

Maume · Maute

Rechtshandbuch Kryptowerte

Blockchain · Tokenisierung
Initial Coin Offerings


C.H. BECK

Vahlen

Maume/Maute
Rechtshandbuch Kryptowerte

Rechtshandbuch Kryptowerte

Blockchain · Tokenisierung · Initial Coin Offerings

Herausgegeben von

Prof. Dr. Philipp Maume, S.J.D. (La Trobe)

Technische Universität München

Prof. Dr. Lena Maute

Universität Augsburg

Mathias Fromberger

Technische Universität München

Bearbeitet von den Herausgebern und

PD Dr. Max Foerster, LL.M.eur., Ludwig-Maximilians-Universität München; *Christoph Gschnaidtner, M.Sc.*, Technische Universität München; *Lars Haffke, M.Sc., LL.M.* (Nottingham), Technische Universität München; *Björn Handke*, Rechtsanwalt in München; *Dr. Verónica Hoch*, Ruhr-Universität Bochum; *Mario Keiling, M.Sc.*, Technische Universität München; *Dr. Jasmin Kollmann*, Senior Consultant in München; *Dr. Anika Patz*, Rechtsanwältin in Berlin; *Dipl.-Kfm. Stephan Romeike*, Technische Universität München; *Dr. Christian Rückert*, Friedrich-Alexander-Universität Erlangen-Nürnberg; *Dr. Daniel Schmid*, Universität Augsburg; *Prof. Dr. Björn Steinrötter*, Universität Potsdam; *Dr. Martin Strauch, LL.M.* (Edinburgh), Rechtsanwalt in München; *Jan Max Wettlaufer*, Rechtsanwalt in Berlin; *Peter Zickgraf*, Ludwig-Maximilians-Universität München; *Patrick Zimmermann*, Technische Universität München

2020



Vahlen

Zitiervorschlag:
Maume/Maute Kryptowerte-HdB

www.beck.de

ISBN Print 978 3 406 73433 5

ISBN E-Book 978 3 406 76243 7

© 2020 Verlag C.H. Beck oHG

Wilhelmstraße 9, 80801 München

Druck und Bindung: Westermann Druck Zwickau GmbH
Crimmitschauer Straße 43, 08058 Zwickau

Satz: 3w+p GmbH, Rimpar

Umschlaggestaltung: Ralph Zimmermann – Bureau Parapluië



chbeck.de/nachhaltig

Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)

Vorwort

Blockchain und Smart Contracts sind Beispiele dafür, wie innovative Technologie neue Anwendungen und Geschäftsmodelle eröffnet. Man kann mit Fug und Recht behaupten, dass seit der Verbreitung des Internets wohl keine technische Neuerung verschiedenste Märkte derart elektrisiert hat. Die Entwicklung ist rasant. So waren vor 2017 „Initial Coin Offerings“ nur eingefleischten Spezialisten ein Begriff. Nur zwei Jahre später konnten wir in Deutschland die ersten öffentlichen Angebote von Kryptowerten mit Billigung der BaFin und auch die Eröffnung lizenzierter Kryptobörsen erleben. In Rekordzeit wurde Ende 2019 die Schaffung von „Kryptowerten“ als neue Investmentklasse durch das Parlament gepeitscht. Nicht nur die Märkte, sondern auch die Politik hat verstanden.

Anzahl und Schwierigkeit der sich stellenden Rechtsfragen sind enorm. Doch ist es eine große Stärke des deutschen Zivilrechts, neue Technologien sinnvoll und dogmatisch sauber erfassen zu können. Ob E-Mail, Onlinebanking oder digitaler Wertpapierhandel, sie alle fußen auf Regeln des Kernzivilrechts, die im Jurastudium in den ersten Semestern vermittelt werden. Im Aufsichts- und Marktordnungsrecht wie zB dem Kapitalmarktrecht ist dies ähnlich, da Regulierung meist anstatt auf die eingesetzte Technologie, auf Tätigkeit und Ergebnis abstellt. Diese Flexibilität darf aber nicht den Blick darauf verstellen, dass die Einpassung neuer Technologien manchmal komplex und mit enormen Schwierigkeiten verbunden ist. So liegt der Fall auch mit Kryptowerten.

Unser „Rechtshandbuch Kryptowerte“ hat es sich zur Aufgabe gemacht, dieses zentrale Anwendungsfeld der Blockchain-Technologie umfassend auszuleuchten. Es ist keine Sammlung unabhängiger Beiträge, sondern bietet vielmehr eine aufeinander abgestimmte Analyse. Es ist in sechs Kapitel untergliedert. Zunächst werden der technische Hintergrund und die ökonomische Bedeutung von Kryptowerten dargestellt (§§ 1–2). Im zweiten Kapitel (§§ 4–10) erfolgt die zivilrechtliche Einordnung hinsichtlich Rechtsnatur, Übertragung, Vertragsrecht mit besonderer Berücksichtigung von Intermediären, Verbraucherschutz und Miningpools sowie Zwangsvollstreckung und Insolvenz. Das dritte Kapitel (§§ 11–14) behandelt die bank- und kapitalmarktrechtlichen Fragestellungen, wie zB den Wertpapierbegriff, Erlaubnispflichten nach KWG und ZAG sowie das Marktmissbrauchsrecht. Kapitel vier (§§ 15, 16) widmet sich den praktisch immens wichtigen Bereichen Datenschutz und Geldwäsche. Für alle in diesem Bereich tätigen Unternehmen stellen sich zudem die im fünften Kapitel (§§ 17–19) behandelten Fragen der steuerlichen Behandlung und Bilanzierung. Das abschließende sechste Kapitel (§§ 20–23) leuchtet die sich stellenden strafrechtlichen Fragen aus und beschränkt sich dabei nicht nur auf die nach deutschem Recht einschlägigen Straftatbestände, sondern umfasst auch internationale Anwendbarkeit und Phänomenologie.

Größere Publikationsprojekte sind immer das Ergebnis von Teamarbeit und dabei insbesondere der kleinen Rädchen, die im Hintergrund wichtige Beiträge liefern. Danken möchten wir dabei zunächst unseren studentischen Mitarbeiterinnen und Mitarbeitern Duygu Söztutar, Luca Wolf, Tobias Hock, Alexander Betz, Fabian Grenzer und Tobias Ostner. Ein besonderer Dank gilt Dominic Deuber.

Das Recht der Kryptowerte steht erst am Anfang einer langen Entwicklung. Wir erwarten, dass Politik, Rechtsprechung und Aufsichtsbehörden in den nächsten Jahren wichtige Weichenstellungen treffen werden. Auch hierzu wollen wir mit diesem Werk einen Beitrag leisten. In dynamischen Rechtsbereichen stehen Herausgeber und Autoren dabei freilich immer vor der kniffligen Frage der Aktualität. Dieses Handbuch ist auf dem Stand 15. März 2020. Insbesondere die Gesetzesänderungen im Zuge der Umsetzung der Fünften EU-Geldwäscherichtlinie zum 1. Januar 2020 sind berücksichtigt.

Für Feedback und Anmerkungen sind wir immer dankbar.

München/Augsburg im April 2020

Philipp Maume

Lena Maute

Mathias Fromberger

Bearbeiterverzeichnis

<i>PD Dr. Max Foerster</i> (Ludwig-Maximilians-Universität München)	§ 9
<i>Mathias Fromberger</i> (Technische Universität München)	§ 1
<i>Christoph Gschnaidtner</i> (Technische Universität München)	§ 2
<i>Lars Haffke</i> (Technische Universität München)	§ 15
<i>Björn Handke</i> (Hogan Lovells)	§ 10
<i>Dr. Verónica Hoch</i> (Ruhr-Universität Bochum)	§ 7
<i>Mario Keiling</i> (Technische Universität München)	§ 19
<i>Dr. Jasmin Kollmann</i> (EY)	§§ 17, 18
<i>Prof. Dr. Philipp Maume</i> (Technische Universität München)	§§ 8, 12, 14, 15
<i>Prof. Dr. Lena Maute</i> (Universität Augsburg)	§§ 4, 5, 6
<i>Dr. Anika Patz</i> (lindenpartners)	§ 13
<i>Stephan Romeike</i> (Technische Universität München)	§ 19
<i>Dr. Christian Rückert</i> (Friedrich-Alexander-Universität Erlangen-Nürnberg)	§§ 20, 21, 22, 23
<i>Dr. Daniel Schmid</i> (Universität Augsburg)	§ 16
<i>Prof. Dr. Björn Steinrötter</i> (Universität Potsdam)	§ 3
<i>Dr. Martin Strauch</i> (Hogan Lovells)	§ 10
<i>Jan Wettlaufer</i> (lindenpartners)	§ 13
<i>Peter Zickgraf</i> (Ludwig-Maximilians-Universität München)	§ 11
<i>Patrick Zimmermann</i> (Technische Universität München)	§ 1

Inhaltsübersicht

Vorwort	V
Bearbeiterverzeichnis	VII
Inhaltsverzeichnis	XI
Literaturverzeichnis	XXI

Kapitel 1 Technische und wirtschaftliche Grundlagen

§ 1 Technische und rechtstatsächliche Grundlagen	1
§ 2 Die Ökonomik von Kryptotoken	32

Kapitel 2 Kryptotoken im Rechtsverkehr

§ 3 Internationale Zuständigkeit und anwendbares Recht bei der Transaktion von Kryptotoken auf dem Primär- und Sekundärmarkt	65
§ 4 Die Rechtsnatur von Kryptotoken	110
§ 5 Die Übertragung von Kryptotoken	130
§ 6 Verträge über Kryptotoken	138
§ 7 Intermediäre des sekundären Kryptohandels	197
§ 8 Verbraucherschutzrecht	218
§ 9 Mining/Minting und Mining/Staking-Pools	241
§ 10 Kryptotoken in Zwangsvollstreckung und Insolvenz	265

Kapitel 3 Kapitalmarkt- und Bankenrecht

§ 11 Initial Coin Offerings (ICOs)	279
§ 12 Finanzdienstleistungsaufsichtsrecht	332
§ 13 Einordnung von Token und Token-Geschäftsmodellen im Recht der Zahlungsdienste	365
§ 14 Marktmissbrauchsrecht	390

Kapitel 4 Compliance und Datenschutz

§ 15 Geldwäsche-Compliance	417
§ 16 Datenschutz	455

Kapitel 5 Steuern und Bilanzierung

§ 17 Ertragsteuerliche Behandlung von Kryptotoken	483
§ 18 Umsatzsteuerliche Behandlung von Kryptotoken	497
§ 19 Bilanzierung	512

Kapitel 6 Strafrecht

§ 20 Phänomenologie	527
§ 21 Strafanwendungsrecht	537
§ 22 Relevante Normen des Kern- und Nebenstrafrechts	547
§ 23 Token im Strafverfahren	585

Stichwortverzeichnis	605
----------------------------	-----

Inhaltsverzeichnis

Vorwort	V
Bearbeiterverzeichnis	VII
Inhaltsübersicht	IX
Literaturverzeichnis	XXI

Kapitel 1 Technische und wirtschaftliche Grundlagen

§ 1 Technische und rechtstatsächliche Grundlagen	1
I. Die Blockchain-Technologie	2
1. Einführung	2
2. Blockchain-Teilnehmer	4
3. Kategorisierung von Blockchains	4
4. Aufbau einer Blockchain	5
5. Transaktion von Token	6
6. Technische Darstellung der Token	8
7. Wallets und Wallet-Anbieter	9
8. Verlängerung der Blockchain durch Verifizierung	10
9. Smart Contracts	17
10. Nachteile der Blockchain-Technologie	19
II. Phänomenologie der Token	19
1. Grundsätzliche Ausgestaltung	19
2. Currency Token	20
3. Investment Token	20
4. Utility Token	20
5. Hybride	21
6. Asset-Backed-Token	21
7. Auf Token basierende Finanzprodukte	21
III. Der Erwerb von Token	22
1. Originärer Erwerb	22
2. Abgeleiteter Erwerb	25
IV. Anonymitätsbestrebungen	28
1. Pseudonymität als Ausgangspunkt	28
2. Tumbler	29
3. Privacy Token	30
§ 2 Die Ökonomik von Kryptotoken	32
I. Einleitung	34
II. Gegenwärtige ökonomische Bedeutung	34
1. Aktuelle (Markt-)Entwicklungen	35
2. Bitcoin	40
3. Initial Coin Offerings (ICOs)	47
III. Kryptotoken als Komplementärwährung	50
1. Charakteristika einer Währung	51
2. Währungscharakteristika von Kryptotoken	54
IV. Kryptotoken jenseits der Währungsthematik	59
1. Ressourcenallokation und negative Externalitäten	59
V. Fazit und Ausblick	63

Kapitel 2 Kryptotoken im Rechtsverkehr

§ 3 Internationale Zuständigkeit und anwendbares Recht bei der Transaktion von Kryptotoken auf dem Primär- und Sekundärmarkt	65
I. Einleitung	69
II. Übergreifende Erwägungen	70
III. („Doppelt“) Autonome und funktionale Qualifikation	72
IV. Rechtsnatur, aprioristische Rechtspositionen und Übertragungsstatut	72
1. Grundfragen	72
2. Currency Token	73
3. Investment Token	75
4. Utility Token	76
V. Vertragsbeziehungen beim Initial Coin Offering (ICO)	77
1. Internationale Gerichtszuständigkeit	77
2. Anwendbares Recht	81
VI. Vertragsbeziehungen auf dem Sekundärmarkt	85
1. Internationale Gerichtszuständigkeit	85
2. Anwendbares Recht	85
VII. Verträge zu Intermediären	88
1. Internationale Gerichtszuständigkeit	88
2. Anwendbares Recht	90
VIII. E-Commerce und Fernabsatz	91
IX. Kapitalmarktrechtliche Prospekthaftung beim ICO	92
1. Internationale Gerichtszuständigkeit	93
2. Anwendbares Recht	97
X. Sonstiges Kapitalmarktdeliktsrecht	104
XI. (Sonstiges) Haftungsrecht	105
1. Internationale Gerichtszuständigkeit	105
2. Anwendbares Recht	105
XII. Mining und Mining Pools	105
1. Internationale Gerichtszuständigkeit	106
2. Anwendbares Recht	107
XIII. Internationales Datenschutzrecht	108
XIV. Zwangsvollstreckung und Insolvenz	109
§ 4 Die Rechtsnatur von Kryptotoken	110
I. Rechtsnatur Blockchain-basierter Kryptotoken	112
1. Die Natur des Kryptotokens	112
2. Kryptotoken als Immaterialgut	113
3. Kryptotoken als relatives Recht?	114
4. Kryptotoken als absolutes Recht?	115
5. Kryptotoken als sonstiges Recht iSv § 823 Abs. 1 BGB?	124
6. Zusammenfassung und Ergebnis	125
7. Überlegungen de lege ferenda	126
II. Besonderheiten bei Currency Token	126
III. Besonderheiten bei Utility Token	126
IV. Besonderheiten bei Investment Token	129
V. Besonderheiten bei Asset-Backed-Token	129
§ 5 Die Übertragung von Kryptotoken	130
I. Grundlagen der Übertragung von Kryptotoken	130
1. On-Chain-Transaktionen	130
2. Off-Chain-Transaktionen	134

II. Besonderheiten bei Utility Token, Investment Token und Asset-Backed-Token	135
§ 6 Verträge über Kryptotoken	138
I. Vertragsschluss	140
1. Wirksamwerden von Willenserklärungen	141
2. Smart Contracts	143
3. Stellvertretung	144
II. Wirksamkeit des Vertrags	145
1. Form	145
2. Bedingter Vertragsschluss	146
3. Willensmängel	147
4. Gesetzliche Verbote und Sittenwidrigkeit	147
5. Geschäftsfähigkeit	148
III. Inhalt der Tokenschuld	149
1. Die Tokenschuld als Geldschuld	149
2. Die Tokenschuld als Gattungsschuld oder Stückschuld	151
3. Leistungshandlung und Leistungsort	152
IV. Erlöschen der Leistungspflicht	155
1. Erfüllung	155
2. Aufrechnung	157
V. Leistungsstörungen	157
1. Anwendbarkeit des allgemeinen Leistungsstörungsrechts	157
2. Haftung für Dritte	157
3. Nichtleistung	158
4. Unmöglichkeit	160
5. Schuldnerverzug	163
6. Schlechtleistung	165
7. Gläubigerverzug	165
8. Störung der Geschäftsgrundlage	165
VI. Rückabwicklung	166
1. Rückabwicklung unwirksamer Verträge nach Bereicherungsrecht	166
2. Rücktritt vom Vertrag	168
3. Verbraucherwiderruf	169
VII. Die Verträge im Einzelnen	169
1. Verträge über Currency Token	170
2. Verträge über Utility Token	180
3. Verträge über Investment Token	189
4. Verträge über Asset-Backed-Token	192
§ 7 Intermediäre des sekundären Kryptohandels – Vertragsrechtliche Fragestellungen	197
I. Intermediäre und ihre Funktionen	198
II. Vertragliche Strukturen	199
1. Plattformvertrag	199
2. Kategorisierung der Tätigkeit des Intermediärs	202
3. On-Chain-Intermediäre	204
4. Off-Chain-Intermediäre	208
III. Nebenpflichten	210
IV. Leistungsstörungen	212
1. On-Chain-Intermediär	212
2. Off-Chain-Intermediär	214
V. Allgemeine Geschäftsbedingungen	215
1. Häufige AGB-Klauseln innerhalb von Plattformverträgen	216

2. AGB-Klauseln mit Implikation für die Userverträge	216
§ 8 Verbraucherschutzrecht	218
I. Übersicht	219
1. Rechtsgrundlagen	219
2. Tokenkategorien	219
3. Kryptobörsen und -wechselstellen	219
II. Anwendbarkeit deutschen Rechts und Gerichtsstand	220
1. Verbrauchervertrag, Art. 6 Abs. 1 Rom I-VO	220
2. Spezifische Grenzen der Rechtswahl, Art. 6 Abs. 2 Rom I-VO	225
3. Gerichtsstand, Art. 18 Abs. 1 Brüssel Ia-VO	225
III. Deutsches Verbraucherschutzrecht	226
1. Verbrauchervertrag, § 310 Abs. 3 BGB iVm § 312 Abs. 1 BGB	226
2. Widerrufsrecht, § 312g BGB	230
3. Informationspflichten	236
4. Verbrauchsgüterkauf	240
§ 9 Mining/Minting und Mining/Staking-Pools – Originärer Erwerb von Token und Erwerb von Transaktionsgebühren durch Einzelne oder Mehrere	241
I. Originärer Erwerb von Token durch Einzelne	242
1. Erwerb von Token im Zuge der Initiierung einer Blockchain auf der Grundlage einer Protokollsoftware	242
2. Erwerb von Token durch Mining oder Minting/Forging	245
3. Erwerb von Token bei einem Initial Coin Offering (ICO)	252
4. Originärer Erwerb von Token im Aufsichtsrecht	252
II. Originärer Erwerb von Token in Pools	253
1. Grundlagen	253
2. Mining-Pools	254
3. Staking-Pools	258
4. Cloud-Mining-Dienst/Mining-Farm	259
5. Mining- und Staking-Pools im Aufsichtsrecht	259
III. Erwerb von Transaktionsgebühren durch Verifikation von Transaktionen auf der Blockchain	261
1. Grundlagen der Transaktionsgebühr	261
2. Auslobung der Transaktionsgebühr	262
3. Anspruch auf die Transaktionsgebühr im Mining-Pool	263
4. Anspruch auf die Transaktionsgebühr im Staking-Pool	263
§ 10 Kryptotoken in Zwangsvollstreckung und Insolvenz	265
I. Einführung	265
II. Möglichkeiten der Zwangsvollstreckung nach der ZPO	266
1. Zwangsvollstreckung in Kryptotoken wegen einer Geldforderung	266
2. Zwangsvollstreckung aus Titel gerichtet auf Kryptotoken	271
3. Zwangsvollstreckung in den Anspruch auf Übertragung eines Kryptotokens (zB bei Online-Wallets)	272
4. Arrest	272
III. Örtliche und internationale Zuständigkeit	273
1. Sachpfändung Hardware-Wallet	273
2. Pfändung des Tokens analog § 857 ZPO	273
3. Sachpfändung des Tokens analog §§ 808 ff. ZPO	274
4. Arrest	274
IV. Kryptotoken in der Insolvenz	274
1. Zuordnung zur Insolvenzmasse	274

2. Herstellung der Verfügungsgewalt und Sicherung durch den Insolvenzverwalter	275
3. Aus- und Absonderung von Kryptotoken nach §§ 47 ff. InsO	275
4. Verwertung von Kryptotoken	276

Kapitel 3 Kapitalmarkt- und Bankenrecht

§ 11 Initial Coin Offerings (ICOs)	279
I. Entwicklung	281
II. Rechtsökonomische Grundlagen	283
1. Der Primärmarkt aus rechtsökonomischer Sicht	283
2. Der Primärmarkt für Token aus rechtsökonomischer Sicht	284
3. Chancen der Unternehmensfinanzierung durch ICOs	285
4. Risiken der Unternehmensfinanzierung durch ICOs	286
III. Rechtsvergleichender Überblick	287
1. Nordamerika	287
2. Asien	289
3. Europa	290
4. Rechtsvergleichende Bilanz	294
IV. Kapitalmarktrechtliche Regulierung von Initial Coin Offerings	294
1. Prospektpflicht nach der Prospekt-VO	295
2. Prospektpflicht nach dem KAGB	326
3. Prospektpflicht nach dem VermAnlG	329
§ 12 Finanzdienstleistungsaufsichtsrecht	332
I. Grundlagen und Überblick	333
1. Rechtsquellen	333
2. Erlaubnispflicht und Rechtsfolgen	334
II. Finanzinstrumente	335
1. Überblick	335
2. Einzelne Definitionen	336
III. Räumlicher Anwendungsbereich	342
1. Systematik und Hintergrund	342
2. Leistungserbringung aus dem Ausland	342
3. Sonderfall: Elektronische Wertpapierhandelsplätze in Drittstaaten	345
IV. Aufsichtsrechtlich relevante Tätigkeiten	346
1. Allgemeines	346
2. Trading-Plattformen	346
3. Kryptoverwahrgeschäft (Wallet-Provider)	356
4. Emittenten	357
5. Krypto-ATM	357
6. Minting/Mining	358
7. Krypto Lending	358
V. Voraussetzungen der Erlaubniserteilung nach § 32 Abs. 1 KWG	359
1. Allgemeines	359
2. Voraussetzungen nach § 33 KWG	359
3. Rechtsfolgen bei Verletzung	363
§ 13 Einordnung von Token und Token-Geschäftsmodellen im Recht der Zahlungsdienste	365
I. Kurzeinführung zum Recht der Zahlungsdienste	366
II. Anknüpfung von Zahlungsdiensten und E-Geld-Geschäften an den Begriff „Geldbetrag“	367
1. Vergleichbare Funktionen von Geld und Token	367

2. Der Begriff „Geldbetrag“ im System des Zahlungsdiensterechts	368
3. Token als Kryptowerte und Rechnungseinheiten	369
III. Ausgestaltung von Token als E-Geld	369
1. Definition von E-Geld	370
2. Einordnung von Currency Token	376
3. Einordnung von Investment Token	378
4. Einordnung von Utility Token	378
5. Hybride Token	378
IV. Zahlungsdienste in Verbindung mit Token-Geschäftsmodellen	379
1. Grundlegende Ziele der Regulierung von Zahlungsdiensten	379
2. Allgemeine Voraussetzungen von Zahlungsdiensten	380
3. Verschiedene Token-Geschäftsmodelle	381
V. Erlaubnisvorbehalt und Folgepflichten bei der Erbringung von E-Geld-Geschäft und Zahlungsdiensten	387
1. Erlaubnisvorbehalt für den Betrieb des E-Geld-Geschäfts	387
2. Erlaubnisvorbehalt für die Erbringung von Zahlungsdiensten	388
3. Aufsichts- und Folgepflichten von Instituten	388
§ 14 Marktmissbrauchsrecht	390
I. Grundlagen und Überblick	391
II. Definitionen	393
1. Finanzinstrumente	393
2. Erfasste Märkte	393
3. Zuständige Aufsichtsbehörde	394
III. Verbote	395
1. Marktmanipulation	395
2. Insiderhandel	400
IV. Offenlegungs- und Transparenzpflichten	407
1. Ad-hoc Publizität	407
2. Insiderlisten	411
3. Directors' Dealings	412

Kapitel 4 Compliance und Datenschutz

§ 15 Geldwäsche-Compliance	417
I. Einleitung	418
II. Token und Geldwäsche-Compliance	419
1. Einführung	419
2. Das Phänomen Token und Geldwäsche	419
3. Vergleich mit Bar- und Giralgeld	420
III. Geldwäscherechtliche Regelungssystematik	421
1. Überblick	421
2. Token im GwG-Begriffssystem	421
3. Territorialer Anwendungsbereich und zuständige Aufsichtsbehörde	423
IV. Kryptointermediäre als GwG-Verpflichtete	424
1. Kryptowechselstellen und Kryptobörsen	424
2. Wallet-Anbieter	425
3. Tumbler	425
4. Umsetzungsdefizit bei Tokenemittenten	425
5. Miner bzw. Mining-Pools	426
6. Sonderfall E-Geld – E-Geld-Institute, E-Geld-Agenten, E-Geld-Vertriebsunternehmen	427
7. Weitere Verpflichtete	428

V. Geldwäscherechtliche Verpflichtungen für Kryptointermediäre	428
1. Überblick	428
2. Pflichten in Bezug auf Risikomanagement (§§ 4–9 GwG)	429
3. Kundensorgfaltspflichten, §§ 10–17 GwG	432
4. Verdachtsmeldepflichten (§§ 43 ff. GwG)	447
5. Transparenzregister für wirtschaftlich Berechtigte	449
6. Öffentliches Register für Public Keys	450
VI. Sanktionen bei Verstoß	451
1. Bußgelder	451
2. Strafrechtliche Sanktionen	453
§ 16 Datenschutz	455
I. Datenschutzrechtliche Herausforderungen in der Blockchain	456
II. Datenverarbeitungsvorgänge bei Nutzung einer Blockchain zur Übertragung von Token	458
1. Verwaltung von Nutzerdaten	458
2. Initiieren von Transaktionen	459
3. Zuordnung der Transaktion durch den Empfänger	460
III. Anwendbarkeit der DS-GVO	460
1. Sachlicher Anwendungsbereich	460
2. Räumlicher Anwendungsbereich	463
IV. Die datenschutzrechtliche Stellung der Beteiligten	464
1. Beteiligte nach der DS-GVO	465
2. Zentrale Blockchain	466
3. Trading-Plattformen	467
4. Dezentrale Blockchain	467
5. Zuordnung der Transaktion durch den Empfänger	470
V. Zulässigkeit der Datenverarbeitung	470
1. Einwilligung	471
2. Erforderlichkeit für die Erfüllung eines Vertrags	471
3. Erforderlichkeit zur Wahrung berechtigter Interessen	473
4. Auftragsverarbeitung	473
5. Datentransfers in Drittstaaten	474
VI. Betroffenenrechte	475
1. Betroffenenrechte in Konflikt mit der Blockchain-Technologie	475
2. Recht auf Auskunft	476
3. Recht auf Berichtigung	476
4. Recht auf Löschung und Recht auf Vergessenwerden	477
VII. Datenschutzaufsicht und Rechtsfolgen von Datenschutzverstößen	477
1. Datenschutzaufsicht	477
2. Rechtsbehelfe, Haftung und Sanktionen	478
VIII. Möglichkeit der Umsetzung einer datenschutzkonformen Blockchain	478
1. Ausschluss der Anwendbarkeit der DS-GVO	479
2. Durchsetzung von Betroffenenrechten	480
IX. Fazit	481

Kapitel 5 Steuern und Bilanzierung

§ 17 Ertragsteuerliche Behandlung von Kryptotoken	483
I. Kurzübersicht	483
II. Einleitung	484
III. Internationale Aspekte	484
IV. Steuerliche Einordnung unterschiedlicher Tokenarten	485
1. Currency Token	485

Inhaltsverzeichnis

2. Utility Token	486
3. Investment Token	486
V. Gewinne und Verluste aus Anschaffungsvorgängen mit Token	487
1. An- und Verkauf von Token	487
2. Mining/Forging von Token	491
3. Initial Coin Offerings	493
VI. Laufende Besteuerung von Erträgen aus Token	494
1. Lending von Token	494
2. Erträge aus Investment Token	495
VII. Offene Fragestellung	495
§ 18 Umsatzsteuerliche Behandlung von Kryptotoken	497
I. Kurzübersicht	497
II. Einleitung	497
III. Grundlegende Funktionsweise der Umsatzsteuer	498
IV. Erwerb von Currency Token	499
1. Umtausch konventioneller Währungen in Currency Token	499
2. Folgefragen zu Wallets und Plattformen	501
3. Zusammenfassung	501
V. Erwerb anderer Tokenarten	502
1. Utility Token	502
2. Investment Token	503
3. Hybride Token	504
4. Zusammenfassung	505
VI. Mining und Forging	505
1. Steuerbarkeit	505
2. Leistungsort	508
3. Steuerbefreiung	509
4. Zusammenfassung	510
VII. Ausblick	510
§ 19 Bilanzierung	512
I. Grundlagen des Jahresabschlusses	512
II. Bilanzierung von Kryptotoken	513
1. Currency Token	513
2. Investment Token	519
3. Utility Token	521
4. Hybride Token	524
5. Weitere Aspekte der Tokenbilanzierung	524
III. Zusammenfassung	524

Kapitel 6 Strafrecht

§ 20 Phänomenologie	527
I. Straftaten mit Token als Geldersatz	528
1. Handel mit illegalen Waren und Dienstleistungen (va im Darknet)	528
2. Erpressungsdelikte	529
3. Fake-Shops	530
4. Menschenhandel und Zwangsprostitution	530
II. Straftaten mit Token als Tatobjekt	530
1. „Diebstahl“ von Token	530
2. Token-Mining auf fremden Systemen	531
3. „Fälschung“ von Token (Double Spending)	531
III. Straftaten im Zusammenhang mit Investitionen in Token	533

IV. Geldwäsche und Terrorismusfinanzierung mit Token	533
V. Steuerhinterziehung	534
VI. Sonstige Straftaten „in“ Blockchain-Systemen	534
1. Einbettung von illegalem Material in der Blockchain	534
2. Kursmanipulation in Kryptowährungssystemen	534
3. Manipulation des Mining-Vorgangs	534
4. Betrieb von Dienstleistungsunternehmen (Wechselbörsen, Walletanbieter) ohne Erlaubnis nach KWG/ZAG	536
§ 21 Strafanwendungsrecht	537
I. Anwendbarkeit nach Weltrechtsprinzip	537
II. Anwendbarkeit bei Tatbegehung im Inland	538
1. Bestimmung des Handlungsorts	538
2. Bestimmung des Erfolgsorts	540
III. Anwendbarkeit nach dem Personalitätsprinzip	546
§ 22 Relevante Normen des Kern- und Nebenstrafrechts	547
I. Straftaten mit Token als Geldersatz	549
1. Handel mit illegalen Waren und Dienstleistungen (va im Darknet)	549
2. Erpressungsdelikte	550
3. Fake-Shops	553
4. Menschenhandel und Zwangsprostitution	553
II. Straftaten mit Token als Tatobjekt	553
1. „Diebstahl“ von Token	553
2. Token-Mining auf fremden Systemen	558
3. „Fälschung“ von Token	563
III. Straftaten im Zusammenhang mit Investitionen in Token	566
IV. Geldwäsche und Terrorismusfinanzierung mit Token	567
1. Geldwäsche, § 261 StGB	567
2. Terrorismusfinanzierung, § 89c StGB	573
V. Steuerhinterziehung	573
VI. Sonstige Straftaten „in“ Blockchain-Systemen	573
1. Einbettung von illegalem Material in der Blockchain	573
2. Kursmanipulation auf Kryptohandelsplattformen	580
3. Manipulation des Mining-Vorgangs	580
4. Betrieb von Dienstleistungsunternehmen (Kryptowechselstellen, Kryptobörsen, Wallet-Anbietern) ohne Erlaubnis nach KWG/ZAG	584
§ 23 Token im Strafverfahren	585
I. Neue Herausforderungen für die Strafverfolgung	586
1. Fehlschlagen von Standardermittlungsmaßnahmen durch Dezentralität und Pseudonymität/Anonymität	586
2. Grenzüberschreitende Ermittlungen	587
II. Ermittlungsmaßnahmen in Blockchain-Systemen und ihrem Umfeld	588
1. Ermittlungsmaßnahmen im Zusammenhang mit Intermediären (Kryptowechselstellen, Kryptobörsen, Wallet-Anbieter)	588
2. Softwaregestützte Ermittlungsmaßnahmen in Blockchain-Systemen	589
3. Verdeckte Ermittlungen und Scheinkäufe	592
4. Sonderproblem: Auslagerung von Ermittlungen auf Sachverständige	596
5. Ausblick: Central User Database in 5. EU-Geldwäscherichtlinie	597

Inhaltsverzeichnis

6. Rechtsschutz gegen Ermittlungsmaßnahmen und Beweisverwertungsverbote	597
III. Einziehung und Sicherstellung von Token	598
1. Einziehung, §§ 73 ff. StGB	598
2. Sicherstellung, §§ 111b ff. StPO	601
3. Übertragung der rechtlichen Fragen auf andere Token als Bitcoin	603
4. Praktische Probleme bei Einziehung und Sicherstellung	603
Stichwortverzeichnis	605

Literaturverzeichnis

- Andres/Leithaus*, Insolvenzordnung (InsO) Kommentar, 4. Aufl. 2018
Baumbach/Hopt, Handelsgesetzbuch Kommentar, 38. Aufl. 2018
Baur/Stürmer, Sachenrecht, 18. Aufl. 2009
Beck'scher Onlinekommentar, StGB, 41. Edition, 2019
Beck'scher Onlinekommentar, ZPO, 23. Edition, 2016
Beck'scher Onlinekommentar, StPO mit RiStBV, und MiStra, 34. Edition, 2019
Beck'scher Onlinekommentar, BGB, 52. Edition, 2019
Beck'scher Onlinekommentar, InsO mit InsVV, EuInsVO und Spezialthemen, 16. Edition, 2019
Beck'sches Handbuch der Personengesellschaften, 4. Aufl. 2014
Beckonline.GROSSKOMMENTAR, BGB, 2019
Beckonline.GROSSKOMMENTAR, GewO, 2017
Beulke/Swoboda, Strafprozessrecht, 14. Aufl. 2018
Braun, Insolvenzordnung (InsO) Kommentar, 5. Aufl. 2012
Ebenroth/Boujong/Joost/Strohn, Handelsgesetzbuch, 3. Aufl. 2015
Eisenberg, Beweisrecht der Strafprozessordnung, 10. Aufl. 2017
Erman, BGB, 14. Aufl./15. Aufl. 2014/2017
Fischer, Strafgesetzbuch mit Nebengesetzen, 66. Aufl. 2019
Grigoleit, Aktiengesetz (AktG) Kommentar, 2012
Heger/Pohlreich, Strafprozessrecht, 2. Aufl. 2018
Henssler/Willemsen/Kalb, Arbeitsrecht Kommentar, 8. Aufl. 2018
Jauernig, Bürgerliches Gesetzbuch, 17. Aufl. 2018
juris PraxisKommentar, BGB, 8. Aufl. 2017 ff.
Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG, EMRK, 8. Aufl. 2019
Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Aufl. 2017
Köhler, BGB Allgemeiner Teil, 42. Aufl. 2018
Koller/Kindler/Roth/Morck, Handelsgesetzbuch (HGB), 8. Aufl. 2015
Lackner/Kühl, Strafgesetzbuch (StGB) Kommentar, 29. Aufl. 2018
Langenbucher, Europäisches Privat- und Wirtschaftsrecht, 4. Aufl. 2017
Larenz/Wolf, Allgemeiner Teil des Bürgerlichen Rechts, 9. Aufl. 2004
Leipziger Kommentar, Strafgesetzbuch, 12. Aufl./13. Aufl. 2009 ff./2019
Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012
Looschelders, Schuldrecht Allgemeiner Teil, 17. Aufl. 2019
Löwe/Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 27. Aufl. 2019
Matt/Renzikowski, Strafgesetzbuch (StGB) Kommentar, 2. Aufl. 2019
Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, 62. Aufl. 2019
Möllers, Juristische Methodenlehre, 1. Aufl./2. Aufl. 2017/2019
Mugdan, Die gesamten Materialien zum Bürgerlichen Gesetzbuch für das Deutsche Reich, 1899
Münchener Kommentar zum Aktiengesetz, 4. Aufl. 2016
Münchener Kommentar zum Bürgerlichen Gesetzbuch, 7. Aufl./8. Aufl. 2016 ff./2018 ff.
Münchener Kommentar zum Handelsgesetzbuch, 2. Aufl./4. Aufl. 2005/2016
Münchener Kommentar zum Strafgesetzbuch, 3. Aufl. 2017 ff.
Münchener Kommentar zur Insolvenzordnung, 3. Aufl./4. Aufl. 2013/2019
Münchener Kommentar zur Strafprozessordnung, 2014 ff.
Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen, 5. Aufl. 2016 ff.
Musielak/Hau, Grundkurs BGB, 16. Aufl. 2019
Musielak/Voit, Zivilprozessordnung (ZPO) Kommentar, 14. Aufl./15. Aufl. 2017/2018

- NomosKommentar, Bürgerliches Gesetzbuch (BGB), 3. Aufl. 2016
Oetker, Handelsgesetzbuch (HGB) Kommentar, 6. Aufl. 2019
Palandt, Bürgerliches Gesetzbuch, 65. Aufl./79. Aufl. 2006/2020
Satzger/Schluckebier/Widmayer, Strafprozessordnung mit GVG und EMRK, 3. Aufl. 2018
Satzger/Schluckebier/Widmayer, Strafgesetzbuch (StGB) Kommentar, 4. Aufl. 2019
Schaub, Arbeitsrecht-Handbuch, 17. Aufl. 2017
Schmidt, Insolvenzordnung (InsO) mit EuInsVO, 19. Aufl. 2016
Schmidt, Gesellschaftsrecht, 5. Aufl. 2020
Schmidt-Bleibtreu/Hofmann/Hennecke, Grundgesetz (GG) Kommentar, 14. Aufl. 2018
Schönke/Schröder, Strafgesetzbuch (StGB) Kommentar, 30. Aufl. 2019
Schulze/Dörner/Ebert/Hoeren/Kemper/Saenger/Scheuch/Schreiber/Schulte-Nölke/Staudinger/Wiese, Bürgerliches Gesetzbuch Handkommentar, 9. Aufl./10. Aufl. 2016/2019
Soergel, Bürgerliches Gesetzbuch mit Einführungsgesetz und Nebengesetzen, 13. Aufl. 2000 ff.
Stadler, Allgemeiner Teil des BGB, 19. Aufl. 2017
Staudinger, J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch, ab 13. Bearbeitung, fortlaufend seit 2007 ff.
Staudinger, Staudinger BGB, Ergänzungsband Eckpfeiler des Zivilrechts, 2012
Stein/Jonas, Kommentar zur Zivilprozessordnung, 22. Aufl./23. Aufl. 2002/2017
Streinz, EUV/AEUV, 3. Aufl. 2018
Systematischer Kommentar zum Strafgesetzbuch, 9. Aufl. 2015 ff.
Thomas/Putzo, Zivilprozessordnung (ZPO) Kommentar, 38. Aufl. 2017
Uhlenbruck, Insolvenzordnung (InsO) Kommentar, 15. Aufl. 2019
Ulmer/Brandner/Hensen, AGB Recht, Kommentar zu den §§ 305–310 und zum UKlaG, 12. Aufl. 2016
von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015
Wessels/Hillenkamp/Schuhr, Strafrecht Besonderer Teil 2, 41. Aufl. 2018
Wiedemann, Gesellschaftsrecht Band II: Recht der Personengesellschaften, 2004
Wolf/Neuner, Allgemeiner Teil des Bürgerlichen Rechts, 11. Aufl. 2016

Kapitel 1 Technische und wirtschaftliche Grundlagen

§ 1 Technische und rechtstatsächliche Grundlagen

Übersicht

	Rn.
I. Die Blockchain-Technologie	1
1. Einführung	1
2. Blockchain-Teilnehmer	7
3. Kategorisierung von Blockchains	9a
4. Aufbau einer Blockchain	13
5. Transaktion von Token	15
6. Technische Darstellung der Token	21
7. Wallets und Wallet-Anbieter	24
8. Verlängerung der Blockchain durch Verifizierung	27
a) Konsensfindung	27
b) Anreizsystem	32
9. Smart Contracts	62
10. Nachteile der Blockchain-Technologie	67
II. Phänomenologie der Token	68
1. Grundsätzliche Ausgestaltung	68
2. Currency Token	70
3. Investment Token	71
4. Utility Token	73
5. Hybride	74
6. Asset-Backed-Token	75
7. Auf Token basierende Finanzprodukte	77
III. Der Erwerb von Token	78
1. Originärer Erwerb	79
a) Initiierung einer Blockchain	79
b) Mining/Forging	80
c) Initial Coin Offering (ICO)	81
2. Abgeleiteter Erwerb	88
a) Direkter abgeleiteter Erwerb	89
b) Trading-Plattformen: Kryptowechselstellen und Kryptobörsen	90
IV. Anonymitätsbestrebungen	102
1. Pseudonymität als Ausgangspunkt	102
2. Tumbler	106
3. Privacy Token	108
a) Ringsignaturen	109
b) Stealth Adressen	110

Literatur:

Antonopoulos, Mastering Bitcoin – Programming the Open Blockchain, 2. Aufl. 2017; *Barsan*, Legal Challenges of Initial Coin Offerings (ICO), *Revue Trimestrielle de Droit Financier* 2017, 54–65; *Berentsen/Schär*, Bitcoin, Blockchain und Kryptoassets; *Chohan*, Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability (University of New South Wales Discussion Paper Series: Notes on the 21st Century) 3, verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080098 (zuletzt aufgerufen 31.1.2020); *Chohan*, Tethering Cryptocurrencies to Fiat Currencies Without Transparency: A Case Study, verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3129978 (zuletzt aufgerufen 31.1.2020); *De Filip-pi/Wright*, Blockchain and the Law; *Diffie/Hellman*, New Directions in Cryptography, *IEEE Transaction on Information Theory* Volume 22 (1976), Issue 6, 644–654; *Fromberger/Haffke*, ICO Market Report 2018/2019 – Performance Analysis of 2018’s Initial Coin Offerings, 2019, verfügbar unter <https://ssrn.com/abstract=3512125> (zuletzt aufgerufen 23.1.2020); *Fromberger/Haffke/Zimmermann*, Kryptowerte und Geldwäs-che – Eine Analyse der 5. Geldwäscherichtlinie sowie des Gesetzesentwurfs der Bundesregierung, *BKR* 2019, 377–386; *Ekkenga*, Bitcoin und andere Digitalwährungen – Spielzeug für Spekulanten oder Systemveränderung durch Privatisierung der Zahlungssysteme?, *CR* 2017, 762–768; *Haffke/Fromberger*, ICO Mar-

ket Report 2017. Performance Analysis of Initial Coin Offerings, 2018, verfügbar unter <https://ssrn.com/abstract=3309271> (zuletzt aufgerufen 31.1.2020); *Hennemann/Sattler*, Immaterialgüter und Digitalisierung; *Kaulartz*, Die Blockchain-Technologie – Hintergründe zur Distributed Ledger Technology und zu Blockchains, CR 2016, 474–480; *Klöhn/Parhofer/Resas*, Initial Coin Offerings (ICOs) – Markt, Ökonomik und Regulierung, ZBB 2018, 89–106; *Küttik-Markendorf*, Rechtliche Einordnung von Internetwährungen im deutschen Rechtssystem am Beispiel von Bitcoin; *Lee Kuo Chuen*, Handbook of digital currency: Bitcoin, Innovation, Financial Instruments, and Big Data; *Maume/Fromberger*, Regulation of Initial Coin Offerings: Reconciling US and EU Securities Laws, 19 Chicago Journal of International Law (2019) 548–585; *Moran*, The Impact of Regulatory Measures Imposed on Initial Coin Offerings in the United States Market Economy, Catholic University Journal of Law and Technology Volume 26 (2018), Issue 2 (7); *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31.1.2020); *Noonan*, Bitcoin or Bust: Can One Really „Trust“ One’s Digital Assets?, Estate Planning & Community Property Law Journal Volume 7 (2014), 583–625; *Rivero*, Distributed Ledger Technology and Token Offering Regulation, verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3134428 (zuletzt aufgerufen 31.1.2020); *Rohr/Wright*, Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets, verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104 (zuletzt aufgerufen 31.1.2020); *Roßbach*, Blockchain-Technologien und ihre Implikationen, verfügbar unter https://blog.frankfurt-school.de/wp-content/uploads/2016/02/Blockchain_FSBlog_part2.pdf (zuletzt aufgerufen 31.1.2020); *Rosenberger*, Bitcoin and Blockchain; *Safferling/Rückert*, Telekommunikationsüberwachung bei Bitcoins, MMR 2015, 788–794; *Small*, Bitcoin: The Napster of Currency, Houston Journal of International Law Volume 37 (2015), Number 2, 581–641; *Werbach/Cornell*, Contracts Ex Machina, Duke Law Journal Volume 67 (2017), Number 2, 313–382; *Witte*, The Blockchain: A Gentle Introduction, verfügbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2887567 (zuletzt aufgerufen 31.1.2020); *Zickgraf*, Initial Coin Offerings – Ein Fall für das Kapitalmarktrecht?, AG 2018, 293–308.

I. Die Blockchain-Technologie

1. Einführung

- 1 Die Blockchain ist erstmalig als Technologie hinter Bitcoin in Erscheinung getreten.¹ Sie ist ein digitales, chronologisch aufgebautes,² **dezentrales, verteiltes und nahezu fälschungssicheres Register, ähnlich einer Datenbank.**

Dieses Register, das auch Distributed Ledger genannt wird, wird durch ein Computernetzwerk auf peer-to-peer-Basis geführt.³ In einem peer-to-peer-Netzwerk werden Daten simultan auf jedem Rechner des Netzwerks gespeichert.⁴ Damit unterscheidet sich das peer-to-peer-System von einem Cloud-System, in dem die gespeicherten Dateien auf verschiedene Computer aufgeteilt werden. Diese **Verteiltheit**⁵ schützt die Blockchain davor, durch lokale Ereignisse Schaden zu nehmen. Kommt es zum Verlust einer Kopie der Blockchain, kann der Verlierende mittels entsprechender Nachricht die weiteren Netzwerkteilnehmer um eine erneute Zusendung bitten. Weichen die gespeicherten Versionen voneinander ab, so gilt stets diejenige, die die längste Blockchain enthält. In diese Version haben die Teilnehmer einer Blockchain die meiste Rechenleistung investiert.⁶

- 2 Einer Blockchain liegt stets ein Quellcode zu Grunde. Dieser bildet die Basis des jeweiligen Netzwerks und legt den Beginn der Blockchain sowie ihre Bedingungen und Eigenschaften fest. Bei dezentralen Systemen ist der Code regelmäßig open-source, dh frei verfügbar.⁷ Auf diesem Code baut in aller Regel eine **Protokollsoftware** auf (auch

¹ *Rosenberger* Bitcoin und Blockchain 63.

² *Nakamoto* Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31.1.2020).

³ Vgl. auch die Zusammenfassung bei *De Filippi/Wright* Blockchain and the Law 13.

⁴ Dazu und im Folgenden *Kaulartz* CR 2016, 474 (475).

⁵ Deshalb nennt man die Blockchain auch Distributed Ledger.

⁶ Vertiefend dazu *Berentsen/Schär* Bitcoin, Blockchain und Kryptoassets 216; s. für die Bitcoin-Blockchain auch *Nakamoto* Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31.1.2020): „The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it“.

⁷ Vgl. *De Filippi/Wright* Blockchain and the Law 21.

Client genannt). Diese stellt die tatsächliche Verknüpfung zwischen dem jeweiligen Netzwerkteilnehmer und der Blockchain her. Bei der Bitcoin-Blockchain kann diese Software zB unter dem Namen „Bitcoin Core“ heruntergeladen werden.⁸ Die Nutzer der Blockchain haben die Möglichkeit, den Code weiterzuentwickeln. Die Implementierung eines Updates setzt aber einen Konsens zwischen den Netzwerkteilnehmern voraus. Allerdings ist nicht jede Blockchain per se open-source und damit öffentlich veränderbar. Zudem steht es dem jeweiligen Initiator frei, die Blockchain für Dritte uneinsehbar zu gestalten und nur einen beschränkten Kreis von Nutzern zuzulassen.

Welche Dynamik die Initiierung einer Blockchain entwickeln kann, wird am Beispiel des Bitcoins und der dahinterstehenden Bitcoin-Blockchain deutlich. Diese Bitcoin-Blockchain war die erste ihrer Art. Sie bildet die Grundlage für die Entwicklung teils sehr ähnlicher, teils deutlich andersartiger Blockchains. Die Idee des Bitcoins basiert auf einem 2008 unter dem Pseudonym *Satoshi Nakamoto*⁹ veröffentlichten Paper.¹⁰ Hierin beschreibt der Entwickler (oder eine Gruppe von Entwicklern) ein digitales, dezentral verwaltetes Register als die Grundlage eines elektronischen „Geldsystems“ auf peer-to-peer-Basis. *Nakamoto* nennt die diesem Konzept zu Grunde liegenden Werteinheiten Bitcoins. Mit der Bitcoin-Publikation legte er sämtliche Aspekte des Bitcoins sowie der dahinterstehenden Blockchain-Technologie offen. *Nakamoto* setzte damit den Grundstein für die Weiterentwicklung der Blockchain im Allgemeinen und des Bitcoin-Systems im Besonderen. Denn nach Initiierung ist dieses System von *Nakamoto* unabhängig; es kommt ihm keine besondere Stellung zu – weder in Sachen Betrieb noch in Sachen Weiterentwicklung der Bitcoin-Blockchain. Einfluss darauf haben die Nutzer des Systems. Dies führte dazu, dass bereits kurze Zeit nach Erscheinen des Artikels zahlreiche Nutzer dem Netzwerk beitraten und die Bitcoin-Blockchain eine beeindruckende Dynamik entwickelte. Der Preis für einen Bitcoin entwickelte sich von 0,000764 USD im Januar 2009 hin zu über 20.000 USD Ende 2017.

Die Hinterlegung digitaler Werteinheiten wie Bitcoins in einer Blockchain ist ein Anwendungsfall, die möglichen Einsatzfelder der Blockchain reichen jedoch deutlich weiter.¹¹ Eine Blockchain kann den aktuellen Status unterschiedlichster Objekte und Beziehungen speichern, so zB auch die rechtliche Zuordnung von Immobilien bzw. Mobilien oder den (Nicht-)Vollzug eines Vertragsverhältnisses. Von besonderem Interesse für dieses Handbuch ist die Zuordnung virtueller, in der Blockchain hinterlegter Werteinheiten an bestimmte Nutzer des jeweiligen Blockchain-Netzwerkes. Diese Werteinheiten sind virtuelle Rechengrößen, denen von den Nutzern einer Blockchain ein gewisser Wert beigegeben wird.¹² Sie werden als **Token** bezeichnet. Jeder Token ist aufgrund der erfolgten Transaktionen individualisierbar.¹³

Den öffentlich zugänglichen Eintragungen in der Blockchain kann zu jeder Zeit entnommen werden, welchem Netzwerk-User welche Token zugeordnet sind; alle jemals getätigten Transaktionen sind in ihr unveränderlich enthalten.¹⁴ User sind in der Lage, Token untereinander zu transferieren, ohne einen Intermediär einzuschalten. Dies senkt zum einen die Transaktionskosten¹⁵ und eliminiert zum anderen das Risiko, dass der Mittelsmann die Transaktion, zB aufgrund von Zahlungsunfähigkeit, vereitelt.

⁸ S. <https://bitcoin.org/de/download> (zuletzt aufgerufen 31. 1. 2020).

⁹ Bis heute ist unklar, wer sich hinter dem Pseudonym verbirgt; statt vieler *Rosenberger* Bitcoin und Blockchain 25ff. Da das verwendete Pseudonym maskulin ist, verwenden wir – ohne damit eine Mutmaßung zu bezwecken – im Folgenden das männliche Personalpronomen.

¹⁰ *Nakamoto* Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31. 1. 2020).

¹¹ Statt vieler *Kaulartz* CR 2016, 474.

¹² Für Details s. insbes. → Rn. 70.

¹³ Jede Transaktion trägt eine Transaktions-ID.

¹⁴ *De Filippi/Wright* Blockchain and the Law 22.

¹⁵ *Nakamoto* Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31. 1. 2020).

- 6 Die Zahl der Token kann dabei fix oder variabel ausgestaltet sein. So ist beispielsweise die Anzahl der jemals entstehenden Bitcoins von Anfang an in dem hinter der Bitcoin-Blockchain stehenden Code festgelegt. Bis etwa ins Jahr 2140 können neue Bitcoins bis zum Erreichen der Höchstgrenze geschaffen werden. Anschließend wird die Gesamtzahl von rund 21.000.000 Bitcoins in der Bitcoin-Blockchain verfügbar sein.¹⁶ Die Gesamtmenge an Token kann auch sofort mit Initiierung einer Blockchain den Usern zugänglich gemacht oder nach dem Eintritt bestimmter Bedingungen ausgeschüttet werden. Auch eine an die jeweilige Nachfragesituation angepasste Erhöhung oder Senkung des Bestandes, ähnlich der Geldpolitik westlicher Zentralbanken, ist denkbar. Zur Senkung des Tokenbestandes kann ein sogenanntes **Burning** durchgeführt werden. Dabei werden Token aus der Blockchain unwiderruflich gelöscht.

2. Blockchain-Teilnehmer

- 7 Die Blockchain-Teilnehmer werden als **Nodes**¹⁷ bezeichnet. Diese lassen sich wiederum in unterschiedliche Kategorien einteilen. So muss zwischen sogenannten Full-Nodes (= vollwertige Knoten) und Light-Nodes (= nicht vollwertige Knoten) unterschieden werden. Dies ergibt sich aus der unterschiedlichen Stellung und Funktion des jeweiligen Netzwerkteilnehmers.
- 8 Die Blockchain ist nicht bei einer zentralen Partei, sondern verteilt auf den Computern aller **Full-Nodes** gespeichert. Jeder von ihnen hält eine vollständige, aktuelle Version vor. Full-Nodes sind umfassend in alle Transaktionsvorgänge der Blockchain einbezogen. Sie empfangen und verschicken nicht nur selbst Token, sondern fungieren als Überwacher und Weiterführer des Blockchain-Registers, indem sie Transaktionen überprüfen und bestätigen. Voraussetzung, um als Full-Node agieren zu können, ist, dass der Netzwerkteilnehmer die bereits bestehende Blockchain von den bisherigen Teilnehmern auf seinen Computer herunterlädt. Dies kann, je nach Verbindung, mehrere Tage dauern. Zu den genauen weiteren Aufgaben eines Full-Nodes (→ Rn. 18).
- 9 **Light-Nodes** nehmen dagegen nicht aktiv an der Erweiterung und dem Schutz der Blockchain teil. Ihre Funktionen innerhalb einer Blockchain sind begrenzt. Sie sind bloße Nutzer der Blockchain. Das heißt, sie versenden und empfangen lediglich die jeweiligen Token der Blockchain. Im Übrigen vertrauen Light-Nodes auf das redliche Verhalten der Full-Nodes.

3. Kategorisierung von Blockchains

- 9a Eine Einteilung der Blockchains lässt sich anhand der Zugriffs- und Nutzungsrechte der Blockchain-Teilnehmer vornehmen. Maßgeblich dafür sind **zwei Abgrenzungsmerkmale: private/public und permissioned/permissionless**.
- 10 Die Abgrenzung zwischen **private/public bezieht sich auf die Einsehbarkeit** der in der Blockchain hinterlegten Informationen. Eine Blockchain ist public, wenn sie zu jederzeit von jedermann einsehbar ist.¹⁸ Dagegen ist eine private Blockchain ein abgegrenztes geschlossenes System, auf dessen Inhalt lediglich eine limitierte Gruppe von Berechtigten Zugriff hat.
- 11 Die Unterscheidung zwischen **permissioned/permissionless betrifft die Teilhaberecht** der Netzwerkteilnehmer. Eine permissionless Blockchain liegt immer dann vor, wenn alle Netzwerkteilnehmer dieselben Teilhaberechte haben, zB Transaktionen vor-

¹⁶ *Werbach/Cornell* Duke Law Journal 67 (2017), 313 (329).

¹⁷ *Nakamoto* Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31.1.2020).

¹⁸ Dazu und im Folgenden *Roßbach* Blockchain-Technologien und ihre Implikationen 2, verfügbar unter https://blog.frankfurt-school.de/wp-content/uploads/2016/02/Blockchain_FSBlog_part2.pdf (zuletzt aufgerufen 31.1.2020).

nehmen können. Divergieren die Teilhaberechte der Netzwerkteilnehmer – ist also beispielsweise nur ein begrenzter Kreis zur Verifizierung von Transaktionen berechtigt – ist sie dagegen als permissioned einzustufen.

Diese beiden Unterscheidungsmerkmale lassen sich beliebig kombinieren, so dass **vier verschiedene Gestaltungsvarianten** möglich sind. Die Bitcoin- und die Ethereum-Blockchain sind beispielsweise public und permissionless, die Ripple- und EOS-Blockchain sind dagegen public und permissioned. 12

4. Aufbau einer Blockchain

Eine Blockchain setzt sich aus einzelnen Blöcken (engl. blocks) zusammen. Die Blöcke bestehen wiederum zum Großteil aus einem **Bündel einer bestimmten Anzahl von Transaktionen**, die über die Blockchain getätigt wurden. Bei der überwiegenden Zahl der Blockchains führt jede im Netzwerk getätigte Transaktion zu einer Verlängerung der Kette.¹⁹ 13

In der Bitcoin-Blockchain werden zum Beispiel etwa 2.500 Einzeltransaktionen je Block gebündelt. Die erzeugten Blöcke werden aneinandergereiht und bilden eine Kette. Dieser Prozess ist namensgebend für die Blockchain.

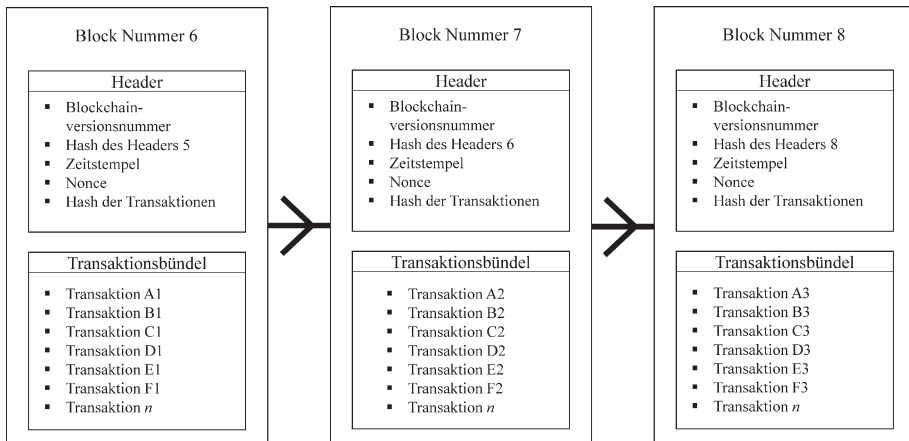


Abbildung 1: Vereinfachte Darstellung einer Blockchain

Jeder Block setzt sich aus verschiedenen Bestandteilen zusammen. Essentiell ist neben dem angesprochenen Transaktionsbündel der sogenannte **Hash**.²⁰ Der Hash ist Bestandteil des sogenannten Headers eines Blocks. Ein Hash ist die Ausgabe einer Hashfunktion. Er dient insbesondere als alphanummerische Prüfsumme – bildlich gesprochen als ein **Fingerabdruck**²¹ – der zugrundeliegenden Daten.²² Der Hash eines Blocks spiegelt alle in ihm enthaltenen Daten, insbesondere die gebündelten Transaktionen, wider. Wird innerhalb des Datenbündels eine Transaktion abgeändert, sei es in Bezug auf eine der Parteien oder die Höhe der transferierten Token, ändert sich auch der Hash. Jeder Block enthält den Hash des vorangegangenen Blocks.²³ Durch diese Bezugnahme des neuen auf 14

¹⁹ De Filippi/Wright Blockchain and the Law 56.

²⁰ De Filippi/Wright Blockchain and the Law 22.

²¹ De Filippi/Wright Blockchain and the Law 22; Kaulartz CR 2016, 474 (475).

²² Snow Anhörung vor dem 114. US Kongress 47, verfügbar unter <https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg20322/pdf/CHRG-114hhrg20322.pdf> (zuletzt aufgerufen 31.1.2020).

²³ De Filippi/Wright Blockchain and the Law 22f.

den vorherigen Block ist stets die Verortung des neuen Blocks innerhalb der Blockchain festgelegt.²⁴ Der Blockheader enthält neben der Versionsnummer der Blockchain²⁵ einen Zeitstempel²⁶. Dieser Stempel belegt, dass die im Block enthaltenen Transaktionsdaten zum ausgewiesenen Zeitpunkt existierten.²⁷ Darüber hinaus ist jeder Block auch mit einer fortlaufenden Nummer gekennzeichnet.

5. Transaktion von Token

- 15 Blocks bestehen bei den meisten Blockchains zu einem Großteil aus Transaktionen der in der Blockchain hinterlegten Token. Um einen Token einem neuen Netzwerkteilnehmer zuzuordnen, verwenden Blockchains das sogenannte **Public-/Private-Key-Konzept**. Dieser kryptographische Mechanismus ist namensgebend für den etwas ungenau geratene²⁸ Begriff der Kryptowährungen. Das Konzept, das auch als asymmetrische Verschlüsselung bezeichnet wird,²⁹ geht auf zwei Kryptographen der Stanford University zurück.³⁰ Jeder Teilnehmer des Netzwerkes verfügt über zwei Schlüssel – einen privaten (Private Key) sowie einen öffentlichen (Public Key).³¹ Die Zahl der Schlüsselpaare ist nicht begrenzt. Ein User kann beliebig viele erstellen und damit Transaktionen unter verschiedensten Pseudonymen tätigen.³²
- 16 Der **Public Key** ist eine Adresse innerhalb der Blockchain, der Token zugeordnet werden können. Diese Adresse dient zugleich als Pseudonym, das für einen bestimmten Netzwerkteilnehmer steht.³³ Damit ist eine Blockchain **kein anonymes, sondern ein pseudonymes System**.³⁴ Verglichen werden kann der Public Key beispielsweise mit einer Kontonummer³⁵ oder einer Emailadresse – insbesondere, wenn diese zum Empfang von Paypal-Zahlungen genutzt wird. Denn auch ein Netzwerkteilnehmer einer Blockchain gibt seinen Public Key an andere weiter, um Token empfangen zu können. Als alternatives Pseudonym zum Erhalt von Token kann im Bitcoin-Netzwerk auch die sogenannte Bitcoin-Adresse verwendet werden. Diese Adresse ist der Hashwert³⁶ des Public Keys.³⁷
- 17 Der **Private Key** verbleibt im Gegensatz zum Public Key exklusiv beim User und wird zur **Signatur von Transaktionen** verwendet.³⁸ Dies sichert die Authentizität und Integrität der Transaktion. Zum einen bürgt der Private Key dafür, dass die Transaktion tatsächlich vom Inhaber des privaten Schlüssels signiert wurde.³⁹ Zum anderen kann so sichergestellt werden, dass der „Versender“ tatsächlich über einen Token verfügt.⁴⁰ Der Private Key ermöglicht zudem den Nachweis, dass der User berechtigt ist, die dem jewei-

²⁴ Rosenberger Bitcoin und Blockchain 66.

²⁵ CryptoCompare What is a Block Header in Bitcoin? <https://www.cryptocompare.com/coins/guides/what-is-a-block-header-in-bitcoin/> (zuletzt aufgerufen 31.1.2020).

²⁶ De Filippi/Wright Blockchain and the Law 23.

²⁷ Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31.1.2020).

²⁸ S. hierzu → Rn. 68.

²⁹ So zB bei Kaulartz CR 2016, 474 (475).

³⁰ Diffie/Hellman IEEE Transaction on Information Theory 22 (1976), 644ff.

³¹ De Filippi/Wright Blockchain and the Law 2.

³² Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31.1.2020); Berentsen/Schär Bitcoin, Blockchain und Kryptoassets 119.

³³ Berentsen/Schär Bitcoin, Blockchain und Kryptoassets 119.

³⁴ De Filippi/Wright Blockchain and the Law 68.

³⁵ Safferling/Rückert MMR 2015, 788 (789).

³⁶ S. zur Erklärung von Hashwerten → Rn. 14.

³⁷ Berentsen/Schär Bitcoin, Blockchain und Kryptoassets 120f.

³⁸ Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31.1.2020); Small Houston Journal of International Law 37 (2015), 581 (588); De Filippi/Wright Blockchain and the Law 16.

³⁹ Kaulartz CR 2016, 474 (475).

⁴⁰ Vgl. Berentsen/Schär Bitcoin, Blockchain und Kryptoassets 119.

ligen Public Key zugeordneten Token zu transferieren.⁴¹ Denn aus dem Private Key kann ein dazugehöriger Public Key mathematisch hergeleitet werden; aus dem Public Key jedoch nicht auf den Private Key geschlossen werden.⁴² Token, die einem bestimmten Public Key zugeordnet sind, können nur von demjenigen transferiert werden, dem der dazugehörige Private Key bekannt ist. Vergleichbar ist dieses Prinzip mit dem Passwort des Paypal-Accounts oder der TAN beim Onlinebanking⁴³. Hier können die zugeordneten Geldeinheiten auch nur dann übertragen werden, wenn der Überweisende das Account-Passwort bzw. die TAN kennt.⁴⁴

Denkbar ist auch, dass ein Netzwerkteilnehmer im Rahmen einer Transaktion der anderen Partei seinen Private Key mitteilt (sog. **off-chain peer-to-peer Transaktion**),⁴⁵ zB um damit eine „Tokenschuld“ zu begleichen. Mittels des Private Keys kann der Empfänger über die Token, die mit dem Private Key verknüpft sind, verfügen. Problematisch ist bei derartigen Transaktionen, dass sich der „Versender“ der Zugriffsmöglichkeit auf den Private Key nicht vollständig begibt.

Zur **Transaktion** eines Tokens, zB eines Bitcoins, sendet der versendende Netzwerkteilnehmer eine entsprechende Transaktionsnachricht unter Zuhilfenahme von Public Key und Private Key an die Blockchain.⁴⁶ Dabei wird diese Nachricht nicht direkt an den Empfänger des Tokens gesendet. Sie wird stattdessen an verschiedene Nodes übermittelt. Die Nodes leiten die Nachricht wiederum an weitere Blockchain-Teilnehmer weiter, bis das gesamte Netzwerk von der Transaktionsnachricht Kenntnis genommen hat.⁴⁷ Die dazu qualifizierten User,⁴⁸ also die Full-Nodes der Blockchain, überprüfen im nächsten Schritt **Integrität und Authentizität** in Bezug auf die versendende Partei. Dazu scannt die bei den Full-Nodes installierte Blockchain-Software sämtliche jemals getätigten Transaktionen.⁴⁹ Erachten mehr als 50% der Full-Nodes die überprüfte Transaktion als gültig,⁵⁰ gilt sie als verifiziert und wird dem Transaktionsbündel eines Blocks hinzugefügt.⁵¹

Bei einer Transaktion eines Tokens auf der Blockchain wird dieser also nicht in tatsächlicher Weise von einem Blockchain-Teilnehmer an einen anderen übermittelt. Vielmehr **ändern sich lediglich die Zuordnungsverhältnisse auf der Blockchain**, also nur die Zuordnung des jeweiligen transferierten Tokens. Ein anderer Node wird als letzter Empfänger (= Zuordnungsobjekt) des Tokens in der Blockchain ausgewiesen.

Beispiel:

Möchte A einen Bitcoin an B senden, benötigt sie den Public Key von B als Empfangsadresse. Die Transaktionsnachricht wird mit As Private Key signiert.⁵² A sendet sodann die Transaktionsnachricht an alle mit ihr verknüpften Nodes. Diese leiten die Nachricht wiederum an alle mit ihnen verknüpften Nodes weiter, bis diese an alle Netzwerkteilnehmer übermittelt wurde. Nach Abschluss des Verifizierungsprozesses durch die Full-Nodes wird der Bitcoin dem Public Key des B zugeordnet. B kann nun anhand des Public Keys von A (als Versenderadresse) erkennen, dass die Transaktion von ihr stammt. Mittels seines Private

⁴¹ Vgl. *Berentsen/Schär* Bitcoin, Blockchain und Kryptoassets 119.

⁴² *Kaulartz* CR 2016, 474 (475); vgl. auch *Berentsen/Schär* Bitcoin, Blockchain und Kryptoassets 119 f.

⁴³ *Safferling/Rückert* MMR 2015, 788 (789).

⁴⁴ Vgl. hierzu *Small* Houston Journal of International Law 37 (2015), 581 (588).

⁴⁵ Zur Off-Chain-Funktionsweise von Trading-Plattformen s. → Rn. 94 ff.

⁴⁶ Vgl. *Nakamoto* Bitcoin: A Peer-to-Peer Electronic Cash System, verfügbar unter <https://nakamotoinstitute.org/bitcoin/> (zuletzt aufgerufen 31.1.2020).

⁴⁷ Für die Weiterleitung ist die Einordnung des Netzwerkteilnehmers als Full- oder Light-Node irrelevant.

⁴⁸ → Rn. 8.

⁴⁹ *De Filippi/Wright* Blockchain and the Law 26.

⁵⁰ Respektive überprüft die bei den Usern installierte Software Integrität und Authentizität und sendet ein (Un-) Gültigkeitssignal an das Netzwerk.

⁵¹ *Rosenberger* Bitcoin und Blockchain 18.

⁵² *De Filippi/Wright* Blockchain and the Law 21.