infolge einer übergeordneten Leitungs- oder Weisungsfunktion, sondern aufgrund eigener faktischer Kontrollmöglichkeiten über Smart Contracts resp. die Anwendung selbst. Die Geschäftsherrenhaftung vermag daher keine eigenständige Grundlage für eine Garantenstellung zu begründen. Der Rückgriff auf diese Figur erweist sich im vorliegenden Kontext als nicht sachgerecht.[671]

3. Qualifizierte Handlungspflicht

386 Weitere Überlegungen zur Garantenstellung sind im vorliegenden Zusammenhang nicht vertieft anzustellen. Entscheidend ist, dass nach schweizerischem Verständnis die Begründung einer Garantenstellung stets eine qualifizierte Handlungspflicht voraussetzt, die über die blosse Bereitstellung einer potenziell missbrauchsanfälligen Infrastruktur hinausgeht.[672] Eine solche Pflicht setzt eine besondere Beziehung zwischen der verpflichteten Person und dem geschützten Rechtsgut voraus und bildet die Kehrseite des Grundsatzes, dass das Strafrecht keine allgemeine Pflicht zur Abwehr fremder Rechtsgutsverletzungen kennt.[673] Welche Anforderungen an das Kriterium der qualifizierten Handlungspflicht zu stellen sind, ist weitgehend ungeklärt, weshalb Zurückhaltung bei der Annahme einer Garantenstellung geboten ist.[674] Moralische oder sittliche Erwartungen genügen dafür nicht.[675]

387 Für Betreiberinnen von dezentralisierten Finanzanwendungen, die eine Gefahrenquelle für die Deliktsbegehung der Geldwäscherei durch Nutzer darstellen, stellt sich damit die Frage, ob sie eine qualifizierte Pflicht trifft, welche sie zur Verhinderung der Gefährdung der Rechtspflege bzw. des staatlichen Einziehungsinteresses verpflichtet. Dies ist zu verneinen: Als Privat-

671 Zustimmend KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 220.

672 Vgl. vorne N 367 ff.; BGE 148 IV 39 E. 2.3.2; 141 IV 249 E. 1.1; 140 IV 11 E. 2.4.2; AK StGB-GRAF, Art. 11 N 10; CR CP I-CASSANI/VILLARD, Art. 11 N 21, 30; EGGER TANNER, S. 132; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 71; vgl. auch Botschaft StGB 1998, S. 2002.

673 BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 67; CONRAD HARI, S. 365; AK StGB-GRAF, Art. 11 N 10; VON ROTZ, S. 74; HK StGB-WOHLERS, Art. 11 N 9; vgl. BGE 148 IV 39 E. 2.3.2; 141 IV 459 E. 4.2; 123 IV 70 E. 2; DONATSCH/GODENZI/TAG, S. 325.

674 BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 71.

675 Botschaft StGB 1998, S. 2002; DAN, N 195; DONATSCH/GODENZI/TAG, S. 325; GETH, N 295; AK StGB-GRAF, Art. 11 N 10 ff.; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 47; STRATENWERTH/BOMMER, AT I, § 14 N 27; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 7; vgl. BGE 123 IV 70 E. 2; 120 IV 98 E. 2c; 108 IV 3 E. 1b; Urteil des BGer 6B_274/2019 vom 28. Februar 2020 E. 2.4.

personen fehlt ihnen die notwendige besondere Beziehung zu diesem Rechtsgut.[676] Eine qualifizierte Handlungspflicht zur Verhinderung oder Anzeige von Geldwäschereihandlungen Dritter wird in der Lehre für Privatpersonen – im Gegensatz zu Polizei-, Justiz- und Zollbeamten sowie von Finanzintermediärinnen im Falle der Verletzung geldwäschereirechtlicher Sorgfaltspflichten – ausdrücklich verneint.[677] Dem ist zuzustimmen. Beamte sind aufgrund ihrer amtlichen Funktion verpflichtet, staatliche Interessen zu schützen und Gefährdungen durch Dritte abzuwehren. Bei Finanzintermediären beruht die Handlungspflicht auf ihrer gesetzlich begründeten Stellung im System der Geldwäschereibekämpfung.[678]

C. Zwischenfazit

388 Eine Garantenstellung der Betreiberinnen dezentralisierter Anwendungen ist im schweizerischen Recht nur aus Gesetz zu begründen – und zwar dort, wo sie als Finanzintermediärinnen den geldwäschereirechtlichen Sorgfaltspflichten unterstehen. Diese Pflichten verleihen ihnen eine qualifizierte Sicherungspflicht zugunsten des staatlichen Einziehungsinteresses und heben sie über eine allgemeine Bürgerpflicht hinaus.

389 Indes entziehen sich Betreiberinnen idealtypisch dezentraler Anwendungen ohne Verfügungsmacht oder sonstige Kontrollmöglichkeiten über Vermögenswerte sowie mit unveränderlichen Smart Contracts dem Regime des Geldwäschereigesetzes. Für solche Konstellationen sowie generell bei dezentralisierten Protokollen, die nicht dem Geldwäschereigesetz unterstellt sind, stellt sich zwar die Frage nach alternativen Entstehungsgründen einer Garantenstellung; weder Ingerenz noch die Herrschaft über eine Gefahrenquelle oder die Geschäftsherrenhaftung vermögen jedoch im vorliegenden Zusammenhang eine qualifizierte Handlungspflicht zu begründen. Privaten fehlt die institutionelle Bestimmung zum Schutz der Rechtspflege, weshalb die blosse Bereitstellung oder Veröffentlichung einer missbrauchsanfälligen Infrastruktur nicht ausreicht, um eine Garantenstellung anzunehmen.

676 Zustimmend KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 614.

677 PK StGB-PIETH/SCHULTZE, Art. 305bis N 20; ACKERMANN/ZEHNDER, Dogmatik, S. 46; CONRAD HARI, S. 365; vgl. ARZT, S. 192; EGGER TANNER, S. 137; GRABER, S. 137; DONATSCH/THOMMEN/WOHLERS, S. 509.

678 Vgl. vorne N 367 ff.; BGE 138 IV 188 E. 6.2.2; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 630 ff.; ACKERMANN/ZEHNDER, Dogmatik, S. 46 ff.; BACHER, S. 235 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 39; DONATSCH/CAVALLO, S. 524; AK StGB-GRAF, Art. 305bis N 17 f.; HK StGB-ISENRING, Art. 305bis N 7 f.; KUNZ, S. 5 f.; MACALUSO/GARBARSKI, S. 1318 ff.; BSK StGB II-PIETH, Art. 305bis N 57; PK StGB-PIETH/SCHULTZE, Art. 305bis N 20.

390 Insgesamt ist festzuhalten, dass eine Garantenstellung für Betreiberinnen dezentralisierter Finanzanwendungen mangels anderer Anknüpfungsgrundlagen lediglich aus dem Geldwäschereigesetz hergeleitet werden kann.

III. Weitere objektive Tatbestandsmerkmale der unechten Unterlassung

A. Hypothetische Kausalität

391 Unechte Unterlassungsdelikte setzen grundsätzlich einen Kausalzusammenhang zwischen der unterlassenen Handlung und dem eingetretenen Erfolg voraus. Die Ursächlichkeitsprüfung bei Unterlassungsdelikten erfolgt auf der Grundlage einer hypothetischen Kausalität.[679] Massgeblich ist, ob der Erfolg bei pflichtgemässem Handeln des Garanten, das heisst bei Vornahme der durch seine Garantenstellung gebotenen Handlung, mit an Sicherheit grenzender Wahrscheinlichkeit ausgeblieben wäre.[680]

392 Die herrschende Lehre und Rechtsprechung setzt (im Hinblick auf die Rechtsstaatlichkeit richtigerweise)[681] voraus, dass der Erfolg mit einem hohen Grad an Wahrscheinlichkeit oder mit an Sicherheit grenzender Wahrscheinlichkeit hätte abgewendet werden können (Wahrscheinlichkeitstheorie).[682] Ein Teil der Lehre vertritt hingegen die sogenannte Risikoerhöhungstheorie, wonach die hypothetische Kausalität bereits dann gegeben ist, wenn das gebotene Verhalten das Risiko des Erfolgseintritts vermindert hätte.[683]

393 Wie in den vorangehenden Ausführungen dargetan, handelt es sich bei der Geldwäscherei durch Unterlassen um ein Erfolgsdelikt.[684] Der Erfolg besteht hierbei in der Begehung der Geldwäscherei durch eine andere Person. Erforderlich ist daher der Nachweis eines hypothetischen Kausalzusammen-

679 DAN, N 334; DONATSCH/GODENZI/TAG, S. 339; FLACHSMANN, S. 82; HURTADO POZO/GODEL, N 841; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 109; TRECHSEL et al., S. 265; vgl. SUMMERMATTER, S. 26 f.

680 BGE 134 IV 255 E. 4.4.1; 117 IV 130 E. 2a; 109 IV 137 E. 2a; CR CP I-CASSANI/VILLARD, Art. 11 N 57; DAN, N 335; DONATSCH/GODENZI/TAG, S. 339 f.; GRAVEN/STRÄULI, S. 91 f.; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 111; RIKLIN, § 19 N 30; STRATENWERTH/BOMMER, AT I, § 14 N 38; TRECHSEL et al., S. 265.

681 M.w.H. TRECHSEL et al., S. 267; CR CP I-CASSANI/VILLARD, Art. 11 N 59; DAN, N 344; GETH, N 290; AK StGB-GRAF, Art. 11 N 20.

682 Vgl. BGE 130 IV 7 E. 3.2; 121 IV 286 E. 3; 116 IV 306 E. 2b; 109 IV 137 E. 2a; 108 IV 3 E. 2; 106 IV 398 E. 3b; 105 IV 18 E. 3a; CR CP I-CASSANI/VILLARD, Art. 11 N 58; DAN, N 344; DONATSCH/GODENZI/TAG, S. 339; GETH, N 289; GRAVEN/STRÄULI, S. 91; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 110; SCHULTZ, S. 128; TRECHSEL et al., S. 267.

683 Vgl. STRATENWERTH/BOMMER, AT I, § 14 N 42; vgl. auch BGE 135 IV 56 E. 5.

684 Vgl. vorne N 297 f.; vgl. auch PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 41.

hangs zwischen der Verletzung der Handlungspflicht und der vom Dritten begangenen Geldwäschereihandlung.[685] Auch das Bundesgericht hat in seinem Leitentscheid die hypothetische Kausalität im Zusammenhang mit der Geldwäscherei durch Unterlassung geprüft. Es hielt fest, dass eine Verdachtsmeldung an die MROS mit hoher Wahrscheinlichkeit erfolgt wäre, wenn die für die Meldung zuständige Generaldirektion über den geldwäschereirelevanten Sachverhalt informiert worden wäre.[686]

Vorliegend ist demnach gemäss der Wahrscheinlichkeitstheorie konkret zu prüfen, ob die gebotene Handlung der Betreiberin nicht hinzugedacht werden kann, ohne dass auch die tatbestandsmässige Verwirklichung der Geldwäscherei durch den Nutzer bzw. die abstrakte Gefährdung der Einziehung mit hoher Wahrscheinlichkeit entfiele.[687] 394

Wie bereits festgehalten, kann eine allfällige Garantenpflicht der Betreiberin ausschliesslich aus dem Geldwäschereigesetz abgeleitet werden.[688] Im konkreten Fall wäre folglich zu prüfen, ob und in welchem Umfang Sorgfaltspflichten im Rahmen der Finanzanwendung implementiert wurden und ob bei deren Einhaltung eine mögliche Gefährdung des Einziehungsinteresses mit einem hohen Grad an Wahrscheinlichkeit unterblieben wäre. 395

Im vorliegenden Kontext fallen als mögliche Grundlagen insbesondere Art. 6 (besondere Sorgfaltspflichten), Art. 9 (Meldepflicht) sowie Art. 10 GwG (Vermögenssperre) in Betracht.[689] 396

Die in Art. 6 GwG vorgesehenen Abklärungspflichten[690] könnten im Rahmen dezentralisierter Finanzanwendungen insbesondere durch präventiv implementierte technische Kontrollmechanismen erfüllt werden, welche auffällige Transaktionen oder Adressen automatisiert identifizieren. Da solche Anwendungen vollautomatisiert ablaufen und die Interaktion der Nutzer ohne vermittelnde Instanz erfolgt, müssen die geldwäschereirechtlichen Pflichten 397

685 BACHARACH, S. 225 f.; BOURQUIN, S. 218 f.; CASSANI/VILLARD, N 6.87; CR CP II-CASSANI/VILLARD, Art. 305bis N 37; CONRAD HARI, S. 369; VON ROTZ, S. 114; a.M. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 611.

686 Urteil des BGer 6B_908/2009 vom 3. November 2010 E. 7 (nicht publiziert in BGE 136 IV 188); vgl. BOURQUIN, S. 218 f.; VON ROTZ, S. 199 f.

687 Vgl. CR CP I-CASSANI/VILLARD, Art. 11 N 58; DAN, N 344; DONATSCH/GODENZI/TAG, S. 339; GETH, N 289; AK StGB-GRAF, Art. 11 N 22; GRAVEN/STRÄULI, S. 91; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 110; SCHULTZ, S. 128; TRECHSEL et al., S. 267.

688 Vgl. vorne N 367 ff.

689 Vgl. vorne N 363 ff.

690 Bei Kryptowerten liegt regelmässig ein erhöhtes Risiko im Sinne von Art. 6 Abs. 2 lit. c GwG i.V.m. Art. 13 f. GwV-FINMA vor, weshalb weitergehende Abklärungspflichten gemäss Art. 15 GwV-FINMA hinzutreten können (STENGEL/PAYDAR, N 18.101; BACHARACH, S. 370 ff.; vgl. BSK GwG-MÜLLER/LÖTSCHER, Art. 6 N 15 ff., 60 ff.).

bereits ex ante, das heisst vor oder während der Nutzung der Anwendung, in die Systemarchitektur eingebettet sein. Dazu zählen Blockchain-Analysetools zur Erkennung von Vermögenswerten mit deliktischem Ursprung (Tainted Coins), Systeme zum Abgleich von Wallet-Adressen mit Sanktions- oder Watchlists sowie Whitelist-Architekturen, die Transaktionen auf zuvor verifizierte Adressen beschränken.[691]

398 Auch die Meldepflicht nach Art. 9 GwG wäre in dezentralisierten Systemen nur dann erfüllbar, wenn sie programmatisch ausgelöst wird. Aufbauend auf den Abklärungsmechanismen muss die Systemarchitektur eine Triggerlogik enthalten, welche bei Vorliegen eines geldwäschereirelevanten Verdachts automatisiert einen Meldeprozess generiert und diesen den Administratoren zur Übermittlung bereitstellt. Ohne eine solche automatisierte Vorverlagerung des Meldeverhaltens würde der Zweck der Meldepflicht – die Weiterleitung sicherungsrelevanter Informationen als Grundlage des Einziehungsinteresses – leerlaufen, weil sich manuelle Interventionen im Echtzeitablauf des Protokolls nicht realisieren lassen.

399 Schliesslich lässt sich auch die Pflicht zur Vermögenssperre nach Art. 10 GwG technisch nur vortransaktional erfüllen. Eine Ex-post-Sperre scheidet aus, da die Transaktion im Zeitpunkt des Abschlusses automatisch und unwiderruflich ausgeführt ist. Eine wirksame Vermögenssperre müsste daher in Form einer programmatischen Freeze- oder Pause-Mechanik implementiert sein, welche den Zugriff oder Transfer bestimmter Token-Bestände bereits bei Eintritt eines Verdachtszustands temporär blockiert. Damit dient die Sperrfunktion nicht bloss der Sanktion, sondern als präventiver Schutzmechanismus, der die Gefährdung des Einziehungsinteresses verhindert, bevor irreparable Vermögensverschiebungen eintreten.[692]

400 Diese technischen Instrumente ermöglichen es einer Betreiberin grundsätzlich, die geldwäschereirechtlichen Sorgfaltspflichten nicht manuell, sondern durch ex ante programmierte Verhaltenslogiken in die Funktionsweise der Anwendung zu integrieren. Entscheidend ist deshalb, ob anzunehmen ist, dass die Einhaltung dieser Pflichten – insbesondere die automatisierte Erkennung, Meldeauslösung und Sperrmechanik – mit hoher Wahrscheinlichkeit geeignet gewesen wäre, die vom Nutzer beabsichtigte Geldwäschereihandlung bzw. die Gefährdung des Einziehungsinteresses zu verhindern. Für die Bejahung der hypothetischen Kausalität spricht insbesondere der Umstand, dass die Betreiberin durch die Einbettung der Abklärungspflichten nach Art. 6 GwG

691 BACHARACH, S. 63 f., 375 f.; vgl. KGGT, NRA 2024, S. 55; ANDREOTTI, S. 300; CARLISLE, S. 83; MAUCHLE, Registrierungsvereinbarung, S. 692 f.; NOSER/INFANGER/LÜDI, N 12.33.

692 Vgl. MAUCHLE, Registrierungsvereinbarung, S. 692 f.; MEIRICH, N 185.

Verdachtsmomente bereits vor Ausführung der Transaktion hätte erkennen können und gestützt darauf die Möglichkeit besass, eine Meldung im Sinne von Art. 9 GwG auszulösen oder die Vermögenssperre nach Art. 10 GwG zu aktivieren. In diesem Szenario wäre die vom Nutzer bewirkte Gefährdung des Einziehungsinteresses mit hoher Wahrscheinlichkeit ausgeblieben.[693]

B. Tatmacht

Eine weitere Voraussetzung für die Strafbarkeit durch Unterlassen ist schliesslich, dass der Täter über die tatsächliche Möglichkeit verfügte, die gebotene Handlung vorzunehmen und den Erfolg abzuwenden (Tatmacht).[694] Handlungsmöglichkeit bedeutet, dass der Garant in der konkreten Situation sowohl physisch als auch psychisch in der Lage gewesen sein muss, die gebotene Handlung auszuführen.[695] Massgeblich sind hierbei nur Handlungen, die ihm nach dem Massstab der Zumutbarkeit realistischerweise abverlangt werden konnten.[696] 401

Im Rahmen der Tatmacht ist folglich zu beurteilen, ob die Betreiberin in der konkreten Situation überhaupt in der Lage war, die gebotenen Handlungen zur Erfolgsabwendung vorzunehmen. Dies hängt wesentlich vom Grad der administrativen Kontrolle über das Protokoll oder die Benutzeroberfläche ab. Verfügt sie (z.B. durch Admin Keys, Upgrade-Mechanismen oder eine zentrale Frontend-Kontrolle) über effektive Eingriffsmöglichkeiten, ist die Handlungsmöglichkeit grundsätzlich zu bejahen. Bei idealtypisch dezentralen Anwendungen ohne administrative Steuerungsbefugnisse, das heisst ohne Modifikationsmöglichkeit der Smart Contracts oder Einfluss über ein kontrolliertes Interface, fehlt es hingegen an der erforderlichen Tatmacht. Die Frage der Tatmacht ist in solchen Fällen allerdings von untergeordneter Bedeutung, weil die Unterlassungsstrafbarkeit bereits daran scheitert, dass mangels persönlicher resp. sachlicher Unterstellung unter das Geldwäschereigesetz 402

693 Selbst bei Zugrundelegung der Risikoerhöhungstheorie ergäbe sich kein anderes Ergebnis, da die Implementierung automatisierter Abklärungs-, Melde- und Sperrmechanismen das Risiko der Vereitelung des staatlichen Einziehungsinteresses reduziert hätte.

694 BGE 116 IV 386 E. 2e; 109 IV 137 E. 2a; Urteil des BGer 6B_1036/2019 vom 16. Januar 2020 E. 2.2; CR CP I-CASSANI/VILLARD, Art. 11 N 56; DAN, N 296 ff.; DONATSCH/GODENZI/TAG, S. 338; FLACHSMANN, S. 74 f.; GRUBMILLER, S. 180 ff.; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 120; MOREILLON, S. 81; STRATENWERTH/BOMMER, AT I, § 14 N 41; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 17.

695 CR CP I-CASSANI/VILLARD, Art. 11 N 56; DAN, N 298 ff.; FLACHSMANN, S. 75; GETH, N 286; GRUBMILLER, S. 180 ff.; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 120; STRATENWERTH/BOMMER, AT I, § 14 N 41; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 17.

696 DAN, N 304 f.; AK StGB-GRAF, Art. 11 N 18; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 121; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 17; m.w.H. zum Kriterium der Zumutbarkeit GRUBMILLER, S. 183 ff.

keine Garantenstellung besteht, welche eine qualifizierte Handlungspflicht zu begründen vermöchte.[697]

C. Gleichwertigkeit von Tun und Unterlassen

403 Gemäss Art. 11 Abs. 3 StGB ist der Täter nur dann wegen Unterlassens strafbar, «wenn ihm nach den Umständen der Tat derselbe Vorwurf gemacht werden kann, wie wenn er die Tat durch ein aktives Tun begangen hätte».[698] Mit dem Gleichwertigkeitskriterium schuf der Gesetzgeber eine weitere Einschränkung der Strafbarkeit, wobei dieses Erfordernis aufgrund seiner Vagheit in der Lehre dogmatische Fragen aufgeworfen hat.[699] Einigkeit besteht darin, dass es sich dabei um ein auf Unrechtsgesichtspunkte bezogenes Kriterium handelt und seine eigenständige Bedeutung darin liegt, dass es nicht darum geht, zu ‹messen›, ob der Vorwurf ‹genauso schwer› wiegt, sondern darum, ob dieselben strafrechtlich relevanten Elemente erfüllt sind – mit Ausnahme der eigentlichen Handlung.[700]

404 Der Gesichtspunkt der Gleichwertigkeit der Geldwäscherei durch Unterlassen mit einem Tun ist folglich regelmässig erfüllt, wenn die Betreiberin sämtliche Unterlassungstatbestandsmerkmale erfüllt und ihr Unterlassen damit denselben strafrechtlichen Vorwurf begründet wie ein Tun.[701]

IV. Subjektiver Tatbestand

A. (Eventual-)Vorsatz

405 Bei der Geldwäscherei handelt es sich um ein Vorsatzdelikt.[702] Gemäss Art. 12 Abs. 2 StGB handelt vorsätzlich, wer die Tat wissentlich und willentlich begeht.

697 Vgl. vorne N 309 ff.

698 Vgl. BGE 141 IV 249 E. 1.1; 113 IV 72 E. 5a; Urteil des BGer 6B_884/2020 vom 19. November 2020 E. 2.2; CR CP I-CASSANI/VILLARD, Art. 11 N 13; DAN, N 397; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 115.

699 CR CP I-CASSANI/VILLARD, Art. 11 N 13; DAN, N 402 ff.; MOREILLON, S. 324 f.; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 21; TRECHSEL et al., S. 268; VON ROTZ, S. 106.

700 DAN, N 412 ff.; vgl. DONATSCH/GODENZI/TAG, S. 340; GETH, N 319; AK StGB-GRAF, Art. 11 N 24; TRECHSEL et al., S. 268; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 21; VON ROTZ, S. 106; a.M. GRUBMILLER, S. 202 f.; vgl. auch BGE 141 IV 249 E. 1.1; 96 IV 155 E. II.4a; 86 IV 218 E. 2.

701 Im Übrigen wird auf die bereits erfolgten Ausführungen und Subsumtionen zu den Unterlassungstatbestandsmerkmalen verwiesen, vgl. vorne N 304 ff.

702 Botschaft StGB 1989, S. 1084; Urteil des BGer 6B_224/2017 vom 17. November 2017 E. 4.2.1; Urteil des BGer 6B_908/2009 vom 3. November 2010 E. 8.1; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 672; LENGAUER/RUCKSTUHL, N 521; STRASSER, S. 150; BSK StGB II-PIETH, Art. 305bis N 59.

Für die Strafbarkeit nach Art. 305bis StGB genügt bereits Eventualvorsatz.[703] Beim unechten Unterlassungsdelikt umfasst der Vorsatz einerseits neben dem Wissen um die Garantenstellung und die daraus fliessende Handlungspflicht, um die Gefährdung des geschützten Rechtsguts sowie um die Möglichkeit, den Eintritt des tatbestandsmässigen Erfolgs durch pflichtgemässes Verhalten abzuwenden, auch die objektiven Tatbestandsmerkmale des relevanten Delikts. Andererseits erfordert der Vorsatz den Willen, trotz dieser Erkenntnis untätig zu bleiben und den Erfolg zumindest in Kauf zu nehmen.[704]

406 Nach allgemeinem Grundsatz muss der Vorsatz bereits vor Beginn der Tathandlung vorliegen und während des gesamten Handlungsverlaufs fortbestehen.[705] Fehlt er im Zeitpunkt der Tatbegehung und tritt erst nachträglich hinzu, bleibt das Verhalten gemäss dem Grundsatz *dolus subsequens non nocet* straflos.[706] Ein erst während der Tatausführung entstehender Vorsatz *(dolus superveniens)* setzt voraus, dass es sich beim betreffenden Delikt um ein Dauerdelikt handelt. Bei der Geldwäscherei nach Art. 305bis StGB handelt es sich indes um ein Zustandsdelikt.[707] Wird daher ein Vermögenswert zunächst gutgläubig entgegengenommen und entsteht der Vorsatz erst nachträglich, bleibt das passive Verhalten straflos. Vorbehalten bleiben freilich Konstellationen, in denen den Täter (trotz gutgläubiger Entgegennahme) nachträglich eine Garantenpflicht trifft.[708]

1. Wissenselement

a) Wissen um Garantenstellung und Handlungspflicht

407 Auf der Wissensseite erfordert das unechte Unterlassungsdelikt, dass der Täter weiss oder zumindest für möglich hält, eine Garantenstellung innezuhaben,

703 Urteil des BGer 6B_908/2009 vom 3. November 2010 E. 8.1; EGGER TANNER, S. 188.

704 ACKERMANN/ZEHNDER, Dogmatik, S. 49; CR CP I-CASSANI/VILLARD, Art. 11 N 61; DAN, N 353 ff.; DONATSCH/GODENZI/TAG, S. 341 f.; AK StGB-GRAF, Art. 11 N 23; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 146; STRATENWERTH/BOMMER, AT I, § 14 N 42 ff.; TRECHSEL et al., S. 268 f.; VEST et al., AT, S. 241 ff.

705 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 696; EGGER TANNER, S. 192; GETH, N 125; GIANNINI, S. 92; GRABER, S. 145; BSK StGB II-PIETH, Art. 305bis N 60; vgl. CR CP I-VILLARD/CORBOZ, Art. 12 N 29; DONATSCH/GODENZI/TAG, S. 118; TRECHSEL et al., S. 118.

706 Urteil des BGer 6B_1362/2020 vom 20. Juni 2022 E. 15.2.5; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 696; DONATSCH/GODENZI/TAG, S. 118; EGGER TANNER, S. 193; GETH, N 125; GIANNINI, S. 92; GRABER, S. 145; AK StGB-GRAF, Art. 305bis N 19; HURTADO POZO/GODEL, N 409.

707 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 696; EGGER TANNER, S. 192; GIANNINI, S. 92; GRABER, S. 145; NADELHOFER DO CANTO, S. 349; PK StGB-TRECHSEL/FATEHMOGHADAM, Art. 12 N 21; TRECHSEL et al., S. 118.

708 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 698; EGGER TANNER, S. 193; GIANNINI, S. 92 f.; GRABER, S. 145.

und dass daraus eine entsprechende Handlungspflicht erwächst.[709] Betreiberinnen dezentralisierter Finanzanwendungen müssen somit für möglich halten, dass sie im Sinne einer Finanzintermediärin dem Geldwäschereigesetz unterstehen und ihnen damit verbundene Sorgfaltspflichten zukommen.

408 Das Wissenselement bereitet in der Regel keine Schwierigkeiten, wenn die Betreiberin auf der von der FINMA geführten Liste bewilligter Institute aufgeführt ist oder sich einer Selbstregulierungsorganisation angeschlossen hat.[710] Problematisch ist hingegen, dass viele dezentralisierte Finanzanwendungen zwar dem Geldwäschereigesetz unterstellt sind, tatsächlich aber weder über eine Bewilligung verfügen noch einer Selbstregulierungsorganisation angehören oder einer klaren Rechtsform zugeordnet sind. In solchen Fällen spricht für ein Wissen um die eigene Unterstellung, wenn die Betreiberin oder das Protokoll in von Aufsichts- oder Strafverfolgungsbehörden (z.B. FINMA, IOSCO oder vergleichbaren internationalen Organisationen) geführten Warnlisten aufgeführt ist.[711] Die FINMA eröffnet in diesen Konstellationen Untersuchungen und fordert die betroffenen Personen zur Stellungnahme auf, wodurch diese über eine mögliche Bewilligungspflicht oder Unterstellung ausdrücklich informiert werden.[712]

409 Der Täter muss die tatsächlichen Voraussetzungen der Garantenstellung erfassen oder zumindest im Sinne einer ‹Parallelwertung in der Laiensphäre› erkennen, dass ihm gegenüber dem bedrohten Rechtsgut eine besondere Verantwortung zukommt, die eine Handlungspflicht begründet, auch wenn ihm die konkrete gesetzliche Grundlage dieser Pflicht nicht bekannt ist.[713]

410 Im vorliegenden Kontext könnte argumentiert werden, dass Betreiberinnen dezentralisierter Protokolle zumindest für möglich halten müssen, dem Geldwäschereigesetz zu unterstehen. Anwendungen, die den Transfer,

709 BGE 109 IV 137 E. 2b; ACKERMANN/ZEHNDER, Dogmatik, S. 49; CR CP I-CASSANI/VILLARD, Art. 11 N 61; DAN, N 361; DONATSCH/GODENZI/TAG, S. 341 f.; GETH, N 309; AK StGB-GRAF, Art. 11 N 23; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 146; STRATENWERTH/BOMMER, AT I, § 14 N 42 ff.; TRECHSEL et al., S. 268; VEST et al., AT, S. 241 ff.; HK StGB-WOHLERS, Art. 11 N 5.

710 Vgl. FINMA, Bewilligte Institute, Personen und Produkte; BSK GwG-FRIGO/JAIN, Art. 14 N 1; OFK GwG-WYSS, Art. 14 N 7 ff.

711 Vgl. FINMA, Warnungen der FINMA; vgl. auch IOSCO, International Securities & Commodities Alerts Network (I-SCAN); Kantonspolizei Zürich, Warnliste; BOHRER et al., S. 37; BLATTER, S. 25; MEIRICH, N 1594; SCHÖNKNECHT, Vorabklärungen, S. 85 f.

712 Vgl. BOHRER et al., S. 37; BLATTER, S. 25 ff.; SCHÖNKNECHT, Vorabklärungen, S. 85 f.

713 ACKERMANN, Unterlassungsrisiken, S. 164; DAN, N 361; FLACHSMANN, S. 38; STRATENWERTH/BOMMER, AT I, § 14 N 44; vgl. auch zur Parallelwertung in der Laiensphäre BGE 129 IV 238 E. 3.2.2; 129 IV 238 E. 3.2.2; 119 IV 242 E. 2d; 99 IV 57 E. 1a; AK StGB-ABO YOUSSEF, Art. 12 N 4; DONATSCH/GODENZI/TAG, S. 119; GRAVEN/STRÄULI, S. 170; BSK StGB I-NIGGLI/MÄDER, Art. 12 N 27; SCHULTZ, S. 190 f.; STRATENWERTH/BOMMER, AT I, § 9 N 72; PK StGB-TRECHSEL/FATEH MOGHADAM, Art. 12 N 6; HK StGB-WOHLERS, Art. 12 N 13.

die Verwahrung oder den Tausch von Vermögenswerten ermöglichen, weisen funktional eine enge Nähe zu klassischen Finanzdienstleistungen auf und lassen eine Unterstellung unter das Geldwäschereigesetz als naheliegend erscheinen. Angesichts der anhaltenden regulatorischen Diskussionen über die Einbeziehung von DeFi-Protokollen in den Anwendungsbereich des Geldwäschereirechts (insbesondere im Lichte der GAFI-Empfehlungen) ist davon auszugehen, dass Betreiberinnen die Möglichkeit ihrer Erfassung durch das Geldwäschereigesetz und der daraus fliessenden geldwäschereirechtlichen Sorgfaltspflichten zumindest erkennen müssen.[714]

b) Wissen um Gefahr, Handlungsmöglichkeit und Kausalität

Beim Erfolgsdelikt setzt der Unterlassungsvorsatz voraus, dass der Täter die Gefahr des Erfolgseintritts sowie die Möglichkeit zu dessen Abwendung erkennt und ihm bewusst ist, dass seine Untätigkeit ursächlich für den Erfolg ist.[715] Wie der Täter eingreifen könnte, braucht ihm nicht im Einzelnen bewusst zu sein. Die für das Vorliegen des Vorsatzes ausschlaggebende Bereitschaft, die Rechtsgutsverletzung bzw. -gefährdung als Konsequenz des eigenen Verhaltens hinzunehmen, zeigt sich bereits darin, dass er sich nicht die Mühe macht, mögliche Rettungsmöglichkeiten in Erwägung zu ziehen, obschon er damit rechnet, dass solche bestehen könnten.[716] 411

Manifestiert sich die Gefahrenlage in einem Delikt eines Dritten, muss sich das Wissen des Garanten auf alle objektiven Tatbestandsmerkmale der einschlägigen Norm erstrecken.[717] 412

Dazu gehört insbesondere das Bewusstsein, dass die Vermögenswerte verbrecherischen Ursprungs sind, wobei es ausreichend ist, wenn die Umstände in der ‹Parallelwertung in der Laiensphäre› nahelegen, dass die Vermögenswerte aus einer schwerwiegenden Vortat stammen, die erhebliche Sanktionen nach sich zieht.[718] An dieses Wissenselement sind keine hohen Anforderungen zu 413

714 Vgl. Bundesrat, DLT, S. 139 ff.; FINMA, Vermögenswerte, S. 1 ff.; GAFI, VASP, S. 1 ff.; GAFI, Update, S. 2 ff.; KGGT, NRA 2024, S. 47 ff.; KGGT, NRA 2018, S. 20 ff.; U.S. Department of the Treasury, S. 3 ff.

715 ACKERMANN/ZEHNDER, Dogmatik, S. 49; CR CP I-CASSANI/VILLARD, Art. 11 N 61; DAN, N 360 ff.; DONATSCH/GODENZI/TAG, S. 341 f.; GETH, N 309; AK StGB-GRAF, Art. 11 N 23; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 146; STRATENWERTH/BOMMER, AT I, § 14 N 43 f.; TRECHSEL et al., S. 268; VEST et al., AT, S. 241 ff.; HK StGB-WOHLERS, Art. 11 N 5.

716 STRATENWERTH/BOMMER, AT I, § 14 N 45.

717 DAN, N 363; CR CP I-CASSANI/VILLARD, Art. 11 N 61; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 145.

718 Vgl. Botschaft StGB 1989, S. 1085; BGE 149 IV 248 E. 6.3; 122 IV 211 E. 2e; 119 IV 242 E. 2b; Urteil des BGer 7B_1059/2023 vom 26. März 2025 E. 3.1.3.2; Urteil des BGer 6B_270/2021 vom 5. Oktober 2022 E. 2.2; Urteil des BGer 6B_295/2022 vom 15. September 2022 E. 1.2; Urteil des BGer 6B_1362/2020 vom 20. Juni 2022 E. 15.2.2; DONATSCH/THOMMEN/

stellen. Bereits wer im Sinne der ‹Willful-Blindness-Theorie› offensichtlich gebotene Abklärungen unterlässt und verdächtige Gelder trotz bestehender Zweifel weiterleitet, handelt mit Wissen um die mögliche deliktische Herkunft.[719]

414 Im vorliegenden Zusammenhang müssen Betreiberinnen dezentralisierter Finanzanwendungen folglich wissen oder zumindest für möglich halten, dass die Vermögenswerte, die Nutzer über die Plattform zu waschen beabsichtigen, einen verbrecherischen Ursprung aufweisen. Im Umfeld dezentralisierter Protokolle können verschiedene objektive Umstände auf ein entsprechendes Wissen hindeuten. Hinweise ergeben sich zunächst aus der Beschaffenheit der auf der Blockchain offen einsehbaren Transaktionshistorie.[720] Dazu zählen Vermögenswerte, die von Adressen stammen, welche in Sanktions- oder Watchlists (z.B. der OFAC oder anderer Aufsichts- und Strafverfolgungsbehörden) geführt werden, oder die mit bereits als verdächtig gekennzeichneten Token-Beständen in Verbindung stehen. Ebenso können behördliche Hinweise oder öffentliche Warnungen über die Nutzung bestimmter Anwendungen zu Geldwäschereizwecken ein solches Bewusstsein indizieren.[721] Auch transaktionsbezogene Faktoren können ein entsprechendes Wissen nahelegen. Dazu gehören ungewöhnlich hohe oder unregelmässige Transaktionsvolumina, eine auffällige Häufung kurzlebiger oder neu erstellter Wallets, die ausschliesslich zum einmaligen Transfer verwendet werden, sowie strukturelle Muster wie eine wiederkehrende Zerstückelung von Beträgen (Smurfing) oder untypische zeitliche Abläufe.[722]

415 Schliesslich muss der Betreiberin bewusst sein, dass sich durch die Einhaltung der geldwäschereirechtlichen Sorgfaltspflichten Geldwäschereihandlungen der Nutzer resp. die Gefährdung der Einziehungsinteressen verhindern lassen.[723]

WOHLERS, S. 505; GRABER, S. 142; AK StGB-GRAF, Art. 305bis N 19; LENGAUER/RUCKSTUHL, N 521; BSK StGB II-PIETH/SCHULTZE, Art. 305bis N 59; PK StGB-PIETH/SCHULTZE, Art. 305bis N 21.

719 Urteil des BGer 6B_627/2012 vom 18. Juli 2013 E. 2.4; AK StGB-GRAF, Art. 305bis N 19; vgl. auch Urteil des BGer 6B_1013/2020 vom 12. März 2024 E. 6.4; Urteil des BGer 6B_627/2012 vom 18. Juli 2013 E. 1.2; Urteil des BGer 6B_321/2010 vom 25. August 2010 E. 3.2.

720 Vgl. vorne N 21.

721 Vgl. MEIRICH, N 500; vgl. auch TEICHMANN, S. 559; Office of Foreign Assets Control, Is it possible to query a digital currency address using OFAC's Sanctions List Search tool?.

722 ACKERMANN/ZEHNDER, Dogmatik, S. 50; PAJAROLA, N 513 f.; vgl. BGE 119 IV 242 E. 2d; Urteil des BGer 6B_627/2012 vom 18. Juli 2013 E. 2.4; Urteil des BGer 6B_321/2010 vom 25. August 2010 E. 4.2.4; Urteil des BGer 6P.23/2000 vom 31. Juli 2000 E. 9d; CR CP I-VILLARD/CORBOZ. Art. 12 N 84; Anhang Ziff. 2 ff. GwV-FINMA.

723 Vgl. DAN, N 360 ff.; DONATSCH/GODENZI/TAG, S. 341 f.; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 147.

Das erforderliche Bewusstsein umfasst die Erkenntnis, dass geldwäschereirelevante Transaktionen durch geeignete technische und organisatorische Massnahmen zur Transaktionsüberwachung und Abklärung (Art. 6 GwG) identifiziert werden und bei Vorliegen eines begründeten Verdachts durch die Meldung an die Meldestelle für Geldwäscherei (Art. 9 GwG) staatliche Sicherungs- und Einziehungsmassnahmen ausgelöst werden können.[724] Die geldwäschereirechtlichen Sorgfaltspflichten dienen gerade dazu, die staatliche Aufspürung und Einziehung deliktischer Vermögenswerte zu ermöglichen und eine weitere Verschleierung ihrer Herkunft zu verhindern.[725] Finanzintermediärinnen nehmen insofern eine präventive Scharnierfunktion ein, indem sie durch Abklärungs- und Meldeverfahren bereits auf der Ebene der Transaktionsabwicklung ansetzen. Daraus folgt, dass einer Betreiberin, welche den geldwäschereirechtlichen Pflichten untersteht, bewusst sein muss, dass deren Befolgung geeignet ist, die Vereitelung der Einziehung zu verhindern oder zumindest zu begrenzen. 416

2. Willenselement

Neben dem Wissen um die Tatumstände muss der Täter den Willen haben, trotz dieser Erkenntnis pflichtgemässes Handeln zu unterlassen und den Eintritt des tatbestandsmässigen Erfolgs zumindest in Kauf zu nehmen.[726] Dies ist jedoch nur in Fällen des direkten Vorsatzes unzweifelhaft, nämlich dort, wo die Tatbestandsverwirklichung das eigentliche Handlungsziel des Täters darstellt oder er sie als unvermeidliche Nebenfolge seines Verhaltens erkennt.[727] 417

Hält der Täter hingegen die Tatbestandsverwirklichung zwar für möglich, handelt aber dennoch, «weil er den Erfolg für den Fall seines Eintritts in Kauf nimmt, sich mit ihm abfindet, mag er ihm auch unerwünscht sein», liegt eine eventualvorsätzliche Begehung vor.[728] Die Inkaufnahme des Erfolgs im 418

724 ACKERMANN/ZEHNDER, Dogmatik, S. 49; vgl. auch HEIERLI, N 78; BSK GwG-IVELL, Art. 9 N 1 ff.; BSK GwG-MÜLLER/LÖTSCHER, Art. 6 N 1 ff.

725 Botschaft GwG 1996, S. 1113; vgl. BOURQUIN, S. 211; KV/KO GwG-HUTZLER, Art. 9 N 3; BSK GwG-IVELL, Art. 9 N 4; SHK GwG-LUCHSINGER, Art. 9 N 6; REINLE, N 87 f.; OFK GwG-THELESKLAF, Art. 9 N 3; vgl. auch BGE 134 III 529 E. 4.2.

726 DAN, N 363; DONATSCH/GODENZI/TAG, S. 342; VON ROTZ, S. 106 f.; gegen das Erfordernis eines Willenselement beim unechten Unterlassungsdelikt STRATENWERTH/BOMMER, AT I, § 14 N 46 ff.

727 STRATENWERTH/BOMMER, AT I, § 9 N 96 ff.; AK StGB-ABO YOUSSEF, Art. 12 N 5; DONATSCH/GODENZI/TAG, S. 122; BSK StGB I-NIGGLI/MÄDER, Art. 12 N 42 ff.; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 12 N 12a.

728 BGE 150 IV 10 E. 5.7.2; 149 IV 57 E. 2.2; 147 IV 439 E. 7.3.1; vgl. AK StGB-ABO YOUSSEF, Art. 12 N 8; BSK StGB I-NIGGLI/MÄDER, Art. 12 N 46; STRATENWERTH/BOMMER, AT I, § 9 N 106; TRECHSEL et al., S. 116; CR CP I-VILLARD/CORBOZ, Art. 12 N 64.

Rahmen des voluntativen Elements markiert zugleich die Grenze zum bewusst fahrlässig handelnden Täter, welcher sich der Tatumstände zwar bewusst ist, jedoch auf den Nichteintritt der Tatbestandsverwirklichung vertraut.[729]

419 Aus dem blossen Wissen um die Möglichkeit des Erfolgseintritts darf indes nicht ohne Weiteres auf Inkaufnahme geschlossen werden.[730] Nach der bundesgerichtlichen Rechtsprechung ist ein solcher Schluss nur zulässig, «wenn sich dem Täter der Erfolg seines Verhaltens als so wahrscheinlich aufdrängte, dass sein Verhalten vernünftigerweise nur als Inkaufnahme dieses Erfolges ausgelegt werden kann».[731] Die Beurteilung richtet sich nach den konkreten Umständen, unter anderem nach der Schwere der Sorgfaltspflichtverletzung, dem Risiko der Tatbestandsverwirklichung sowie nach Beweggrund und Art der Tathandlung.[732]

420 Übertragen auf den vorliegenden Kontext kann von Eventualvorsatz ausgegangen werden, wenn die Betreiberin trotz drohender Gefahr einer Geldwäschereihandlung untätig bleibt und dabei die Realisierung dieser Gefahr zumindest in Kauf nimmt.[733]

421 Ob eine solche Inkaufnahme vorliegt, ist anhand der konkreten Umstände zu beurteilen. Massgebend sind dabei insbesondere die Schwere der Verletzung geldwäschereirechtlicher Sorgfaltspflichten sowie die Nähe zum Eintritt der Geldwäschereihandlung des Nutzers. Auch bei dezentralisierten Strukturen stellt sich dabei die zusätzliche Schwierigkeit, dass es in Abwesenheit von Geständnissen regelmässig an einem unmittelbaren Nachweis der inneren Willensrichtung fehlt, weshalb sich die richterliche Feststellung des Eventualvorsatzes auf eine sorgfältige Analyse äusserlich feststellbarer Indizien und Erfahrungsregeln stützen muss.[734] Gerade im Hinblick auf die Straflosigkeit der fahrlässig begangenen Geldwäscherei erweist sich die Beurteilung, ob

729 BGE 147 IV 439 E. 7.3.1; DONATSCH/GODENZI/TAG, S. 124; BSK StGB I-NIGGLI/MÄDER, Art. 12 N 58; STRATENWERTH/BOMMER, AT I, § 9 N 106; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 12 N 14; CR CP I-VILLARD/CORBOZ, Art. 12 N 7.

730 BGE 135 IV 12, E. 2.3.2; 133 IV 9 E. 4.1; Urteil des BGer 6B_775/2011 vom 4. Juni 2012 E. 2.4.1; AK StGB-ABO YOUSSEF, Art. 12 N 9; HK StGB-WOHLERS, Art. 12 N 8.

731 BGE 147 IV 439 E. 7.3.1; 137 IV 1 E. 4.2.3; 133 IV 222 E. 5.3; DONATSCH/GODENZI/TAG, S. 124; AK StGB-ABO YOUSSEF, Art. 12 N 10; BSK StGB I-NIGGLI/MÄDER, Art. 12 N 53; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 12 N 15.

732 BGE 147 IV 439 E. 7.3.1; 135 IV 12 E. 2.3.2; 134 IV 29 E. 3; Urteil des BGer 6B_1084/2023 vom 29. November 2023 E. 1.2.2; DONATSCH/GODENZI/TAG, S. 125; AK StGB-ABO YOUSSEF, Art. 12 N 9; STRATENWERTH/BOMMER, AT I, § 9 N 107; PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 12 N 15.

733 Vgl. STRATENWERTH/BOMMER, AT I, § 14 N 49 ff.

734 BGE 134 IV 26 E. 3.2.2; 130 IV 58 E. 8.4; Urteil des BGer 6B_1071/2019 vom 5. November 2020 E. 2.2; AK StGB-ABO YOUSSEF, Art. 12 N 9; ACKERMANN/ZEHNDER, Dogmatik, S. 51; DONATSCH/GODENZI/TAG, S. 125; STRASSER, S. 155; VEST, Zufall, S. 953 ff.; CR CP I-VILLARD/CORBOZ, Art. 12 N 77 f.; HK StGB-WOHLERS, Art. 12 N 6.

eine Inkaufnahme des Erfolgs vorlag oder der Täter im Sinne bewusster Fahrlässigkeit pflichtwidrig darauf vertraute, dass sich das erkannte Risiko nicht verwirklichen werde, als heikle Gratwanderung.[735]

Im Folgenden werden mögliche Indizien aufgeworfen, die auf ein Inkaufnehmen im Sinne der dargelegten Grundsätze von Lehre und Rechtsprechung des Bundesgerichtes hindeuten. 422

Ein potenzieller Hinweis auf die Inkaufnahme durch Betreiberinnen dezentralisierter Anwendungen liegt in der Missachtung der Sorgfaltspflichten nach dem Geldwäschereigesetz, der Geldwäschereiverordnung und der Geldwäschereiverordnung-FINMA.[736] Letztere enthält im Anhang verschiedene durch die FINMA herausgearbeitete Anhaltspunkte, die auf Geldwäscherei hindeuten.[737] 423

In der Rechtsprechung und Lehre werden namentlich Verstösse gegen Art. 6, Art. 9 und Art. 10 GwG als Anzeichen für eventualvorsätzliches Handeln diskutiert.[738] Dabei genügt die Verletzung einer einzelnen Pflicht in der Regel nicht. Ausschlaggebend sind vielmehr der Umfang und das Gewicht der Pflichtverletzungen sowie die Frage, inwieweit geldwäschereirechtliche Sorgfaltspflichten überhaupt implementiert wurden.[739] Die Pflichtverletzung steht dabei in Wechselwirkung zur Intensität des vom Täter erkannten Risikos der Tatbestandsverwirklichung.[740] 424

735 Vgl. Botschaft 1989, S. 1061; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 672; ACKERMANN/ZEHNDER, Dogmatik, S. 50; GIANNINI, S. 135; GRABER, S. 141 ff.; SCHUBARTH, S. 522; STRASSER, S. 158.

736 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 676 ff.; ACKERMANN/ZEHNDER, Dogmatik, S. 48 f.; BOURQUIN, S. 249 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 42; STRASSER, S. 158; vgl. BGE 134 III 529 E. 4.3; Urteil des BGer 6B_1362/2020 vom 20. Juni 2022 E. 15.2.4; Urteil des BGer 6S.56/2007 vom 30. März 2007 E. 3.1; CASSANI/VILLARD, N 6.94; OFK StGB-ISENRING, Art. 305bis N 20.

737 STRASSER, S. 155; vgl. BSK GwG-LANDOLT/GEMPERLI, Art. 3 N 111; PAJAROLA, N 514 m.V.a. Anhang Ziff. 2 ff. GwV-FINMA.

738 ACKERMANN/ZEHNDER, Dogmatik, S. 49; BOURQUIN, S. 251; CASSANI/VILLARD, N 6.94; CR CP II-CASSANI/VILLARD, Art. 305bis N 42; STRASSER, S. 158; vgl. Urteil des BGer 6B_1362/2020 vom 20. Juni 2022 E. 15.2.4; Urteil des BGer 6S.56/2007 vom 30. März 2007 E. 3.1.

739 Das Bundesgericht hat diese Rechtsprechung jüngst wieder bestätigt: «Dass das Nichtwissen um die verbrecherische Herkunft von Vermögenswerten auf einer Verletzung von gesetzlichen Pflichten als Finanzintermediär beruht, reicht nach der Rechtsprechung für den Nachweis des (Eventual-)Vorsatzes in Bezug auf die Verletzung des Geldwäschereitatbestands von Art. 305bis StGB nicht aus» (Urteil des BGer 6B_1180/2023 vom 24. September 2025 E. 1.4.3.5); Urteil des BGer 6B_1362/2020 vom 20. Juni 2022 E. 15.2.4; Urteil des BGer 6S.56/2007 vom 30. März 2007 E. 3.3; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 676; BACHARACH, S. 227; BOURQUIN, S. 249 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 42; HEIERLI, N 78; OFK StGB-ISENRING, Art. 305bis N 55.

740 VEST, Zufall, S. 954.

425 Gemäss Art. 6 GwG hat die Finanzintermediärin Art und Zweck der gewünschten Geschäftsbeziehung risikobasiert zu identifizieren, wobei sich der Umfang der vorzunehmenden Abklärungen nach dem individuellen Geldwäschereirisiko richtet, das insbesondere von der Art der Dienstleistung, der Herkunft und Struktur der Vermögenswerte sowie den Transaktionsmustern abhängt (sogenannter risikobasierter Ansatz).[741] Erhöhte Abklärungspflichten kommen bei Branchen und Produkten mit erhöhtem Geldwäschereirisiko im Sinne von Art. 13 Abs. 2 GwV-FINMA zum Tragen, etwa bei Geschäften mit virtuellen Währungen, deren technische Eigenschaften – namentlich die Möglichkeit anonymer und grenzüberschreitender Übertragungen – ein erhöhtes Risiko begründen und daher weitergehende Prüfungen nach Art. 15 GwV-FINMA auslösen.[742]

426 Eine einfache Verletzung von Art. 6 GwG begründet zwar für sich allein noch keinen Eventualvorsatz, entfaltet aber Indizwirkung.[743] Deutlich stärker wiegt hingegen, wenn Betreiberinnen gegen verstärkte Abklärungspflichten verstossen, da diese Pflichten gerade für Tätigkeiten gelten, die aufgrund ihres erhöhten Geldwäschereirisikos – wie beim Betrieb dezentralisierter Finanzanwendungen – einer vertieften Prüfung bedürfen.[744]

427 Schliesslich bestehen bei einem begründeten Verdacht, dass die in die Geschäftsbeziehung involvierten Vermögenswerte im Zusammenhang mit einer strafbaren Handlung nach Art. 305bis Ziff. 1 StGB stehen oder aus einem Verbrechen oder einem qualifizierten Steuervergehen herrühren, die Pflicht zur Meldung im Sinne von Art. 9 GwG sowie einer allfälligen Vermögenssperre nach Art. 10 GwG.[745] Auch deren Missachtung stellt ein gewichtiges Indiz für Eventualvorsatz dar.[746]

741 Botschaft GAFI 2007, S. 6284; BSK GwG-MÜLLER/LÖTSCHER, Art. 6 N 3 f.; STENGEL/RUCKSTUHL, N 592; STENGEL/PAYDAR, N 18.100; OFK GwG-WYSS, Art. 6 N 3 ff.

742 BSK GwG-MÜLLER/LÖTSCHER, Art. 6 N 36 ff.; LUCHSINGER/PORTMANN, S. 43; STENGEL/PAYDAR, N 18.101; vgl. auch LUCHSINGER/PORTMANN, S. 49 m.V.a. KGGT, NRA 2024, S. 47 ff.; MOLO/DRZALIC, S. 55 f.; RONC/SCHUPPLI, S. 534.

743 Vgl. Urteil des BGer 6B_1180/2023 vom 24. September 2025 E. 1.4.3.5; Urteil des BGer 6B_1362/2020 vom 20. Juni 2022 E. 15.2.4; Urteil des BGer 6S.56/2007 vom 30. März 2007 E. 3.3; ACKERMANN/ZEHNDER, Dogmatik, S. 49; BACHARACH, S. 227; CASSANI/VILLARD, N 6.94; EGGER TANNER, S. 189.

744 Vgl. ACKERMANN/ZEHNDER, Dogmatik, S. 49; STRASSER, S. 158.

745 BSK GwG-IVELL, Art. 9 N 6 ff., Art. 10 N 11 ff.; SHK GwG-LUCHSINGER, Art. 9 N 20 ff.; STENGEL/PAYDAR, N 18.116 ff.; OFK GwG-THELESKLAF, Art. 9 N 3 ff.; OFK GwG-THELESKLAF, Art. 10 N 1 ff.

746 BGE 134 III 529 E. 4.3; KV/KO StGB-ACKERMANN/ZEHNDER Art. 305bis N 656; ACKERMANN/ZEHNDER, Dogmatik, S. 49; HEIERLI, N 78; BSK GwG-IVELL, Art. 10 N 56; REINLE, N 659; STRASSER, S. 158; STRATENWERTH/BOMMER, BT II, § 57 N 60; OFK GwG-THELESKLAF, Art. 10 N 10.

Selbst wenn zum Zeitpunkt der geldwäschereirelevanten Transaktion noch kein Vorsatz besteht, kann bei nachträglich eintretender Bösgläubigkeit eine vorsätzliche Unterlassung ausnahmsweise angenommen werden. Dies ist der Fall, wenn die Betreiberin erst später von der deliktischen Herkunft der Vermögenswerte erfährt und dennoch passiv bleibt, da sich aus der Meldepflicht eine Garantenpflicht ergibt.[747] 428

In einer Gesamtbetrachtung ist schliesslich zu berücksichtigen, dass dezentralisierte Finanzanwendungen uneingeschränkt zugänglich sind und Nutzer direkt mit dem Protokoll interagieren, wodurch der gesamte Ablauf automatisiert und ohne Eingriffsmöglichkeit der Betreiberin erfolgt.[748] Für eine Inkaufnahme des Taterfolgs spricht insbesondere, wenn keinerlei Kontroll- oder Abklärungsmassnahmen zur Erfüllung der geldwäschereirechtlichen Sorgfaltspflichten technisch implementiert wurden.[749] Bei der Beurteilung sind zudem die Art der Finanzanwendung und ihre inhärente Funktionalität zu berücksichtigen, da insbesondere bei anonymisierenden oder herkunftsverschleiernden Strukturelementen – etwa bei Kryptomixern oder Handelsprotokollen, die den Handel mit stark anonymisierenden Kryptowährungen wie Monero ermöglichen – der Eventualvorsatz besonders naheliegt.[750] 429

Eine Inkaufnahme des Taterfolgs kann überdies Ausdruck bewussten Nicht-wissen-Wollens (‹willful blindness›) sein, wenn die Betreiberin trotz eindeutiger Anhaltspunkte, die zu weiterführenden Abklärungen veranlassen müssten, bewusst darauf verzichtet, genauere Kenntnis über die Herkunft der Vermögenswerte oder die Zielrichtung der Transaktion zu erlangen.[751] Vor dem Hintergrund der systemimmanenten Pseudonymität der Nutzer und gegebenenfalls zusätzlicher anonymisierender Funktionen der Anwendung spricht insbesondere das vollständige Unterlassen jeglicher Abklärungsbemühungen für eine solche Gleichgültigkeit. 430

747 Vgl. vorne N 406; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 698; EGGER TANNER, S. 193; GIANNINI, S. 92 f.; GRABER, S. 145.

748 Vgl. vorne N 71 ff.

749 Vgl. ACKERMANN, Unterlassungsrisiken, S. 165; STRASSER, S. 153 f.

750 Vgl. BACHARACH, S. 68; vgl. auch Anhang Ziff. 2 ff. GwV-FINMA; ANDREOTTI, S. 609 f.; IKEMEYER/KRIMPHOVE, S. 432, 435; MEIRICH, N 137; MURPHY.

751 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 683; ACKERMANN/ZEHNDER, Dogmatik, S. 51; BOURQUIN, S. 252; EGGER TANNER, S. 189; GIANNINI, S. 90; AK StGB-GRAF, Art. 305bis N 19; HEIERLI, S. 90; HERREN, S. 1120; KERN, Kunsthandel, S. 378; STRASSER, S. 154, 158; vgl. Urteil des BGer 6B_627/2012 vom 18. Juli 2012 E. 1.2, 2.4; Urteil des BGer 6B_835/2008 vom 20. April 2009 E. 4; vgl. auch BGE 135 IV 12 E. 2.3.1; Urteil des BGer 6B_1355/2020 vom 14. Januar 2022 E. 5.4.3; Urteil des BStGer SK.2022.2 vom 6. Juni 2023 E. 10; Urteil des BStGer CA.2021.15 vom 20. Juni 2022 E. 2.3.6.

B. Irrtümer

431 In der Doktrin wird einhellig vertreten, dass das Verhalten des Täters nach den Regeln des Sachverhaltsirrtums gemäss Art. 13 StGB zu beurteilen ist, wenn er einen oder mehrere der subjektiven Umstände verkennt.[752] Weist eine Betreiberin somit einen Vorsatzmangel in Bezug auf Garantenstellung, Kausalität, Tatmacht oder Gefahrensituation auf, ist von Straflosigkeit auszugehen. War der Irrtum vermeidbar, käme nach Art. 13 Abs. 2 StGB eine Strafbarkeit wegen fahrlässiger Begehung in Betracht, welche beim Tatbestand der Geldwäscherei allerdings ausgeschlossen ist.[753] Kein Sachverhaltsirrtum liegt hingegen vor, wenn sich die Betreiberin bewusst für ein Nichtwissen entscheidet.[754]

432 Erkennt die Betreiberin zwar ihre aus dem Geldwäschereigesetz erwachsende Garantenstellung, irrt jedoch über den Umfang der daraus folgenden Pflichten und bleibt deshalb untätig, ist ihr Verhalten unter dem Gesichtspunkt des Rechtsirrtums nach Art. 21 StGB zu würdigen.[755] Dass sich eine Betreiberin, die um ihre Garantenstellung als Finanzintermediärin weiss, bei Unterlassung der damit verbundenen gesetzlichen Pflichten in einem Gebotsirrtum befindet, erscheint nicht denkbar. Auf eine vertiefte Erörterung wird daher verzichtet.

C. Zwischenfazit

433 Bei der Geldwäscherei in der Form des unechten Unterlassungsdelikts sowie als Vorsatzdelikt müssen Betreiberinnen dezentralisierter Finanzanwendungen sowohl um ihre Garantenstellung als Finanzintermediärinnen als auch um die daraus fliessenden Handlungspflichten wissen. Erforderlich sind zudem das Bewusstsein für die Gefährdung des geschützten Rechtsguts sowie die Möglichkeit, den Eintritt des tatbestandsmässigen Erfolgs durch pflichtgemässes Verhalten abzuwenden. Auf der Willensseite verlangt der Vorsatz schliesslich die Inkaufnahme des Erfolgs, mithin den Entschluss, trotz dieser Erkenntnis untätig zu bleiben.

752 DAN, N 378; DONATSCH/GODENZI/TAG, S. 341; AK StGB-GRAF, Art. 11 N 23; STRATENWERTH/BOMMER, AT I, § 14 N 44; TRECHSEL et al., S. 268 f.; VEST et al., AT, S. 242.

753 Vgl. Botschaft 1989, S. 1061; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 672; GIANNINI, S. 135; GRABER, S. 141 ff.; STRASSER, S. 158.

754 BGE 135 IV 12 E. 2.3.1; Urteil des BGer 6B_910/2019 vom 15. Juni 2020 E. 2.2.4.4; Urteil des BGer 6B_997/2014 vom 22. Dezember 2014 E. 2.2; AK StGB-ABO YOUSSEF, Art. 13 N 2; BSK StGB I-NIGGLI/MÄDER, Art. 13 N 10.

755 DAN, N 378; DONATSCH/GODENZI/TAG, S. 342; GETH, N 309; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 147; STRATENWERTH/BOMMER, AT I, § 14 N 44; TRECHSEL et al., S. 268 f.; VEST et al., AT, S. 243.

Im Vordergrund steht bei Betreiberinnen dezentralisierter Protokolle primär Eventualvorsatz. Das Wissenselement bezieht sich hierbei vor allem auf das Erkennen der Gefahr, dass Nutzer über die Anwendung Geldwäschereihandlungen vornehmen könnten. Objektive Umstände wie auf der Blockchain offen einsehbare Transaktionsmuster, Transaktionen mit Adressen auf Sanktions- oder Watchlists (z.B. der OFAC) oder behördliche Warnungen zu bestimmten Protokollen können ein solches Wissen nahelegen. Gleiches gilt für transaktionsbezogene Auffälligkeiten wie ungewöhnlich hohe oder unregelmässige Volumina, kurzlebige Wallets oder fragmentierte Transfers (Smurfing). 434

Das voluntative Element – die Inkaufnahme des Erfolgs – manifestiert sich in der Missachtung geldwäschereirechtlicher Pflichten (GwG, GwV, GwV-FINMA). Einzelne Pflichtverletzungen begründen zwar regelmässig noch keinen Eventualvorsatz, entfalten jedoch Indizwirkung, deren Gewicht sich nach der Schwere der Pflichtverletzung und der Nähe zum Risikoeintritt bestimmt. Besonders stark wirkt diese Indizwirkung, wenn Betreiberinnen jegliche Sorgfaltsmassnahmen unterlassen, etwa keine Abklärungen gemäss Art. 6 GwG i.V.m. Art. 13 ff. GwV-FINMA vornehmen oder Meldepflichten nach Art. 9 GwG ignorieren. Dies gilt umso mehr, als der Umgang mit virtuellen Währungen aufgrund ihrer technischen Eigenschaften (insbesondere der Pseudonymität und der Möglichkeit grenzüberschreitender Transfers) per se erhöhte geldwäschereirechtliche Risiken birgt und daher verstärkte Abklärungspflichten auslöst. Ein Verzicht auf die technische Implementierung jeglicher geldwäschereirechtlicher Sorgfaltspflichten in die Anwendung lässt auf ein bewusstes Nicht-wissen-Wollen schliessen und stellt in diesem Zusammenhang ein besonders gewichtiges Indiz für eine Inkaufnahme dar. 435

In der Gesamtbetrachtung spricht die vollständige Abwesenheit technischer oder organisatorischer Sorgfaltsvorkehrungen für eine Inkaufnahme. Dies gilt in besonderem Masse, wenn die Anwendung anonymisierende oder herkunftsverschleiernde Funktionalitäten aufweist, wie sie etwa bei Kryptomixern oder Privacy Coins bestehen. In solchen Fällen ist von Eventualvorsatz auszugehen. 436

V. Versuch

Die herrschende Lehre bejaht den Versuch bei der unechten Unterlassung.[756] Uneins ist sich die Doktrin indes hinsichtlich des Versuchsbeginns. So werden im Wesentlichen drei Ansätze vertreten. Danach soll der Versuch beginnen, 437

756 DAN, N 483; STRATENWERTH/BOMMER, AT I, § 15 N 1 ff.; CR CP I-CASSANI, Art. 11 N 62; DONATSCH/GODENZI/TAG, S. 343; AK StGB-GRAF, Art. 11 N 6; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 142; VEST et al., AT, S. 244.

sobald der Garantenpflichtige die erste Handlungsmöglichkeit verstreichen lässt, durch Unterlassen eine unmittelbare Gefahr für das Rechtsgut herbeiführt oder die letzte Rettungsmöglichkeit ungenutzt lässt.[757] Die mittlere Lösung wird in der herrschenden Lehre bevorzugt, da sie erlaubt, sowohl vollendete als auch unvollendete Versuche zu erfassen.[758] Der Versuch ist demzufolge dann vollendet, wenn der Unterlassungstäter die nach seiner Vorstellung letzte Möglichkeit zum rettenden Eingreifen hat verstreichen lassen und der Erfolg trotzdem nicht eingetreten ist.[759]

438 Wie bereits festgehalten, liegt bei der Geldwäscherei durch Unterlassen der Erfolg in der Vornahme der Geldwäschereihandlung durch den Dritten bzw. in der abstrakten Gefährdung des staatlichen Einziehungsinteresses.[760] Der Anwendungsbereich des Versuchs durch Unterlassen ist insofern bei den Betreiberinnen nicht denkbar, als bereits die durch den Nutzer bewirkte abstrakte Gefährdung des Rechtsguts bzw. ein Verhalten, das typischerweise die Möglichkeit einer Rechtsgutsgefährdung begründet, genügt und der Erfolg im weiteren Sinne (die Deliktsbegehung des Dritten) damit eintritt.[761] Die für den Versuchsbeginn ausschlaggebende Gefährdung des Rechtsguts fällt somit mit der Vollendung des Geldwäschereitatbestands zusammen, was bei dezentralisierten Anwendungen grundsätzlich bereits beim direkten Interagieren des Nutzers mit dem Protokoll der Fall ist.[762]

VI. Fazit

439 Dieses Kapitel ging der Frage nach, ob und unter welchen Voraussetzungen Betreiberinnen dezentralisierter Finanzanwendungen wegen Geldwäscherei durch Unterlassen nach Art. 305bis i.V.m. Art. 11 StGB strafrechtlich verantwortlich gemacht werden können, wenn Nutzer ihre Protokolle für Geldwäschereihandlungen verwenden.

757 DAN, N 486; CR CP I-CASSANI, Art. 11 N 62; AK StGB-GRAF, Art. 11 N 6; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 142; STRATENWERTH/BOMMER, AT I, § 15 N 2 f.

758 DAN, N 486; CR CP I-CASSANI, Art. 11 N 62; DONATSCH/GODENZI/TAG, S. 343; AK StGB-GRAF, Art. 11 N 6; GRAVEN/STRÄULI, S. 266 f.; STRATENWERTH/BOMMER, AT I, § 15 N 3; VEST et al., AT, S. 245; a.M. BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 142.

759 HURTADO POZO/GODEL, N 848; RIKLIN, AT I, § 19 N 36; STRATENWERTH/BOMMER, AT I, § 15 N 3; TRECHSEL et al., S. 269.

760 Vgl. vorne N 296 ff.; ACKERMANN, Eignungsdelikt, S. 4; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 394 f., 745; DONATSCH/THOMMEN/WOHLERS, S. 502; EGGER TANNER, S. 121; FUCHS, N 183; GRABER, S. 133; VEST, Geldwäscherei, S. 55; vgl. auch BGE 145 IV 491 E. 2.3.2; Urteil des BGer 6B_332/2019 vom 29. Oktober 2019 E. 2.1.2.

761 Vgl. vorne N 175 f.

762 Vgl. vorne N 275.

Ausgangspunkt bildet die Erkenntnis, dass die Geldwäscherei nach Art. 305bis StGB auch in Form eines unechten Unterlassungsdelikts begangen werden kann und als Erfolgsdelikt in Erscheinung tritt, weil sich der tatbestandsmässige Erfolg in der Gefährdung des staatlichen Einziehungsinteresses durch die vom Nutzer begangene Geldwäschereihandlung verwirklicht. Die Geldwäscherei des Nutzers ist der Betreiberin, welche zu ihrer Verhinderung verpflichtet ist, als täterschaftlich herbeigeführter Unterlassungserfolg vorzuwerfen. 440

Die Grundlage einer solchen Handlungspflicht ergibt sich aus einer Garantenstellung, welche eine qualifizierte Pflicht zum Schutz des staatlichen Einziehungsinteresses voraussetzt. Eine solche Pflicht lässt sich ausschliesslich aus dem Geldwäschereigesetz herleiten. Dessen Sorgfalts- und Meldepflichten bezwecken sowohl die Lokalisierung und Sicherung der Einziehung deliktischer Vermögenswerte als auch die Identifikation und strafrechtliche Verfolgung der hinter den Transaktionen stehenden Personen. Finanzintermediärinnen nehmen damit eine Sonderstellung im staatlichen Kampf gegen die Geldwäscherei ein. Ihre Pflichten gehen über eine blosse ‹allgemeine Bürgerpflicht› hinaus und stehen in engem funktionalem Bezug zum Rechtsgut des Schutzes der Rechtspflege. Ein derart spezifischer Bezug kann ausserhalb des Geldwäschereigesetzes – etwa im Rahmen der Ingerenz, der Herrschaft über eine Gefahrenquelle oder der Geschäftsherrenhaftung – nicht begründet werden. 441

Eine auf das Geldwäschereigesetz gestützte Garantenstellung besteht jedoch nur, wenn die Betreiberinnen dessen Anwendungsbereich unterstehen. Dies ist namentlich dann der Fall, wenn sie als Finanzintermediärinnen im Sinne von Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. b GwV tätig sind und über Kontroll- oder Einflussmöglichkeiten auf den Transaktionsablauf verfügen. Eine örtliche Unterstellung setzt zudem eine gewisse physische Präsenz von gewisser Dauer in der Schweiz voraus, etwa wenn die Betreiberinnen ihre administrativen oder technischen Funktionen von hier aus wahrnehmen. 442

Da es sich bei der Geldwäscherei durch Unterlassen um ein Erfolgsdelikt handelt, muss zwischen dem Eintritt des Erfolgs und der pflichtwidrigen Untätigkeit ein hypothetischer Kausalzusammenhang bestehen. Dabei ist im Grundsatz zu berücksichtigen, dass eine technische Implementierung zur Abklärung der Hintergründe einer Transaktion sowie eine damit verbundene Meldung an die MROS oder die Anordnung einer Vermögenssperre die Gefährdung des staatlichen Einziehungsinteresses mit hoher Wahrscheinlichkeit hätte verhindern können. Ob die Betreiberin über die hierfür erforderliche Tatmacht verfügt, das heisst überhaupt in der Lage ist, die gebotenen Handlungen vorzunehmen, hängt letztlich davon ab, ob ihr tatsächliche Kontroll- 443

oder Eingriffsmöglichkeiten in den Transaktionsablauf zur Verfügung stehen. Diese Eigenschaft fehlt bei idealtypisch dezentralen Finanzanwendungen in der Regel.

444 Auf subjektiver Ebene setzt die Strafbarkeit Vorsatz voraus. Betreiberinnen müssen zumindest für möglich halten, dass ihre Anwendung zu Geldwäschereizwecken missbraucht wird und die darüber transferierten Vermögenswerte deliktischer Herkunft sind. Angesichts der Transparenz öffentlicher Blockchains lassen sich entsprechende Indikatoren (etwa ungewöhnliche Transaktionsmuster, wiederkehrende Wechsel zwischen Wallet-Clustern, Verbindungen zu sanktionierten Adressen oder behördliche Warnhinweise) regelmässig erkennen. Unterbleiben trotz solcher Anhaltspunkte jegliche Abklärungen, spricht dies dafür, dass die Betreiberin sich der deliktischen Herkunft der übertragenen Vermögenswerte bewusst ist.

445 Hinsichtlich des Willenselements verlangt der Eventualvorsatz, dass die Betreiberin die deliktische Verwendung ihrer Anwendung zumindest in Kauf nimmt. Entscheidend sind insoweit in erster Linie die Schwere und Systematik der Verletzung geldwäschereirechtlicher Sorgfaltspflichten. Einzelne Versäumnisse oder punktuelle Fehlleistungen reichen hierfür grundsätzlich nicht aus. Im Umgang mit dezentralisierten Finanzanwendungen ist jedoch zu berücksichtigen, dass bereits aufgrund der pseudonymen und grenzüberschreitenden Nutzungslage erhöhte Abklärungspflichten bestehen. Eine Inkaufnahme liegt vorwiegend dann nahe, wenn keinerlei technische oder organisatorische Massnahmen zur Umsetzung der Sorgfaltspflichten getroffen wurden. Ein solches Verhalten deutet – gerade vor dem Hintergrund der systemimmanenten Anonymität – auf bewusste Gleichgültigkeit bzw. ein Nicht-Wissen-Wollen hin, insbesondere dann, wenn die Anwendung zusätzlich anonymisierende oder herkunftsverschleiernde Funktionalitäten aufweist.

Kapitel 3: Strafrechtliche Anschlussfragen

446 Es wurde aufgezeigt, dass Betreiberinnen dezentralisierter Finanzanwendungen, deren Infrastruktur von Dritten zur Geldwäscherei genutzt wird, als Unterlassungstäterinnen aufgrund pflichtwidriger Untätigkeit nach Art. 305bis StGB strafrechtlich verantwortlich sein können. Das nachfolgende Kapitel widmet sich den sich daraus ergebenden strafrechtlichen Folgefragen. Zunächst wird geprüft, unter welchen Voraussetzungen die Qualifikationstatbestände der schweren Fälle nach Art. 305bis Ziff. 2 StGB auf Betreiberinnen übertragbar sind (I.). Anschliessend werden die Konkurrenzfragen zwischen Gehilfenschaft und täterschaftlicher Unterlassung und bei mehrfacher geld-

wäschereirelevanter Nutzung durch verschiedene Nutzer sowie die Konkurrenz zu eigenständig sanktionierten Sorgfaltspflichtverletzungen nach Art. 305ter StGB und Art. 37 GwG geklärt (II.). Zuletzt werden die Anknüpfungspunkte der schweizerischen Strafhoheit bei Inland- und Auslandtaten im Kontext dezentralisierter Protokolle untersucht (III.).

I. Schwere Fälle von Geldwäscherei

Im Regelfall bedroht Art. 305bis Ziff. 1 StGB die Geldwäscherei mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe. In schweren Fällen nach Art. 305bis Ziff. 2 StGB kann die Strafe auf bis zu fünf Jahre Freiheitsstrafe oder Geldstrafe erhöht werden.[763] Bei den schweren Fällen liegt jeweils ein persönliches Merkmal im Sinne von Art. 27 StGB vor, sodass der Täter oder die Teilnehmerin das qualifizierende Tatbestandsmerkmal persönlich erfüllen muss.[764] 447

Das nachfolgende Kapitel untersucht, inwieweit diese Qualifikationstatbestände auf Betreiberinnen dezentralisierter Finanzanwendungen – als Gehilfinnen oder Unterlassungstäterinnen – übertragbar sind und in welchen Konstellationen eine Erhöhung des Strafrahmens in Betracht kommt. 448

Im Einzelnen wird zunächst untersucht, ob Betreiberinnen als Mitglieder einer kriminellen bzw. terroristischen Organisation oder als Mitglieder einer Bande in Betracht kommen. Anschliessend wird geprüft, ob eine gewerbsmässige Begehung mit grossem Umsatz oder erheblichem Gewinn einschlägig ist und ob darüber hinaus – über die Generalklausel – weitere Konstellationen als schwere Fälle qualifiziert werden können. 449

A. Mitglieder einer kriminellen oder terroristischen Organisation

Ein schwerer Fall nach Art. 305bis Ziff. 2 lit. a StGB stellt die Mitgliedschaft in einer kriminellen oder terroristischen Organisation im Sinne von Art. 260ter StGB dar.[765] 450

763 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 716; CR CP II-CASSANI/VILLARD, Art. 305bis N 46; EGGER TANNER, S. 208; BSK StGB II-PIETH, Art. 305bis N 63; PK StGB-PIETH/SCHULTZE, Art. 305bis N 23.

764 BGE 105 IV 182 E. 2a; 70 IV 125; Urteil des BGer 6B_976/2015 vom 27. September 2016 E. 10.3.2; Urteil des BGer 6B_207/2013 vom 10. September 2013 E. 1.3.2; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 716; EGGER TANNER, S. 207; PK StGB-TRECHSEL/JENAL, Art. 146 N 32; HK StGB-SCHLEGEL, Art. 139 N 10.

765 BGE 132 IV 132 E. 4.1.1; 129 IV 271 E. 2.3.1; ACKERMANN et al., S. 228; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 717; CR CP II-CASSANI/VILLARD, Art. 305bis N 50; EGGER TANNER, S. 208; AK StGB-GRAF, Art. 305bis N 22; OFK StGB-ISENRING, Art. 305bis N 69;

451 Im vorliegenden Zusammenhang stellen sich hierbei zwei Fragen: Zum einen ist zu prüfen, ob eine Betreiberschaft von mehr als drei Personen, die sich durch Unterlassen der Geldwäscherei strafbar macht, als Verbrechensorganisation qualifiziert werden kann. Zum anderen ist zu untersuchen, ob Betreiberinnen von dezentralisierten Anwendungen bei deren Nutzung zur Geldwäscherei durch eine kriminelle oder terroristische Organisation nach Art. 260ter StGB als deren Mitglied eingeordnet werden können.

452 Für das Vorliegen einer Organisation nach Art. 260ter StGB setzt die bundesgerichtliche Rechtsprechung «eine strukturierte Gruppe von mindestens drei – im Allgemeinen mehr – Personen voraus, die mit dem Ziel geschaffen wurde, unabhängig von einer Änderung ihrer Zusammensetzung dauerhaft zu bestehen, und die sich namentlich durch die Unterwerfung ihrer Mitglieder unter Anweisung, durch systematische Arbeitsteilung, durch Intransparenz und durch in allen Stadien ihrer verbrecherischen Tätigkeit vorherrschende Professionalität auszeichnet».[766] Die genannten Merkmale müssen nicht kumulativ erfüllt sein. Es genügt vielmehr, dass einzelne Kriterien bei einer qualitativen und quantitativen Gesamtbetrachtung auf ein entsprechendes Gefährdungspotenzial hinweisen.[767]

453 Das entscheidende Kriterium in der Abgrenzung der kriminellen zu legalen Organisationen liegt im Zweck der Organisation.[768] Das zentrale und in organisatorischen Vorkehrungen manifestierte Anliegen der Organisation muss gemäss Art. 260ter Abs. 1 lit. a StGB im Begehen von Gewaltverbrechen oder der Bereicherung mit verbrecherischen Mitteln oder im Begehen von Gewaltverbrechen zur Einschüchterung der Bevölkerung, zur Nötigung eines Staates oder einer internationalen Organisation bestehen.[769] Unter Gewaltverbrechen fallen Verbrechen im Sinne von Art. 10 Abs. 2 StGB, bei denen Gewalt

BSK StGB II-PIETH, Art. 305bis N 64; PK StGB-PIETH/SCHULTZE, Art. 305bis N 24; HK StGB-WOHLERS, Art. 305bis N 25.

766 BGE 132 IV 132 E. 4.1.1; 133 IV 235 E. 4.2; 129 IV 271 E. 2.3.1; Urteil des BGer 6B_238/2013 vom 22. November 2013 E. 9.1.1; vgl. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 717; EGGER TANNER, S. 208 f.; CR CP II-LIVET, Art. 260ter N 5; PAJAROLA, N 86; PK StGB-TRECHSEL/VEST, Art. 260ter N 4; AK StGB-UHRMEISTER, Art. 260ter N 2.

767 Botschaft organisierte Kriminalität 2018, S. 6471; BSK StGB II-ENGLER, Art. 260ter N 6; PAJAROLA, N 87 ff.; AK StGB-UHRMEISTER, Art. 260ter N 5; OFK StGB-WEDER, Art. 260ter N 10.

768 PAJAROLA, N 140; KV/KO StGB-PAJAROLA/OEHEN/THOMMEN, Art. 260ter N 345; STRATENWERTH/BOMMER, BT II, § 40 N 23.

769 BSK StGB II-ENGLER, Art. 260ter N 9 ff.; CR CP II-LIVET, Art. 260ter N 12a; PAJAROLA, N 143; KV/KO StGB-PAJAROLA/OEHEN/THOMMEN, Art. 260ter N 349 ff.; STRATENWERTH/BOMMER, BT II § 40 N 23; PK StGB-TRECHSEL/VEST, Art. 260ter N 6; AK StGB-UHRMEISTER, Art. 260ter N 6 f.; OFK StGB-WEDER, Art. 260ter N 20.

im strafrechtlichen Sinn angewendet wird.[770] Die Bereicherung mit verbrecherischen Mitteln erfasst als Verbrechen qualifizierte Vermögensdelikte sowie sonstige gewinnbringende Delikte, namentlich auch den schweren Fall der Geldwäscherei nach Art. 305bis Ziff. 2 StGB.[771] Der verbrecherische Zweck muss den Hauptzweck der Organisation bilden, was gleichwohl die Verfolgung legaler Nebenzwecke nicht ausschliesst.[772]

Der Qualifikationstatbestand nach Art. 305bis Ziff. 2 Abs. 2 lit. a StGB verlangt, dass der Geldwäschereitäter die Vermögenswerte als Mitglied der Verbrechensorganisation waschen muss, was erfordert, dass der Täter die Organisation nicht lediglich unterstützt, sondern sich an ihr beteiligt.[773] Insofern muss er in die Organisationsstruktur eingegliedert sein und eine Tätigkeit entfalten, die einen Beitrag zur Verfolgung des verbrecherischen Zwecks der Organisation leistet.[774] 454

Schliesslich müssen die Mitglieder Vorsatz hinsichtlich der Begehung von Geldwäscherei in ihrer Eigenschaft als Mitglieder einer Verbrechensorganisation aufweisen.[775] 455

1. Betreiberschaft als kriminelle oder terroristische Organisation

Es stellt sich die Frage, ob Betreiberschaften dezentralisierter Finanzanwendungen, die zur Geldwäscherei genutzt werden, als kriminelle oder terroristische Organisationen im Sinne von Art. 260ter StGB qualifiziert werden können. Bei einer Gesamtbetrachtung der vom Bundesgericht entwickelten Kriterien lässt sich ein gewisses Mindestmass an organisatorischer Struktur grundsätzlich bejahen. Der Betrieb eines dezentralisierten Protokolls erfordert 456

770 Dazu zählen namentlich Delikte wie Art. 111, 112, 122, 140, 156, 183-185 und 221 (vgl. Botschaft StGB 1993, S. 300; BSK StGB II-ENGLER, Art. 260ter N 10; CR CP II-LIVET, Art. 260ter N 15; PAJAROLA, N 155 ff.; STRATENWERTH/BOMMER, BT II, § 40 N 23; PK StGB-TRECHSEL/VEST, Art. 260ter N 7; AK StGB-UHRMEISTER, Art. 260ter N 6).

771 Mögliche Delikte stellen auch Art. 183-185, 195, 196, 240 ff. StGB sowie Art. 19 BetmG dar (vgl. Botschaft StGB 1993, S. 300; DONATSCH/THOMMEN/WOHLERS, S. 207 f.; BSK StGB II-ENGLER, Art. 260ter N 6; CR CP II-LIVET, Art. 260ter N 16; PAJAROLA, N 148 ff.; KV/KO StGB-PAJAROLA/OEHEN/THOMMEN, Art. 260ter N 361 ff.; PK StGB-TRECHSEL/VEST, Art. 260ter N 8).

772 BSK StGB II-ENGLER, Art. 260ter N 9; CR CP II-LIVET, Art. 260ter N 14; PAJAROLA, N 143; KV/KO StGB-PAJAROLA/OEHEN/THOMMEN, Art. 260ter N 347; PK StGB-TRECHSEL/VEST, Art. 260ter N 6.

773 BGE 129 IV 271 E. 2.4; Urteil des BGer 6S.365/2005 vom 8. Februar 2006 E. 2.3; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 719; EGGER TANNER, S. 210.

774 BGE 129 IV 271 E. 2.4; Urteil des BGer 6S.365/2005 vom 8. Februar 2006 E. 2.3; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 719.

775 BGE 146 IV 338 E. 4.4.1; 142 IV 175 E. 5.4.2; 129 IV 271 E. 2.5; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 720; BSK StGB II-ENGLER, Art. 260ter N 6; PAJAROLA, N 257 ff.; PK StGB-TRECHSEL/VEST, Art. 260ter N 11; AK StGB-UHRMEISTER, Art. 260ter N 13.

regelmässig eine funktionale Arbeitsteilung – etwa zwischen technischer Entwicklung, Systemwartung, Verwaltung von Vermögenswerten und Kommunikation – sowie ein hohes Mass an Koordination und technischer Expertise.[776] Auch eine gewisse Dauerhaftigkeit ist inhärent, da die Aufrechterhaltung des Betriebs typischerweise auf Kontinuität ausgelegt ist und nicht auf kurzfristiger Zusammenarbeit beruht. Ferner ist die personelle Intransparenz, etwa durch pseudonyme Beteiligte oder fehlende öffentliche Identifikation der Betreiberinnen, charakteristisch und kann das Gefährdungspotenzial im Sinne der Rechtsprechung erhöhen.[777] In vielen Fällen besteht zudem eine funktionale Austauschbarkeit der Mitglieder, da die Aufgaben nicht an bestimmte Personen gebunden sind und neue Beteiligte bestehende Rollen übernehmen können, ohne den Fortbestand der Anwendung zu gefährden. Demgegenüber fehlt es regelmässig an einer hierarchischen Struktur im Sinne einer Unterordnung unter Weisungen oder einer zentralisierten Entscheidungsgewalt. Der dezentralisierte Charakter der Aufgabenverteilung und die Abwesenheit einer Befehlskette sprechen gegen die Annahme einer hierarchisch organisierten Einheit im Sinne von Art. 260ter StGB.

457 Insgesamt kann somit festgehalten werden, dass Betreiberschaften zwar einzelne strukturelle Merkmale einer Organisation aufweisen und damit ein gewisses Gefährdungspotenzial entfalten können, die Einordnung als kriminelle Organisation im Sinne von Art. 260ter StGB jedoch letztlich vom verfolgten Zweck abhängt. Entscheidend ist daher, ob die Tätigkeit der Betreiberschaft auf die Begehung von Bereicherungs-, Gewalt- oder Terrorverbrechen ausgerichtet ist.

458 Da Betreiberinnen ausschliesslich auf digitaler Ebene handeln und ihr Tun sich im Betrieb bzw. in der Interaktion mit Smart Contracts erschöpft, kommt als Deliktskategorie einzig ein Bereicherungsverbrechen in Betracht. Dieses müsste – dem Verbrechenserfordernis entsprechend – eine qualifizierte Form der Geldwäscherei darstellen, etwa die gewerbsmässige Begehung im Sinne von Art. 305bis Ziff. 2 lit. c StGB.[778] Fraglich ist jedoch, ob die Begehung solcher Delikte den Hauptzweck der Betreiberschaft bildet. Dies lässt sich nur bei Anwendungen bejahen, deren gesamte Struktur auf die Verschleierung der Herkunft von Vermögenswerten und damit auf die Ermöglichung von Geldwäscherei ausgerichtet ist – etwa bei anonymisierenden Protokollen wie Mixer.[779] Bei

776 Vgl. vorne N 118 ff.

777 Vgl. vorne N 53.

778 PAJAROLA, N 149; vgl. DONATSCH/THOMMEN/WOHLERS, S. 207 f.; BSK StGB II-ENGLER, Art. 260ter N 6; PK StGB-TRECHSEL/VEST, Art. 260ter N 8; AK StGB-UHRMEISTER, Art. 260ter N 6.

779 Vgl. vorne N 89 ff.

den meisten dezentralisierten Finanzanwendungen fehlt es hingegen an einem solchen verbrecherischen Hauptzweck. Sie dienen primär der technischen Bereitstellung oder Verwaltung von Finanzdienstleistungen und weisen, soweit sie deliktisch missbraucht werden, lediglich eine faktische Missbrauchsanfälligkeit auf.[780] Diese genügt nicht, um eine Organisation im Sinne von Art. 260ter StGB zu begründen.

2. Betreiberinnen als Mitglieder krimineller oder terroristischer Organisationen

Im Weiteren stellt sich die Frage, ob Betreiberinnen dezentralisierter Finanz- 459
anwendungen, deren Dienste von einer kriminellen oder terroristischen Organisation genutzt werden, als Mitglieder dieser Organisation gelten könnten. Eine solche Einordnung setzt jedoch voraus, dass eine tatsächliche Eingliederung in die Organisationsstruktur besteht und die Betreiberinnen an der deliktischen Zweckverfolgung mitwirken.[781] Im vorliegenden Zusammenhang fehlt es an einer solchen Eingliederung, da Betreiberinnen dezentralisierter Protokolle ausserhalb der organisatorischen Struktur der kriminellen Gruppierung agieren, die ihre Anwendung allenfalls zu Geldwäschereizwecken nutzt. Selbst wenn die technische Infrastruktur deliktische Aktivitäten faktisch ermöglicht oder erleichtert, begründet dies keine strukturelle Zugehörigkeit zur Organisation. Mangels organisatorischer Einbindung und funktionaler Teilhabe an der Zweckverfolgung ist eine Qualifikation der Betreiberinnen als Mitglieder im Sinne von Art. 260ter StGB daher abzulehnen.

B. Bandenmitglied

Ein weiterer Qualifikationstatbestand liegt in der Begehung der Geldwäsche- 460
rei als Mitglied einer Bande, die sich zur fortgesetzten Ausübung dieses Delikts zusammengeschlossen hat (Art. 305bis Ziff. 2 lit. b StGB).[782] Der Begriff der Bande entspricht jenem, wie er in Art. 139 Ziff. 3 StGB, Art. 140 Ziff. 3 StGB sowie Art. 19 Abs. 2 lit. b BetmG verwendet wird.[783]

780 Vgl. vorne N 85 ff.

781 BGE 129 IV 271 E. 2.4; Urteil des BGer 6S.365/2005 vom 8. Februar 2006 E. 2.3; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 719.

782 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 723 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 52; EGGER TANNER, S. 210; GRABER, S. 151; AK StGB-GRAF, Art. 305bis N 23; OFK StGB-ISENRING, Art. 305bis N 70; BSK StGB II-PIETH, Art. 305bis N 65; PK StGB-PIETH/SCHULTZE, Art. 305bis N 25.

783 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 723; CR CP II-CASSANI/VILLARD, Art. 305bis N 53; EGGER TANNER, S. 210; KRONENBERG, S. 50; AK StGB-GRAF, Art. 305bis N 23; BSK StGB II-PIETH, Art. 305bis N 65.

461 Nach der Rechtsprechung des Bundesgerichts ist eine Bande gegeben, «wenn zwei oder mehrere Täter sich mit dem ausdrücklich oder konkludent geäusserten Willen zusammenfinden, inskünftig zur Verübung mehrerer selbständiger, im Einzelnen möglicherweise noch unbestimmter Straftaten zusammenzuwirken».[784] Erforderlich sind Mindestansätze einer organisatorischen Struktur sowie eine derartige Intensität des Zusammenwirkens, dass von einem stabilen, wenn auch allenfalls nur kurzlebigen Team gesprochen werden kann.[785] Nicht relevant ist, ob es sich dabei um einen hierarchisch oder demokratisch organisierten Zusammenschluss handelt und ob der deliktische Zweck der einzige und ursprüngliche Zweck davon ist.[786] Zweck der Qualifizierung ist die besondere Gefährlichkeit, welche sich daraus ergibt, dass der Zusammenschluss den Einzelnen psychisch und physisch stärkt und die fortgesetzte Verübung solcher Delikte voraussehen lässt.[787]

462 Der Qualifikationstatbestand nach Art. 305bis Ziff. 2 lit. b StGB verlangt darüber hinaus, dass es sich um eine Bande handelt, die sich gerade zum Zweck der fortgesetzten Begehung von Geldwäschereihandlungen zusammengefunden hat, und der Täter als Mitglied dieses Zusammenschlusses tätig wird.[788]

463 In subjektiver Hinsicht muss sich der Täter des Zusammenschlusses und dessen deliktischer Zielrichtung bewusst sein. So hat sein Vorsatz die bandenmässige Tatbegehung zu umfassen, was einen auf die gemeinsame Verübung mehrerer Delikte gerichteten Willen voraussetzt.[789]

464 Im vorliegenden Zusammenhang könnte zwar aufgrund der Vielzahl potenziell deliktischer Transaktionen sowie gewisser organisatorischer Ansätze auf Seiten der Betreiberschaft an Elemente einer Bande erinnert werden. Eine solche Qualifikation scheitert jedoch am zentralen Gefährlichkeitsmoment, das dem Bandenbegriff zugrunde liegt. Es fehlt an der psychisch-physischen Verstärkung der Beteiligten durch den Zusammenschluss, welcher

784 BGE 147 IV 176 E. 2.4.2; 135 IV 158 E. 2; 100 IV 219 E. 1; Urteil des BGer 6B_702/2021 vom 27. Januar 2023 E. 1.3.3; EGGER TANNER, S. 210; GODENZI, S. 143; KRONENBERG, S. 51; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 123; HK StGB-SCHLEGEL, Art. 139 N 13a.

785 BGE 147 IV 176 E. 2.4.2; 135 IV 158 E. 3.2; 132 IV 132 E. 5.2; KRONENBERG, S. 52; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 123; CR CP II-PAPAUX, Art. 139 N 77; AK StGB-SIMMLER/SELMAN, Vor Art. 137 ff. N 21; PK StGB-TRECHSEL/JENAL, Art. 139 N 16.

786 BGE 72 IV 110 E. 2; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 130; AK StGB-SIMMLER/SELMAN, Vor Art. 137 ff. N 21.

787 BGE 135 IV 158 E. 2; 132 IV 132 E. 5.2; 124 IV 86 E. 2b; Urteil des BGer 6B_1145/2016 vom 7. April 2017 E. 1.3; KRONENBERG, S. 52; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 126 f.

788 Urteil des BGer 6B_531/2013 vom 17. Februar 2014 E. 3; Urteil des BGer 6B_535/2014 vom 5. Januar 2016 E. 3.3; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 724; EGGER TANNER, S. 211; vgl. BSK StGB II-NIGGLI/RIEDO, Art. 139 N 129; vgl. auch GODENZI, S. 150 ff.

789 BGE 147 IV 176 E. 2.4.2; 135 IV 158 E. 2; 124 IV 86 E. 2b; CR CP II-PAPAUX, Art. 139 N 79; KRONENBERG, S. 54; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 131; HK StGB-SCHLEGEL, Art. 139 N 13b; PK StGB-TRECHSEL/JENAL, Art. 139 N 17.

die Begehung weiterer Delikte erleichtern oder fördern würde.[790] Bei dezentralisierten Finanzanwendungen – selbst in Fällen fortgesetzter geldwäschereirelevanter Nutzung wie bei Mixern – entfällt dieses Moment, da das Protokoll unabhängig von der Zahl und Interaktion der Beteiligten funktioniert. Angesichts der in Rechtsprechung und Lehre anerkannten engen Auslegung des Bandenbegriffs erscheint eine Einordnung als Bande im Sinne von Art. 305bis Ziff. 2 lit. b StGB daher nicht gerechtfertigt.[791] Allenfalls liesse sich in Konstellationen mit Multisignature-Administrationsstrukturen (das heisst Systemen, bei denen mehrere Personen ihre digitalen Signaturen leisten müssen, um eine Transaktion oder administrative Handlung freizugeben) eine gewisse wechselseitige Abhängigkeit annehmen.[792] Doch auch hier fehlt es regelmässig an jener psychischen Dynamik, die den Einzelnen in seinem deliktischen Willen bestärkt und die für das erhöhte Gefährdungspotenzial einer Bande charakteristisch ist.

C. Gewerbsmässige Geldwäscherei

Schliesslich liegt ein Qualifikationsgrund vor, wenn der Geldwäschereitäter gewerbsmässig vorgeht und dabei einen grossen Umsatz oder einen erheblichen Gewinn erzielt (Art. 305bis Ziff. 2 lit. c StGB).[793] Der Begriff der Gewerbsmässigkeit entspricht demjenigen in Art. 139 Ziff. 2 StGB, Art. 146 Abs. 2 StGB und Art. 19 Abs. 2 lit. c BetmG.[794] 465

Nach ständiger Rechtsprechung des Bundesgerichts ist Gewerbsmässigkeit gegeben, «wenn sich aus der Zeit und den Mitteln, die der Täter für die deliktische Tätigkeit aufwendet, aus der Häufigkeit der Einzelakte innerhalb eines bestimmten Zeitraums sowie aus den angestrebten und erzielten Einkünften ergibt, dass er die deliktische Tätigkeit nach Art eines Berufs ausübt».[795] 466

790 Vgl. BGE 135 IV 158 E. 2; KRONENBERG, S. 52; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 126 f.

791 Vgl. Urteil des BGer 6B_1145/2016 vom 7. April 2017 E. 1.3; Urteil des BGer 6B_510/2013 vom 3. März 2014 E. 3; STRATENWERTH/JENNY/BOMMER, BT I, § 13 N 100; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 122; AK StGB-SIMMLER/SELMAN, Vor Art. 137 ff. N 21.

792 Vgl. vorne N 128.

793 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 731; CR CP II-CASSANI/VILLARD, Art. 305bis N 55; EGGER TANNER, S. 210; GRABER, S. 151; AK StGB-GRAF, Art. 305bis N 24; OFK StGB-ISENRING, Art. 305bis N 72; BSK StGB II-PIETH, Art. 305bis N 66; PK StGB-PIETH/SCHULTZE, Art. 305bis N 26; HK StGB-WOHLERS, Art. 305bis N 26.

794 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 731; CR CP II-CASSANI/VILLARD, Art. 305bis N 56; AK StGB-GRAF, Art. 305bis N 24; CR CP II-PAPAUX, Art. 139 N 64; PK StGB-PIETH/SCHULTZE, Art. 305bis N 26.

795 BGE 129 IV 253 E. 2a; 123 IV 113 E. 2c; 119 IV 129 E. 3a; 117 IV 159 E. 2a; EGGER TANNER, S. 212; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 89; CR CP II-PAPAUX, Art. 139 N 66; AK StGB-SIMMLER/SELMAN, Vor Art. 137 ff. N 20; PK StGB-TRECHSEL/JENAL, Art. 146 N 33.

467 Erforderlich ist, dass der Täter die Absicht hat, durch sein deliktisches Verhalten regelmässige, nicht unerhebliche Einnahmen zu erzielen, die einen wesentlichen Beitrag zu seiner Lebensführung leisten. Hierbei muss es sich nicht um die Haupteinnahmequelle handeln; auch Nebeneinkünfte können genügen.[796] Die Geldwäschereitat muss bereits mehrfach begangen worden sein, und es muss aus den gesamten Umständen hervorgehen, dass der Täter zu einer Vielzahl an Geldwäschereihandlungen bereit gewesen wäre.[797]

468 Das Kriterium des grossen Umsatzes ist erfüllt, wenn Vermögenswerte von über CHF 100'000 gewaschen werden. Ein erheblicher Gewinn hingegen liegt bei einem Betrag von mehr als CHF 10'000 vor.[798]

469 Der Betrieb dezentralisierter Finanzanwendungen erfordert einen erheblichen und kontinuierlichen Einsatz von Zeit, technischen Mitteln und organisatorischen Ressourcen. Durch die Erhebung von Transaktionsgebühren oder anderen nutzungsabhängigen Entgelten erzielen die Betreiberinnen regelmässige Einnahmen.

470 Bietet eine Betreiberin eine Finanzanwendung ohne Beachtung der geldwäschereirechtlichen Sorgfaltspflichten an und ist diese somit schrankenlos zugänglich, liegt darin eine Bereitschaft, eine Infrastruktur bereitzustellen, über welche eine Vielzahl geldwäschereirelevanter Transaktionen abgewickelt werden kann. Die technische Architektur solcher Systeme ermöglicht unbegrenzt häufige Interaktionen der Nutzer mit den zugrunde liegenden Smart Contracts und damit die wiederholte Begehung gleichartiger Delikte.

471 Infolge dieser Automatisierung und der stetig anfallenden Gebühreneinnahmen lässt sich auch ohne individuelle Eingriffe ein fortlaufendes, einkommensorientiertes Handeln nach Art eines Berufs annehmen. Die Schwellenwerte eines grossen Umsatzes (über CHF 100'000) oder eines erheblichen Gewinns (über CHF 10'000) werden angesichts der bei dezentralisierten Anwendungen typischerweise hohen Transaktionsvolumina rasch erreicht.[799] Die planmässige Ausgestaltung des Betriebs sowie die auf Dauer angelegte

796 BGE 119 IV 129 E. 3a; 116 IV 319 E. 4b; 99 IV 80 E. 7; 79 IV 9 E. 1; EGGER TANNER, S. 213; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 99; AK StGB-SIMMLER/SELMAN, Vor Art. 137 ff. N 20; PK StGB-TRECHSEL/JENAL, Art. 146 N 33, 35.

797 BGE 147 IV 176 E. 2.2.1; 129 IV 188 E. 3.1.2; 129 IV 253 E. 2.2; 119 IV 129 E. 3a; Urteil des BGer 6B_1214/2019 vom 1. Mai 2020 E. 3.3; EGGER TANNER, S. 213; BSK StGB II-NIGGLI/RIEDO, Art. 139 N 95 ff.; CR CP II-PAPAUX, Art. 139 N 70; PK StGB-TRECHSEL/JENAL, Art. 146 N 35 f.

798 BGE 147 IV 176 E. 2.2.1; 129 IV 188 E. 3.1.3; 129 IV 253 E. 2.2; GRABER, S. 153; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 733 ff.; CR CP II-CASSANI/VILLARD, Art. 305bis N 59; EGGER TANNER, S. 214 f.; AK StGB-GRAF, Art. 305bis N 24; BSK StGB II-PIETH, Art. 305bis N 66.

799 Vgl. MEIRICH, N 264, 396, 1355 ff.; ANDREOTTI, S. 212; REGGIANI, S. 120.

Gebührenstruktur lassen dabei auf die Absicht schliessen, durch die fortgesetzte deliktische Tätigkeit regelmässige und nicht unerhebliche Einkünfte zu erzielen.

D. Weitere schwere Fälle

Neben den in Art. 305bis Ziff. 2 StGB ausdrücklich genannten Qualifikationstatbeständen können aufgrund des nicht abschliessenden Charakters der Bestimmung auch weitere schwere Fälle sui generis in Betracht fallen, sofern diese in objektiver und subjektiver Hinsicht gleich schwer wiegen wie die im Gesetz aufgeführten Beispiele.[800] In Übereinstimmung mit der Lehre könnte dies etwa dann zutreffen, wenn die Geldwäschereihandlung Vermögenswerte betrifft, die aus Kriegsverbrechen oder einem Genozid stammen, oder wenn sie im Zusammenhang mit kriminellen Organisationen erfolgt, ohne dass eine Mitgliedschaft im Sinne von Art. 305bis Ziff. 2 lit. a StGB besteht.[801] 472

Die Verwendung dezentralisierter Finanzanwendungen zur Umlagerung von Kryptowerten aus besonders schweren Vortaten ist in der Praxis naheliegend. Kryptowerte werden nachweislich im Zusammenhang mit bewaffneten Konflikten, der Umgehung internationaler Sanktionen sowie organisierter Kriminalität eingesetzt und anschliessend über intermediärsfreie oder anonymisierende Anwendungen verschleiert.[802] In solchen Konstellationen kommt die Anwendung der Generalklausel von Art. 305bis Ziff. 2 StGB grundsätzlich in Betracht. 473

E. Fazit

Im Ergebnis zeigt sich, dass die Qualifikationstatbestände von Art. 305bis Ziff. 2 StGB bei Betreiberinnen dezentralisierter Finanzanwendungen nur eingeschränkt Anwendung finden. Eine Einordnung als kriminelle oder terroristische Organisation scheitert am fehlenden verbrecherischen Hauptzweck der Betreiberschaft. Lediglich bei Anwendungen, deren gesamte Struktur auf 474

800 Urteil des BGer 6B_535/2014 vom 5. Januar 2016 E. 3.2.1; Urteil des BGer 6B_217/2013 vom 28. Juli 2014 E. 4.1; Urteil des BGer 6B_1013/2010 vom 17. Mai 2011 E. 6.2; vgl. BGE 114 IV 164 E. 2b; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 740; CR CP II-CASSANI/VILLARD, Art. 305bis N 47 ff.; EGGER TANNER, S. 216; AK StGB-GRAF, Art. 305bis N 21; BSK StGB II-PIETH, Art. 305bis N 66; PK StGB-PIETH/SCHULTZE, Art. 305bis N 27; HK StGB-WOHLERS, Art. 305bis N 24.

801 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 740 f.; CR CP II-CASSANI/VILLARD, Art. 305bis N 47; EGGER TANNER, S. 216; GRABER, S. 153 f.; AK StGB-GRAF, Art. 305bis N 21; PK StGB-PIETH/SCHULTZE, Art. 305bis N 27.

802 Vgl. KGGT, NRA 2024, S. 72 f.; KGGT, NRA 2018, S. 27 f.

die Verschleierung von Vermögenswerten ausgerichtet ist – etwa bei Kryptomixern –, liesse sich dies bejahen. Die Annahme einer Bande scheidet angesichts des eng auszulegenden Gefährlichkeitsmoments aus.

475 Demgegenüber erscheint die gewerbsmässige Geldwäscherei als praktisch relevantester Qualifikationsgrund. Die dauerhafte Bereitstellung einer automatisierten, gebührenbasierten Infrastruktur lässt auf ein planmässiges, einkommensorientiertes Handeln schliessen, bei dem die Schwellenwerte für erheblichen Gewinn oder Umsatz rasch erreicht werden können.

476 Sofern Vermögenswerte aus einem Genozid oder Kriegsverbrechen stammen, kann schliesslich auch eine Qualifikation über die Generalklausel in Betracht fallen.

II. Konkurrenzen

477 Der nachfolgende Abschnitt befasst sich zunächst mit dem Konkurrenzverhältnis zwischen Gehilfenschaft und täterschaftlicher Unterlassung, wenn beide an dieselbe Geldwäschereihandlung eines Nutzers anknüpfen. Danach wird erörtert, wie mehrere geldwäschereirelevante Handlungen verschiedener Nutzer konkurrenzrechtlich einzuordnen sind und welche Bedeutung dabei der Qualifikation der Gewerbsmässigkeit zukommt. Abschliessend widmet sich der letzte Teil dem Konkurrenzverhältnis zwischen der Geldwäscherei nach Art. 305bis StGB und eigenständig sanktionierten Verletzungen geldwäschereirechtlicher Sorgfaltspflichten nach Art. 305ter StGB sowie Art. 37 GwG.

A. Gehilfenschaft und täterschaftliche Unterlassung

478 Bei Betreiberinnen bestimmter dezentralisierter Anwendungen – etwa deliktisch konzipierter Kryptomixer – kann sich eine Strafbarkeit nach Art. 305bis StGB sowohl aus der Bereitstellung der Finanzanwendung als auch aus pflichtwidriger Untätigkeit ergeben. Fraglich ist, in welchem Konkurrenzverhältnis diese beiden strafbaren Verhaltensweisen zueinanderstehen.

479 Von echter Konkurrenz im Sinne von Art. 49 Abs. 1 StGB spricht man, wenn der Täter mehrere nebeneinander anwendbare, sich nicht gegenseitig ausschliessende Tatbestände verwirklicht, was entweder durch eine einheitliche Handlung (Idealkonkurrenz) oder durch mehrere voneinander unabhängige Handlungen (Realkonkurrenz) geschehen kann.[803] Unechte Konkurrenz liegt dagegen vor, wenn das Verhalten zwar mehrere Tatbestände erfüllt, der

803 DONATSCH/GODENZI/TAG, S. 428; STRATENWERTH/BOMMER, AT I, § 19 N 1; TRECHSEL et al., S. 301 ff.; PK StGB-TRECHSEL/SEELMANN, Art. 49 N 2.

Unrechtsgehalt der Tat jedoch bereits durch einen oder mehrere Tatbestände vollständig erfasst wird, sodass die übrigen aus Gründen der Spezialität, Konsumtion, Subsidiarität oder Alternativität zurücktreten.[804]

Subsidiarität besteht, wenn ein Tatbestand nur Anwendung findet, sofern kein anderer vorrangig eingreift.[805] Eine typische Fallgruppe ergibt sich im Verhältnis der Beteiligungsformen: Die leichtere – etwa die Gehilfenschaft oder Anstiftung – wird von der Täterschaft verdrängt.[806] 480

Begeht die Betreiberin im Zusammenhang mit derselben Haupttat eines Nutzers sowohl eine Gehilfenschaft als auch eine täterschaftliche Unterlassung, tritt die Gehilfenschaft aufgrund ihres subsidiären Charakters hinter die täterschaftliche Verantwortlichkeit zurück. Schuldspruch und Strafe richten sich folglich ausschliesslich nach der (täterschaftlich) begangenen Geldwäscherei durch Unterlassen.[807] 481

B. Mehrfache Geldwäscherei

Begeht die Betreiberin Geldwäscherei – sei es durch die Bereitstellung der Anwendung oder durch pflichtwidriges Untätigbleiben – in Zusammenhang mit mehreren, voneinander unabhängigen Geldwäschereihandlungen verschiedener Nutzer, stellt sich die Frage nach dem Konkurrenzverhältnis dieser Einzeldelikte untereinander und zu einem allfälligen Qualifikationstatbestand der Gewerbsmässigkeit. 482

Bei der Idealkonkurrenz verwirklicht der Täter durch eine einzelne Handlung bzw. durch ein einheitliches, zusammengehörendes Tun entweder mehrere verschiedene Tatbestände (ungleichartige Idealkonkurrenz) oder denselben Tatbestand mehrfach (gleichartige Idealkonkurrenz).[808] 483

Realkonkurrenz liegt dagegen vor, wenn der Täter durch mehrere voneinander unabhängige Handlungen entweder denselben Tatbestand mehrmals oder verschiedene Tatbestände erfüllt.[809] Entscheidend ist, ob das Verhalten 484

804 DONATSCH/GODENZI/TAG, S. 428; POPP, S. 191; CR CP I-STOLL, Art. 49 N 50 ff.; STRATENWERTH/BOMMER, AT I, § 18 N 5 ff.

805 BSK StGB I-ACKERMANN, Art. 49 N 50; DONATSCH/GODENZI/TAG, S. 428; GRAVEN/STRÄULI, S. 338 f.; vgl. BGE 125 IV 124 E. 2c; 105 IV 248 E. 1; 93 IV 39 E. 2.

806 STRATENWERTH/BOMMER, AT I, § 18 N 10, § 13 N 163; BSK StGB I-ACKERMANN, Art. 49 N 63; HK StGB-WOHLERS, Vor Art. 49 N 5; vgl. BGE 104 IV 72 E. 1; 101 IV 47 E. 4b; 93 IV 39 E. 2.

807 BSK StGB I-ACKERMANN, Art. 49 N 68; DONATSCH/GODENZI/TAG, S. 429; PK StGB-TRECHSEL/SEELMANN, Art. 49 N 2; vgl. Urteil des BGer 6B_614/2019 vom 3. Dezember 2019 E. 2.4.2.

808 BGE 133 IV 297 E. 4.1; DONATSCH/GODENZI/TAG, S. 437; BSK StGB I-ACKERMANN, Art. 49 N 76; PK StGB-TRECHSEL/SEELMANN, Art. 49 N 1.

809 BGE 133 IV 297 E. 4.1; DONATSCH/GODENZI/TAG, S. 433; CR CP I-STOLL, Art. 49 N 7; STRATENWERTH/BOMMER, AT I, § 19 N 7; HK StGB-WOHLERS, Vor Art. 49 N 11.

als Handlungseinheit oder als Handlungsmehrheit zu qualifizieren ist. Eine natürliche Handlungseinheit nimmt die Rechtsprechung an, wenn mehrere Einzelhandlungen «auf einem einheitlichen Willensakt beruhen und wegen des engen räumlichen und zeitlichen Zusammenhangs bei objektiver Betrachtung als einheitliches Geschehen erscheinen».[810]

485 Wenn die Betreiberin also durch eine einmalige Protokollbereitstellung mehreren Nutzern Gehilfenschaft zu verschiedenen Geldwäschereihandlungen leistet, liegt gleichartige Idealkonkurrenz vor.[811]

486 Bleibt sie hingegen bei mehreren voneinander unabhängigen Geldwäschereihandlungen verschiedener Nutzer pflichtwidrig untätig, ist zu prüfen, ob eine Unterlassungseinheit vorliegt. Diese besteht, wenn der Täter mehrere Handlungsmöglichkeiten ungenutzt lässt, um denselben Erfolg abzuwenden.[812] Im vorliegenden Zusammenhang betrifft das Unterlassen jedoch jeweils unterschiedliche, voneinander unabhängige Geldwäschereidelikte. Es fehlt somit an einem identischen Unrechtserfolg, weshalb Realkonkurrenz anzunehmen ist. Auch eine natürliche Handlungseinheit liegt nicht vor, da die Delikte der Nutzer weder in engem zeitlichem noch räumlichem Zusammenhang stehen.

487 Verwirklicht die Betreiberin somit den Tatbestand der Geldwäscherei – sei es durch Gehilfenschaft oder durch Unterlassen – mehrfach aufgrund unabhängiger Handlungen verschiedener Nutzer, greift keine der Fallgruppen der unechten Konkurrenz. Der einzige Zusammenhang zwischen den strafbaren Verhaltensweisen liegt in der Person der Betreiberin.[813] Es ist daher von echter Konkurrenz auszugehen, womit eine Strafschärfung gemäss Art. 49 Abs. 1 StGB zur Anwendung gelangt.[814]

488 Art. 49 StGB findet indes trotz echter Konkurrenz keine Anwendung, wenn eine Strafschärfung bereits aufgrund des Vorliegens des Qualifikationstatbestands der gewerbsmässigen Geldwäscherei nach Art. 305bis Ziff. 2 lit. c StGB vorgegeben ist.[815]

---

810 BGE 133 IV 256 E. 4.5.3; 131 IV 83 E. 2.4.5; Urteil des BGer 6B_1200/2021 vom 15. September 2023 E. 3.2; AK StGB-SIMMLER/SELMAN, Art. 49 N 3; CR CP I-STOLL, Art. 49 N 8; STRATENWERTH/BOMMER, AT I, § 19 N 12.

811 Vgl. auch BGE 124 IV 145 E. 3a; HK StGB-WOHLERS, Vor Art. 49 N 10.

812 BSK StGB I-ACKERMANN, Art. 49 N 29; POPP, S. 190.

813 Vgl. STRATENWERTH/BOMMER, AT I, § 19 N 8.

814 DONATSCH/GODENZI/TAG, S. 429 f.; BSK StGB I-ACKERMANN, Art. 49 N 77; AK StGB-SIMMLER/SELMAN, Art. 49 N 7 ff.; PK StGB-TRECHSEL/SEELMANN, Art. 49 N 7 ff.

815 BGE 116 IV 121, E. 2b/aa; Urteil des BGer 6B_1214/2021 vom 26. Oktober 2022 E. 2.1.5; Urteil des BGer 6B_1366/2016 vom 6. Juni 2017 E. 4.4.2; DONATSCH/GODENZI/TAG, S. 435; AK StGB-SIMMLER/SELMAN, Art. 49 N 6; STRATENWERTH/BOMMER, AT I, § 19 N 18.

C. Konkurrenztatbestände bei Sorgfaltspflichtverletzungen

Eine Strafbarkeit der Geldwäscherei durch Unterlassen nach Art. 305bis StGB setzt im vorliegenden Kontext voraus, dass die Betreiberin geldwäschereirechtliche Handlungspflichten pflichtwidrig unterlässt. Die Verletzung solcher Sorgfaltspflichten ist indes teilweise eigenständig sanktioniert und kann daher neben den Geldwäschereitatbestand treten. So macht sich etwa strafbar, wer als Finanzintermediärin die nach den Umständen gebotene Sorgfalt zur Feststellung der Identität der wirtschaftlich berechtigten Person verletzt (Art. 305ter Abs. 1 StGB). Ebenso unterliegt die Verletzung der Meldepflicht nach Art. 9 GwG einer eigenständigen Sanktion nach Art. 37 GwG. In beiden Konstellationen stellt sich die Frage nach dem Konkurrenzverhältnis zu Art. 305bis StGB. 489

Werden sowohl der Tatbestand von Art. 305bis StGB als auch jener von Art. 305ter StGB erfüllt, tritt gemäss den Materialien sowie einhelliger Doktrin der Tatbestand der mangelnden Sorgfalt bei Finanzgeschäften nach Art. 305ter StGB in unechter Konkurrenz hinter den Geldwäschereitatbestand zurück.[816] 490

Strittig ist indes das Konkurrenzverhältnis zwischen Art. 305bis StGB und Art. 37 GwG. In den Materialien sowie in Teilen der Lehre wird eingewendet, eine unechte Konkurrenz führe zu einer sachlich nicht gerechtfertigten Privilegierung der bloss meldepflichtigen Finanzintermediärin gegenüber einer Geldwäscherin ohne Eigenschaft der Finanzintermediärin.[817] Dem ist jedoch entgegenzuhalten, dass Art. 37 GwG und Art. 305bis StGB die gleichen Interessen schützen,[818] weshalb die Übertretung nach Art. 37 GwG hierbei folgerichtig aufgrund unechter Konkurrenz vom Geldwäschereitatbestand als Vergehen bzw. (bei Qualifikation) Verbrechen konsumiert wird.[819] 491

D. Fazit

Zusammenfassend ist festzuhalten, dass bei Betreiberinnen dezentralisierter Finanzanwendungen eine Strafbarkeit wegen Gehilfenschaft hinter die täterschaftliche Unterlassung zurücktritt, sofern beide Handlungsformen 492

816 Botschaft 1989, S. 1090; Urteil des BStGer SK.2004.13 vom 6. Juni 2005 E. 4.1; CR CP II-CASSANI/VILLARD, Art. 305bis N 67; EGGER TANNER, S. 237 f.; GRABER, S. 213; BSK StGB II-PIETH, Art. 305ter N 36; AK StGB-GRAF, Art. 305ter N 19.

817 Votum Villiger (BR), AB 1997 S. 606; gl.M. KV/KO GwG-HUTZLER, Art. 9 N 149; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 698; vgl. auch THOMMEN, S. 430; VON ROTZ, S. 147.

818 Vgl. hierzu die Ausführungen unter N 176; vgl. auch OFK GwG-FINGERHUTH, Art. 37 N 1; SHK GwG-HILF, Art. 37 N 2.

819 Gl.M. SHK GwG-HILF, Art. 37 N 38; CR CP II-CASSANI/VILLARD, Art. 305bis N 68; CR LBA-GARBARSKI/MACALUSO, Art. 37 N 53; BSK GwG-PEYER, Art. 37 N 53; THOMMEN, S. 430.

dieselbe Haupttat des Nutzers betreffen. Liegen hingegen mehrere voneinander unabhängige Geldwäschereihandlungen verschiedener Nutzer vor, bei denen sich die Betreiberin jeweils entweder durch Gehilfenschaft oder durch pflichtwidriges Unterlassen strafbar macht, ist grundsätzlich von echter Konkurrenz auszugehen. Eine Strafschärfung nach Art. 49 Abs. 1 StGB entfällt jedoch, wenn bereits der Qualifikationstatbestand der gewerbsmässigen Geldwäscherei erfüllt ist, welcher den erhöhten Unrechtsgehalt fortgesetzter deliktischer Tätigkeit abschliessend erfasst. Soweit neben Art. 305bis StGB auch eigenständig sanktionierte Sorgfaltspflichtverletzungen einschlägig sind, stehen Art. 305ter StGB und Art. 37 GwG in unechter Konkurrenz zum Geldwäschereitatbestand und treten hinter diesen zurück.

III. Strafanwendungsrecht

493 Im Folgenden ist zu klären, unter welchen Voraussetzungen Betreiberinnen dezentralisierter Finanzanwendungen, die sich einer Geldwäscherei durch Unterlassen strafbar machen, der schweizerischen Strafhoheit unterliegen. Dazu wird zunächst geprüft, wann eine solche Konstellation als Inlandtat im Sinne von Art. 3 i.V.m. Art. 8 StGB zu qualifizieren ist. Anschliessend wird untersucht, ob und in welchen Fällen eine Zuständigkeit über die Regeln der extraterritorialen Strafanwendung (Art. 4-7 StGB) eröffnet sein kann. Die Analyse folgt damit der Unterscheidung zwischen Inland- und Auslandtaten und berücksichtigt sowohl Unterlassungstäterschaft als auch Gehilfenschaft.

A. Inlandtaten

494 Die Anwendbarkeit des schweizerischen Strafrechts bei Verstössen gegen Art. 305bis StGB richtet sich nach den allgemeinen Bestimmungen des Schweizerischen Strafgesetzbuches, das heisst nach den Art. 3-8 StGB.[820] Die wichtigste Anknüpfungsregel im Bereich der Geldwäscherei bildet das in Art. 3 Abs. 1 StGB verankerte Territorialitätsprinzip, wonach auf den Begehungsort der Straftat in der Schweiz abgestellt wird.[821]

820 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 790; CR CP II-CASSANI/VILLARD, Art. 305bis N 60; BSK StGB II-PIETH, Art. 305bis N 68b; STRATENWERTH/BOMMER, AT I, § 5 N 5.

821 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 791; DONATSCH/GODENZI/TAG, S. 54, 67; AK StGB-SIMON, Art. 3 N 7; TRECHSEL et al., S. 69; vgl. auch BGE 121 IV 145 E. 2b/bb; 118 Ia 137 E. 2a; 111 IV 1 E. 2a; 99 IV 123 E. 1a.

1. Unterlassung

Im Kontext von Unterlassungsdelikten wird dieses Prinzip in Art. 8 Abs. 1 StGB konkretisiert: Es ist auf denjenigen Ort abzustellen, an dem der Täter pflichtwidrig untätig bleibt, resp. denjenigen, wo er hätte handeln müssen.[822] Ist die gebotene Handlung nicht an einen bestimmten Ort gebunden, gilt nach bundesgerichtlicher Rechtsprechung als Handlungsort jeder bis zu diesem Zeitpunkt faktisch gewählte, vorübergehende Aufenthaltsort des Unterlassungstäters.[823] 495

Daneben kann beim unechten Unterlassungsdelikt auch der Erfolgsort einen Anknüpfungspunkt für die Zuständigkeit bilden.[824] Während die ältere Rechtsprechung den Erfolgsbegriff im Zusammenhang mit Art. 8 StGB noch einem engen, technischen Verständnis zuführte,[825] versteht die neuere Praxis des Bundesgerichts Erfolg in einem weiteren Sinne und bejaht einen Erfolgsort auch bei Tätigkeits- und abstrakten Gefährdungsdelikten.[826] Nach dieser Rechtsprechung findet sich ein territorialer Anknüpfungspunkt bei Geldwäscherei auch am Erfolgsort, also an dem Ort, wo sich die Folgen der Vereitelungshandlung auf die Vermögenswerte auswirken.[827] 496

Bei Betreiberinnen von dezentralisierten Protokollen, die sich der Geldwäscherei durch Unterlassung strafbar machen, können sich nach den zuvor erläuterten Grundsätzen der Art. 3 und Art. 8 StGB drei territoriale Anknüpfungspunkte für eine schweizerische Zuständigkeit ergeben: Dazu zählen der Ort der pflichtwidrigen Untätigkeit der Betreiberinnen, der Ort – im Sinne des weiten Erfolgsbegriffs –, an dem sich die Folgen der Vereitelungshandlung auswirken, sowie der Handlungsort des Nutzers. 497

822 BGE 141 IV 205 E. 5.2; 125 IV 14 E. 2c/aa; Urteil des BGer 6B_556/2021 vom 5. Januar 2022 E. 1.2; Urteil des BGer 6B_1045/2014 vom 19. Mai 2015 E. 5.2; DONATSCH/GODENZI/TAG, S. 56; CR CP I-HARARI / LINIGER GROS, Art. 8 N 20; BSK StGB I-POPP/KESHELAVA, Art. 8 N 11; AK StGB-SIMON, Art. 8 N 4; STRATENWERTH/BOMMER, AT I, § 5 N 7; TRECHSEL et al., S. 69 f.; PK StGB-TRECHSEL/VEST, Art. 8 N 5.

823 GLESS, N 166; BSK StGB I-POPP/KESHELAVA, Art. 8 N 11; AK StGB-SIMON, Art. 8 N 4; vgl. BGE 141 IV 205 E. 5.2; Urteil des BGer 6B_123/2014 vom 2. Dezember 2014 E. 2.3.

824 BSK StGB I-POPP/KESHELAVA, Art. 8 N 12; TRECHSEL et al., S. 69 f.; vgl. AK StGB-SIMON, Art. 8 N 7.

825 CR CP I-HARARI / LINIGER GROS, Art. 8 N 26 f.; AK StGB-SIMON, Art. 8 N 6; STRATENWERTH/BOMMER, AT I, § 5 N 5; vgl. BGE 105 IV 326 E. 3c; 118 Ia 141.

826 STRATENWERTH/BOMMER, AT I, § 5 N 5; DONATSCH/GODENZI/TAG, S. 55; CR CP I-HARARI / LINIGER GROS, Art. 8 N 30 ff.; AK StGB-SIMON, Art. 8 N 7; vgl. BGE 141 IV 336 E. 1.1; 128 IV 145 E. 2e; 125 IV 177 E. 2; 124 IV 241 E. 4c; Urteil des BGer 6B_44/2022 vom 20. Dezember 2022 E. 2.4; Urteil des BGer 6B_659/2014 vom 22. Dezember 6.2.1.

827 Urteil des BGer 6B_880/2018 vom 31. Oktober 2018 E. 4.1 m.V.a. DYENS, N 1084; vgl. Urteil des Cour de Justice (GE) ACPR/710/2018 vom 30. November 2018 E. 4.1.4; BACHARACH, S. 230; CR CP I-HARARI / LINIGER GROS, Art. 8 N 34e; VILLARD, S. 157 f.

498 Eine räumliche Anwendbarkeit des Strafgesetzbuches besteht zunächst, wenn die Betreiberinnen in der Schweiz hätten handeln müssen.[828] Dies ist der Fall, sofern sie eine Garantenstellung gestützt auf das schweizerische Geldwäschereigesetz innehaben und daraus resultierende Handlungspflichten nicht erfüllt wurden.[829] Damit korrespondiert die territoriale Anknüpfung im Strafrecht mit der örtlichen Unterstellung unter das Geldwäschereigesetz.[830] Eine solche ergibt sich gemäss Art. 2 Abs. 1 lit. a GwV, wenn eine finanzintermediäre Tätigkeit in der Schweiz ausgeübt oder von der Schweiz aus betrieben wird.[831] Vorausgesetzt ist eine physische Präsenz von gewisser Dauerhaftigkeit, etwa durch Wohnsitz oder formelle Niederlassung in der Schweiz. Eine solche Präsenz kann sich auch in Form einer faktischen Zweigniederlassung manifestieren, wenn Personen in der Schweiz dauerhaft für die Betreiberin tätig sind oder von hier aus wesentliche Funktionen ausüben.[832] Bei idealtypisch dezentralen Anwendungen – also solchen ohne zentrale Kontroll- oder Eingriffsmöglichkeiten und mit unveränderlichen Smart Contracts – kann ein territorialer Bezug höchstens im Zeitpunkt der initialen Bereitstellung der Smart Contracts bestehen, was regelmässig nicht genügt, um eine Dauerhaftigkeit zu begründen.[833] Im Vergleich dazu können bei Anwendungen mit zentralisierenden Elementen Anknüpfungspunkte über Personen entstehen, die über Admin Keys oder sonstige Eingriffsmöglichkeiten verfügen, deren Tätigkeit für das Funktionieren der Smart Contracts unerlässlich ist (etwa durch das Betreiben von Interfaces oder die Bereitstellung technischer Infrastruktur).[834] Werden für den fortlaufenden Betrieb Server oder vergleichbare Infrastruktur dauerhaft in der Schweiz betrieben, kann diese technische Verankerung als funktionales Äquivalent einer faktischen Niederlassung qualifiziert werden

828 Vgl. BGE 141 IV 205 E. 5.2; 125 IV 14 E. 2c/aa; Urteil des BGer 6B_556/2021 vom 5. Januar 2022 E. 1.2; Urteil des BGer 6B_1045/2014 vom 19. Mai 2015 E. 5.2; DONATSCH/GODENZI/TAG, S. 56; CR CP I-HARARI/LINIGER GROS, Art. 8 N 20; BSK StGB I-POPP/KESHELAVA, Art. 8 N 11; AK StGB-SIMON, Art. 8 N 4; STRATENWERTH/BOMMER, AT I, § 5 N 7; TRECHSEL et al., S. 69; PK StGB-TRECHSEL/VEST, Art. 8 N 5.

829 Vgl. vorne N 307 ff.

830 Vgl. auch GLESS/BACHMANN, N 21.56 ff.

831 Vgl. STENGEL/PAYDAR, N 18.34; CR LBA-CASSANI, Art. 1 N 19; BSK GwG-GRETER, Art. 2 Abs. 3 N 51; SHK GwG-SCHÄREN, Art. 2 N Fn. 59; ZYSSET/NAGEL, S. 144; vgl. auch FINMA-RS 11/1.

832 FINMA-RS-11/2, N 28.2 f.; CR LBA-CASSANI, Art. 1 N 20 ff.; BSK GwG-GRETER, Art. 2 Abs. 3 N 48 f.; MEIRICH, N 699 ff.; SHK GwG-SCHÄREN, Art. 2 N 67 ff.; OFK GwG-WYSS, Art. 2 N 3; ZYSSET/NAGEL, S. 145 f.

833 Vgl. vorne N 355; MEIRICH, N 666.

834 Vgl. vorne N 355; NOSER/INFANGER/LÜDI, N 12.33.

und damit den territorialen Anwendungsbereich des schweizerischen Strafrechts eröffnen.[835]

Eine schweizerische Zuständigkeit kann sich ferner aus dem Handlungsort des Nutzers im Sinne des Erfolgsortes ergeben, sofern das Delikt des Dritten – also die Geldwäschereihandlung des Nutzers – in der Schweiz ausgeführt wird.[836] Als Handlungsort gilt der Ort, an dem sich der Täter während der tatbestandsmässigen Handlung physisch befindet.[837] Im vorliegenden Zusammenhang ist dies gegeben, wenn der Nutzer sich in der Schweiz befindet und von hier aus mit dem Smart Contract interagiert, indem er die Transaktion signiert und an das Netzwerk übermittelt.[838] Damit ist grundsätzlich auch bei ausländischen Finanzintermediären nicht ausgeschlossen, dass sich eine schweizerische Strafgewalt begründen lässt.[839] 499

Schliesslich kann das schweizerische Strafrecht auch dann Anwendung finden, wenn sich die Vereitelungswirkung auf Vermögenswerte in der Schweiz auswirkt.[840] In diesem Zusammenhang ist erneut auf die bereits erläuterten Kriterien zur Lokalisierung dezentralisierter Protokolle im schweizerischen Territorium abzustellen.[841] 500

2. Gehilfenschaft

Bei der Gehilfenschaft stellt die ständige Rechtsprechung des Bundesgerichts angesichts ihres akzessorischen Charakters auf den Begehungsort der Haupttat ab.[842] Die herrschende Lehre verlangt indes über den Wortlaut hinaus, dass 501

835 Vgl. DONATSCH/GODENZI/TAG, S. 56; DYENS, N 675, 680; HEIMGARTNER, S. 126 f.; SCHWARZENEGGER, S. 119 ff.; insbesondere zur Bedeutung in der Schweiz betriebener Server für das Vorgehen der Strafverfolgungsbehörden vgl. auch COVIELLO/MÄDER/BAUMGARTNER.

836 Vgl. vorne N 296; vgl. auch PK StGB-TRECHSEL/FATEH-MOGHADAM, Art. 11 N 2; BSK StGB I-NIGGLI/MUSKENS, Art. 11 N 41.

837 DONATSCH/GODENZI/TAG, S. 54; GLESS/BACHMANN, N 21.18; AK StGB-SIMON, Art. 8 N 3; TRECHSEL et al., S. 70; HK StGB-WOHLERS, Art. 8 N 2; vgl. Urteil des BGer 6B_252/2022 vom 11. April 2023 E. 2.3.1; Urteil des BGer 6B_44/2022 vom 20. Dezember 2022 E. 2.1; Urteil des BGer 6B_45/2021 vom 27. April 2022 E. 3.1; Urteil des BGer 6B_86/2009 vom 29. Oktober 2009 E. 2.3.

838 Vgl. GLESS/BACHMANN, N 21.20, CASSANI/VILLARD, N 1.34; DONATSCH/GODENZI/TAG, S. 54; CR CP I-HARARI / LINIGER GROS, Art. 8 N 41; HEIMGARTNER, S. 122; SCHWARZENEGGER, S. 118; TRECHSEL et al., S. 70.

839 GLESS/BACHMANN, N 21.57; CASSANI/VILLARD, N 1.59; MACALUSO, S. 119 f.

840 Urteil des BGer 6B_880/2018 vom 31. Oktober 2018 E. 4.1 m.V.a. DYENS, N 1084; vgl. Urteil des Cour de Justice (GE) ACPR/710/2018 vom 30. November 2018 E. 4.1.4; BACHARACH, S. 230; CR CP I-HARARI / LINIGER GROS, Art. 8 N 34e; VILLARD, S. 157 f.

841 Vgl. BACHARACH, S. 231 f.

842 BGE 144 IV 265 E. 2; 108 Ib 301 E. 5; 104 IV 77 E. 7b; 81 IV 37; 80 IV 34; Urteil des BGer 6B_86/2009 vom 29. Oktober 2009 E. 2.3.

die Haupttat auch am Ort des Teilnehmerhandelns strafbar sei.[843] Der bundesgerichtlichen Linie ist jedoch zu folgen. Zum einen entspricht sie dem akzessorischen Charakter der Teilnahmehandlungen. Zum anderen hat der Gesetzgeber im Rahmen der Revision des Allgemeinen Teils des Strafgesetzbuches nicht nur bewusst darauf verzichtet, die im Vorentwurf vorgeschlagene Norm zur Teilnahme an Auslandtaten in das Gesetz aufzunehmen, sondern ausdrücklich klargestellt, dass eine solche Verknüpfung «in einem anderen Zusammenhang» geregelt werden muss und dies nicht im Wege einer Ergänzung von Art. 3 StGB geschehen kann.[844]

502 Stellt man, dem Bundesgericht folgend, auf den Begehungsort des Täters ab, ist im vorliegenden Kontext auf den Ort der geldwäschereirelevanten Handlung des Nutzers abzustellen, mithin auf den physischen Ort, an dem er mit den Smart Contracts interagiert. Darüber hinaus kann – trotz Fehlens eines Erfolgs im engeren Sinn – gemäss bundesgerichtlicher Rechtsprechung auch am Ort angeknüpft werden, an dem sich die Vereitelungswirkung auf inländische Vermögenswerte auswirkt. Gemeint ist derjenige Ort, wo das Protokoll betrieben bzw. administriert wird, einschliesslich des Standorts jener Server-Infrastruktur – sofern vorhanden –, über welche der Betrieb oder administrative Kernfunktionen der Anwendung abgewickelt werden.[845]

B. Extraterritoriale Strafanwendung

503 Soweit eine Tat nicht nach den zuvor dargestellten Grundsätzen als Inlandtat zu qualifizieren ist, liegt eine Auslandtat vor. Die Voraussetzungen einer extraterritorialen Strafanwendung sind in den Art. 4–7 StGB geregelt.[846] Eine schweizerische Zuständigkeit kann sich somit ergeben, wenn es sich um ein Staatsschutzdelikt (Art. 4 StGB), eine Straftat gegen Minderjährige (Art. 5 Abs. 1 StGB), eine aufgrund staatsrechtlicher Verpflichtung zu verfolgende Tat (Art. 6 StGB) oder subsidiär um eine andere Auslandtat im Sinne von Art. 7 StGB handelt.[847]

843 CASSANI/VILLARD, N 1.54; DONATSCH/GODENZI/TAG, S. 57; CR CP I-HARARI / LINIGER GROS, Art. 8 N 54; HURTADO POZO/GODEL, N 174; BSK StGB I-POPP/KESHELAVA, Art. 8 N 16.

844 Vgl. Botschaft StGB 1998, S. 1992; Bundesamt für Justiz, Bericht 1993, S. 17; BGE 144 IV 265 E. 2; vgl. auch CR CP I-HARARI / LINIGER GROS, Art. 8 N 54; DONATSCH/GODENZI/TAG, S. 57; STRATENWERTH/BOMMER, AT I, § 5 N 90.

845 Vgl. vorne N 499.

846 DONATSCH/GODENZI/TAG, S. 51; GLESS/BACHMANN, N 21.65; AK StGB-SIMON, Art. 3 N 2 f.; HK StGB-WOHLERS, Vor Art. 3 N 2.

847 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 791; DONATSCH/GODENZI/TAG, S. 58 ff.; GLESS/BACHMANN, N 21.66; STRATENWERTH/BOMMER, AT I, § 5 N 10 ff.; TRECHSEL et al., S. 66 ff.

Im Kontext der Geldwäscherei scheiden mehrere dieser Konstellationen bereits dem Gegenstand nach aus. So handelt es sich dabei weder um ein Staatsschutzdelikt im Sinne von Art. 4 StGB noch um eine Straftat gegen Minderjährige nach Art. 5 StGB. Auch eine Strafverfolgungspflicht gestützt auf staatsvertragliche Verpflichtungen im Sinne von Art. 6 StGB besteht nicht.[848] Zwar verpflichtet sich die Schweiz zur Umsetzung internationaler Standards, insbesondere der Empfehlungen der GAFI; eine durch ein internationales Abkommen obligatorische Strafverfolgungspflicht begründen diese dadurch allerdings nicht.[849] 504

Damit verbleibt bei Betreiberinnen als Grundlage für eine schweizerische Strafgewalt allein Art. 7 StGB, der das aktive und passive Personalitätsprinzip sowie die stellvertretende Strafrechtspflege regelt. Nach dem aktiven Personalitätsprinzip ist das schweizerische Strafrecht anwendbar, wenn der Täter Schweizer Staatsbürger ist, die Tat auch am Begehungsort strafbar ist oder dieser keiner Strafgewalt unterliegt, sich der Täter in der Schweiz befindet oder ihr wegen dieser Tat ausgeliefert würde und es sich bei der betreffenden Tat um ein Auslieferungsdelikt handelt – also um eine Straftat von gewisser Schwere (vgl. Art. 35 Abs. 1 lit. a IRSG).[850] 505

Ob das passive Personalitätsprinzip – verstanden als eine Anknüpfung an die Schweizer Staatsangehörigkeit der durch das Delikt betroffenen Person – Anwendung findet, hängt davon ab, welche Rechtsgüter der Tatbestand der Geldwäscherei schützt. Wird ausschliesslich das staatliche Einziehungsinteresse als Schutzgut verstanden, scheidet mangels Individualbetroffenheit eine Anwendung aus.[851] Wird hingegen auch das Interesse der durch die Vortat geschädigten Person als mitgeschütztes Rechtsgut anerkannt, erlaubt dies eine Zuständigkeit gestützt auf das passive Personalitätsprinzip.[852] 506

Sind weder die Betreiberin noch die durch die Vortat geschädigte Person Schweizer Staatsangehörige, kommt schliesslich die stellvertretende Strafrechtspflege gemäss Art. 7 Abs. 2 StGB in Betracht.[853] Diese setzt voraus, dass 507

848 Vgl. GLESS/BACHMANN, N 21.67 ff.; KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 791, 806.

849 GLESS/BACHMANN, N 21.71, 21.

850 Urteil des BGer 6B_452/2022 vom 16. November 2023 E. 2.1.2; DONATSCH/GODENZI/TAG, S. 63 f.; GLESS/BACHMANN, N 21.75; BSK StGB I-POPP/KESHELAVA, Art. 7 N 2 ff.; AK StGB-SIMON, Art. 7 N 4; HK StGB-WOHLERS, Art. 7 N 3.

851 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 805; vgl. DONATSCH/THOMMEN/WOHLERS, S. 493 f.; PK StGB-PIETH/SCHULTZE, Art. 305bis N 6.

852 Vgl. BGE 146 IV 211 E. 4.2.1; 145 IV 335 E. 3.1; 129 IV 322 E. 2.2.4; gl.M. CR CP II-CASSANI/VILLARD, Art. 305bis N 10; AK StGB-GRAF, Art. 305bis N 1; OFK StGB-ISENRING, Art. 305bis N 9; HK StGB-WOHLERS, Art. 305bis N 1; krit. KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 97.

853 KV/KO StGB-ACKERMANN/ZEHNDER, Art. 305bis N 808; DONATSCH/GODENZI/TAG, S. 65 f.; GLESS/BACHMANN, N 21.77; CR CP I-HENZELIN, Art. 7 N 13; BSK StGB I-POPP/KESHELAVA, Art. 7 N 12; HK StGB-WOHLERS, Art. 7 N 6.

ein Auslieferungsbegehren aus Gründen abgewiesen wurde, die nicht die Art der Tat betreffen, die Tat auch am Begehungsort strafbar ist oder dieser keiner Strafgewalt unterliegt, sich der Täter in der Schweiz befindet und es sich wiederum um ein Auslieferungsdelikt handelt.[854]

508 Insgesamt kommt eine schweizerische Strafhoheit bei Geldwäscherei ausserhalb von Inlandtaten von Betreiberinnen dezentralisierter Anwendungen mangels Erfüllung der Voraussetzungen nach Art. 4–6 StGB einzig gestützt auf Art. 7 Abs. 1 und 2 StGB in Betracht, mithin im Rahmen des aktiven und passiven Personalitätsprinzips sowie der stellvertretenden Strafrechtspflege.

C. Fazit

509 Eine schweizerische Zuständigkeit knüpft bei Inlandtaten an territoriale Bezugspunkte im Sinne von Art. 3 i.V.m. Art. 8 StGB an. Bei Unterlassungsdelikten ergeben sich solche Anknüpfungspunkte einerseits am Ort, an dem der Unterlassungstäter hätte handeln müssen. Eine pflichtwidrige Untätigkeit liegt bei Betreiberinnen dezentralisierter Anwendungen dann in der Schweiz vor, wenn sie dem Geldwäschereigesetz unterstehen, das heisst ihre geldwäschereirelevante Geschäftstätigkeit von der Schweiz aus ausüben. Insofern überschneiden sich die Grundsätze der strafrechtlichen Anknüpfung mit jenen der örtlichen Unterstellung unter das Geldwäschereigesetz.

510 Ein weiterer territorialer Anknüpfungspunkt besteht am Ort des Erfolgs. Eine Zuständigkeit kann sich demnach auch ergeben, wenn der Nutzer die geldwäschereirelevante Handlung (als Erfolg im weiteren Sinn) von der Schweiz aus vornimmt oder, der bundesgerichtlichen Rechtsprechung folgend, sich die Vereitelungswirkung auf inländische Vermögenswerte auswirkt. Letzteres hängt wiederum von der Lokalisierung der Anwendung im schweizerischen Territorium ab.

511 Sofern sich die Betreiberin lediglich als Gehilfin strafbar gemacht hat, ist für die Bestimmung der örtlichen Zuständigkeit auf den Begehungsort des Haupttäters, mithin des Nutzers, abzustellen. Anknüpfen lässt sich dabei einerseits an den physischen Ort, an dem sich der Nutzer bei der Interaktion mit der Anwendung befindet. Andererseits kann auch jener Ort massgeblich sein, an dem sich die Vereitelungswirkung auf inländische Vermögenswerte auswirkt, das heisst der Ort, von dem aus die Betreiberin das Protokoll administriert, bzw. am Serverstandort.

854 DONATSCH/GODENZI/TAG, S. 65 f.; GLESS/BACHMANN, N 21.77; CR CP I-HENZELIN, Art. 7 N 15; BSK StGB I-POPP/KESHELAVA, Art. 7 N 14; AK StGB-SIMON, Art. 7 N 10; STRATENWERTH/BOMMER, AT I, § 5 N 20; HK StGB-WOHLERS, Art. 7 N 6.

Liegt keine Inlandtat vor, kommt eine Strafbarkeit nach den Regeln über Aus- 512
landtaten gemäss Art. 4–7 StGB in Betracht. Staatsschutzdelikte, Taten gegen Minderjährige oder auf völkerrechtlichen Verpflichtungen beruhende Delikte scheiden im Kontext der Geldwäscherei aus, sodass einzig das Personalitätsprinzip sowie die stellvertretende Strafrechtspflege nach Art. 7 StGB als Grundlage verbleiben. Eine schweizerische Zuständigkeit ist folglich gegeben, wenn die Betreiberin die schweizerische Staatsangehörigkeit besitzt, die durch die Vortat geschädigte Person Schweizerin ist oder subsidiär die Voraussetzungen der stellvertretenden Strafrechtspflege erfüllt sind.

Schlussbetrachtung

Zusammenfassung der wesentlichen Ergebnisse

Diese Untersuchung ist der Forschungsfrage nachgegangen, ob Betreiberinnen dezentralisierter Finanzanwendungen strafrechtlich belangt werden können, wenn Nutzer diese Technologien zur Geldwäscherei verwenden. Am Beispiel von Art. 305bis StGB wurde untersucht, wie Verantwortlichkeit in einem Umfeld begründet werden kann, das durch Dezentralisierung und automatisierte Systemlogik geprägt ist. 513

Dezentralisierte Finanzanwendungen bilden das Pendant zu traditionellen Finanzdienstleistungen, unterscheiden sich jedoch grundlegend in ihrer Ausgestaltung. Sie operieren ohne Intermediäre, sind weltweit und ohne Zugangsbeschränkungen nutzbar und werden pseudonym verwendet. Im Zusammenhang mit dem Begriff der Dezentralisierung hat diese Arbeit zwischen idealtypisch dezentralen und dezentralisierten Anwendungen unterschieden. Erstere zeichnen sich dadurch aus, dass das Protokoll nach der initialen Bereitstellung unveränderlich programmiert ist, keinerlei administrative Steuerung zulässt und die vollständige Kontrolle über die Vermögenswerte bei den Nutzern verbleibt. Dezentralisierte Anwendungen hingegen sind zwar ebenfalls öffentlich zugänglich und erlauben eine selbständige Interaktion der Nutzer mit dem Protokoll; sie unterstehen jedoch fortbestehenden administrativen Eingriffsmöglichkeiten durch eine Betreiberin. 514

Diese Offenheit und Automatisierung schaffen neue ökonomische Möglichkeiten, eröffnen jedoch zugleich ein erhebliches Missbrauchspotenzial. So werden Kryptowerte aus Deliktsphänomenen wie Ransomware-Erpressung, Scams, Darknet-Märkten, Drogen- und Waffenhandel bis hin zur Terrorismusfinanzierung regelmässig über solche Systeme geleitet, um ihre Herkunft zu verschleiern und die staatlichen Zugriffsmöglichkeiten zu erschweren. 515

Die Frage, wer und welches Verhalten bei von Automatisierung geprägten Konstrukten strafrechtliche Verantwortlichkeit auslöst, hängt entscheidend davon ab, wie der Betreiberbegriff verstanden wird. Diese Arbeit legt bewusst ein weites Verständnis des Betreibens zugrunde, um sowohl Protokolle mit zentralisierenden Elementen als auch idealtypisch dezentral ausgestaltete Anwendungen zu erfassen. Betreiben im weiteren Sinne umfasst dabei zwei Ebenen: zum einen das Bereitstellen bzw. Veröffentlichen der Anwendung auf der Blockchain (Deployment), zum anderen das Betreiben im engeren Sinne, 516

das sich durch fortbestehende technische Eingriffsmöglichkeiten im Frontend oder Backend auszeichnet.

517 Das Betreiben von Anwendungen ist im Grundsatz durch eine überwiegend passive Rolle der Administratoren geprägt. Auf dieser Grundlage konnte sich die Prüfung einer strafrechtlichen Verantwortlichkeit wegen Begehens einer Geldwäscherei nach Art. 305bis StGB einzig auf ein aktives Tun im Sinne des initialen Bereitstellens der Anwendung (Deployment) stützen.

518 Beim Bereitstellen des Protokolls handelt es sich um einen Gehilfenbeitrag. Durch dieses Zurverfügungstellen schaffen die Betreiberinnen eine technische Grundlage (oder ein Werkzeug), die es dem Nutzer durch Interaktion damit ermöglicht, Geldwäschereihandlungen durchzuführen. Die Untersuchung hat ergeben, dass eine Strafbarkeit einerseits daran scheitert, dass die Bereitstellung grundsätzlich keinen deliktischen Sinnbezug aufweist, das heisst, das Zurverfügungstellen eben nicht lediglich im Hinblick auf Geldwäschereihandlungen der Nutzer als sinnvoll erscheint. Andererseits scheitert sie auch im Vorsatz über das Fördern einer bestimmten Haupttat. Die anonyme sowie zeitlich und inhaltlich unbestimmte Nutzung dezentralisierter Protokolle macht es der Betreiberin regelmässig unmöglich, die wesentlichen Merkmale einer bestimmten Geldwäschereihandlung im Voraus zu erfassen. Ein Vorsatz kommt daher nur ausnahmsweise in Betracht, wenn die Funktionsarchitektur selbst einen eindeutig deliktischen Kontext vorgibt – etwa bei Kryptomixern mit technischer Anbindung an einschlägige Darknet-Ökosysteme.

519 Vor diesem Hintergrund wandte sich der nächste Teil der Arbeit der Frage zu, ob sich aufgrund der automatisierten Funktionsweise und der weitgehenden Passivität des Betriebs eine Strafbarkeit wegen Geldwäscherei durch Unterlassen ergeben kann, wenn Betreiberinnen Geldwäschereihandlungen ihrer Nutzer auf öffentlich zugänglichen Anwendungen nicht verhindern. Eine Garantenstellung und damit verbundene Handlungspflichten zur Erfolgsabwendung lassen sich ausschliesslich aus dem Geldwäschereigesetz ableiten, namentlich aus dessen Sorgfalts- und Meldepflichten wie Art. 6, Art. 9 und Art. 10 GwG. Eine sachliche, persönliche und örtliche Unterstellung der dezentralisierten Protokolle bzw. ihrer Betreiberinnen unter das Geldwäschereigesetz ist bei technologieneutraler Betrachtung grundsätzlich möglich, entfällt jedoch insbesondere bei idealtypisch dezentralen Anwendungen, bei denen Betreiberinnen keine tatsächlichen Kontroll- oder Einflussmöglichkeiten haben.

520 Auf subjektiver Ebene ergeben sich Indizien für das Wissenselement in der Regel aus öffentlich einsehbaren transaktionsbezogenen Anhaltspunkten. Für Eventualvorsatz spricht insbesondere, dass keinerlei technische oder

organisatorische Massnahmen zur Umsetzung der geldwäschereirechtlichen Sorgfaltspflichten implementiert wurden und damit potenzielle Vereitelungshandlungen der Nutzer gleichgültig in Kauf genommen werden. Dieses Gewicht erklärt sich vor dem Hintergrund, dass dezentralisierte Anwendungen aufgrund der Pseudonymität der Nutzer und der hohen Transaktionsdynamik einer erhöhten Abklärungspflicht unterstehen.

Eine qualifizierte Geldwäscherei kommt primär im Rahmen der Gewerbs- 521
mässigkeit in Betracht (Art. 305bis Ziff. 2 lit. c StGB). Die dauerhafte, gebührenfinanzierte Bereitstellung einer Infrastruktur weist regelmässig einen berufsähnlichen Geschäftsbetrieb auf, bei dem die Schwelle zu erheblichen ökonomischen Erträgen erfahrungsgemäss rasch überschritten wird.

Für dezentralisierte Protokolle besteht eine schweizerische Zuständigkeit 522
bei Unterlassung insbesondere dann, wenn die Betreiberin ihre geldwäschereirelevante Geschäftstätigkeit faktisch von der Schweiz aus ausübt, wie durch die Administration des Protokolls, den Einsatz von Admin Keys oder den Betrieb des Webinterfaces. Ein weiterer territorialer Bezug ergibt sich, wenn die Vereitelungswirkung der unterlassenen Handlung inländische Vermögenswerte betrifft. Macht sich die Betreiberin lediglich der Gehilfenschaft strafbar, richtet sich die Zuständigkeit primär nach dem Begehungsort des Nutzers bzw. dem Ort der Vereitelungswirkung. Fehlt ein solcher Inlandsbezug, kommt eine schweizerische Strafgewalt nur ausnahmsweise nach Art. 7 StGB in Betracht.

Schlussfolgerungen

Diese Arbeit hat aufgezeigt, dass aufgrund der vollautomatisierten Funktions- 523
weise dezentralisierter Protokolle und der damit einhergehenden grundlegenden Passivität der Betreiberinnen ein strafrechtlich relevantes Tun einzig an das initiale Bereitstellen der Anwendung anknüpfen kann. Eine Begehensstrafbarkeit kommt sowohl bei idealtypisch dezentralen als auch bei dezentralisierten Anwendungen nur in einem äusserst engen Anwendungsbereich in Betracht, namentlich bei Kryptomixern, deren Funktionslogik auf eine Verschleierung von Transaktionswegen – etwa durch Anbindungen an einschlägige Darknet-Ökosysteme – ausgelegt ist. Für die überwiegende Mehrzahl dezentralisierter Finanzanwendungen wird sich die Frage strafrechtlicher Verantwortlichkeit daher primär im Rahmen einer Unterlassensstrafbarkeit stellen.

Die Analyse hat zudem gezeigt, dass die Verantwortlichkeit durch Un- 524
terlassen im Kern davon abhängt, an welcher Stelle einer Anwendung auf dem Kontinuum der (administrativen) Dezentralisierung die Betreiberin

positioniert ist. Entscheidend ist mithin, in welchem Umfang faktische Kontroll- und Eingriffsmöglichkeiten in den Protokollbetrieb bestehen. Dies spiegelt sich in mehreren Prüfungsstufen wider: Die Begründung einer Garantenstellung auf Grundlage des Geldwäschereigesetzes setzt ein Mindestmass an administrativer Steuerbarkeit voraus, um in dessen sachlichen Anwendungsbereich sowie in die damit verbundenen Sorgfalts- und Meldepflichten zu fallen. Auch auf der Ebene der territorialen Unterstellung hängt ein Bezug zur Schweiz davon ab, ob administrative Funktionen tatsächlich von hier aus ausgeübt werden. Die im Kontext dezentralisierter Konstrukte bestehenden Rechtsunsicherheiten hinsichtlich persönlicher, sachlicher und räumlicher Unterstellung erweisen sich daher als zentral für die strafrechtliche Verantwortlichkeit und müssen in der Aufsichtspraxis adressiert werden.

525 Insgesamt hat die Untersuchung ergeben, dass Betreiberinnen dezentralisierter Anwendungen nach Art. 305bis StGB sowohl wegen Begehung – wenn auch nur in einem eng begrenzten Anwendungsbereich – als auch wegen Unterlassens nach Art. 11 StGB für Geldwäschereihandlungen von Nutzern strafrechtlich zur Verantwortung gezogen werden können. Ob eine Strafbarkeit greift, hängt nicht nur von der funktionalen Ausrichtung der Anwendung, sondern insbesondere vom Grad der Dezentralisierung ab: Idealtypisch dezentrale Anwendungen ermöglichen bestenfalls in Ausnahmefällen eine Begehensstrafbarkeit. Eine Unterlassensstrafbarkeit scheidet dort vollständig aus. Demgegenüber können dezentralisierte Anwendungen auch die Voraussetzungen einer Unterlassensstrafbarkeit erfüllen.

526 Diese Ergebnisse stehen im Einklang mit dem strafrechtlichen Prinzip, dass grundsätzlich niemand für die Straftaten Dritter verantwortlich gemacht werden kann. Verantwortlichkeit entsteht jedoch immer dann, wenn eine Betreiberin einen ihr zurechenbaren Gefahrenbereich schafft und über gesteigerte Kontroll- und Einflussmöglichkeiten verfügt, die geeignet wären, geldwäschereirelevante Handlungen der Nutzer zu verhindern. In diesem Sinne fällt der Schleier der Technologie in jenen Fällen, in welchen faktische Steuerungsmacht besteht. Wo Geldwäschereirisiken geschaffen und beherrschbar sind, ist – im Sinne des Grundsatzes ‹same risk, same rules› – eine Annäherung an die strafrechtliche Behandlung jener off-chain agierenden traditionellen Finanzintermediäre zu begrüssen.

Über die Autorin:
Lisa Reggiani absolvierte das Studium der Rechtswissenschaften sowie das Promotionsstudium an der Universität Zürich. Im Rahmen ihrer Dissertation war sie wissenschaftliche Assistentin an den Lehrstühlen von Prof. Dr. Christian Schwarzenegger und Prof. Dr. Gian Ege an der Universität Zürich. Daneben sammelte sie praktische Erfahrungen in einem Blockchain-Start-up. Ihre Forschungsinteressen liegen im Wirtschaftsstrafrecht, insbesondere im Bereich der Geldwäscherei sowie der strafrechtlichen Verantwortlichkeit im Zusammenhang mit der Blockchain-Technologie.

021 – Roger Plattner: **Digitales Verwaltungshandeln – Rechtliche Aspekte der Digitalisierung in der öffentlichen Verwaltung**

In einer Zeit, in der die meisten Aufgaben des Alltagslebens online erledigt werden können, werden auch an die öffentliche Verwaltung steigende Ansprüche bezüglich Erreichbarkeit, Verfügbarkeit und Vereinfachung ihrer Dienstleistungen gestellt. Daher wurden in den letzten Jahren unter dem Begriff des «E-Government» zahlreiche Verwaltungsdienstleistungen digitalisiert. Neben allen positiven Aspekten ist diese Digitalisierung auch mit Herausforderungen sowie Gefahren für die Rechtstellung Privater verbunden.

Die vorliegende Monographie soll einen Beitrag zur Beantwortung der Frage leisten, wie die mit der Digitalisierung einhergehenden Veränderungen im Bereich des Verwaltungshandelns rechtlich zu beurteilen sind. Dabei werden einerseits Technologien und Phänomene, welche im Handeln der öffentlichen Verwaltung bereits zum Einsatz gelangen, auf ihre Vereinbarkeit mit dem bestehenden Rechtsrahmen beleuchtet. Anderseits werden sich abzeichnende, künftigen Entwicklungen aufgezeigt und mit kritischem Blick auf mögliche rechtliche Probleme untersucht.



Erhältlich als Druckausgabe und
Open Access unter suigeneris-verlag.ch

044 – Alex Attinger: **Wirtschaftliche Berechtigung – Konzepte und Dogmatik**

Trotz zunehmender Verbreitung und Relevanz sind grundlegende Fragen zur wirtschaftlichen Berechtigung ungeklärt: Gibt es Verwandtschaften und Zusammenhänge zwischen verschiedenen Anwendungsfällen? Gibt es ein einheitliches Konzept? Wie ist wirtschaftliche Berechtigung rechtsdogmatisch einzuordnen?

Zur Beantwortung dieser Fragen, werden in dieser Dissertation die wichtigsten Konzepte wirtschaftlicher Berechtigung analysiert und auf inhaltliche, funktionale und strukturelle Gemeinsamkeiten hin untersucht, um eine Dogmatik der wirtschaftlichen Berechtigung herauszuschälen.

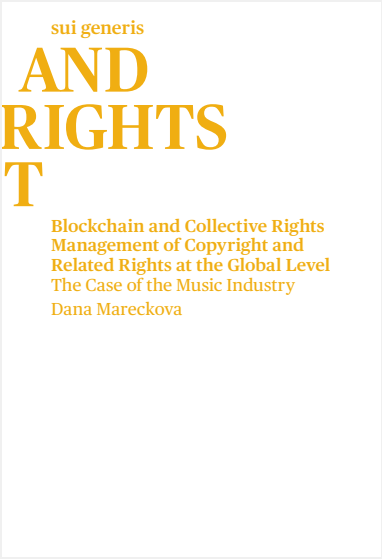
Es zeigt sich, dass es kein einheitliches Konzept wirtschaftlicher Berechtigung gibt. Die strukturellen und funktionalen Gemeinsamkeiten verdichten sich jedoch zu einer Rechtsfigur der wirtschaftlichen Berechtigung, aus der sich wichtige Erkenntnisse für Praxis und Gesetzgebung ergeben.



Erhältlich als Druckausgabe und
Open Access unter suigeneris-verlag.ch

057 – Dana Mareckova: **Blockchain and Collective Rights Management of Copyright and Related Rights at the Global Level – The Case of the Music Industry**

Online music streaming has become an important source of revenue within the music industry, but the necessary licensing of musical works and sound recordings can still be quite cumbersome. The thesis discusses what blockchain is, how it could facilitate global licensing, and whether it could replace or improve the current system of collective rights management.



Available in print and Open Access at
suigeneris-verlag.ch

sui generis ist ein Verein, der sich der Förderung des freien Zugangs zu juristischer Literatur, Gerichtsurteilen, Behördenentscheidungen und Gesetzesmaterialien verschrieben hat. Unter dem Label *sui generis* erscheint seit 2014 eine juristische Open-Access-Fachzeitschrift. 2019 erfolgte die Gründung des *sui generis* Verlags.

In der *sui generis* Reihe werden juristische Dissertationen und Habilitationen sowie Lehrbücher und Fachpublikationen einem breiten Publikum zugänglich gemacht. Die Bücher erscheinen als gedruckte Werke und online. Die digitale Version ist weltweit kostenlos zugänglich (Open Access). Die Urheberrechte verbleiben bei den AutorInnen; die Werke werden unter einer Creative-Commons-Lizenz veröffentlicht.

Bisher bei *sui generis* erschienen:

Grundlagen

019 – APARIUZ XXII: **Unter Gleichen**
025 – Severin Meier: **Indeterminacy of International Law?**
026 – Marc Thommen: **Introduction to Swiss Law (2nd edition, 2022)**
028 – APARIUZ XXIII: **Recht in der Krise**
044 – Alex Attinger: **Wirtschaftliche Berechtigung – Konzepte und Dogmatik**
051 – APARIUZ XXIV: **Der Prozess**
052 – Arezoo Sang Bastian: **Between Islamic and Secular Law**

Öffentliches Recht

009 – Dominik Elser: **Die privatisierte Erfüllung staatlicher Aufgaben**
010 – David Henseler: **Datenschutz bei drohnengestützter Datenbearbeitung durch Private**
015 – Frédéric Erard: **Le secret médical**
016 – Valentin Botteron: **Le contrôle des concentrations d'entreprises**
017 – Monika Pfyffer von Altishofen: **Ablehnungs- und Umsetzungsraten von Organtransplantationen – mögliche Ursachen und denkbare Auswege**
018 – Kristin Hoffmann: **Kooperative Raumplanung: Handlungsformen und Verfahren**
020 – Raphaël Marlétaz: **L'harmonisation des lois cantonales d'aide sociale**
021 – Roger Plattner: **Digitales Verwaltungshandeln**
024 – Marina Piolino: **Die Staatsunabhängigkeit der Medien**
027 – Maja Łysienia: **Seeking Convergence?**
033 – Joséphine Boillat / Stéphane Werly: **20 ans de la transparence à Genève**
034 – Nora Camenisch: **Journalistische Sorgfalt: Rechtliche und medienethische Anforderungen**
036 – Jeremias Fellmann: **Das Verbot von extremistischen Organisationen im schweizerischen Recht**
037 – Nils Reimann: **Foreign Electoral Interference: Normative Implications in Light of International Law, Human Rights, and Democratic Theory**
040 – Constance Kaempfer: **Les mécanismes de mise en œuvre du droit international par les cantons suisses**
041 – Lukas Valis: **Digitale Ökonomie: Erforderlichkeit sektorspezifischer ex-ante Regulierung?**
045 – Corina Ingold: **Das Kompensationsprinzip im Schweizer Raumplanungsrecht**

046 – Miriam Lüdi: **Zielkonflikt zwischen Lärmschutz und Siedlungsverdichtung**

047 – Luca Ruggiero: **Effets non coordonnés dans le contrôle des concentrations horizontales européen**

053 – Yannick Weber: **Die Nichtigkeit im öffentlichen Recht**

058 – Olga Uehlinger: **Auswirkungen des BEPS-Projekts der OECD auf die Steuerordnung der Schweiz: Umsetzung des Aktionspunkts 5**

061 – Pauline Meyer: **La cybersécurité des infrastructures critiques et la gestion de cyberincidents en droit suisse**

066 – Roman Schuppli: **Die bevölkerungsnahe Polizei(-arbeit) und ihre Grenzen**

067 – Marc Wohlwend: **Zur Kausalität zwischen psychosozialen Belastungen am Arbeitsplatz und Erkrankungen**

068 – Tobias Egli: **Der Grundsatz der Siedlungsentwicklung nach innen und seine Umsetzung**

069 – Natalie Pompe: **Constitutional Rights in the Digital Context. Exploring a Translation of the Constitutional Political Rights into the Digital Sphere**

070 – Vladislava Talanova: **Biobanques humaines, internormativité et gouvernance. Etude de la gouvernance des biobanques sous l'angle du droit suisse**

071 – Livia Enzler: **Frozen Conflicts in International Law. Challenging Legal Categories in the Post-Soviet Space**

072 – Marisa Beier: **Das Recht auf angemessene Wohnung im UNO-Pakt I. Menschenrechtliche Analyse im Kontext der Obdachlosigkeit**

074 – Raphaël Bagi: **Les droits des personnes LGBTIQ – Propositions en faveur d'une politique suisse cohérente en droit national et international**

076 – Jelena Protic: **La légitimité démocratique des instruments internationaux de droit souple**

Privatrecht

011 – Lorenz Raess: **Court Assistance in the Taking of Evidence in International Arbitration**

012 – Christoph Hurni / Christian Josi / Lorenz Sieber: **Das Verfahren vor dem Berner Kindes- und Erwachsenenschutzgericht**

013 – Emanuel Bittel: **Die Rechnungsstellung im schweizerischen Obligationenrecht**

022 – Nicole Roth: **Miteigentum an Grundstücken und einfache Gesellschaft**

023 – Reto Pfeiffer: **Vertragliche Rechtsfolge der «Verwendung missbräuchlicher Geschäftsbedingungen» (Artikel 8 UWG)**

030 – Christoph Mettler: **Der Anscheinsbeweis im schweizerischen Zivilprozess**

035 – Florent Thouvenin / Eva-Maria Messerle: **Zur Geschichte des Eigengebrauchs im schweizerischen Urheberrecht – Entwicklung, Erkenntnisse, Quellen**

038 – Lukas Hussmann: **International anwendbare Streitgenossenschaftsgerichtsstände**

039 – Ruedi Ackermann: **Der Mietvertrag mit mehreren Mietern**

042 – Andreas Wehowsky: **Expedited Procedures in International Commercial Arbitration**

043 – Myriam Christ: **Le profilage dans le cadre d'une procédure d'embauche entre particuliers**

050 – Ricarda Stoppelhaar: **Die Indirekte Stellvertretung**

056 – Saskia Thomi: **Die Verantwortungsgemeinschaft**

057 – Dana Mareckova: **Blockchain and Collective Rights Management of Copyright and Related Rights at the Global Level: The Case of the Music Industry**

063 – Simon R. Lang: **Einordnung und Gestaltung der Rechtsverhältnisse in der Stromversorgung**

064 – Johannes Lukas Hermann: **Das pactum de non cedendo im System der Unabtretbarkeit von Forderungen**

073 – Helen Keller / Corina Heri: **Reparation for Climate Change: The Successes and Limits of Litigation**
077 – Honor Felisberto: **L'œuvre dérivée à l'ère numérique**

Strafrecht

014 – Stephan Bernard: **Was ist Strafverteidigung?**
029 – Simone Walser / Nora Markwalder / Martin Killias: **Tötungsdelikte in der Schweiz von 1990 bis 2014**
031 – Martin Klingler: **Füllung der Gesetzeslücken im schweizerischen Adhäsionsverfahren**
032 – Nicolas Leu: **Kritik der objektiven Zurechnung**
048 – Benjamin Clément: **Die strafbare Unterlassung der allgemeinen Lebensrettungspflicht**
049 – Martin Seelmann: **Strafzumessung und Doppelverwertung**
054 – Sonja Mango-Meier: **Verantwortlichkeit des Fahrzeughalters bei geringfügigen Widerhandlungen gegen das schweizerische Strassenverkehrsrecht durch eine unbekannte Täterschaft**
055 – Sena Hangartner: **Strafrechtliche Dopingbekämpfung in der Schweiz**
059 – Delphine Brun: **Dangerosité : du juge influencé par l'expert au juge indépendant**
060 – Luca Ranzoni: **Gerechte Strafen ohne Gleichheit?**
062 – Marc Thommen: **Der Staatsanwalt als Richter. Dürfen Freiheitsstrafen in Strafbefehlen ausgefällt werden?**
065 – Florian Jenal: **Die privatklägerische Strafklage gemäss Schweizerischer Strafprozessordnung – und einige Überlegungen zur Restorative Justice**
075 – Dominique Diethelm: **Die audiovisuelle Aufzeichnung strafprozessualer Einvernahmen, Zur Notwendigkeit der Einführung einer Aufzeichnungspflicht**
078 – Luca Schoop: **Die Staatsanwaltschaft als Zivilrichterin – Der Entscheid über Zivilforderungen im Strafbefehlsverfahren (Art. 353 Abs. 2 StPO)**

Dieses Werk ist erschienen in der Reihe *sui generis,*
herausgegeben von Marc Thommen.

1. Auflage 30. Oktober 2026
© 2026 Lisa Reggiani
Die Rechtswissenschaftliche Fakultät der Universität Zürich hat vorliegende Arbeit am 27. Mai 2026 auf Antrag von Prof. Dr. Gian Ege und Prof. Dr. Monika Simmler als Dissertation mit dem Prädikat *magna cum laude* abgenommen.

Abdruck der von der Rechtswissenschaflichen Fakultät der Universität Zürich genehmigten Dissertation.

Dieses Werk wurde unter einer Creative Commons Lizenz als Open Access veröffentlicht, die bei Weiterverwendung nur die Nennung des Urhebers erfordert (CC BY 4.0 – https://creativecommons.org/licenses/by/4.0).



Die Druckvorstufe dieser Publikation wurde vom Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung unterstützt.

ISBN: 978-3-907297-79-7
DOI: 10.38107/079
Korrektorat: Christoph Meyer
Gestaltung: Müller+Hess, Basel
Druck: Ebner & Spiegel, Ulm
Zentrales Auslieferungslager in der EU ist die GVA Göttingen,
Anna-Vandenhoeck-Ring 36, 37081 Göttingen, info@gva-verlage.de

sui generis Verlag, Viaduktstrasse 21, 8005 Zürich
www.suigeneris-verlag.ch, info@suigeneris-verlag.ch

079

GELDWÄSCH MITTELS DEZENTRAL FINANZANW

Blockchainbasierte Finanzanwendungen verändern die Art und Weise, wie Vermögenswerte transferiert und verwaltet werden. Mit der Dezentralisierung verschwinden jedoch zugleich klassische Verantwortungsstrukturen. Wer kann strafrechtlich zur Verantwortung gezogen werden, wenn Nutzer solche Systeme zur Geldwäscherei verwenden? Die vorliegende Arbeit beantwortet diese bislang weitgehend ungeklärte Frage am Beispiel von Art. 305bis StGB und legt dabei einen besonderen Schwerpunkt auf die Unterlassensstrafbarkeit der Betreiberinnen.

sui generis
ISBN 978-3-907297-79-7
DOI 10.38107/079