

Internetrecht und Digitale Gesellschaft

Band 15

Virtuelle Kryptowährungen und Geldwäsche

Von

Johanna Grzywotz



Duncker & Humblot · Berlin

JOHANNA GRZYWOTZ

Virtuelle Kryptowährungen und Geldwäsche

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 15

Virtuelle Kryptowährungen und Geldwäsche

Von

Johanna Grzywotz



Duncker & Humblot · Berlin

Der Fachbereich Rechtswissenschaft
der Friedrich-Alexander-Universität Erlangen-Nürnberg
hat diese Arbeit im Sommersemester 2018
als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten
© 2019 Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-15550-7 (Print)
ISBN 978-3-428-55550-5 (E-Book)
ISBN 978-3-428-85550-6 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

*Meinen Eltern und
meiner großen Schwester gewidmet,
gefolgt von der Grünen Insel.*

Vorwort

Diese Arbeit wurde im Sommersemester 2018 vom Fachbereich der Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg als Dissertationsschrift angenommen. Für die Drucklegung konnten Literatur und Rechtsprechung bis Frühjahr 2018 berücksichtigt werden.

Die Niederschrift wäre mir ohne die Unterstützung zahlreicher Personen nicht möglich gewesen. Auch wenn Worte nicht ausreichen, um meine Dankbarkeit auszudrücken, möchte ich es an dieser Stelle wenigstens versuchen.

Mein Dank gebührt zuvorderst meinem Doktorvater, Professor Dr. Christoph Safferling, LL.M. (LSE), der nicht nur diese Arbeit betreut hat, sondern mir auf meinem Lebensweg sowohl fachlich als auch menschlich mit Rat und Tat stets zur Seite stand. Auch dafür, dass er mir die Gelegenheit gegeben hat, Teil seines großartigen Lehrstuhl-Teams zu sein – das ich in bester Erinnerung behalten werde – bin ich zutiefst dankbar. Nicht nur für die zügige Erstellung des Zweitgutachtens schulde ich zudem Professor Dr. Hans Kudlich Dank, sondern auch für die hervorragende Arbeitsatmosphäre auf dem „Strafrechtsflur“ – für die ich neben ihm auch Professor Dr. Christian Jäger und Professorin Dr. Gabriele Kett-Straub von Herzen danken möchte.

Großen Dank schulde ich zudem meinem guten Freund und ehemaligen Kollegen Dr. Christian Rückert zunächst für die wertvollen Kommentare, Anmerkungen und Diskussionen zu der vorliegenden Schrift, aber auch für die hervorragende Arbeitsatmosphäre in unserem Büro während meiner Zeit am Lehrstuhl, die wohl für immer unerreicht bleiben wird (#CRJG4life). Danken möchte ich auch Anna Reiß für das zügige und gründliche Korrekturlesen der Arbeit. Darüber hinaus gebührt Malte Möser und Olaf Markus Köhler mein Dank für das Korrekturlesen der technischen Aspekte dieser Schrift und für ihre unsagbare Geduld, die sie meinen (nächtlichen) Hilferufen – bedingt durch mein (anfänglich) technisches Unvermögen – entgegengebracht haben. In diesem Zusammenhang schulde ich auch den Partnern des vom BMBF geförderten BITCRIME-Projekts, im Rahmen dessen diese Dissertationsschrift entstanden ist – allen voran Projektleiter Professor Dr. Rainer Böhme und Projektkoordinatorin Dr. Paulina Jo Pesch – Dank.

Danken möchte ich außerdem meinen unersetzbaren Freundinnen Dr. Gloria Berghäuser, Charlotte Sapinel und Marlene Wüst, deren offenes Ohr und – wortwörtlich – offenen Türen mir stets Halt gegeben haben und die nicht müde geworden sind, mich zu ermutigen, auch wenn ich es fertigge-

bracht habe, mich und meine Probleme in den Mittelpunkt jedes Gesprächs zu stellen.

Großen Dank schulde ich ferner meinen Eltern, Andreas und Brigitte Grzywotz, die mich in allen Lebensentscheidungen unterstützt haben, ohne auch nur eine Sekunde an mir zu zweifeln und ihre eigenen Belange stets hintenangestellt haben. Ohne ihre unermüdliche Unterstützung und Ermutigung hätte ich meinen Weg so nicht beschreiten können. Gleichsam danken möchte ich meiner Schwester, Franziska Grzywotz, nicht nur für das zügige Korrekturlesen der vorliegenden Arbeit und das Redigieren von allem, was im Laufe meines Lebens angefallen ist, sondern auch für das größte Maß an bedingungsloser Unterstützung, das eine „große“ Schwester einer „kleinen“ entgegenbringen kann.

Schließlich und letztlich wäre die schnelle Fertigstellung der Arbeit nicht möglich gewesen ohne die finanzielle Unterstützung, die mir durch die Verleihung des Fakultätsfrauenpreises der rechts- und wirtschaftswissenschaftlichen Fakultät der Friedrich-Alexander-Universität Erlangen-Nürnberg zu Teil wurde, wofür ich zutiefst dankbar bin.

Fuldatal, im Oktober 2018

Johanna Grzywotz

Inhaltsverzeichnis

Kapitel 1

Einleitung	21
A. Problembeschreibung	21
B. Gang der Untersuchung	23

Kapitel 2

Das neue technische Phänomen virtueller Währungen	25
A. Zum Begriff	25
I. Geschlossene Systeme	25
II. Systeme mit unidirektionalem Geldfluss	26
III. Systeme mit bidirektionalem Geldfluss	26
B. Insbesondere: Kryptowährungen	27
I. Zentrale Merkmale	27
II. Beispiele	27
C. Hintergründe zu Bitcoin	28
I. Entstehung	28
II. Funktionsweise und Begrifflichkeiten	30
1. Bitcoins als reine wertenthaltene Information	30
a) Transaktionen als Änderung wertzuweisender Informationen	31
b) Asymmetrische Kryptographie bei Bitcoin	31
aa) Privater Schlüssel	31
bb) Öffentlicher Schlüssel	32
cc) Bitcoin-Adresse	33
c) Aufbau einer Transaktion	33
d) Schlüssel-Verwaltung – Sog. Wallets	35
aa) Als Datei auf einer lokalen Festplatte	36
bb) Passwort-geschützte Wallets	37
cc) Offline-Aufbewahrung	37
dd) „Air-Gapped“ Aufbewahrung	38
ee) Passwort-abgeleitete Schlüssel	39
ff) Web-Wallets/Hosted Wallets	39
2. Dezentralisierte Konsensfindung	40

a)	Eindeutige Zuordnung von Bitcoins durch die sog. Blockchain . . .	40
b)	Ergänzung der Blockchain durch das sog. Bitcoin-Mining	42
aa)	Erstellen eines Blocks	42
bb)	Finden des sog. Proof-of-Works	44
cc)	Längste Kette als einzig gültige Blockchain	45
dd)	Exkurs: Spaltung der Blockchain – Bitcoin Cash	46
ee)	Anreiz zum Mining	46
ff)	Mining-Pools	48
c)	Verhinderung des „Double-Spendings“	49
3.	Bitcoin und die Realwelt	50
a)	Kernsystem	50
b)	Ökosystem	51
c)	Finanzsektor und Realwirtschaft	53
III.	Rechtliche Einordnung	54
1.	Abgrenzung zu Bargeld, Buchgeld und E-Geld	54
2.	Einordnung als Rechnungseinheit nach dem Kreditwesengesetz (KWG)	56

Kapitel 3

Das Phänomen der Geldwäsche 58

A.	Die Entwicklung des Geldwäschetatbestands	58
I.	Internationaler Ursprung	59
1.	US-President's Commission von 1984	59
2.	Wiener Konvention von 1988	60
3.	FATF 1989	61
4.	Konvention des Europarates von 1990	62
5.	Die EG-Richtlinie vom 10. Juni 1991	64
II.	Der heutige Tatbestand der Geldwäsche im StGB	65
1.	Der ursprüngliche Tatbestand	65
2.	Änderungen der ursprünglichen Norm	67
3.	Sinn und Zweck der Norm	69
4.	Geschütztes Rechtsgut	70
a)	Rechtsgut aller Tatbestände	72
aa)	Finanzsystem sowie Wirtschafts- und Finanzkreislauf	72
bb)	Staatlicher Einziehungs- und Verfallsanspruch	72
cc)	Schutz der Ermittlungstätigkeit	73
dd)	Innere Sicherheit der Bundesrepublik Deutschland	73
b)	Zusätzliches Rechtsgut des Abs. 2	74
c)	Das identifizierte Rechtsgut durch die Rechtsprechung	75
d)	Zwischenergebnis	76
5.	Deliktsnatur	76

Inhaltsverzeichnis	11
6. Rezeption des Tatbestands	77
B. Herkömmliche Geldwäschetechniken	79
I. 3-Phasen-Modell als die häufigste Systematisierung der Geldwäsche- phasen	79
1. Einspeisung (Placement)	80
2. Verschleierung (Layering)	83
3. Integration	85
4. Zusammenfassung	86
II. Verluste im Rahmen der „herkömmlichen“ Geldwäsche	87

Kapitel 4

Koinzidenz von Bitcoin und Geldwäsche	89
A. Stellungnahmen zu virtuellen Kryptowährungen	89
I. FATF	89
1. New Payment Products and Services Guidance (Juni 2013)	90
2. Virtual Currencies – Key Definitions and Potential Anti-money Laundering and Counter-terrorist Financing Risks (Juni 2014)	90
a) Definition virtueller Währungen	90
b) Klassifizierung/Bestimmung von Teilnehmern	91
c) Potentielle Geldwäsche- und Terrorismusfinanzierungsrisiken	91
aa) Allgemeine potentielle Risiken	91
bb) Risiken speziell bei Bitcoin	92
3. Guidance for a Risk-based Approach – Virtual Currencies (Juni 2015)	93
4. Emerging Terrorist Financing Risks (Oktober 2015)	93
II. Europäische Bankenaufsicht (Juli 2014)	94
1. Definition virtueller Währungen	94
2. Vorteile und Risiken	94
III. Europäische Zentralbank (Oktober 2012 und Februar 2015)	95
IV. Europäische Union (Juli 2016)	96
V. Geldwäschegefahr als gemeine Komponente einer zunehmenden Befas- sung mit virtuellen Währungen	97
B. Eignung von Bitcoins zur Geldwäsche	97
I. Förderliche Eigenschaften	98
1. Dezentralität	98
2. Pseudonymität	99
3. Globalität	100
II. Geldwäschetechniken	100
1. Einspeisung	101
a) Platzierung von inkriminierten Werten im Bitcoin-System	101
b) Platzierung von inkriminierten Bitcoins	103
2. Verschleierung	103

a) „Einfache“ Transaktionen	103
b) Bitcoin Transaktion unter Verwendung sog. Mixing-Services . . .	104
aa) Web-Wallet Dienstleister als Mixing-Services	104
bb) Spezialisierte zentrale Mixing-Dienste	105
(1) Funktionsweise	106
(2) Risiken	107
cc) Dezentrale Mixing-Dienste	107
c) Zusammenfassung	108
3. Integration	109
a) Herkömmliche Wege	109
b) Spezialfall: Kauf von Mining-Hardware	109
4. Fazit: Bitcoin als taugliches Geldwäschewerkzeug	110
III. Verluste im Rahmen der Geldwäsche mit Bitcoins	110

Kapitel 5

„Bitcoinspezifische“ Untersuchung des § 261 StGB	112
A. Anwendbarkeit des deutschen Strafrechts	112
I. Grundlegende Ausführungen zur Anwendbarkeit des deutschen Strafrechts	112
1. Handlungs- und Erfolgsort beim abstrakten Gefährungsdelikt	113
a) Handlungsort bei abstrakten Gefährungsdelikten	113
b) Erfolgsort bei abstrakten Gefährungsdelikten	114
aa) „Globale Zuständigkeit“ des deutschen Strafrechts	115
bb) Vermittelnde Ansichten	115
cc) Kein Erfolgsort bei abstrakten Gefährungsdelikten	117
dd) Stellungnahme	117
2. Handlungs- und Erfolgsort beim Erfolgsdelikt	118
II. Handlungs- und Erfolgsort bei Geldwäschehandlungen mit Bitcoins	119
1. Abstrakte Gefährungsdelikte (§ 261 Abs. 1 Var. 1 und 2, Abs. 2 StGB)	119
2. Erfolgsdelikte (§ 261 Abs. 1 Var. 3 und 4 StGB)	120
a) Tätigen einer „einfachen“ Transaktion	121
aa) Inhaber der Empfänger-Adresse befindet sich in Deutschland	121
bb) Bitcoins befinden sich in Deutschland	122
(1) Wallet als Belegenheitsort von Bitcoins	122
(2) Blockchain als Belegenheitsort von Bitcoins	123
(3) Kein zentraler physischer Belegenheitsort bei Bitcoins	123
cc) Transaktionsbezogener Anknüpfungspunkt	124
(1) Transaktion wird mit Hilfe eines deutschen Dienstleisters ausgeführt	124

(2) Transaktion wird durch einen deutschen Bitcoin-Knoten weitergeleitet	125
(3) Transaktion wird von einem deutschen Miner/Mining-Pool verarbeitet	126
(4) Bestätigen des Blocks durch einen deutschen Miner/Mining-Pool	127
dd) Zusammenfassung: Erfolgsort beim Tätigen einer „einfachen“ Transaktion	128
b) Tätigen einer Transaktion mit Mixing-Services	128
c) „Umtauschtransaktion“	129
d) Annahme einer Transaktion	129
e) Aufnahme einer inkriminierten Transaktion durch den Miner/Mining-Pool	130
f) Betreiben eines Dienstleistungs-Services	130
g) Zwischenfazit: Dezentraler Erfolgsort bei Geldwäschehandlungen mit Bitcoin	131
III. Lösungsansatz	131
1. Lösungsweg auf nationaler Ebene über das Strafanwendungsrecht	132
a) Handlungsort als einziger Anknüpfungspunkt	132
b) Globaler Erfolgsort	132
c) Vermittelnde These: Eingeschränkte Anwendung der Ubiquitätstheorie bei dezentralem Erfolgsort	135
aa) Bestimmtheitsgebot	136
bb) Willkürverbot	138
cc) „Ne bis in idem“	139
dd) Verhältnismäßigkeit	140
2. Lösungsweg auf völkerrechtlicher Ebene über bi- und/oder multilaterale Abkommen	142
3. Ergänzung des § 9 Abs. 1 StGB und Schließung völkerrechtlicher Abkommen	143
B. Die einzelnen Tatbestandsvoraussetzungen des § 261 StGB	144
I. Rechtswidrige Vortat	144
1. Gelistete Straftatbestände	145
a) Handel mit illegalen Gütern und Dienstleistungen	145
aa) § 29 Abs. 1 S. 1 Nr. 1 BtMG	146
bb) §§ 51 ff. WaffG	147
b) Betrugs- und Computerbetrugskonstellationen (§§ 263, 263a StGB)	147
aa) Subsumtion von Bitcoins unter den Vermögensbegriff	148
bb) Gewerbs- oder bandenmäßige Begehung	148
c) Erpressungskonstellationen	149
aa) Klassische Erpressungskonstellationen	150
bb) Digitale Erpressung	151

(1) Ransomware und Cryptolocker	151
(2) DDoS-Attacken	152
cc) Gewerbs- und bandenmäßige Begehung	152
d) Terrorismusfinanzierung	153
e) Zusammenfassung	154
2. Neue Konstellationen	154
a) Fremdnütziges Bitcoin-Mining	155
aa) Strafrechtliche Bewertung des fremdnütziges Bitcoin-Minings	155
(1) Bitcoin-Mining mittels Schadsoftware	155
(a) Entziehung elektrischer Energie (§ 248c StGB)	157
(aa) Tatobjekt: Elektrische Energie	157
(bb) Tathandlung: Entziehen der Energie aus einer Anlage oder Einrichtung mit Hilfe eines Leiters	158
(b) Computerbetrug (§ 263a StGB)	158
(aa) Tathandlung: Unrichtiges Gestalten eines Programms	158
(α) Gestaltung eines Programms	159
(β) Unrichtigkeit der Gestaltung	159
(bb) Vermögenserhebliche Beeinflussung des Ergebnisses einer Datenverarbeitung	161
(cc) Vorsatz und Bereicherungsabsicht	162
(c) Ausspähen von Daten (§ 202a StGB)	163
(d) Abfangen von Daten (§ 202b StGB)	164
(e) Datenveränderung (§ 303a StGB)	164
(f) Computersabotage (§ 303b StGB)	166
(g) Erschleichen von Leistung (§ 265a StGB)	167
(h) Sachbeschädigung (§ 303 StGB)	168
(i) Vorbereitungshandlungen	169
(2) Bitcoin-Mining mittels Software-Update ohne Zustimmung	169
(a) Ausspähen von Daten (§ 202a StGB)	169
(b) Datenveränderung (§ 303a StGB)	170
(c) Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)	170
(3) Bitcoin-Mining mittels Software mit Zustimmung	171
(a) Computerbetrug (§ 263a StGB)	171
(b) Ausspähen von Daten (§ 202a StGB)	172
(c) Datenveränderung (§ 303a Abs. 1 StGB)	172
(d) Sachbeschädigung (§ 303 StGB)	173
(4) Bitcoin-Mining im Rahmen von Cloud-Computing mittels Botnetz kostenloser Testzugänge	173
(a) Computerbetrug (§ 263a StGB)	174

(b) Erschleichen von Leistung (§ 265a StGB)	175
(c) Fälschung beweis erheblicher Daten (§ 269 StGB)	176
(5) Bitcoin-Mining mittels fremden Cloud-Zugangs	177
(a) Computerbetrug (§ 263a StGB)	177
(aa) Unbefugte Verwendung von Daten	177
(bb) Vermögenserheblichkeit des Datenverarbeitungs- vorgangs, Vermögensschaden und Stoffgleichheit	179
(b) Ausspähen von Daten (§ 202a StGB)	180
(6) Bitcoin-Mining mittels Nutzung fremder Rechner	180
(a) Entziehen elektrischer Energie (§ 248c StGB)	181
(b) Computerbetrug (§ 263a StGB)	181
(7) Zusammenfassung: Strafbarkeit des fremdnützigen Bitcoin-Minings	182
bb) Bedeutung des Bitcoin-Minings für die Geldwäsche	182
b) Sog. Bitcoin-Diebstahl	183
aa) „Bitcoin-Diebstahl“ im weiteren Sinne	184
(1) Phishing	184
(2) Hacking	187
(3) Sonderfall: Entwenden einer Hardware-Wallet	188
(a) Diebstahl (§ 242 StGB)	188
(aa) Vergleich zum Sparbuch und der EC-Karte	190
(bb) Übertragung auf Hardware-Wallet	190
(cc) Zwischenergebnis	191
(b) Unterschlagung (§ 246 StGB)	191
(c) Das Auslesen der privaten Schlüssel (§§ 202, 202a StGB)	192
bb) „Bitcoin-Diebstahl“ im engeren Sinne	192
(1) Untreue (§ 266 StGB)	192
(2) Computerbetrug (§ 263a StGB)	194
(3) Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB)	195
(4) Datenveränderung (§ 303a StGB)	197
(a) Löschen von Daten	198
(b) Unbrauchbarmachen von Daten	198
(c) Verändern von Daten	199
(5) Computersabotage (§ 303b StGB)	201
cc) Bedeutung des „Bitcoin-Diebstahls“ für die Geldwäsche	201
3. Erweiterung des Vortatenkatalogs um § 303a Abs. 1 StGB	202
II. Gegenstand	203
1. „Klassische“ Definition des Gegenstandsbegriffs	203
2. Bitcoins als Sache oder (Forderungs-)Recht i. S. d. „klassischen“ Definition	204

3. Auslegung des Gegenstandsbegriffs	205
a) Grammatische Auslegung	205
aa) Allgemeiner Wortsinn	206
bb) Rechtlicher Wortsinn	206
(1) Eigentum an Bitcoins	206
(2) Gemeinfreiheit von Bitcoins	208
(3) Immaterialgüterrechte an Bitcoins	208
(4) Virtuelles Eigentum an Bitcoins	209
(5) Keine Rechte an Bitcoins	211
cc) Keine Begrenzung der Gegenstandsdefinition durch den allgemeinen Wortsinn	211
b) Historische Auslegung	212
c) Systematische Auslegung	213
aa) Gegenstand im Zivilrecht	213
bb) Gegenstandsbegriff bei der Einziehung (§§ 73 ff. StGB)	215
(1) „Erlangtes Etwas“ und Gegenstandsbegriff	215
(2) Ausrichtung des § 261 StGB an §§ 73 ff. StGB?	216
cc) Bedeutung des § 261 Abs. 7 StGB	218
dd) Überschrift der Norm	219
ee) Keine eindeutige Systematik	219
d) Teleologische Auslegung	219
aa) Geldfunktionen	220
bb) Folge der fehlenden Geldfunktion von Bitcoins für die teleo- logische Auslegung des Gegenstandsbegriffs	222
4. Abstrakte Legaldefinition des Gegenstandsbegriffs als Lösung der Auslegung	223
a) Herleitung: „Virtual Property“ Diskussion aus den USA	223
b) Merkmale einer abstrakten Gegenstandsdefinition des § 261 StGB	225
aa) Abgrenzbarkeit	226
bb) Vermögenswert	226
cc) Ausschlussfunktion	227
(1) Generelle Übertragung auf Bitcoin	227
(2) Exkurs: Output, über den jeder verfügen kann	228
c) Vorschlag einer Legaldefinition des Gegenstandsbegriffs in § 261 StGB	228
III. Herrühren	228
1. Auslegung des Begriffs „Herrühren“	229
2. Aufstellung von Anforderungen an das Herrühren anhand einer Zuordnung zu Fallgruppen	231
a) Unmittelbar aus der Vortat erlangte Gegenstände	231
b) Surrogate	233
aa) Allgemeine Ausführungen	233

bb) Surrogate bei Bitcoin	234
c) Vermischung illegaler und legaler Werte	235
aa) Begriffsbestimmung	235
bb) Bemakelung der neuen Gegenstände bei Vermischung	236
(1) Total- oder Teilkontamination	236
(a) Literaturauffassungen zur Total- oder Teilkontamination bei Vermischung	236
(b) Annahme einer Totalkontamination durch die Rechtsprechung	237
(2) Bemakelungsschwelle	238
(a) Literaturauffassungen zur Bemakelungsschwelle	238
(b) „Bemakelungsformel“ der Rechtsprechung	239
(3) Erneute Surrogation eines „Mischgegenstands“	240
(a) Literaturauffassungen zur weiteren Surrogation	240
(b) Keine eindeutige Rechtsprechung zur weiteren Surrogation	241
(4) Stellungnahme	242
(a) Zur Verfassungsmäßigkeit der Totalkontaminationslehre bei der Vermischung von Giralgeld	242
(b) Zur Notwendigkeit einer Bemakelungsschwelle	245
cc) Übertragung auf Bitcoins	245
(1) Technische Grundlagen einer Transaktion	246
(2) Vermischung von Bitcoins in Transaktionen	246
(a) Vermischung auf Basis der Inputs	246
(b) Als Transaktionsgebühren	248
(3) Auswirkungen der Vermischung auf das Bitcoin-System	249
(4) Lösungsansatz	250
(a) Grund für die Totalkontaminationslehre bei Buchgeld	250
(b) Umsetzbarkeit der Teilkontamination bei Bitcoin	251
(aa) Unterschied zwischen Bitcoin und Giralgeld im Hinblick auf eine Teilkontamination	251
(bb) Transaktionssperrlisten als Vorbild für die Umsetzung der Teilkontamination	252
(α) „Poison-Modell“	253
(β) „Haircut-Modell“	254
(γ) Anordnungsbasierte Modelle	255
(cc) Geeignetes Modell zur Umsetzung einer Teilkontamination	255
(c) Verfassungsrechtliche Gründe für eine Teilkontamination bei Bitcoin	258
(d) Bemakelungsschwelle	260
dd) Ausblick: Lösungsansatz für Giralgeld?	260

IV. Tathandlungen	261
1. Tathandlungen des § 261 Abs. 1 StGB	261
a) Verbergen	262
b) Herkunft verschleiern	262
c) Das Vereiteln oder Gefährden der Einziehung oder Sicherstellung	263
d) Das Vereiteln oder Gefährden des Auffindens und der Herkunftsermittlung	264
2. Tathandlungen des § 261 Abs. 2 StGB	264
a) Sich oder einem Dritten verschaffen	265
b) Verwahren	266
c) Verwenden	267
3. Täterschaftlich verwirklichte Handlungen bei Bitcoin	267
a) Tätigen einer „einfachen“ Transaktion	267
aa) Das Verbergen	268
bb) Das Verschleiern der Herkunft	269
cc) Das Vereiteln oder Gefährden einer staatlichen Zugriffsmaßnahme	269
(1) Die Einziehung und Sicherstellung von Bitcoins	269
(a) Die Sicherstellung, sofern nur die Einziehung des Wertes von Taterträgen bejaht wird	270
(b) Die Einziehung und Sicherstellung bei Online-Wallets	271
(c) Exkurs: Die Sicherstellung, sofern die Einziehung von Taterträgen bejaht wird	271
(2) Insbesondere: Das Vereiteln oder Gefährden der staatlichen Zugriffsmaßnahmen	272
(a) Bei Annahme der Einziehung des Wertes von Taterträgen	273
(b) Spezialfall: Online-Wallet	274
(c) Exkurs: Bei Bejahung der Einziehung von Taterträgen und Tatprodukten, Tatmitteln und Tatobjekten	275
dd) Das Gefährden oder Vereiteln der Herkunftsermittlung oder des Auffindens	276
ee) § 261 Abs. 2 StGB	277
(1) Tathandlungen	278
(2) Bedeutung des Abs. 6	278
ff) Zwischenergebnis	279
b) Tätigen einer Transaktion mit Mixing-Services	280
aa) Das Verbergen und Verschleiern der Herkunft	280
bb) Weitere Tathandlungen	281
cc) Insbesondere: CoinJoin-Transaktionen	281
c) „Umtauschtransaktion“	281
aa) Das Verbergen und Verschleiern der Herkunft	282

bb) Gefährdungs- und Vereitelungstatbestand	282
cc) Tathandlungen des Abs. 2	284
dd) Sonderfall: Transaktion an einen Umtauschdienstleister bei Vorliegen eines Härtefalls	284
d) Die Entgegennahme einer inkriminierten Transaktion	285
aa) Tathandlungen des Abs. 1	286
bb) Tathandlungen des Abs. 2	288
e) Aufnahme einer inkriminierten Transaktion durch den Miner	288
aa) Tathandlungen des Abs. 1 und Abs. 2	288
bb) Insbesondere: Sichverschaffen und Verwahren	289
cc) Sonderfall: Mining-Pool	291
f) Das Betreiben eines Dienstleistungsunternehmens	291
aa) Das bloße Betreiben des Services	292
bb) Konkrete Tathandlung der Dienstleister	292
(1) Mixing-Service	292
(2) Zahlungsdienstleister	293
(3) Umtauschdienstleister	293
4. Beihilfehandlungen	294
a) Dienstleistungen	294
b) Zurverfügungstellen einer Bitcoin-Adresse	294
5. Zusammenfassung	295
V. Die innere Tatseite	295
1. Vorsätzliche Geldwäsche	296
a) Allgemeine Anforderungen an die vorsätzliche Geldwäsche	296
aa) Ungeschriebene Einschränkungen	297
bb) Geschriebene Besonderheiten	298
b) Generelle Ausführungen zum Vorsatz bei Geldwäschehandlungen mit Bitcoin	299
c) Auswirkung einer Transaktionssperlliste auf den Vorsatz	300
aa) Nachvollziehbarkeit des „Geldwegs“	300
bb) Praktische Auswirkungen auf die vorsätzliche Geldwäsche	301
(1) Bzgl. des Herrührens aus der Katalogtat	302
(a) Listung der geldwäschetauglichen Taten	302
(b) Listung aller Straftaten	303
(2) Bzgl. der Tathandlung	303
2. Leichtfertigkeit	304
a) Allgemeine Anforderungen	305
b) Generell Leichtfertigkeit bei Bitcoin-Transaktionen?	306
c) Auswirkungen einer Transaktionssperlliste auf den Leichtfertig- keitstatbestand	307
aa) Kenntnis der Listung bei Listung aller Straftaten	307
bb) Erkundigungspflicht des Nutzers bei ausschließlicher Lis- tung geldwäschetauglicher Straftaten	307

3. Folgen der Auswirkung einer Transaktionssperlliste auf die innere Tatseite	309
a) Unterschiedliche Wertigkeit von Bitcoins	309
b) Umgang mit Entwertung von Bitcoins durch die Sperllisten	310
4. Einschränkung des § 261 StGB durch analoge Anwendung des Abs. 2 und Abs. 6	311
5. Exkurs: Risikobewertungsdienste	313
a) Funktionsweise/Konzept eines Risikobewertungsdienstes bei Bitcoin	313
b) Bestehende Risikobewertungsmodelle	315
aa) Hintergründe des GwG	315
bb) Insbesondere: Die Meldepflicht von Verpflichteten nach § 43 GwG	316
cc) Strafbarkeit des Bankmitarbeiters im Zusammenhang mit § 43 GwG	318
(1) Konstellation 1	319
(a) Bedeutung der Anhaltspunktepapiere	319
(aa) Anhaltspunktepapiere und Vorsatzerfordernisse	319
(bb) Normative Wirkung der Anhaltspunktepapiere	321
(b) Bedeutung der Empirie	322
(c) Zwischenergebnis	325
(2) Konstellation 2	326
c) Übertragung der aufgestellten Grundsätze auf Bitcoin	328
aa) Transfer von „gelb“ gelisteten Bitcoins	328
bb) Transfer von „grün“ gelisteten Bitcoins	329
d) Risikobewertungsdienste als Beitrag zur Konkretisierung der inneren Tatseite	330

Kapitel 6

Zusammenfassung	331
Literaturverzeichnis	342
Sachwortverzeichnis	369

Kapitel 1

Einleitung

Am 29. Oktober 1969 fiel auf dem Gelände der University of California in Los Angeles der Startschuss für die Ära des Internets. Damals wurde ein Computer durch eine 50-Kilobit-Datenleitung mit einem anderen, der sich im Stanford Research Institute befand, verbunden. Übertragen werden sollte das Wort „Login“. Bevor der Rechner abstürzte gelang über eine Entfernung von gut 500 Kilometern die Übertragung der Buchstaben „L“ und „o“. Beim „g“ endete der Prozess. Um 22.30 Uhr am selben Tag wurde die erneute Übertragung schließlich erfolgreich durchgeführt.¹

Vergleicht man die Geburtsstunde des Internets mit seiner heutigen Bedeutung, so ist eine rasante Entwicklung zu konstatieren. Das Internet ist aus dem alltäglichen Leben nicht mehr wegzudenken. So erkennt z.B. die zivilrechtliche Rechtsprechung an, dass das Internet auch im privaten Bereich eine so zentrale Bedeutung in der alltäglichen Lebensführung einnimmt, dass bei Nutzungsausfall auch ohne Nachweis eines konkreten Schadens ein Ersatzanspruch besteht.² Eine Betrachtung der Zahlen der Internetnutzer weltweit unterstreicht, dass das Internet aus unserem Leben nicht mehr wegzudenken ist. Waren es Ende 2000 noch 360 Millionen Internetnutzer, so wurden Ende 2017 bereits 4,16 Milliarden verzeichnet, was einem Bevölkerungsanteil von 54,4% entspricht.³

A. Problembeschreibung

Neben zahlreichen Vorteilen der weltweiten Vernetzung, wie z. B. dem raschen Austausch von Informationen zwischen beliebig vielen Personen,⁴ hat das Internet auch seine Schattenseiten. So bieten sich für Kriminelle eine Vielzahl an Möglichkeiten, die Vorteile des Internets für ihre Zwecke zu

¹ s. zu diesen dargestellten Anfängen des Internets: https://www.welt.de/welt_print/article1308095/Der-29-Oktober-ist-Internet-Tag.html; <http://www.sueddeutsche.de/digital/internet-jubilaeum-ja-wir-haben-das-l-1.143932> (alle Links zuletzt abgerufen am 18.01.2018).

² s. dazu: BGH, Urt. v. 24.01.2013 – III ZR 98/12 = BGHZ 196, 101.

³ <http://www.internetworldstats.com/stats.htm> (zuletzt abgerufen am 23.08.2018).

⁴ *Hilgendorf*, ZStW 113 (2001), 650.

missbrauchen. Die sog. Cyberkriminalität hat in den letzten Jahren an Bedeutung gewonnen. Nach der Definition des Bundeskriminalamtes umfasst

„Cybercrime die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden“.⁵

Als besonders problematisch im Hinblick auf die Bekämpfung wird die rasante Entwicklung des Deliktsbereichs identifiziert.⁶ Oftmals sind durch Cyberkriminalität nicht nur Einzelpersonen, sondern ein größerer Teil der Gesellschaft betroffen. So befiel im Mai 2017 z.B. die erpresserische Software „WannaCry“ weltweit mehr als 240.000 Computer, darunter auch (insbesondere in Großbritannien) sog. kritische Infrastrukturen, wie z.B. Krankenhäuser.⁷ Die Täter nutzten dabei eine vorhandene Sicherheitslücke bei Windows-Betriebssystemen aus, um die Schadsoftware einzuschleusen. War ein Computersystem befallen, so wurden Daten des Systems verschlüsselt und für deren Freigabe die Zahlung von Bitcoins gefordert.⁸ Bei letzteren handelt es sich um eine dezentrale virtuelle Kryptowährung – ein globales, legales Phänomen dieses Jahrzehnts. Dieses „virtuelle Geld“ bietet seinen Nutzern viele Vorteile: Aufgrund der Tatsache, dass es unabhängig von Notenbanken, Staaten und Kreditinstituten direkt zwischen den Nutzern gehandelt wird, entzieht es sich nahezu vollständig staatlichen Eingriffsmöglichkeiten, der Einsatz ist weltweit möglich und es garantiert (vermeintliche) Anonymität. All diese Eigenschaften ziehen jedoch auch Kriminelle an und stellen somit eine große Herausforderung für Strafverfolger und die Prävention von Kriminalität dar.⁹

Ein Kriminalitätsphänomen, das im Zusammenhang mit virtuellen Kryptowährungen stets Erwähnung findet, ist Geldwäsche. Aufgrund der o.g. Eigenschaften verwundert dies zunächst nicht. Neben der Problematik, wie

⁵ s. zu dieser Definition: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html (zuletzt abgerufen am 18.01.2018).

⁶ https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html (zuletzt abgerufen am 18.01.2018).

⁷ s. Berichte über „WannaCry“ z.B. unter: <http://www.handelsblatt.com/unternehmen/it-medien/cyberangriff-mit-wanna-cry-die-spuren-fuehren-nach-nordkorea/19843548.html>; <http://www.sueddeutsche.de/digital/wannacry-europol-warnt-vor-eskalation-der-angriffe-mit-erpresser-software-1.3504847>; <https://www.heise.de/news/ticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html> (alle Links zuletzt abgerufen am 18.01.2018).

⁸ Eine Schadsoftware, die dergestalt arbeitet, wird als Ransomware bezeichnet. Dabei handelt es sich um eine erpresserische Schadsoftware, die den Zugriff auf das infizierte Gerät erschwert oder gänzlich verhindert. Die Freigabe wird nach Leistung einer Zahlung versprochen.

⁹ s. zu alledem auch schon: *Böhme/Grzywotz/Pesch/Rückert/Safferling*, Prävention von Straftaten mit Bitcoins und Alt-Coins, S. 1.

Geldwäsche mit Bitcoins effektiv verfolgt bzw. schon verhindert werden kann, ist die Frage aufzuwerfen, ob das materielle Recht neuen technischen Phänomenen, wie Bitcoin, gewachsen ist. Es ist nicht zu leugnen, dass die Entwicklung von Recht und Technik stark auseinandergeht. Während sich letztere Materie rasant weiterentwickelt, entsteht der Eindruck, dass das Recht dem Tempo dieser Entwicklung nicht gewachsen ist und der Technologie „hinterherhinkt“.

Anhand der Geldwäsche mit Bitcoins untersucht diese Arbeit, inwiefern neue technische Phänomene, wie virtuelle Kryptowährungen, das materielle Strafrecht vor Herausforderungen stellen.

B. Gang der Untersuchung

Um sich sinnvoll mit dieser Problematik auseinanderzusetzen, ist zunächst eine technische Beschreibung des Phänomens virtueller Kryptowährungen am Beispiel von Bitcoin als bekanntester Vertreter vorzunehmen (Kap. 2). Darüber hinaus ist zum einen eine Auseinandersetzung mit dem bestehenden Geldwäschetatbestand, der im deutschen Strafgesetzbuch in § 261 normiert ist, zum anderen eine Analyse bereits bestehender Geldwäschetechniken, unerlässlich (Kap. 3). Schließlich treffen mit Geldwäsche und Bitcoin zwei globale Phänomene aufeinander (Kap. 4). Dass darin eine „Gefahr“ erblickt wird, wird anhand der Darstellung von Stellungnahmen internationaler Institutionen zu dieser Problematik unterstrichen (Kap. 4, A.). Inwiefern Bitcoin sich tatsächlich zur Geldwäsche eignet, insbesondere, welche Eigenschaften der virtuellen Kryptowährung als Katalysator für die Geldwäsche anzusehen sind und welche neuen Geldwäschetechniken sich hieraus ergeben, wird in einem weiteren Schritt dargestellt (Kap. 4, B.). Der Schwerpunkt dieser Arbeit liegt sodann auf einer „bitcoinspezifischen“ Analyse des § 261 StGB (Kap. 5). Dabei wird die Frage nach der Anwendbarkeit des deutschen Strafrechts (Kap. 5, A.) einer Untersuchung der einzelnen Tatbestandsmerkmale (Kap. 5, B.) vorangestellt. Im Rahmen der Analyse rechtswidriger Vortaten mit Bitcoin (Kap. 5, B. I.) werden neben „bekannten“ Konstellationen, wie das o.g. Beispiel einer digitalen Erpressung, neue Fallkonstellationen, die durch das neue technische Phänomen Bitcoin entstehen, untersucht – namentlich das sog. fremdnützige Bitcoin-Mining und der sog. Bitcoin-Diebstahl. Im weiteren Verlauf wird der Gegenstandsbegriff des § 261 StGB in den Blick genommen und ausgelegt (Kap. 5, II). Hauptaugenmerk im Bereich des Tatbestandsmerkmals „Herrühren“ (Kap. 5, B. III.) ruht auf der Frage nach dem Umgang mit der Vermischung legaler und illegaler Werte. Bereits hier wird auf den Vorschlag ein Präventionskonzept, den sog. Transaktions-sperrlistenansatz, einzuführen, eingegangen. Eine noch größere Bedeutung