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. Veronica 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

C.H.BECK

Vahlen

Zitiervorschlag:
Maume/Maute Kryptowerte-HdB

www.beck.de

ISBN Print 978 3 406 73433 5
ISBN E-Book 978 3 406 76243 7

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 Parapluie

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

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

Inhaltsübersicht

Inhaltsverzeichnis

Kapitel 2 Kryptotoken im Rechtsverkehr

Kapitel 3 Kapitalmarkt- und Bankenrecht

Kapitel 5 Steuern und Bilanzierung

Literaturverzeichnis

Andres/Leithaus, Insolvenzordnung (InsO) Kommentar, 4. Aufl. 2018
Baumbach/Hopt, Handelsgesetzbuch Kommentar, 38. Aufl. 2018
Baur/Stürner, 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

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 Filippi/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 Geldwäsche – 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; *Kütük-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. 3

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 beigemessen wird.[12] Sie werden als **Token** bezeichnet. Jeder Token ist aufgrund der erfolgten Transaktionen individualisierbar.[13] 4

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 Transaktionskosten[15] und eliminiert zum anderen das Risiko, dass der Mittelsmann die Transaktion, zB aufgrund von Zahlungsunfähigkeit, vereitelt. 5

[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 25 ff. 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.

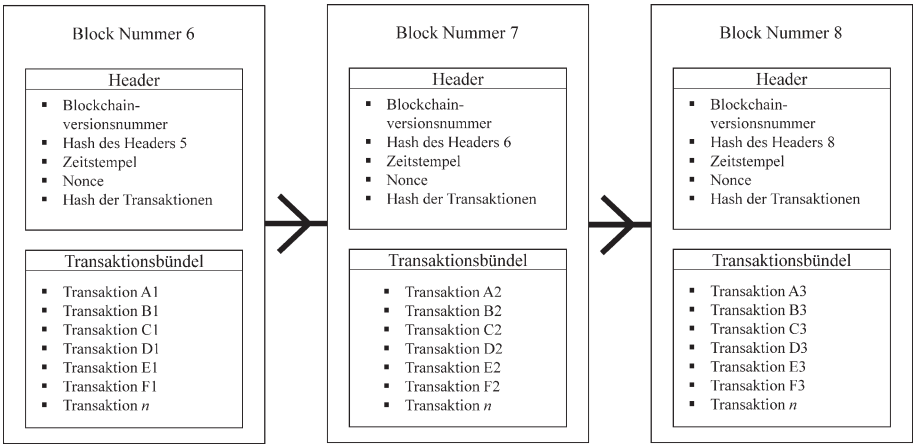

Abbildung 1: Vereinfachte Darstellung einer Blockchain

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 Blockchain[25] einen Zeitstempel[26]. 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 geratenen[28] 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 Kontonummer[35] 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 Hashwert[36] 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] *CryptoCopare* What is a Block Header in Bitcoin? https://www.cryptocompare.com/coins/guides/what-is-ablock-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), 644 ff.
[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 120 f.
[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 Onlinebanking[43]. 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] 18

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 (= Zuordnungssubjekt) des Tokens in der Blockchain ausgewiesen. 19

Beispiel: 20

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.