

Timo Purkott
Barbara Scheben (Hrsg.)

KRYPTO-ASSET COMPLIANCE

Umsetzung der Regulierung
und Geldwäsche-Prävention

SCHÄFFER
POESCHEL

Hinweis zum Urheberrecht:

Alle Inhalte dieses eBooks sind urheberrechtlich geschützt.

Bitte respektieren Sie die Rechte der Autorinnen und Autoren, indem Sie keine ungenehmigten Kopien in Umlauf bringen.

Dafür vielen Dank!

Krypto-Asset-Compliance

Timo Purkott/Barbara Scheben (Hrsg.)

Krypto-Asset-Compliance

Umsetzung der Regulierung und Geldwäsche-Prävention

Schäffer-Poeschel Verlag Stuttgart

Bibliografische Information der Deutschen Nationalbibliothek

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

Print: ISBN 978-3-7910-6332-4 Bestell-Nr. 11605-0001
ePub: ISBN 978-3-7910-6333-1 Bestell-Nr. 11605-0100
ePDF: ISBN 978-3-7910-6334-8 Bestell-Nr. 11605-0150

Timo Purkott/Barbara Scheben (Hrsg.)

Krypto-Asset-Compliance

1. Auflage, Oktober 2025

© 2025 Schäffer-Poeschel Verlag für Wirtschaft · Steuern · Recht GmbH
Breitscheidstr. 10, 70174 Stuttgart
www.schaeffer-poeschel.de | service@schaeffer-poeschel.de

Bildnachweis (Cover): Starkekonzepte, Christina Peter, Wörthsee

Produktmanagement: Anna Pietras

Lektorat: Barbara Buchter, extratour, Freiburg

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Alle Rechte, insbesondere die der Vervielfältigung, des auszugsweisen Nachdrucks, der Übersetzung und der Einspeicherung und Verarbeitung in elektronischen Systemen, vorbehalten. Der Verlag behält sich auch eine Nutzung des Werks für Text und Data Mining im Sinne von § 44b UrhG vor. Alle Angaben/Daten nach bestem Wissen, jedoch ohne Gewähr für Vollständigkeit und Richtigkeit.

Schäffer-Poeschel Verlag Stuttgart
Ein Unternehmen der Haufe Group SE

Sofern diese Publikation ein ergänzendes Online-Angebot beinhaltet, stehen die Inhalte für 12 Monate nach Einstellen bzw. Abverkauf des Buches, mindestens aber für zwei Jahre nach Erscheinen des Buches, online zur Verfügung. Ein Anspruch auf Nutzung darüber hinaus besteht nicht.

Sollte dieses Buch bzw. das Online-Angebot Links auf Webseiten Dritter enthalten, so übernehmen wir für deren Inhalte und die Verfügbarkeit keine Haftung. Wir machen uns diese Inhalte nicht zu eigen und verweisen lediglich auf deren Stand zum Zeitpunkt der Erstveröffentlichung.

Inhaltsübersicht

Abkürzungsverzeichnis	15
Vorwort	19
A Einführung	21
1 Technische Grundlagen von Krypto-Assets	23
<i>Dirk Siegel</i>	
2 Entwicklung und Regulierung von Krypto-Assets: Historie, Markttrends, Skandale	43
<i>Robert Wilkens / Yannik Lindt</i>	
B Kapitalmarkt- und Bankaufsichtsrecht	69
3 Kapitalmarkt- und bankaufsichtsrechtliche Aspekte von Krypto-Assets	71
<i>Ulrich Keunecke / Marc Pussar</i>	
C Anti-Financial Crime	103
4 Prävention von Geldwäsche und Terrorismusfinanzierung	105
<i>Alexander Geschonneck / Robert Wilkens</i>	
5 Prävention von Verstößen gegen Finanzsanktionen	137
<i>Timo Purkott / Alexander Klöpffer</i>	
6 Ransomware-Zahlungen	151
<i>Barbara Scheben / Yannik Lindt</i>	
7 Praktische Umsetzung von Sicherungsmaßnahmen	169
<i>Timo Purkott / Alexander Klöpffer</i>	
D Tax- und Accounting-Compliance	183
8 Bilanz- und steuerrechtliche Aspekte von Krypto-Assets	185
<i>Hanne Böckem / Caroline Geuer / Florian Merkel / Malte Shurety / Dennis Rennekamp</i>	
E Datenschutzrecht	237
9 Krypto-Assets und Datenschutzrecht	239
<i>Maik Ringel</i>	
Literaturverzeichnis	273
Autorinnen und Autoren	283

Inhaltsverzeichnis

Abkürzungsverzeichnis	15
Vorwort	19
A Einführung	21
1 Technische Grundlagen von Krypto-Assets	23
<i>Dirk Siegel</i>	
1.1 Überblick	23
1.2 Das Bitcoin-Blockchain-Netzwerk	24
1.3 Blockchain-Netzwerke mit Smart-Contract-Fähigkeit am Beispiel Ethereum	31
1.4 DeFi – Decentralized Finance	35
1.5 Risiken und weitere Entwicklung	39
2 Entwicklung und Regulierung von Krypto-Assets: Historie, Markttrends, Skandale	43
<i>Robert Wilkens / Yannik Lindt</i>	
2.1 Historie und Marktentwicklung von Krypto-Assets	43
2.1.1 Die Zeit vor Bitcoin	43
2.1.2 Die Anfänge: Bitcoin und die Blockchain-Technologie	45
2.1.3 Die erste Welle: Altcoins und die Diversifizierung des Marktes	46
2.1.4 Die zweite Welle: Initial Coin Offerings (ICOs) und regulatorische Herausforderungen	47
2.1.5 Die dritte Welle: DeFi und NFTs	49
2.1.6 Technologische Innovationen und ihre Auswirkungen	50
2.1.7 Ein schnell wachsendes Ökosystem	50
2.1.8 Institutionelle Akzeptanz und Investitionen	52
2.1.9 Digitales Zentralbankgeld als Gegenentwurf?	52
2.1.10 Aktueller Stand mit Blick auf die Zukunft	53
2.2 Regulatorische Entwicklungen in Deutschland und der EU	56
2.2.1 Internationale Standards der FATF	58
2.2.2 Fünfte EU-Geldwäscherichtlinie und Umsetzung in Deutschland	59
2.2.3 eWPG und DLT Pilot Regime	60
2.2.4 Erstreckung der »Travel Rule« auf Kryptotransaktionen	61
2.2.5 Verabschiedung der Verordnung »Markets in Crypto Assets« (MiCA)	61
2.3 Wesentliche Skandale in der Geschichte der Krypto-Assets	63
2.3.1 FTX: Ein Fall von Missmanagement und Betrug	63
2.3.2 OneCoin: Ein Ponzi-System im digitalen Zeitalter	64
2.3.3 Große Hacks: Sicherheitslücken und ihre Folgen	65

B	Kapitalmarkt- und Bankaufsichtsrecht	69
3	Kapitalmarkt- und bankaufsichtsrechtliche Aspekte von Krypto-Assets	71
	<i>Ulrich Keunecke / Marc Pussar</i>	
3.1	Einleitung	71
3.2	Rechtliche Einordnung von Krypto-Assets	72
3.3	Liquidität und Handel	74
3.4	Verwahrung und Zugang	74
3.5	Kapitalmarktregulierung für Krypto-Assets	75
3.5.1	Regulierungsweichen für Krypto-Assets	76
3.5.2	Anforderungen an Token-Emissionen	77
3.5.2.1	Emission von ART-Token	77
3.5.2.2	Emission von EMT-Token	79
3.5.2.3	Emission sonstiger von MiCAR erfasster Kryptowerte (Utility Token)	80
3.5.2.4	Emissionsanforderungen bei Token, die als Finanzinstrument qualifizieren	81
3.5.2.5	Inhalt und Form eines Kryptowerte-Whitepapers	82
3.5.2.6	Berichtigung eines Kryptowerte-Whitepapers	84
3.5.2.7	Marketingmitteilungen	84
3.5.2.8	Haftung für den Inhalt eines Kryptowerte-Whitepapers	85
3.5.3	Tokenisierung von Vermögenswerten	86
3.5.3.1	Immobilien-Token	86
3.5.3.2	Equity-Token	87
3.6	Bankaufsichtsrechtliche Aspekte	88
3.6.1	Entwicklung der Regulierung von Krypto-Assets	88
3.6.2	Regulierungsrahmen für Krypto-Assets in Deutschland	90
3.6.3	Kreditwesengesetz	91
3.6.4	Wertpapierinstitutsgesetz	91
3.6.5	Gesetz über elektronische Wertpapiere	92
3.6.6	MiCAR	92
3.6.7	Zahlungsdienstenaufsichtsgesetz	93
3.6.8	DLT-Pilot Regime	94
3.6.9	Zusammenspiel der relevanten Normen	94
3.6.10	Erlaubnis und Zulassungstatbestände für Krypto-Assets	96
3.6.10.1	Einlagengeschäft	96
3.6.10.2	Kreditgeschäft	96
3.6.10.3	Verwahrung und Verwaltung von Kryptowerten	97
3.6.10.4	Betrieb einer Handelsplattform	97
3.6.10.5	Tausch von Kryptowerten gegen Geld	98
3.6.10.6	Ausführung von Kundenaufträgen	99
3.6.10.7	Platzierung von Kryptowerten	99

3.6.10.8	Annahme und Übermittlung von Aufträgen	100
3.6.10.9	Beratung zu Kryptowerten / Anlageberatung	101
3.6.10.10	Portfolioverwaltung von Kryptowerten	101
3.6.10.11	Transferdienstleistungen	102
3.7	Ausblick zur Regulierung von Krypto-Assets	102
C	Anti-Financial Crime	103
4	Prävention von Geldwäsche und Terrorismusfinanzierung	105
	<i>Alexander Geschonneck / Robert Wilkens</i>	
4.1	Einleitung	105
4.2	Was versteht man unter Geldwäsche und Terrorismusfinanzierung?	106
4.3	Die Nutzung von Krypto-Assets für Zwecke der Geldwäsche und Terrorismusfinanzierung	109
4.4	Entwicklung und Ausmaß der krypto-basierten Geldwäsche und Terrorismusfinanzierung	114
4.5	Regulatorischer Rahmen	117
4.6	Verpflichtete: Wer muss geldwäscherechtliche Vorgaben einhalten?	121
4.6.1	Verpflichtete aus dem Finanzsektor	122
4.6.2	Verpflichtete aus dem Nicht-Finanzsektor	123
4.7	Von den Verpflichteten einzuhaltende Anforderungen	125
4.7.1	Risikomanagement	126
4.7.1.1	Risikobasierter Ansatz	126
4.7.1.2	Risikoanalyse	127
4.7.1.3	Interne Sicherungsmaßnahmen	129
4.7.2	Sorgfaltspflichten gegenüber Kunden	132
4.7.3	Meldepflichten	135
4.8	Fazit	136
5	Prävention von Verstößen gegen Finanzsanktionen	137
	<i>Timo Purkott / Alexander Klöpffer</i>	
5.1	Was versteht man unter Finanzsanktionen?	137
5.2	Die Nutzung von Krypto-Assets zur Umgehung von Sanktionen	138
5.2.1	Überblick	138
5.2.2	Ausgewählte Mechanismen zur Umgehung von Sanktionen mit Krypto-Assets	138
5.2.2.1	Alternative Zahlungswege	138
5.2.2.2	Mining	139
5.2.2.3	Verwendung von Mixing-Diensten	140

5.3	Regulatorischer Rahmen	143
5.3.1	Finanzsanktionen der EU	144
5.3.1.1	Überblick	144
5.3.1.2	Auch Krypto-Asset-Transaktionen sind erfasst	144
5.3.1.3	Anforderungen an die Verhinderung von Sanktionsverstößen	145
5.3.1.4	Ausblick: Sanctions Compliance zukünftig Teil der Anti-Geldwäsche-Vorgaben	146
5.3.2	Exkurs: Finanzsanktionen der USA	148
6	Ransomware-Zahlungen	151
	<i>Barbara Scheben / Yannik Lindt</i>	
6.1	Einleitung	151
6.2	Ransomware-Attacken	152
6.3	Die Attraktivität von Kryptowährungen für Cyberkriminelle	154
6.4	Vor- und Nachteile der Zahlung von Lösegeld	155
6.5	Strafrechtliche Aspekte der Zahlung von Lösegeldern	155
6.5.1	Interessenabwägung	157
6.5.2	Zahlung an Angreifer im Ausland	160
6.5.3	Handlungsempfehlungen	161
6.5.4	Exkurs: Ein Blick in die USA	164
6.6	Fazit und Ausblick	166
7	Praktische Umsetzung von Sicherungsmaßnahmen	169
	<i>Timo Purkott / Alexander Klöpfer</i>	
7.1	Einleitung	169
7.1.1	Regulatorischer Hintergrund	169
7.1.2	Relevanz des Geschäftsmodells und der angebotenen Dienstleistungen	170
7.1.3	Anpassung und Neuaufbau von Prozessen	170
7.1.4	Software	170
7.1.5	Fachwissen der (Compliance-)Mitarbeiter	171
7.2	Die Risikoanalyse als Ausgangspunkt	171
7.2.1	Verpflichtete nach dem Geldwäschegesetz	171
7.2.2	Entwicklung und Status quo im Finanzsektor	172
7.3	Umsetzung und Ausgestaltung von Sicherungsmaßnahmen	173
7.3.1	Einleitung	173
7.3.2	Einsatz von »Blockchain Analytics«	173
7.3.2.1	Hintergrund und Überblick	173
7.3.2.2	Ausgewählte Methoden der Risikoattribution	174
7.3.2.3	Anwendungsfälle für Blockchain Analytics in der Compliance	176
7.3.3	»Travel Rule«	179
7.3.3.1	Historische Entwicklung	179
7.3.3.2	Der regulatorische Rahmen in Deutschland	180

7.3.3.3	Praktische Umsetzung der Regulierung	181
7.3.3.4	Technische Herausforderungen und Lösungsansätze	181
D	Tax- und Accounting-Compliance	183
8	Bilanz- und steuerrechtliche Aspekte von Krypto-Assets	185
	<i>Hanne Böckem / Caroline Geuer / Florian Merkel / Malte Shurety / Dennis Rennekamp</i>	
8.1	Einleitung	185
8.2	Grundlagen der Bilanzierung	186
8.2.1	IFRS	186
8.2.2	HGB	187
8.2.3	Ertragsteuerliche Besonderheiten	188
8.3	Bilanzierung von Payment Token	189
8.3.1	Sachverhalt	189
8.3.2	IFRS	190
8.3.2.1	Bilanzierung beim Halter	190
8.3.2.2	Bilanzierung beim Emittenten	192
8.3.3	HGB	192
8.3.3.1	Bilanzierung beim Halter	192
8.3.3.2	Bilanzierung beim Emittenten	195
8.3.4	Ertragsteuerrechtliche Besonderheiten	195
8.3.4.1	Ertragsteuerliche Besonderheiten beim Halter	196
8.3.4.2	Ertragsteuerliche Besonderheiten beim Emittenten	201
8.3.4.3	Veräußerungsvorgänge	202
8.4	Bilanzierung von Security und Asset Token	205
8.4.1	Sachverhalt	205
8.4.2	IFRS	206
8.4.2.1	Bilanzierung beim Halter	206
8.4.2.2	Bilanzierung beim Emittenten	209
8.4.3	HGB	210
8.4.3.1	Bilanzierung beim Halter	210
8.4.3.2	Bilanzierung beim Emittenten	212
8.4.4	Ertragsteuerrechtliche Besonderheiten	213
8.4.4.1	Ertragsteuerliche Besonderheiten beim Halter	213
8.4.4.2	Ertragsteuerliche Besonderheiten beim Emittenten	214
8.5	Bilanzierung von Utility Token	214
8.5.1	Sachverhalt	214
8.5.2	IFRS	215
8.5.2.1	Bilanzierung beim Halter	215
8.5.2.2	Bilanzierung beim Emittenten	217

8.5.3	HGB	218
8.5.3.1	Bilanzierung beim Halter	218
8.5.3.2	Bilanzierung beim Emittenten	219
8.5.4	Ertragsteuerrechtliche Besonderheiten	220
8.5.4.1	Ertragsteuerliche Besonderheiten beim Halter	220
8.5.4.2	Ertragsteuerliche Besonderheiten beim Emittenten	221
8.6	Ertragsteuerliche Mitwirkungs- und Erklärungspflichten	221
8.6.1	Allgemeine Mitwirkungspflichten	221
8.6.1.1	Mitwirkung bei der Steuererklärung	221
8.6.1.2	Erweiterte Mitwirkungspflichten bei Auslandssachverhalten	221
8.6.2	Dokumentationspflichten	222
8.6.2.1	Grundsatz: Lückenlose Nachvollziehbarkeit	222
8.6.2.2	Erforderliche Inhalte der Dokumentation	222
8.6.3	Besonderheiten bei Steuerreports	222
8.6.3.1	Voraussetzungen für die Anerkennung	222
8.6.3.2	Kursbewertung anhand von Tageskursen	223
8.6.4	Aufbewahrungspflichten	223
8.6.4.1	Privatvermögen	223
8.6.4.2	Besondere Schwellen bei hohen Einkünften	223
8.6.5	Besondere Pflichten bei Betriebsvermögen	223
8.7	Umsatzsteuerliche Behandlung	224
8.7.1	Allgemeines zur Umsatzsteuer	224
8.7.2	Umsatzsteuer beim Halter	227
8.7.2.1	Halten von Krypto-Assets als unternehmerische Tätigkeit	227
8.7.2.2	Handel mit Payment Token	228
8.7.2.3	Handel mit Security Token und Asset Token	229
8.7.2.4	Handel mit Utility Token	230
8.7.2.5	Probleme im Zusammenhang mit dem Leistungsort	231
8.7.3	Umsatzsteuer beim Emittenten	232
8.7.3.1	Ausgabe von Krypto-Assets als unternehmerische Tätigkeit	233
8.7.3.2	Ausgabe von Payment Token	233
8.7.3.3	Ausgabe von Security Token und Asset Token	234
8.7.3.4	Ausgabe von Utility Token	234
8.7.3.5	Vorsteuerabzug im Zusammenhang mit Token-Emissionen	234
8.7.4	Besonderheiten beim Mining	235
8.8	Ausblick	236

E	Datenschutzrecht	237
9	Krypto-Assets und Datenschutzrecht	239
	<i>Maik Ringel</i>	
9.1	Rechtliche Grundlagen des Datenschutzes	239
9.2	Anwendungsbereich des Datenschutzrechts	240
9.2.1	Sachlicher Anwendungsbereich	240
9.2.1.1	Automatisierte Verarbeitung von Daten	240
9.2.1.2	Verarbeitung personenbezogener Daten	241
9.2.2	Räumlicher Anwendungsbereich	244
9.3	Adressaten datenschutzrechtlicher Pflichten	245
9.3.1	Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO	245
9.3.2	Gemeinsame Verantwortliche	249
9.3.3	Auftragsverarbeiter	250
9.4	Grundsätze der Verarbeitung personenbezogener Daten	251
9.5	Rechtmäßigkeit der Verarbeitung	254
9.5.1	Einwilligung der Betroffenen	254
9.5.2	Verarbeitung zur Anbahnung und Erfüllung von Verträgen	256
9.5.3	Verarbeitung zur Erfüllung rechtlicher Verpflichtungen	258
9.5.3.1	Geldwäscherechtliche Pflicht zur Identifizierung von Kunden	259
9.5.3.2	Sanktionsrechtliches Bereitstellungsverbot	259
9.5.3.3	Pflicht zur Unterhaltung eines angemessenen Risikomanagements	261
9.5.4	Verarbeitung zur Wahrung berechtigter Interessen	262
9.5.5	Verarbeitung von besonderen Kategorien personenbezogener Daten	265
9.6	Transparenzpflichten und Betroffenenrechte	265
9.6.1	Informationspflichten	265
9.6.2	Betroffenenrechte	267
9.6.2.1	Recht auf Auskunft	267
9.6.2.2	Recht auf Berichtigung	267
9.6.2.3	Recht auf Löschung	268
9.6.2.4	Recht auf Einschränkung der Verarbeitung	269
9.7	Datentransfer in Drittstaaten	269
9.8	Weitere Compliance-Vorschriften	271
	Literaturverzeichnis	273
	Autorinnen und Autoren	283

Abkürzungsverzeichnis

a. A.	Andere Ansicht
Abs.	Absatz
AktG	Aktiengesetz
AO	Abgabenordnung
Art.	Artikel
ART	Asset-Referenced Token
AStG	Außensteuergesetz
AWG	Außenwirtschaftsgesetz
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BayLfD	Bayerischer Landesbeauftragter für den Datenschutz
BDSG	Bundesdatenschutzgesetz
BFH	Bundesfinanzhof
Bio.	Billionen
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drucks.	Bundestags-Drucksache
CASP	Crypto Asset Service Provider
CBDC	Central Bank Digital Currency
CCAF	Cambridge Center for Alternative Finance
CFSP-Liste	Consolidated Financial Sanctions Party List
CSDR	Central Securities Depositories Regulation
DAO	Dezentrale autonome Organisation
dAPI	Decentral Application Programming Interface
dApp	Decentralised Application (dezentrale Anwendung)
DeAI	Dezentralisierte KI
DeFi	Decentralised Finance
DePIN	Decentralised Physical Infrastructure Networks (Dezentrale physische Infrastrukturnetzwerke)
DEX	Decentralised Exchanges (dezentrale Börsen für Krypto-Assets)
DLT	<i>Distributed Ledger Technology</i>
DORA	Digital Operational Resilience Act
DPoS	Delegated Proof of Stake
DSGVO	Datenschutz-Grundverordnung
EBA	European Banking Authority
EDSA	Europäischer Datenschutzausschuss
EFRAG	European Financial Reporting Advisory Group

EMT	E-Money Token
ESMA	European Securities and Markets Authority
EStG	Einkommensteuergesetz
ETO	Equity-Token-Offerings
EuGH	Europäischer Gerichtshof
EZB	Europäische Zentralbank
EU-Prospekt-VO	EU-Prospektverordnung
eWpG	Gesetz über elektronische Wertpapiere
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSB	Financial Stability Board
FVOCI	Fair Value through Other Comprehensive Income
FVTPL	Fair Value through Profit or Loss
GASP	Gemeinsame Außen- und Sicherheitspolitik
ggf.	gegebenenfalls
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GO Rh-Pf	Gemeindeordnung Rheinland-Pfalz
GRCh	Charta der Grundrechte der Europäischen Union
GTVO	Geldtransferverordnung
GwG	Geldwäschegesetz
HGB	Handelsgesetzbuch
i. d. R.	in der Regel
i. S. d.	im Sinne des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IASB	International Accounting Standards Board
ICO	Initial Coin Offering
ICRI	Counter Ransomware Initiative
IFRIC	IFRS Interpretations Committee
IFRS	International Financial Reporting Standards
IoT	Internet of Things
ITS	Implementing Technical Standards
KAGB	Kapitalanlagegesetzbuch
KMAG	Kryptomärkteaufsichtsgesetz
KPI	Key Performance Indicator
KryptoWTransferV	Kryptowertetransferverordnung
KWG	Kreditwesengesetz
KYC	Know your Customer
lit.	littera (Buchstabe)
m. w. N.	mit weiteren Nachweisen
MaRisk	Mindestanforderungen an das Risikomanagement
MiCA	Markets in Crypto Assets

MiCAR	Markets in Crypto-Assets Regulation
MiFID	Markets in Financial Instruments Directive (Finanzmarkttrichtlinie)
MiFIR	Markets in Financial Instruments Regulation
Mio.	Million(en)
Mrd.	Milliarde(n)
MTF	Multilateral Trading Facility (Multilaterales Handelssystem)
MwStSystRL	Mehrwertsteuer-Systemrichtlinie
MwStVO	Mehrwertsteuer-Durchführungsverordnung
NFT	Non-Fungible Token
NGO	Non-governmental Organisation
Nr.	Nummer
OFAC	Office of Foreign Assets Control
OK	Organisierte Kriminalität
OSINT	Open Source Intelligence
OTF	Organised Trading Facility (Organisiertes Handelssystem)
OWiG	Gesetz über Ordnungswidrigkeiten
PoS	Proof of Stake
Rn.	Randnummer
RTS	Regulatory Technical Standard
S.	Seite
SDN-Liste	Specially Designated Nationals and Blocked Persons list
SGB	Sozialgesetzbuch
SPV	Special Purpose Vehicle (Zweckgesellschaft)
StGB	Strafgesetzbuch
STO	Security-Token-Offerings
TOM	Technischen und organisatorischen Maßnahmen
u. E.	unseres Erachtens
USD	US-Dollar
USDT	Tether (US-Dollar nachbildende Kryptowährung)
UStG	Umsatzsteuergesetz
VAG	Versicherungsaufsichtsgesetz
VASP	Virtual Asset Service Provider
VermAnlG	Vermögensanlagegesetz
VVG	Versicherungsvertragsgesetz
VwGO	Verwaltungsgerichtsordnung
WpPG	Wertpapierprospektgesetz
WpIG	Wertpapierinstitutsgesetz
ZAG	Zahlungsdienstaufsichtsgesetz

Vorwort

Liebe Leserinnen und Leser,

die Blockchain-Technologie hat das Potenzial, viele Aspekte unseres Lebens, unserer Unternehmen und unserer Wirtschaft grundlegend zu verändern. Durch Blockchain-basierte Krypto-Assets entstand die Möglichkeit, Transaktionen dezentralisiert, schnell, transparent, sicher und zuverlässig durchzuführen – und das ohne zentrale Bestätigungsinstanz, global und voll automatisierbar. Die sich daraus ergebenden Potenziale gehen weit über den ursprünglichen Zweck alternativer Zahlungssysteme hinaus, sodass sich kontinuierlich neue spannende Anwendungsfälle entwickeln.

Branchenübergreifend setzen sich Unternehmen mit den Einsatzmöglichkeiten digitaler Assets auseinander. Vor allem der Finanzsektor greift das Thema proaktiv auf, um Märkte zu vereinfachen und Prozesse effizienter zu gestalten. Gleichzeitig sehen sich Unternehmen dabei auch mit vielfältigen Herausforderungen konfrontiert. Wenn es darum geht, die Potenziale von Krypto-Assets gewinnbringend für das eigene Geschäftsmodell nutzbar zu machen, werden insbesondere die damit verbundenen rechtlichen Unsicherheiten als wesentlicher Hemmfaktor wahrgenommen. Zwar haben sich die regulatorischen Rahmenbedingungen in den letzten Jahren nach und nach konkretisiert, dennoch zeigt sich, dass die Entwicklung der diesbezüglichen rechtlichen Vorgaben – ebenso wie die Entwicklung des Kryptosektors insgesamt – von einer hohen und anhaltenden Dynamik geprägt ist.

Mit dem vorliegenden Buch wollen wir unseren Beitrag dazu leisten, die regulatorische Landschaft rund um die geschäftliche Nutzung von Krypto-Assets greifbar zu machen. Unser Ziel war es, Entscheidungsträgern¹ und Compliance-Verantwortlichen einen fundierten und anwendungsorientierten Leitfaden an die Hand zu geben, der das Thema aus den verschiedenen Compliance-Perspektiven prägnant und verständlich beleuchtet.

Ob es dabei um die Akzeptanz von Kryptowährungen als Zahlungsmittel, das Anbieten von Krypto-Dienstleistungen oder die Ausgabe eigener Krypto-Token geht – die damit verbundenen Compliance-Fragen sind so vielfältig wie die Arten und Verwendungsmöglichkeiten von Krypto-Assets selbst. Daher werfen wir in diesem Buch gemeinsam mit unseren renommierten Expertinnen und Experten aus den verschiedenen Fachbereichen der Prüfungs- und Beratungspraxis einen umfassenden Blick auf den Themenkomplex Krypto-Asset Compliance, stellen die unterschiedlichen regulatorischen Anforderungen dar und geben Hinweise zu deren praktischer Handhabung.

1 Aus Gründen der besseren Lesbarkeit verwenden wir in diesem Buch bei Personenbezeichnungen und personenbezogenen Substantiven das generische Maskulinum. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Neben kapitalmarkt- und bankaufsichtsrechtlichen Fragen widmen wir uns dabei unter anderem den Bereichen Datenschutz, Tax- und Accounting-Compliance sowie der Verhinderung von Geldwäsche, Terrorismusfinanzierung und Verstößen gegen Finanzsanktionen. Eine Einführung sowohl in die technischen Aspekte von Krypto-Transaktionen und Blockchain-Technologie als auch in die wesentlichen Entwicklungen des Krypto-Marktes trägt darüber hinaus zum ganzheitlichen Verständnis bei.

Dieses Sammelwerk wäre ohne die engagierte Arbeit und Expertise unserer Autoren nicht möglich gewesen. Wir danken allen, die ihre Zeit und ihr Wissen eingebracht haben, um dieses Werk zu einem wertvollen Beitrag für die Krypto-Asset Compliance zu machen. Ein besonderer Dank gilt *Anna Pietras* und *Claudia Knapp* vom Schäffer-Poeschel Verlag, die uns bei der Veröffentlichung unterstützt haben, sowie unserer Lektorin *Barbara Buchter*, die mit ihrer sorgfältigen Arbeit zur Qualität des Werkes beigetragen hat. Ebenso möchten wir die redaktionelle Unterstützung von *Christine Sittner* und *Alexandra Knöfel* hervorheben, die mit ihrem Einsatz und ihrer Expertise maßgeblich zum Gelingen dieses Projekts beigetragen haben.

Wir hoffen, dass Sie durch die Lektüre inspiriert werden, die Chancen dieser vielversprechenden Technologie zu nutzen und gleichzeitig die notwendigen Schritte zur Einhaltung von Compliance-Vorgaben zu unternehmen.

Mit besten Grüßen

Die Herausgeber

A Einführung

1 Technische Grundlagen von Krypto-Assets

Dirk Siegel

Key Facts

- Krypto-Assets sind digitale Einheiten, die auf einer Blockchain verwaltet werden.
- Blockchains beschreiben eine Art dezentral bzw. verteilt geführte Datenstruktur, die redundant und unveränderlich bei den Teilnehmenden des jeweiligen Netzwerks gespeichert und daher nicht auf zentrale Instanzen angewiesen ist.
- Neben der ersten und nach wie vor bedeutendsten Bitcoin-Blockchain existieren inzwischen zahlreiche weitere Blockchains mit unterschiedlichen technischen Spezifikationen und Eigenschaften, wie etwa die Ethereum-Blockchain, auf der auch kleine Programme (Smart Contracts) abgelegt und ausgeführt werden können.
- Smart Contracts bieten die Möglichkeit, Prozesse innerhalb einer Blockchain-Umgebung zu automatisieren, was zur Etablierung Blockchain-basierter Finanzinstrumente und -dienstleistungen (Decentralized Finance – DeFi) geführt hat.

1.1 Überblick

Krypto-Assets sind Werte oder Rechte, die dezentral organisiert durch Blockchains abgebildet werden.¹

Krypto-Assets werden also durch die ihr zugrunde liegende Technologie (und nicht etwa durch die Natur des Wertes bzw. die Asset-Klasse) definiert. Die Blockchain-Technologie erlaubt sichere Transaktionen und ein hohes Maß an Automatisierung, ohne dass zentrale, als integer vorausgesetzte Institutionen (Banken, Zentralbanken, Börsen etc.) nötig sind.

Das Erzeugen von Transaktionssicherheit in einem Netzwerk von Akteuren, die sich nicht vertrauen (und sich in der Regel nicht einmal kennen), ist die einzigartige Leistung der Blockchain-Technologie. In diesem Kapitel erläutern wir die Technologie, die dies alles ermöglicht und die somit die Basis für alle Krypto-Assets darstellt.

In [Kapitel 1.2](#) werden wir zunächst die grundsätzlichen technischen Merkmale einer Blockchain anhand der Bitcoin-Blockchain, der ersten und wertmäßig nach wie vor relevantesten Blockchain, beschreiben und erklären.

In [Kapitel 1.3](#) erläutern wir die zusätzlichen Features von Blockchain-Netzwerken, die Smart Contracts und damit – technisch gesehen – eine zweite Variante von Krypto-Assets unterstüt-

¹ Vgl. Art. 3 Abs. 1 Nr. 5 MiCA Verordnung (2023/1114); Bülow (2019).

zen. Das wird an einem Beispiel verdeutlicht, nämlich am Beispiel Ethereum, der derzeit wichtigsten Plattform für diesen Blockchain-Typ.

Smart Contracts verwalten nicht nur Krypto-Assets, sie ermöglichen auch das Abbilden zahlreicher Finanzdienstleistungen ohne die Vermittlung traditioneller Banken. Das Zusammenwirken von auf Smart Contracts basierenden Komponenten hat das Feld Decentralized Finance bzw. »DeFi« entstehen lassen, das wir in [Kapitel 1.4](#) behandeln. Die technische Basis von Krypto-Assets verändert sich fortlaufend. Wir zeigen daher im abschließenden [Kapitel 1.5](#) Risiken, deren Mitigationen und einige generelle Trends der Weiterentwicklung der Blockchain-Technologie auf.

1.2 Das Bitcoin-Blockchain-Netzwerk

Die technische Basis für das Verwalten von Krypto-Assets ist in der Regel ein Blockchain- beziehungsweise ein DLT-Netzwerk. DLT steht für *Distributed Ledger Technology* und stellt eine Verallgemeinerung der Blockchain-Technologie dar, wobei die Unterschiede für unsere Zwecke nicht wesentlich sind.

Da die Blockchain-Technologie auf mannigfaltige Weise kryptografische Verfahren nutzt, hat sich für die mit ihrer Hilfe abgebildeten Assets der Name »Krypto-Assets« etabliert.

Die Initialzündung der Blockchain-Technologie erfolgte am 9. Januar 2009 mit dem Start des Bitcoin-Blockchain-Netzwerks. Noch heute ist die Bitcoin-Blockchain – gemessen am Wert der auf ihr abgebildeten Assets (den »Bitcoins«) – die bedeutendste Blockchain, obwohl es mittlerweile tausende andere, auf technologischen Varianten basierende Blockchain-Netzwerke gibt.

Wir werden daher die Erläuterung der technischen Grundlagen und der Funktionsweise einer Blockchain am Beispiel der Bitcoin-Blockchain durchführen und an den entsprechenden Stellen auf wesentliche Varianten bei anderen Blockchain-Netzwerken verweisen.

Das Bitcoin-Blockchain-Netzwerk funktioniert als digitales Register (als »Ledger«) für Bitcoins: Es bildet alle Bitcoins (und ihre Untereinheiten) ab und führt Buch über alle in Bitcoin getätigten Transaktionen.

Grundsätzlich ließe sich ein solches Register sehr einfach mit den Werkzeugen klassischer Datenbank-Technologien erstellen. Satoshi Nakamoto², das Mastermind hinter der Bitcoin-Blockchain, wollte allerdings drei wesentliche Zusatzanforderungen erfüllen:

1. Nicht eine zentrale Stelle sollte den Ledger führen, stattdessen sollten die am Blockchain-Netzwerk Beteiligten die Führung und Sicherung des Ledgers gemeinschaftlich übernehmen.

² Nakamoto (2008).

2. Anonyme Zahlungen sollten – wie beim Bargeld – möglich sein.
3. Das digitale Register sollte ein Höchstmaß an Sicherheit bieten, damit sich auch signifikante Werte abbilden lassen.

Hintergrund

Das Ziel der Dezentralität, das Abrücken von zentralen Instanzen wie Banken und staatlichen Institutionen, war wohl motiviert von der Weltfinanzkrise 2007–2008, die auch als eine Krise dieser zentralen Institutionen wahrgenommen wurde.

Alle im Folgenden erläuterten Designkriterien und ihre Umsetzungen in der Bitcoin-Blockchain dienen dazu, die genannten Anforderungen im Kontext eines dezentralen Netzwerks umzusetzen.

Redundanz

Ein hohes Maß an Sicherheit ergibt sich daraus, dass der digitale Ledger nicht an einer Stelle, sondern identisch auf jedem Knoten der Bitcoin-Blockchain geführt wird: Derzeit besteht das Bitcoin-Netzwerk aus mehreren Tausend (ca. 20.000 per Juni 2025) Knoten, die alle eine identische Version des Bitcoin-Ledgers speichern.

Unveränderlichkeit

Die Redundanz der Bitcoin-Knoten schützt zwar vor Datenverlust und Manipulation, schafft aber auch folgendes Problem: Wie kann die Gleichheit und Integrität einer großen Anzahl von Ledger-Instanzen garantiert werden?

Der Lösungsansatz besteht darin, den Datenbestand als Verkettung von Blöcken (daher auch der Name) darzustellen, und zwar so, dass im Netzwerk eine Übereinstimmung nur hinsichtlich des jeweils neuen Blocks (bestehend aus den jeweils neu zu speichernden Transaktionen) erzielt werden muss, während alle vorausgehenden Blöcke als unveränderlich angesehen werden.

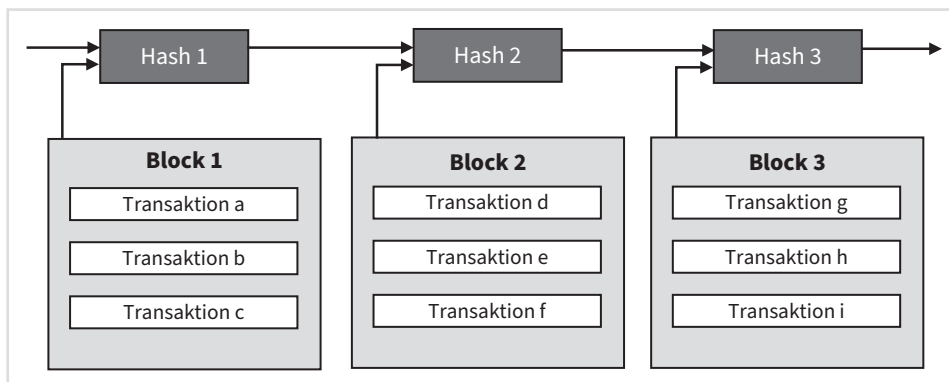


Abb. 1: Vereinfachte Darstellung der Blockchain-Struktur (in Anlehnung an Wilkens/Falk, 2019, S. 6)

Blöcke fassen die Transaktionen zusammen, die innerhalb der sogenannten Blockzeit (bei Bitcoin: 10 Minuten) auftreten. Naturgemäß ist es viel einfacher, im Netzwerk Einigkeit über einen Block (der derzeit³ ca. 2 Megabyte Daten umfasst) zu erzielen als über den vollständigen Datenbestand der ganzen Blockchain (dieser beträgt derzeit ca. 660 Gigabyte).

Um die Unveränderlichkeit bestehender Blöcke zu garantieren, enthält jeder Block als Teil seines Datenbestands im sogenannten Header einen Fingerabdruck (technisch: den Hash, siehe Abb. 1 und im Kasten »Vertiefung« unten). Ändert man einen Block, dann würde dies sogleich zu einem Mismatch mit seinem im Nachfolgeblock gespeicherten Fingerabdruck führen: Ein solcher Datenbestand wird sofort als nicht integer erkannt und aussortiert.

Vertiefung

Das Konzept der Hash-Funktion ist in der Kryptografie von höchster Bedeutung. Vereinfacht zeichnet sich eine Hash-Funktion durch zwei Eigenschaften aus:

- Sie bildet beliebig große Datenmengen auf einer Zahl mit vorgegebener Bitzahl ab (z. B. mappt der verbreitete SHA256-Algorithmus einen beliebigen Input immer auf eine Zahl mit 256 Bits).
- Selbst kleinste Abweichungen im Input führen zu komplett anderen Ergebnissen. Dieses Streuen der Ergebnisse erklärt den englischen Namen (Hash = Hackfleisch) und macht das Invertieren (das Finden eines Inputs, der zu einem gegebenen Output führt) äußerst aufwendig – oder bei gegebener Rechnerleistung faktisch unmöglich.

Digitale Signaturen

Bitcoin nutzt – so wie alle anderen wichtigen Kryptowährungen auch – das kryptografische Verfahren der **Digitalen Signatur**, um Transaktionen zu sichern. Digitale Signaturen kommen in verwandter Form auch bei einer Vielzahl anderer Anwendungsfälle zum Einsatz.

Ein sogenannter **Private Key** (mit 256 Byte Länge) ist vom Nutzenden selbst zu wählen und geheim zu halten.⁴

Der sogenannte **Public Key** wird aus dem Private Key durch Anwenden einer Hash-Funktion errechnet. Der Falltürcharakter der Hash-Funktion stellt sicher, dass der Private Key aus dem Public Key nicht zurückgerechnet werden kann.

Will ein Nutzender über die an seine Adresse gesendeten Bitcoins verfügen, erstellt er aus seinem Private Key und den Transaktionsdaten eine **Digitale Signatur**. Mittels Public Key kann

3 »Derzeit« bezieht sich, wenn wir Schätzzahlen angeben, immer auf die Mitte des Jahres 2025.

4 Da der Verlust des Private Keys unwiederbringlich dazu führt, dass man nicht mehr über empfangene Bitcoins verfügen kann, hat sich ein ganzer Dienstleistungsbereich (die sogenannten Wallet Provider) etabliert, der Endnutzenden hilft, ihre Private Keys sicher zu speichern – wir gehen weiter unten auf diesen Sachverhalt ein.

nun jeder im Netzwerk die Gültigkeit der Digitalen Signatur verifizieren (ohne dafür den Private Key kennen zu müssen).

Konsensmechanismus

Das Netzwerk muss Konsens hinsichtlich des neuen Blocks (und nur in Hinblick auf diesen) erzielen (vgl. Abschnitt »Unveränderlichkeit«). Dazu muss zunächst geprüft werden, ob die Transaktionen, die in den nächsten Block Eingang finden sollen, echte und erlaubte Transaktionen sind, die den Regeln des Protokolls entsprechen. Diese Überprüfung übernimmt die Knotensoftware, indem sie u. a. die oben erwähnten Signaturen der Transaktionen verifiziert.

Des Weiteren muss verhindert werden, dass einzelne Knoten das Netzwerk mit neuen Blöcken überschwemmen (spammen) oder versuchen, alternative Versionen der Blockchain (sogenannte »Forks«/Abzweigungen) zu erzeugen.

Das in der Bitcoin-Blockchain implementierte Verfahren zur Vermeidung solcher Aktionen ist das sogenannte Proof-of-Work.⁵ Es stellt sicher, dass beim Festschreiben eines neuen Blocks eine signifikante Rechenarbeit geleistet werden muss. Im Detail funktioniert das Verfahren bei der Bitcoin-Blockchain wie folgt:

Das Bitcoin-Regelwerk (das sogenannte Bitcoin Protocol) stellt die Knoten untereinander in einen Wettbewerb, welcher von ihnen den nächsten Block für verbindlich erklären und der Blockchain hinzufügen kann. Als Incentivierung erhält der Knoten, der den Wettbewerb gewinnt, neu geschöpfte Bitcoins – derzeit 3,125 Bitcoins (ca. 300.000 US-Dollar) pro Block. Die Aufgabe, die im Wettbewerb gelöst werden soll, besteht darin, den Datenbestand des neu zu erzeugenden Blocks durch Hinzufügen weiterer frei wählbarer Bytes (der sogenannten Nonce) so zu ergänzen, dass der Hash-Wert des sich so ergebenden Datensatzes kleiner als eine vorgegebene Zahl ist.

Aufgrund der Irreversibilität des Hash-Algorithmus kann diese Aufgabe nur durch Ausprobieren gelöst werden. Im Durchschnitt müssen derzeit ca. $1,25 \cdot 10^{14}$ (125.000.000.000.000) Möglichkeiten ausprobiert werden, um eine Lösung zu finden. Die Schwierigkeit (Difficulty) der Wettbewerbsaufgabe wird laufend der im Bitcoin-Netzwerk zur Verfügung stehenden Rechenperformance (der »Hash Power«) angepasst: Steigt die Hash Power des Netzwerks und sinkt so die Blockzeit unter 10 Minuten, wird die Schwierigkeit erhöht. Das System kalibriert sich somit selbst.

Eine weitere wesentliche Konsequenz des Proof-of-Work ist, dass aus dem Wettbewerb zufällig verteilt immer andere Knoten als Sieger hervorgehen. Dieses Zufallselement bei der Auswahl

5 Spamming ist bekanntermaßen u. a. auch im Bereich E-Mail ein Problem. Auch dort kommen Proof-of-Work-artige Verfahren als Gegenmaßnahme zum Einsatz.