Recht Wirtschaft Steuern

Handbuch

Omlor / Link (Hrsg.)

Kryptowährungen und Token

dfv Mediengruppe

R&W
Fachmedien Recht und Wirtschaft

RECHT WIRTSCHAFT STEUERN

Kryptowährungen und Token

Herausgegeben von

Prof. Dr. Sebastian Omlor, LL.M. (NYU), LL.M. Eur.

und

Dr. Mathias Link, LL.M. (Columbia)

Bearbeitet von

Lutz Auffenberg, LL.M. (London); Jens Berger;
Prof. Dr. Hanne Böckem; Marco Brinkmann;
Dr. Martin Diehl; Dr. Felix Fischer; Oliver Gaberle;
Dr. Caroline Geuer; Christian Grebe; Daniel Gritsch;
Steffen Günther; Christian Hänchen; Prof. Dr. Alexander Koch;
Dr. Katharina Kubik; Thorsten Kühn; Prof. Dr. Matthias Lehmann,
D.E.A. (Paris II), LL.M., J.S.D. (Columbia); Dr. Mathias Link, LL.M.
(Columbia); Prof. Dr. Cornelia Manger-Nestler, LL.M. (Eur. Int.);
Prof. Dr. Sebastian Omlor, LL.M. (NYU), LL.M. Eur.;
Dr. Stephan Pachinger, LL.M.; Prof. Dr. Thorsten Poddig;
Tobias Rump; Mag. Eva Schneider, MSc; Dr. Andreas Schwennicke;
Prof. Dr. Daniela Seeliger; Dr. Dirk Siegel; Dr. Judith Sild;
Prof. Dr. Armin Varmaz; Nermin Varmaz;
Univ.-Prof. Dr. Christiane Wendehorst, LL.M. (Cantab.);
Dr. Marcus Werner; Dr. Michael Wildscheck, D.J.C.E. (Strasbourg)

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über www.dnb.de abrufbar.

ISBN: 978-3-8005-1739-8

dfv Mediengruppe

www.ruw.de

Druckvorstufe: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Beltz Bad Langensalza GmbH, 99947 Bad Langensalza

Printed in Germany

Vorwort

Die Blockchain-Technologie bildet ein Innovationszentrum des umfassenden Prozesses der Digitalisierung. Als Lebensader namentlich von Industrie 4.0, dem Internet of Things (IoT), von FinTech und Decentralized Finance (DeFi) katalysiert die Blockchain-Technologie den digitalen Wandel am Wirtschafts- und Finanzstandort Deutschland. Damit stehen zugleich Kryptowährungen und Token im Mittelpunkt, deren technologische Basis ebenfalls eine Blockchain bildet. Token entwickeln sich dabei über das Phänomen der Tokenisierung zu Wertpapieren im funktionalen Sinn; mit dem Inkrafttreten des eWpG hat der deutsche Gesetzgeber die Türen für diese evolutionären Prozess weit geöffnet.

Ungeachtet dieser empirischen Umwälzungen steckt die rechtliche Erfassung der Blockchain-Technologie und der darauf abgebildeten Vermögenswerte noch in den Anfängen. Das vorliegende Handbuch hat sich zum Ziel gesetzt, zu einer kohärenten Systematisierung des sich entwickelnden „Rechts der Blockchain" beizutragen und damit zugleich Rechtsunsicherheiten abzubauen. Versammelt sind hochkarätige Autorinnen und Autoren aus den unterschiedlichen Berufsfeldern, die mit den Rechtsfragen der Kryptowährungen und Token befasst sind; einbezogen sind daher insbesondere die Rechtswissenschaft, die Beraterschaft, die Wirtschaftsprüfung und die Finanzverwaltung.

Thematisch deckt das Werk die relevanten Rechtsgebiete ab, die von der Blockchain-Technologie als rechtliche Querschnittsmaterie betroffen sind: das Zivil-, Aufsichts-, Steuer-, Bilanzrecht in gesamter Breite, zudem die Spezialgebiete des Wettbewerbs-, Datenschutz-, Geldwäsche- und Strafrechts. Vorangestellt werden die ökonomischen, währungspolitischen und technischen Grundlagen. Abschließend finden sich zudem Länderberichte zu Liechtenstein, Österreich und Luxemburg, die jeweils eigenständige Regulierungsakzente setzen. Das Handbuch ist im Wesentlichen auf dem Stand von Januar 2021.

Die Herausgeber danken allen Autorinnen und Autoren sowie dem Verlagsteam um Frau Bourgon, Frau Brücker, Frau Grüttner und Frau Dr. Koster für das sorgsame Lektorat und die vertrauensvolle Zusammenarbeit.

Marburg und Frankfurt, im Mai 2021

Sebastian Omlor
Mathias Link

Bearbeiterverzeichnis

Lutz Auffenberg, LL.M. (London)	Rechtsanwalt und Fachanwalt für Bank und Kapitalmarktrecht, Partner, FIN LAW, Frankfurt am Main
Jens Berger	Dipl-Kfm., CPA, Partner, Deloitte GmbH Wirtschaftsprüfungsgesellschaft, Frankfurt am Main
Prof. Dr. Hanne Böckem	Wirtschaftsprüferin, Partnerin Department of Professional Practice KPMG AG Wirtschaftsprüfungsgesellschaft, Honorarprofessorin Humboldt-Universität zu Berlin
Marco Brinkmann	Steuerberater, Partner, Ebner Stolz Wirtschaftsprüfer Steuerberater Rechtsanwälte Partnerschaft mbB, Frankfurt am Main
Dr. Martin Diehl	Deutsche Bundesbank, Leiter Analysen im Zahlungsverkehr und der Wertpapierabwicklung
Dr. Felix Fischer	Steuerberater, Deloitte GmbH Wirtschaftsprüfungsgesellschaft, Frankfurt am Main
Oliver Gaberle	Wirtschaftsprüfer, Partner im Bereich Strategy and Transactions, Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft, Eschborn
Dr. Caroline Geuer	Wirtschaftsprüferin, Department of Professional Practice KPMG AG Wirtschaftsprüfungsgesellschaft, Berlin
Christian Grebe	Diplom-Finanzwirt (FH), Finanzbehörde Hamburg
Daniel Gritsch	Univ.-Ass. Mag. iur., Institut für Zivilrecht der Universität Wien
Steffen Günther	Wissenschaftlicher Mitarbeiter, Lehrstuhl für ABWL, insb. Finanzwirtschaft, Universität Bremen
Christian Hänchen	Diplom-Finanzwirt (FH), Finanzbehörde Hamburg
Prof. Dr. Alexander Koch	Rechtsanwalt in Bonn, Honorarprofessor an der Philipps-Universität Marburg

Dr. Katharina Kubik	Rechtsanwältin im Bereich Steuerrecht, Freshfields Bruckhaus Deringer PartG mbB, Wien
Thorsten Kühn, CFA	Director im Bereich Strategy and Transactions, Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft, Eschborn
Prof. Dr. Matthias Lehmann, D.E.A. (Paris II), LL.M., J.S.D. (Columbia)	Lehrstuhl für Privatrecht, Internationales Privatrecht und Rechtsvergleichung, Universität Wien
Dr. Mathias Link, LL.M. (Columbia)	Partner bei der PricewaterhouseCoopers GmbH, Frankfurt am Main und Düsseldorf
Prof. Dr. Cornelia Manger-Nestler, LL.M. (Eur. Int.)	Professur für Deutsches und Internationales Wirtschaftsrecht, Hochschule für Technik, Wirtschaft und Kultur (HTWK), Leipzig
Prof. Dr. Sebastian Omlor, LL.M. (NYU), LL.M. Eur.	Direktor des Instituts für das Recht der Digitalisierung (Professur für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Bankrecht sowie Rechtsvergleichung), Philipps-Universität Marburg
Dr. Stephan Pachinger, LL.M.	Rechtsanwalt und Partner im Bereich Kapitalmarktrecht, Freshfields Bruckhaus Deringer PartG mbB, Wien
Prof. Dr. Thorsten Poddig	Lehrstuhl für ABWL, insb. Finanzwirtschaft, Universität Bremen
Tobias Rump	Rechtsanwalt und Managing Associate, Linklaters LLP, Düsseldorf
Mag. Eva Schneider, MSc	Rechtsanwältin im Bereich Finanzierungs- und Finanzmarktaufsichtsrecht, Freshfields Bruckhaus Deringer PartG mbB, Wien
Dr. Andreas Schwennicke	Rechtsanwalt und Notar, LSP Lindemann Schwennicke & Partner Partnerschaft von Rechtsanwälten mbB, Berlin
Prof. Dr. Daniela Seeliger	Rechtsanwältin und Partner, Linklaters LLP, Düsseldorf
Dr. Dirk Siegel	Partner Financial Services, KPMG AG Wirtschaftsprüfungsgesellschaft

Dr. Judith Sild	Assistenzprofessorin, Lehrstuhl für Bank- und Finanzmarktrecht, Institut für Wirtschaftsrecht, Universität Liechtenstein, Vaduz
Prof. Dr. Armin Varmaz	Lehrstuhl für internationales Finanzmanagement, Hochschule Bremen
Nermin Varmaz	Rechtsanwalt (Syndikusrechtsanwalt), Senior Legal Counsel, BLG Logistics Group AG & Co. KG, Bremen
Univ.-Prof. Dr. Christiane Wendehorst, LL.M. (Cantab.)	Institut für Zivilrecht und Institut für Digtalisierung und Recht, Universität Wien
Dr. Marcus Werner	Dipl.-Inform., Rechtsanwalt, Fachanwalt für Informationstechnologierecht, Fachanwalt für Handels- und Gesellschaftsrecht, Partner von WERNER Rechtsanwälte Informatiker, Köln
Dr. Michael Wildscheck, D.J.C.E. (Strasbourg)	Vice President und Assistant General Counsel, J.P. Morgan Bank Luxembourg S.A., Großherzogtum Luxemburg

Inhaltsverzeichnis

Teil 2
Zivilrecht

Teil 4
Bilanzrecht

Abkürzungsverzeichnis

a. a. O.	am angegebenen Ort
a. A.	anderer Ansicht
a. E.	am Ende
a. F.	alte Fassung
ABl.	Amtsblatt
ABl. EG	Amtsblatt der Europäischen Gemeinschaft
ABl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz
Abschn.	Abschnitt
ACD	Administration des contributions directes
AED	Administration de l'enregistrement, des domaines et de la TVA
AEUV	Vertrag über die Arbeitsweise der Europäischen Union (EU-Arbeitsweisevertrag)
AG	Aktiengesellschaft; Die Aktiengesellschaft (Zeitschrift)
AGB	Allgemeine Geschäftsbedingungen
AIF	Alternative Investmentfonds
AIFM	Verwalter alternativer Investmentfonds
AIFM-Gesetz	Gesetz vom 12. Juli 2013 über die Verwalter alternativer Investmentfonds
AktG	Aktiengesetz
Alt.	Alternative
AML-Gesetz	Gesetz vom 12. November 2004 zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung
Anm.	Anmerkung
Art.	Artikel
Aufl.	Auflage
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BB	Betriebs-Berater (Zeitschrift)
BeckOK	Beck'scher Onlinekommentar
Begr.	Begründung
betr.	betreffend
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BMF	Bundesministerium für Finanzen

BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BörsG	Börsengesetz (D)
BR-Drs.	Bundesratsdrucksache
brit.	britisch
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
bzw.	beziehungsweise
CAA	Commissariat aux Assurances
CF	Corporate Finance (Zeitschrift)
CR	Computer und Recht (Zeitschrift)
CSSF	Commission de Surveillance du Secteur Financier
d. h.	das heißt
DB	Der Betrieb (Zeitschrift)
DepotG	Depotgesetz
ders.	derselbe
dies.	dieselbe
DStR	Deutsches Steuerrecht
DWG	Gesetz vom 6. April 2013 über dematerialisierte Wertpapiere
EFRAG	European Financial Reporting Advisory Group
EG	Europäische Gemeinschaft
einschl.	einschließlich
EIOPA	European Insurance and Occupational Pensions Authority / Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung
ESMA	European Securities and Markets Authority / Europäische Wertpapier- und Marktaufsichtsbehörde
EStB	Der Ertrag-Steuerberater (Zeitschrift)
EStG	Einkommensteuergesetz
ESZB	Europäisches System der Zentralbanken
ETF	Exchange Traded Fund
ETN	Exchange Traded Note
ETV	Exchange Traded Vehicle
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
EUR	Euro

EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
evtl.	eventuell
EWR	Europäischer Wirtschaftsraum
EZB	Europäische Zentralbank
f./ff.	(fort-)folgende
FAQ	Frequently Asked Questions
FATF	Financial Action Task Force
Fn.	Fußnote
FR	Finanz-Rundschau
FS	Festschrift
GewO	Gewerbeordnung
GewStG	Gewerbesteuergesetz
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GrCh	Europäische Grundrechtecharta
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GWB	Gesetz gegen Wettbewerbsbeschränkungen
h. M.	herrschende Meinung
HGB	Handelsgesetzbuch
Hs.	Halbsatz
i. d. R.	in der Regel
i. H. v.	in Höhe von
i. S. d.	im Sinne des/der
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
ICO	Initial Coin Offerings
IEO	Initial Exchange Offerings
IFRS	International Financial Reporting Standards
insb.	insbesondere
InsO	Insolvenzordnung
IT	Informationstechnologie
ITRB	Der IT-Rechts-Berater (Zeitschrift)
IWF	Internationaler Währungsfonds

K&R	Kommunikation und Recht (Zeitschrift)
KAGB	Kapitalanlagegesetzbuch
Kap.	Kapitel
KWG	Kreditwesengesetz
L.I.R.	Gesetz vom 4. Dezember 1967 über die Einkommensteuer
Lfg.	Lieferung
LG	Landgericht
lit.	littera / Buchstabe
Ls.	Leitsatz
LSE	London Stock Exchange
m. w. N.	mit weiteren Nachweisen
MDR	Monatsschrift für Deutsches Recht (Zeitschrift)
mind.	mindestens
Mio.	Million(en)
MMR	Multimedia und Recht (Zeitschrift)
Mrd.	Milliarde(n)
MTF	Multilateral Trading Facility
MüKo	Münchener Kommentar
NASDQ	National Association of Securities Dealers Automated Quotations
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	NJW-Rechtsprechungsreport (Zeitschrift)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NYSE	New York Stock Exchange
NZA	Neue Zeitschrift für Arbeitsrecht
o. Ä.	oder Ähnliche
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-operation and Development)
OGAW	Organismus für gemeinsame Anlagen in Wertpapieren
OLG	Oberlandesgericht
OTF	Other Trading Facility
OVG	Oberverwaltungsgericht
Q&A	Questions and Answers
RdF	Recht der Finanzinstrumente (Zeitschrift)

RegE	Regierungsentwurf
rev.	revised/revidiert
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache (EuGH)
Rspr.	Rechtsprechung
S.	Seite, Satz (bei Rechtsnormen)
SEC	Securities and Exchange Commission
sect.	section
SGB I	Sozialgesetzbuch Erstes Buch
Slg.	Sammlung
sog.	sogenannte
st. Rspr.	ständige Rechtsprechung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TGE	Token Generating Events
Tz.	Textziffer
u. Ä.	und Ähnliche
u. a.	unter anderem; und andere
u. U.	unter Umständen
u.	und
U.S.	United States
USD	U.S. Dollar
usw.	und so weiter
v. a.	vor allem
Var.	Variante
VG	Verwaltungsgericht
vgl.	Vergleiche
VO	Verordnung
Vol.	Volume
vs	versus
WM	Zeitschrift für Wirtschafts- und Bankrecht
WpHG	Wertpapierhandelsgesetz
WpPG	Wertpapierprospektgesetz
WpÜG	Wertpapiererwerbs- und Übernahmegesetz
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)

z. B.	zum Beispiel
ZBB	Zeitschrift für Bankrecht und Bankwirtschaft
ZfpW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZHR	Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht
Ziff.	Ziffer
ZIP	Zeitschrift für Wirtschaftsrecht
zit.	zitiert
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht
ZVglRWiss	Zeitschrift für Vergleichende Rechtswissenschaft

Teil 1
Grundlagen

Kapitel 1 Rechtliche und finanzökonomische Grundlagen

Literatur: *Al-Yahyaee/Mensi/Ko/Yoon/Kang*, Why cryptocurrency markets are inefficient: The impact of liquidity and volatility, The North American Journal of Economics and Finance, 52, 2020, 101168; *Allen/Gale*, A welfare comparison of intermediares and financial markets in Germany and the US, European Economic Review, 39, 1995, 179; *Allen/Gale*, Innovations in Financial Services, Relationship, and Risk Sharing, Management Science, 45, 1999, 1239; *Allen/Santomero*, The Theory of Financial Intermediation, Journal of Banking and Finance, 21, 1998, 1461; *Allen/Santomero*, What do financial intermediares do?, Journal of Banking and Finance, 25, 2001, 271; *Auer-Reinsdorff/Conrad* (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019; *Bamberger/Roth/Hau/Poseck* (Hrsg.), Beck'scher Online-Kommentar BGB, 55. Edition, 2020; *Banerjee*, A simple model of herd behavior, The quarterly journal of economics, 107, 1992, 797; *Becher*, So funktioniert die Blockchain, 2018, https://www.pcwelt.de/a/so-funktioniert-die-blockchain, 3389680 (zuletzt abgerufen am 29.9.2020); *Beck*, Behavioral Economics: Eine Einführung, 2014; *Becker*, Bankbetriebslehre, 3. Aufl. 1997; *Becker/Peppmeier*, Bankbetriebslehre, 5. Aufl. 2002; *Belleflamme/Lambert/Schwienbacher*, Crowdfunding: Tapping the right crowd, Journal of Business Venturing, 5, 2014, 585; *Berger/Udell*, Relationship lending and lines of credit in small firm finance, Journal of business, 1995, 351; *Bhattacharya/Thakor*, Contemporary Banking Theory, Journal of Financial Intermediation, 3, 1993, 2; *Bialluch-von Allwörden/von Allwörden*, Initial Coin Offerings: Kryptowährungen als Wertpapier oder Vermögensanlage?, WM 2018, 2118; *Bordo*, Equation of Exchange, in: Eatwell/Milgate/Newman (eds), Money. The New Palgrave, 1989, S. 151; *Braunei/Mestel*, Cryptocurrency-portfolios in a mean-variance framework, Finance Research Letters, 28, 2019, 259; *Breidenbach/Glatz* (Hrsg.), Rechtshandbuch Legal Tech, 2018; *Chaum*, Blind Signatures for Untraceable Payments, in: Chaum/Rivest/Sherman (eds), Advances in Cryptology, 1983, S. 199; *Chemmanur/Fulghieri*, Investment bank reputation, information production, and financial intermediation, Journal of Finance, 49, 1994, 57; *Choi/Lehar/Stauffer*, Bitcoin Microstructure and the Kimchi Premium, SSRN Electronic Journal, 2018; *Copeland/Weston/Shastri*, Financial theory and corporate policy, 2005; *Erbguth/Fasching*, Wer ist Verantwortlicher einer Bitcoin-Transaktion? Anwendbarkeit der DS-GVO auf die Bitcoin-Blockchain, ZD 2017, 560; *Fama*, Efficient Capital Markets, A Review of Theory and Empirical Work, Journal of Finance, 25, 1970, 383; *Fama*, Banking in the Theory of Finance, Journal of monetary economics, 6, 1980, 39; *Freixas/Rochet*, Microeconomics of banking, 1997; *Fromberger/Haffke*, Kryptowerte und Geldwäsche, BKR 2019, 377; *Gordon*, Dividends, Earnings, and Stock Prices, The Review of Economics and Statistics, 41 (2), 1959, 105; *Gorton*, Reputation formation in early bank note markets, Journal of political Economy, 104, 2, 1996, 346; *Greenbaum/Thakor*, Contemporary Financial Intermediation, 1995; *Grossman/Hart*, The costs and benefits of ownership: A

theory of vertical and lateral integration, Journal of political economy, 94, 1986, 691; *Gupta*, A Brief History of Blockchain, Harvard Business Review, 2017; *Habermann* (Hrsg.), J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch: Staudinger BGB – Buch 1: Allgemeiner Teil: §§ 164–240, 2019; *Hahn/Wilkens*, ICO vs. IPO – Prospektrechtliche Anforderungen bei Equity Token Offerings, ZBB 31/2019, 10; *Hahn/Wons*, Initial Coin Offering (ICO), 2018; *Hartmann-Wendels/Pfingsten/Weber*, Bankbetriebslehre, 2018; *Härdle/Harvey/Reule*, Understanding Cryptocurrencies, Journal of Financial Econometrics, 18, 2, 2020, 181; *Hofert*, Blockchain-Profiling. Verarbeitung von Blockchain-Daten innerhalb und außerhalb der Netzwerke, ZD 2017, 161; *Hornuf/Schilling*, Are Equity Crowdfunding Investors Active Investors?, Max Planck Institute for Innovation & Competition Research Paper No. 19–15, CESifo Working Paper No. 7884, 2019; *Hu/Valera/Oxley*, Market efficiency of the top market-cap cryptocurrencies: Further evidence from a panel framework, Finance Research Letters, 31, 2019, 138; *Iansiti/Lakhani*, The Truth About Blockchain, Harvard Business Review, January-February 2017 issue, 118; *Ingersoll*, Theory of financial decision making, 1987; *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278; *Klöhn/Parhofer/Resas*, Initial Coin Offerings, ZBB 30/2018, 89; *Kristoufek/Vosvrda*, Cryptocurrency market efficiency ranking: Not so straightforward, Physica A: Statistical Mechanics and its Applications, 531, 2019, S. 120853; *Kunschke/Schaffelhuber* (Hrsg.), FinTech. Grundlagen – Regulierung – Finanzierung – Case Studies, 2018; *LeRoy/Werner*, Principles of financial economics, 2014; *Makarov/Schoar*, Trading and arbitrage in cryptocurrency markets, Journal of Financial Economics, 135, 2, 2020, 293; *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden. Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen, NVwZ 2017, 1251; *Momtaz*, Initial Coin Offerings, PLOS ONE, 15, 2020, e0233018; *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, Working Paper, 2008, https://bitcoin.org/bitcoin.pdf; *Neuberger*, Mikroökonomik der Bank: eine industrieökonomische Perspektive, 1998; *Quintais/Bodó/Giannopoulou/Ferrari*, Blockchain and the Law: A Critical Evaluation, Stanford Journal of Blockchain and Policy No. 2019-01; *Ramadan*, Cross-sectional absolute deviation approach for testing the herd behavior theory: The case of the ASE Index, International Journal of Economics and Finance, 7, 2015, 188; *Rockoff*, The Free Banking Era: A Reexamination, Journal of Money, Credit and Banking, 6, 1974, 141; *Rolnick/Weber*, New Evidence on the Free Banking Era, The American Economic Review, 73, 1983, 1080; *Säcker/Rixecker/Oetker/Limperg* (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Aufl. 2019; *Schlund/Pongratz*, Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung, Deutsches Steuerrecht, 2018, 598; *Schmidt/Hackethal/Tyrell*, Disintermediation and the role of banks in Europe: an international comparison, Journal of Financial Intermediation, 8, 1999, 36; *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431; *Schulz*, Das macht Blockchain. Die Technik hinter Bitcoin & Co., c't 2017, Heft 23, 103; *Schulz*, Vertrag denkt mit. Smart Contracts in der Ethereum-Blockchain, c't 2017, Heft 23, 108; *Sharma*, Public vs. Private Blockchain: A Comprehensive Comparison, https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/ (zuletzt abgerufen am 29.9.2020); *Sharpe*, Asymmetric information, bank lending, and implicit contracts: A stylized model of customer relationships, Journal of Finance, 45, 1990, 1069; *Sharpe*, Asset allocation: Management style and performance measurement, Journal of Portfolio Management, 18, 1992, 7; *Shleifer/Vishny*, The limits of arbitrage, Journal of Finance, 52, 1997, 35; *Siering/Izzo-Wagner* (Hrsg.), Vermögensanlagengesetz, 2017; *Simmchen*, Blockchain (R)Evolution. Verwendungsmöglichkeiten und Risiken, MMR 2017, 162; *Spindler*, Initial Coin Offerings und Prospektpflicht und -haftung, WM 2018, 2109; *Tran/Leirvik*,

Efficiency in the markets of cryptocurrencies, Finance Research Letters, 35, 2020, 101382; *Varmaz*, Rentabilität im Bankensektor: Identifizierung, Quantifizierung und Operationalisierung werttreibender Faktoren, 2006; *Varmaz, A./Varmaz, N.*, Eine empirische Analyse von Initial Coin Offerings (ICO), Vierteljahreshefte zur Wirtschaftsforschung, DIW Berlin, 87, 2018, S. 129; *Veil*, Token-Emissionen im europäischen Kapitalmarktrecht, ZHR 2019, 346; *Walter*, Bitcoin, Libra und sonstige Kryptowährungen aus zivilrechtlicher Sicht, NJW, 2019, 3609; *Wie*, Liquidity and market efficiency in cryptocurrencies, Economic Letters, 168, 2018, 21; *Weitnauer*, Initial Coin Offerings (ICO): Rechtliche Rahmenbedingungen und regulatorische Grenzen, BKR 2018, 231; *Welzel/Eckert/Kirstein/Jacumeit*, Mythos Blockchain: Herausforderung für den öffentlichen Sektor, Kompetenzzentrum öffentliche Informationstechnologie, Fraunhofer-Institut für Offene Kommunikationssysteme, 2017; *Willems*, Funktionsweise und Risiken von virtuellen Währungen, Compliance-Berater, 2016, 325; *Zargar/Kumar*, Information inefficiency of Bitcoin: A study based on high-frequency data, Finance Research Letters, 47, 2019, 344; *Zickgraf*, Initial Coin Offerings – Ein Fall für das Kapitalmarktrecht?, Die Aktiengesellschaft, 2018, 293; *Zöllner*, Kryptowährungen vs. Virtuelle Währungen. Die überschießende Umsetzung der Fünften EU-Geldwäscherichtlinie, BKR 2020, 117.

Übersicht

I. Einleitung

Der starke Preisanstieg von Bitcoin in den Jahren 2017 und 2018 hat das breite öffentliche Interesse auf den Markt für Kryptowährungen gelenkt. Denn jenseits des Bitcoins hat sich eine Token-Ökonomie entwickelt, in der mithilfe der sog. Blockchain[1] die Umsetzung verschiedenster Projekte und Finanzierungsstrate- **1**

1 Der Begriff „Blockchain" wird unten unter Rn. 23 ff. näher erläutert.

gien möglich geworden ist. Der bislang wenig regulierte Markt hat innerhalb kurzer Zeit vielen Start-up-Unternehmen ermöglicht, erhebliche Geldmittel durch Ausgabe von sog. Token[2] zur Investitionsfinanzierung einzusammeln.

2 Bei der Finanzierung mit Token und sog. Kryptowährungen handelt es sich aus der ökonomischen Perspektive um eine Frage der klassische Finanzierungs- und der Prinzipal-Agenten-Theorie. Das Neuartige an der Token-Ökonomie ist nicht die Verteilung von Rechten und Pflichten, wie z. B. bei einem Bankkredit oder bei einer Beteiligungsfinanzierung, sondern die Verifizierung und Dokumentation durch die Blockchain sowie die Automatisierung der Ausübung von Rechten und Pflichten durch die ausgegebenen Token in Verbindung mit Smart Contracts.

3 Um die Besonderheiten der Blockchain, der Token und der Kryptowährungen zu beleuchten, wird in Abschnitt II (Rn. 4–18) eine Kurzeinführung in die klassische Finanzierungstheorie gegeben. Dort wird das Reputationsvermögen als ein Grund für das Entstehen von Finanzinstitutionen und das Fehlen eines solchen als ein Grund für die Aufkommen von Bitcoin und der Blockchains herausgearbeitet. In Abschnitt III (Rn. 22–34) wird die Funktionsweise von Blockchains erläutert, die die Funktion eines Ledgers aus dem Rechnungswesen übernimmt. Im Abschnitt IV (Rn. 35–63) werden die gängigen Definitionen von Token, ihre Verwendung und ihre rechtliche Einordnung beleuchtet. Der Abschnitt V (Rn. 64–83) ist ein empirischer Überblick über den aktuellen, weltweiten Kryptomarkt mit einem besonderen Schwerpunkt auf der Auswertung von Renditen aus der Investorensicht.

II. Finanzierungstheorie und Token-Ökonomie

1. Funktionen von Märkten

4 Ein Markt ist allgemein eine formelle oder informelle Einrichtung, in der sich freiwillig Käufer[3] und Verkäufer bestimmter Produkte (Güter oder Dienstleistungen) physisch oder virtuell treffen, um ökonomische Transaktionen mittels des Handels durchzuführen. Ein Finanzmarkt ist ein spezieller Markt, auf dem Finanztitel (auch: Finanzkontrakte, Finanzverträge) gehandelt werden. In der einfachsten Abstraktion stehen sich auf dem Finanzmarkt Kapitalgeber (z. B. private Haushalte, Institutionen) und Kapitalnehmer (z. B. Unternehmen) gegenüber. Kapitalgeber und Kapitalnehmer agieren nach ihren spezifischen Plänen und entscheiden nach eigenen Zielvorstellungen und Optimierungskalkülen.

2 Der englische Begriff „Token" hat mehrere Bedeutungen. Die adäquateste Bedeutung im Zusammenhang mit Kryptowährungen ist ein Voucher, der zum Einlösen von Gütern und/oder Dienstleistungen benutzt wird.

3 Der einfacheren Lesbarkeit halber wird nur die männliche Schreibweise verwendet. Grundsätzlich sind jedoch beide Geschlechter gemeint.

Die eigentliche Transaktion der Kapitalüberlassung kann direkt über den Finanzmarkt erfolgen und/oder durch eine Institution begleitet werden, wobei ihr Grad der Beteiligung in der Transaktion variieren kann.

Der Finanzmarkt als ein Ort der Transaktion von Finanzkontrakten übernimmt Koordinations- und Allokationsfunktion. Die Koordinationsfunktion erleichtert durch formelle oder informelle Einrichtungen den Kapitalaustausch zwischen den Marktteilnehmern.[4] Die Allokationsfunktion sorgt für den mengenmäßigen Ausgleich zwischen dem Angebot und der Nachfrage, wobei der Ausgleich durch den sich bildenden Preis determiniert wird. Der Preis der Einheit eines Gutes gibt Auskunft über seine Knappheit. Die freiwillige Selbstkontrolle sowie die regulatorischen Eingriffe des Staates können zu einer Auswahlfunktion der Märkte führen. Durch die Auswahlfunktion werden Zugangsbeschränkungen aufgebaut, weil dann an einem Markt nur zugelassene Marktteilnehmer handeln dürfen. **5**

Ein Finanzmarkt übernimmt auch die Losgrößentransformation, die Fristentransformation und die Kreditrisikotransformation.[5] Durch die Losgrößentransformation wird eine mengenmäßige Anpassung der Kapitalbeträge zwischen Kapitalgebern, die in der Regel kleinere Beträge an einen Kapitalnehmer vergeben wollen, und Kapitalnehmern, die in der Regel höhere Summen für Investitionsprojekte benötigen, geschaffen. Durch Stückelung der Kapitalsumme können sich Kapitalgeber bereits mit sehr kleinen Geldbeträgen an der Finanzierung beteiligen. Ein liquider Markt mit der Möglichkeit des jederzeitigen und schnellen Handelns ohne hohe Such- und Transaktionskosten erleichtert die Fristentransformation. Kapitalnehmer, die lange Fristen der Kapitalüberlassung präferieren, können Finanztitel (z. B. Aktien, Anleihen) mit langen Laufzeiten ausgeben. Kapitalgeber können durch den jederzeitigen Verkauf und Kauf ihre Präferenzen bzgl. der Länge der Kapitalüberlassung realisieren. Ein liquider Markt ist ebenfalls eine Grundvoraussetzung für die Risikotransformation. Dabei kann jeder Kapitalgeber ein Portfolio aus unterschiedlichen Finanztitel bilden, das seine persönliche Risikopräferenz widerspiegelt. Die spezifische Funktionsweise der Finanzierung mit Token, ihre Nutzung, ihre Funktionsweise sowie ihr Handel an den Kryptobörsen werden in den nachfolgenden Abschnitten näher beschrieben. Im Kern handelt es sich um eine Finanzierung von riskanten Projekten in ihren frühen Phasen. Daher erfüllen die Krypto- und die Token-Märkte ebenfalls die hier beschriebenen Marktmechanismen und übernehmen ebenfalls die zuvor besprochenen Funktionen, ohne die sich ein Finanzmarkt nicht ausbilden würde. **6**

4 Beispiele sind regulierte Präsenzbörsen (z. B. NYSE, LSE), ein Handelssystem (z. B. XETRA, NASDAQ etc.) oder eine Verbindung von Händlern (z. B. Online-Banking).

5 Vgl. u. a. *Freixas/Rochet*, Microeconomics of banking, S. 4–5; *Becker*, Bankbetriebslehre, S. 19; *Neuberger*, Mikroökonomik der Bank, S. 19–20; *Becker/Peppmeier*, Bankbetriebslehre, S. 22.

7 Der Preis für die Finanzkontrakte spielt eine zentrale Rolle für den Ausgleich zwischen Angebot und Nachfrage.[6] Dieser Preis wird im Regelfall durch einen Zins ausgedrückt, der in der Ökonomie das Wachstum des Kapitals beschreibt und als Rendite bezeichnet wird. Die Rendite kann Prämien beinhalten, die üblicherweise in Zeit-, Kredit- und/oder Risikoprämie unterteilt werden.[7] Die Zeitprämie ist eine „Geduldsprämie", die den risikolosen Transfer des Konsums von heute in die Zukunft anzeigt. Die Kreditprämie berücksichtigt als Entlohnung die Möglichkeiten der Insolvenz des Kapitalnehmers. Die Risikoprämie beinhaltet die Entlohnung für die risikoaversen Kapitalgeber, damit sie sich an einem unsicheren Geschäft beteiligen. Das wesentliche Merkmal der Kredit- und der Risikoprämie ist die Berücksichtigung von Ausfall- und Marktpreisänderungsrisiko. Beim Ausfallrisiko handelt es sich um ein einseitiges Risiko, da für den Kapitalgeber nur negative Szenarien (z. B. Zahlungsausfall, Insolvenzen) eintreten können. Ein Kredit trägt typischerweise nur das Ausfallrisiko und der Kapitalgeber erhält höchstens die versprochene nominale Zinszahlung. Das Marktpreisänderungsrisiko ist zweiseitig, weil für den Kapitalgeber sowohl negative als auch positive Szenarien möglich sind. Beteiligungen am Eigenkapital des Unternehmens können beispielsweise in höheren (niedrigeren) Gewinnbeteiligungen oder in höheren (niedrigeren) Marktwerten enden. Das Marktpreisänderungsrisiko wird insbesondere durch die Schwankungen der Renditen (und der Preise) gemessen.

8 Die Kryptowährungen und die Ausgabe von Token eignen sich nicht zur typischen lehrbuchmäßigen Systematisierung von Finanzierung in Fremd- und Beteiligungsfinanzierung.[8] Eine Theorie der Token-Finanzierung existiert zwar noch nicht, aber ihre Merkmale sind sehr ähnlich zum Crowdfunding. Crowdfunding beinhaltet einen öffentlichen Aufruf, zumeist über das Internet, zur Bereitstellung von Finanzmitteln als Spenden oder im Austausch gegen ein noch zu erstellendes Produkt bzw. eine zu erstellende Dienstleistung oder gegen eine andere Form der Belohnung zur Unterstützung von Crowdprojekten für bestimmte Zwecke.[9] Aufgrund der Restriktionen zahlreicher Jurisdiktionen können Crowdprojekte keinen Aufruf zur Beteiligungen am Eigenkapital oder am Fremdkapital starten, weil dazu spezielle vertragliche Ausgestaltungen notwendig wären.[10]

---

6 Vgl. *Ingersoll*, Theory of financial decision making, S. 25–30; *LeRoy/Werner*, Principles of financial economics, S. 10–30.

7 Vgl. *Copeland/Weston/Shastri*, Financial theory and corporate policy, S. 125 ff.

8 Für eine Darstellung der Nutzung von Token vgl. unten Rn. 35.

9 Vgl. *Belleflamme/Lambert/Schwienbacher*, Journal of Business Venturing 5, 2014, 600 f.

10 In jüngerer Vergangenheit werden vermehrt Konstruktionen in Form von stillen Gesellschaften beim Crowdfunding beobachtet. Vgl. z. B. *Hornuf/Schilling/Schwienbacher*, Are Equity Crowdfunding Investors Active Investors?, S. 10.

Die Kapitalgeber beim Crowdfunding können als Entlohnungskomponente neben dem Produkt auch eine Gewinnbeteiligung („Profit-Sharing") erhalten.

Typischerweise gibt es beim Crowdfunding, ähnlich zu den Kryptowährungen, nur eine Idee und noch kein fertiges Produkt. Folglich kommt zu den Ausfall- und Preisänderungsrisiken die Unsicherheit über die Qualität des Projektes. Bei einer asymmetrischen Informationsverteilung, bei der der Kapitalnehmer entweder die Qualität des Produktes zeitlich vor den Kapitalgebern erfährt, aber nicht beeinflussen kann (Hidden Information) oder durch seine Aktionen die Produktqualität beeinflussen kann (Hidden Action), entstehen sog. Agency-Kosten, die die Finanzierung des Projekts gefährden.[11] In einer vereinfachenden Betrachtung werden bei Qualitätsunsicherheit gemäß der Prinzipal-Agenten-Theorie Projekte hoher Qualität nur dann von rationalen Agenten finanziert, wenn eine Gewinnbeteiligung (als Signal) und glaubhafte Pläne angeboten werden. Projekte niedriger Qualität können bei asymmetrischer Information und Qualitätsunsicherheit durch Einräumung von Kaufwahlrechten vor dem öffentlichen Verkaufsstart (sog. Vor-Kaufrechte) und einen hohen Preisnachlass finanziert werden. Projekte mittlerer Qualität werden folglich gar nicht von rationalen Agenten finanziert. Auf ähnliche Art und Weise lässt sich die Finanzierung durch Token und Kryptowährungen beschreiben. Der sog. Initial-Return, der die Rendite am ersten Handelstag eines Tokens misst, ist sehr hoch und beträgt im Durchschnitt ca. 80 %.[12] Folglich haben die frühen Investoren einen Preisnachlass von ca. 80 % auf den Projektwert erhalten. **9**

2. Funktionen von Institutionen am Finanzmarkt

An einer Finanztransaktion können sich eine oder mehrere Institutionen mit unterschiedlicher Intensität beteiligen. Die beteiligten Institutionen am Kapitalmarkt erfüllen im Wesentlichen zwei Aufgaben: Makler- und Intermediärsfunktion. Der Unterschied zwischen diesen Funktionen liegt in der Rolle der Institution im Finanzvertrag. **10**

Bei der Maklerfunktion begleitet eine Institution den Handel zwischen den Kapitalgebern und den Kapitalnehmern mit komplementären Interessen oder macht diesen Finanzkontrakt überhaupt erst möglich, ohne jedoch selbst Teil der vertraglichen Beziehung zu werden. Beispiele von Institutionen mit einer Maklerfunktion sind amtliche, halb-amtliche und nichtamtliche Börsen, Finanz- und Börsenmakler, Ratingagenturen, Börseninformationsdienste, Versicherungen, Investmentbanken, aber auch Wirtschaftsprüfer, Anwälte, Beratungsunternehmen etc. Die Grundlage der Maklerfunktion ist ein Informations- und Wissens- **11**

11 Vgl. auch für die nachfolgende Ergebnisse der theoretischen Analyse *Belleflamme/Lambert/Schwienbacher*, Journal of Business Venturing 5, 2014, 599–606.

12 Vgl. z. B. *Varmaz/Varmaz*, DIW 2018, S. 136 und die dort angegebene Literatur.

stand, der den Makler in die Lage versetzt, nicht unmittelbar beobachtbare Signale und Informationen zu extrahieren.[13] Dabei spielen die Wiederverwendbarkeit und die Beobachtbarkeit von Informationen eine entscheidende Rolle. Als Beispiel seien Ratingagenturen genannt, bei denen die Institutionen komplexe Informationen sammeln und sie zu einer Einschätzung für Kunden verarbeiten. Aufgrund der Mehrdimensionalität und Komplexität kann es dabei zu unterschiedlichen Einschätzungen durch verschiedene Institutionen kommen. Daher spielt bei der Maklerfunktion die Reputation eine entscheidende Rolle.[14] Die zahlreichen Handelsplattformen von Token und Kryptowährungen erfüllen im Wesentlichen die Maklerfunktion, weil sie häufig adäquate IT-Infrastruktur zum Handel von Token und Kryptowährungen bereitstellen. Daneben gibt es in der jüngeren Vergangenheit Bemühungen, die sog. Initial Exchange Offerings (IEO) als eine alternative Finanzierungsform in der Token-Ökonomie zu etablieren. Dabei sollen die beteiligten Handelsplattformen die Qualität der Projekte vorab prüfen und durch die Aufnahme auf die eigene Handelsplattform ihre Qualität signalisieren.

12 Die stärkste Beteiligung am Finanzvertrag übernehmen Finanzinstitutionen wie Banken in der Rolle eines Intermediärs, der in die Finanzbeziehung anstelle der originären Kapitalgeber und Kapitalnehmer tritt.[15] Banken bieten anstelle der originären Transaktion zwei separate Dienstleistungen an:

1. Sie bieten Depositen für die Kapitalgeber an und werden zu Kapitalnehmern.
2. Sie vergeben Kredite an die Kapitalnehmer und werden selber zu Kapitalgebern.

13 Somit erbringen Banken Dienstleistungen, die im Wettbewerb zu einer unmittelbaren Finanzierung über den Finanzmarkt stehen.[16] Die Existenz von Banken ist dann gerechtfertigt, wenn sie die Finanzierungsleistung günstiger als der Markt oder einzigartige Leistungen erbringen, zu denen der Finanzmarkt nicht der Lage ist.[17] Banken können die Finanzierungsleistungen dann günstiger erbringen, wenn sie einerseits von den Kunden als Institutionen mit hoher Qualität wahrgenommen werden und daher niedrige Kredit- und Risikoprämien zu zah-

13 Vgl. z. B. *Bhattacharya/Thakor*, Journal of Financial Intermediation, 1993, 8; *Neuberger*, Mikroökonomik der Bank, S. 18–19.

14 Vgl. z. B. *Freixas/Rochet*, Microeconomics of banking, S. 7; *Greenbaum/Thakor*, Contemporary Financial Intermediation, S. 52; *Gorton*, Journal of political Economy, 1996, 350 ff.

15 Vgl. z. B. *Hartmann-Wendels/Pfingsten/Weber*, Bankbetriebslehre, S. 81 ff.

16 Vgl. *Allen/Gale*, European Economic Review, 1995, 179–209.

17 Vgl. z. B. *Schmidt/Hackethal/Tyrell*, Journal of Financial Intermediation, 199, 36–67. Eine vertiefte Darstellung der Vor- und Nachteile von Finanzierungsbeziehungen über Banken sowie Erklärungsansätze zu ihrer Existenz neben Finanzmärkten findet sich bei *Varmaz*, Rentabilität im Bankensektor, 2006, S. 22–52.

len haben und andererseits eine hohe Expertise bei der Auswahl von Kreditnehmern mit guter Bonität und folglich selber weniger Kreditausfälle haben.

Bei der Auswahl einer Bank gehen die ursprünglichen Kapitalgeber und -nehmer Risiken ein. Der Kapitalgeber muss ihre hohe Bonität beobachten und sich sicher sein, dass sie nicht mit dem ursprünglichen Kapitalnehmer zu seinem Schaden zusammenarbeitet. Auf der anderen Seite kann die Bank eine Hausbankbeziehung zu einem Kreditnehmer aufbauen und so mehr über seine Projekte, Aktivitäten und letztlich Qualität lernen.[18] Diesen Informationsvorsprung kann die Bank in zweifacher Hinsicht nutzen. Sie kann ex ante implizite Leistungen bei Problemen gewähren, die durch unvollständige Verträge entstehen. Gleichzeitig hat der Kapitalnehmer weniger Anreize, schadhafte Aktionen zu unternehmen, wenn er künftig weitere Finanzierungen benötigt. Allerdings kann die Bank den Informationsvorsprung ex ante und ex post (im Sinne der Vertragstheorie) nutzen, um höhere Risikoprämien als angemessen zu verlangen, wenn der Bankwechsel mit noch höheren Zinsen verbunden ist. Daher hat der Kapitalnehmer nur dann einen Anreiz, der Bank mehr Einblicke in die eigenen Projekte zu gewähren, wenn er ihr vertraut. Folglich ist der Aufbau von Reputation gegenüber den Kapitalgebern und -nehmern eine besondere Leistung, die die Banken bei der Intermediation übernehmen. **14**

Banken und ähnliche Intermediäre mit direkter Beteiligung am originären Finanzvertrag existieren aktuell nicht in der Token-Ökonomie. Daher stellt sich die Frage, wie das Vertrauen in die Ausführung der Finanztransaktionen in der Token-Ökonomie aufgebaut wird. Dazu ist die nachfolgende Analyse der Reputation in den Finanzkontrakten notwendig. **15**

3. Reputation als impliziter Bestandteil von Finanzkontrakten

Reputation ist ein impliziter Bestandteil von unvollständigen Finanzkontrakten[19] bei asymmetrischer Informationsverteilung. Eine Institution kann als Makler oder als Intermediär mit ihrer Reputation die gute Qualität der Finanzkontrakte signalisieren. Investmentbanken können bei einem Gang an die Börse (IPO, Ini- **16**

18 Vgl. z. B. *Allen/Gale*, Management Science, 1999, S. 1245; *Allen/Santomero*, Journal of Banking and Finance, 1998, 1472; *Allen/Santomero*, Journal of Banking and Finance, 2001, 280 ff.; *Berger/Udell*, Journal of business, 1995, 360 f.

19 Zur Definition von unvollständigen Finanzkontrakten vgl. *Grossman/Hart*, Journal of political economy, 1986, 696 ff. Sie fokussieren sich auf die Klasse von Verträgen, bei denen es unmöglich ist, jede zukünftige Eventualität zu berücksichtigen oder zu versichern. In der Praxis sind Verträge häufig unvollständig, weil nicht jeder zukünftige Umweltzustand bekannt ist. Die Autoren definieren Eigentum als residuales Kontrollrecht, d. h. das Recht zu entscheiden, wenn der ursprünglich vereinbarte Vertrag keine Regelung spezifiziert hat.

tial Public Offering) durch ihre Reputation die Qualität der jungen Firmen signalisieren und durch die Preissetzung für die jungen Aktien die Risikoprämie angemessen berücksichtigen.[20] Investmentbanken mit hoher Reputation können höhere Gebühren bei den IPOs durchsetzen. Daher sind sie in der Regal rentabler als andere Banken, solange sie ihre hohe Reputation behalten und durch Fehlsignale an die Kapitalgeber nicht verlieren. Ähnlich können Finanzintermediäre ihre Reputation aufbauen, um günstiger an die Einlagen von Kapitalgebern zu kommen und in einer Hausbankbeziehung ihren Informationsvorsprung gegenüber anderen Instituten auszubauen.[21] Allerdings ist der Aufbau einer hohen Reputation nicht kostenlos und dauert in der Regel lange. Der Aufbau lohnt sich, solange eigene hohe Reputation einer Bank durch andere Banken nicht kostengünstig durch falsche Signale imitiert werden kann. Die Reputation kann, meist sehr schnell, durch Fehlsignale verloren werden. Dann vertrauen die Kapitalgeber und -nehmer den Informationen einer Institution nicht mehr. Als Beispiele seien Wirtschaftsprüfungsgesellschaften genannt, die die (früheren und aktuellen) Bilanzmanipulationen gar nicht oder erst spät aufgedeckt haben.

17 An dieser Stelle mag der Einwand kommen, dass die Finanzkontrakte durch den ordnenden regulatorischen Rahmen im Finanz- und Bankensektor geschützt werden und daher das ordnungsgemäße Funktionieren von Finanzmärkten gewährleistet wird. Nach dieser Sichtweise müssten die Token-Ökonomie und der Kryptomarkt reguliert werden, um schlechte von guten Risiken trennen zu können. Dies ist aus zwei Gründen zumindest verkürzt.

18 Erstens, das Funktionieren von Finanzmärkten und Banken sowie die Ausgabe von Zahlungsmitteln durch Banken ohne eine staatliche Regulierung hat historische Vorbilder, von denen hier nur auf die sog. Free-Banking-Era in den USA eingegangen wird. Während dieser Periode gab es keine Regulierung durch die US-amerikanischen Behörden, die Eintrittsbarrieren in den Bankenmarkt waren sehr niedrig und den Banken war es erlaubt, eigene Banknoten auszugeben, die als Zahlungsmittel akzeptiert waren.[22] Einige heute noch angesehene Banken in New York sind in dieser Periode entstanden. In der früheren Literatur wurde diese Periode mit zahlreichen Wildcat-Banks mit betrügerischen Absichten als ein besonderer Grund angeführt, warum es einer Bankenregulierung bedarf. Die Wildcat-Banken zeichneten sich vor allem durch das Overissuing aus, indem sie Finanzpapiere mehrfach und für Anleger nicht sichtbar auf denselben Sicherungsbetrag an Geld oder an Gold bezogen. Dieses Problem wird aktuell im Zu-

20 Vgl. z. B. *Chemmanur/Fulghieri*, Journal of Finance, 1994, 60 ff. Die aktuellen Versuche der Etablierung von IEOs können als Versuch interpretiert werden, Reputation aufzubauen.

21 Vgl. *Sharpe*, Journal of Finance, 1990, 1075–1980.

22 Vgl. *Rolnick/Weber*, American Economic Review, 1983, S. 1080–1082.

sammenhang mit dem Double-Spending in der Token-Ökonomie diskutiert. Aber mehrere finanztheoretische Modelle zeigen Wege auf, wie wenig regulierte Finanz- und Bankenmärkte stabil sind und es bleiben.[23] Die neueren empirischen Erhebungen und Untersuchungen zeichnen ein deutlich differenzierteres Bild, nach dem das Problem von Wildcat-Banks existierte, aber nahezu alle Banken nach dem Ende der Free-Banking-Era in der Lage waren, ihren Kunden mindestens den nominalen Einzahlungsbetrag zu erstatten.[24] Zusammenfassend lässt sich aus der historischen Episode nicht generell die Hypothese ablehnen, dass die Finanz- und Bankenmärkte ohne eine staatliche Regulierung stabil operieren, solange das Vertrauen der Kapitalnehmer und -geber in die Reputation der Banken vorhanden ist. Die empirischen Analysen haben sogar Hinweise hervorgebracht, nach denen erst sporadische Eingriffe der US-amerikanischen Bundesstaaten zu teilweise chaotischen Zuständen und erheblichen Reputationsverlusten in die Funktionsfähigkeit der Märkte und Banken geführt haben.

Zweitens, regulatorische Eingriffe können Nutzen und Kosten stiften. Die Regu- **19**
lierung als solche ist aus ökonomischer Perspektive dann gerechtfertigt, wenn der Nutzen des Eingriffs mindestens den entstehenden Kosten entspricht. Der Nutzen der Regulierung ist vor allem dann gegeben, wenn Marktversagen durch erhebliche Informationsasymmetrien, externe Effekte und/oder durch Marktmacht vorliegt. Ferner ist bei der Nutzenanalyse auch wichtig zu prüfen, ob der regulatorische Eingriff die intendierte Wirkung überhaupt erzielt. Als Beispiel eines regulatorischen Eingriffs seien die Zugangsbeschränkungen durch die BaFin in Deutschland genannt. Denn erst eine Zulassung durch die BaFin erlaubt das Betreiben von Bankgeschäften oder den Vertrieb bestimmter Finanzprodukte. Ähnliche Regelungen bestehen auch bei dem Verkauf von Aktien während des Börsengangs im Hinblick auf die Prospekthaftung. Diese Zulassungen prüfen, ob bestimmte Qualifikationen (z. B. akademische Ausbildung, Zertifizierung und/oder Berufserfahrung) vorliegen und/oder Mindeststandards eingehalten werden. Durch die Zugangsbeschränkung wird Nutzen gestiftet, wenn die Kapitalgeber oder -nehmer die Qualifikation der Personen, der Institutionen oder der Produkte nicht oder nur unter exorbitant hohen Kosten herausfinden können. Denn ein Mindestmaß an Qualifikation im Umgang mit dem Risiko ist hilfreich bei der Auswahl risikobehafteter Anlagen. Ein Problem kann entstehen, wenn die Kapitalgeber und -nehmer die bloße Zulassung als ein Zeichen der Qualität interpretieren. Opportunistisch handelnde Akteure können mit der Zulassung durch die BaFin, beispielsweise für ihre Produkte, werben, obwohl die Zulassung in keiner Beziehung zur Qualität, zur Rendite oder zum Risiko des

23 Vgl. *Fama*, Journal of Finance, 1980, 45 f.

24 Vgl. *Rolnick/Weber*, American Economic Review, 1983, 1080–1082; *Gorton*, Journal of Political Economy, 1996, 350 ff.; *Rockoff*, Journal of Money, Credit and Banking, 1974, 141–167.

Produktes steht. Folglich imitieren diese Akteure die hohe Qualität von angesehenen Banken durch die staatliche Regulierung, weil einige Kapitalgeber und -nehmer die Signale falsch interpretieren. Ähnliches lässt sich für die Zulassung von Ratings von Ratingagenturen zur Beurteilung von Kreditausfallrisiken beobachten. Nach der herrschenden Regulierung sind sie grundsätzlich zur Berechnung der Eigenmittelunterlegung von Banken zugelassen. Aus der Zulassung leitet sich allerdings kein Signal über die Qualität des Ratings ab. In den Regulierungsvorschriften sind sogar die internen Bankmodelle ökonomisch begünstigt, weil mit ihnen die Risikogewichtung, und somit die Kosten für die Banken, geringer als nach den Ratings der Agenturen ausfallen kann. Viele private (und gerade in Deutschland öffentlich-institutionelle) Anleger haben während der Finanzkrise schlechte Erfahrungen mit der Qualität von Ratingagenturen, bedingt durch erhebliche Verluste, gemacht. Die Kosten der Regulierung können auch eine geringere Wettbewerbsintensität und steigende Kosten für die Erfüllung der Regulierungsanforderungen sein, die auf alle anderen Kunden umgelegt werden.

20 Die ökonomische Theorie der Regulierung stark verkürzt zusammenfassend lässt sich als Befund festhalten, dass die Regulierung das Funktionieren der Märkte erleichtern kann, sie aber keineswegs die Reputation (im Sinne guter Qualität) von Finanzmarktteilnehmern ersetzt.

21 Der Reputationsverlust der Finanzinstitutionen und auch der Regulierungsbehörden wird als ein Grund für das Entstehen der Blockchains und Kryptowährungen wie Bitcoin genannt. Das Bitcoin-White-Paper startet mit der Beschreibung des Vertrauensverlustes in die Finanzinstitutionen: „Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. […] it […] suffers from the inherent weaknesses of the trust based model." Und weiter auf der ersten Seite: „What is needed is an electronic payment system based on cryptographic proof instead of trust […]."[25] Der motivierende Gedanke bei der Entstehung der Blockchain und des Bitcoins war der Glaube, den Reputationsverlust von Finanzinstituten während der Finanz- und Bankenkrise im Jahr 2008 durch einen Reputationsaufbau mithilfe kryptografischer Verfahren und eines globalen Peer-to-Peer-Netzwerkes zu begegnen. Aus Sicht der ökonomischen Theorie handelt es sich dabei um ein Delegationsproblem, bei dem die Nutzer des Netzes (z. B. des Zahlungsverkehrs) ihre Aufgabe der Überwachung an eine dritte Partei übergeben, wobei die Aufgabe nicht mehr einer zentralen Institution, sondern der Mehrheit der Netzwerkteilnehmer zufällt. Allerdings wird hier auch auf die Reputation der Programmierer vertraut, die die Blockchains verwalten und durch-

25 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, S. 1.

aus zum Schaden der Anleger handeln könnten.[26] Die Funktionsweise von Blockchains und ihre Einordnung werden im nächsten Abschnitt erläutert.

III. Arten und Funktionsweisen von Blockchains

Die Blockchain-Technologie, obgleich in Teilen als „disruptive" Technologie dargestellt,[27] ist seit ihrer Entstehung in 2008[28] ein umstrittenes und in vielen Facetten diskutiertes Gebiet.[29] In der rechtswissenschaftlichen Literatur wird ihr zwischen einem teils zurückhaltenden Interesse und vorsichtiger Skepsis angesichts der Komplexität bei der rechtlichen Einordnung begegnet.[30] Vereinfachend lässt sich die Blockchain als eine besondere Form eines Ledgers beschreiben. In der Ökonomie ist der Ledger als das Hauptbuch (oder Kassenbuch) aus dem Rechnungswesen bekannt, mit dem vor allem die Dokumentation aller Geschäftsvorfälle in einem Unternehmen verzeichnet wird. So wird mit der Bitcoin-Blockchain der Transfer der Bitcoin zwischen den anonymen Konten erst validiert und dann in der Blockchain dauerhaft protokolliert. Die Validierung wird nicht von einer zentralen Stelle vorgenommen, sondern von einem zufälligen Rechner, der als erster eine schwierige mathematische Aufgabe löst. Die Protokollierung der Geschäftsvorfälle zwischen den anonymen Konten geschieht durch alle Rechner im Blockchain-Netzwerk und ist jederzeit und für alle öffentlich verfügbar. Die Dokumentationsfunktion einer Blockchain lässt sich losgelöst von der Anwendung als Kryptowährung nutzen. Als Beispiele sei- **22**

26 Wenn die frühe Diskussion unmittelbar nach der Veröffentlichung des White Papers, insb. zwischen *Satoshi Nakamoto* und *James A. Donald*, auf der Webseite https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html verfolgt wird, wurden bereits damals die heute diskutierten Schwachstellen des Proof-of-Works-Ansatzes sehr wohl erkannt, u. a. dass eine Entität mit der Hälfte der Rechenleistung das Netz beherrschen kann. Damals, zwei Wochen nach der Insolvenz von Lehman Brothers, wurden die staatlichen Regierungen dessen verdächtigt.

27 Vgl. *Simmchen*, MMR 2017, 162; *Hofert*, ZD 2017, 161; *Schrey/Thalhofer*, NJW 2017, 1431. Gegen eine solche Darstellung sprechen sich *Iansiti/Lakhani*, The Truth About Blockchain, Harvard Business Review 2017, aus: „(B)lockchain is not a 'disruptive' technology, which can attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly. Blockchain is a *foundational* technology: It has the potential to create new foundations for our economic and social systems."

28 Die erste größere Verbreitung einer Blockchain im Sinne einer verteilten Datenbank erfolgte durch die Veröffentlichung des White Papers zu Bitcoin im Jahre 2008, vgl. Fn. 25.

29 Vgl. etwa *Gupta*, A Brief History of Blockchain, Harvard Business Review 2017, https://hbr.org/2017/02/a-brief-history-of-blockchain (zuletzt abgerufen am 29.9.2020); *Schlund/Pongratz*, DStR 2018, 598; *Schrey/Thalhofer*, NJW 2017, 1431.

30 *Schlund/Pongratz*, DStR 2018, 598, 600; *Schrey/Thalhofer*, NJW 2017, 1431; *Simmchen*, MMR 2017, 162; *Hofert*, ZD 2017, 161; *Martini/Weinzierl*, NVwZ 2017, 1251.

en die Aufzeichnungen der Katasterämter genannt. Die Dokumentation der Transaktion zwischen den Parteien muss nicht zwangsläufig durch eine zentrale Institution erfolgen und könnte in eine Blockchain ausgelagert werden. Die Grundlagen der Funktionsweise jener Blockchains und ihre rechtliche Einordnung werden nachfolgend vorgestellt.

1. Grundaufbau von Blockchains

23 Die zu diesem Thema häufig referenzierte BaFin bezeichnet Blockchains als „fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert, nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet werden".[31] Diese allgemein gehaltene Definition verdeutlicht zumindest die Vielzahl der Ausgestaltungsmöglichkeiten einer Blockchain. Zwei Bestandteile hebt der Ansatz jedoch treffend hervor: die Verifizierung von Datentransaktionen und die Dezentralität der Datenbanken.

24 Im technischen Sinne ist die Blockchain eine verteilte Datenbank zum Speichern von Daten.[32] Obgleich dies beim ersten Anklang nicht spektakulär klingt, ist die technische Vorgehensweise beachtenswert: Die Daten werden in einen sog. „Block" geschrieben, bis sein Fassungsvermögen erreicht ist und der Prozess in den nächsten Block übergeht.[33] Dieser Ablauf setzt sich beliebig oft fort – der nächste Block verweist auf den vorangegangenen, womit eine Kette von sich referenzierenden Blöcken entsteht.[34]

25 Um zu validieren, ob die jeweiligen Blöcke tatsächlich zusammengehören, wird auf das sog. „Hashing" zurückgegriffen. Ein Hash ist eine bestimmte Abfolge von Buchstaben und Zahlen, die je nach Datensatz individuell und damit stets unterscheidbar ist.[35] Erstellt wird ein Hash durch das sog. „Mining", in dessen Rahmen ein nachträglich nicht mehr modifizierbarer Arbeitsnachweis („proof

31 Vgl. BaFin Journal, Mitteilungen der Bundesanstalt für Finanzdienstleistungsaufsicht, Februar 2016.

32 Vgl. *Schulz*, c't 2017, Heft 23, 103; *Schulz*, c't 2017, Heft 23, 108; *Schrey/Thalhofer*, NJW 2017, 1431; *Simmchen*, MMR 2017, 162; *Quintais/Bodó/Giannopoulou/Ferrari*, Blockchain and the Law: A Critical Evaluation, Stanford Journal of Blockchain and Policy 2019; ferner die Legaldefinition der Vermont Statutes Annotated, T.12 § 1913(a): „'blockchain technology' means a mathematically secured, chronological, and decentralized consensus ledger or database, whether maintained via Internet interaction, peer-to-peer network, or otherwise."

33 Vgl. *Schrey/Thalhofer*, NJW 2017, 1431; *Simmchen*, MMR 2017, 162.

34 Vgl. *Schrey/Thalhofer*, NJW 2017, 1431.

35 Vgl. *Becher*, So funktioniert die Blockchain, PC-Welt 2018, https://www.pcwelt.de/a/so-funktioniert-die-blockchain,3389680 (zuletzt abgerufen am 29.9.2020).

of work") erstellt wird.[36] Dabei handelt es sich um eine schwer zu berechnende, doch ohne Weiteres überprüfbare Zahl, die als Basis für eine Regel gilt, der jeder neuer Block nachkommen muss.[37] Auf diese Weise muss ein Programm, das einen neuen Block berechnet, so lange einen Hash berechnen, bis die vordefinierte Bedingung eingetreten ist.[38] Im „Block Header", der Kopfzeile des jeweiligen Blocks, findet die Verbindung zwischen den Hashes statt: Der Hash aus der aktuellen Transaktion und der Hash aus dem vorangegangenen Block werden an dieser Stelle gespeichert.[39]

Essenzieller Bestandteil dieses Ablaufs ist, dass jeder am Peer-to-Peer-Netzwerk teilnehmende Rechner die vollständige Kette mit sämtlichen enthaltenen Transaktionen speichert, um eine umfassende Transparenz herzustellen und Authentizität zu gewährleisten.[40] Zusätzlich sichert dieses System ab, dass eine Partei nicht schon vorher über den von der Transaktion betroffenen Gegenstand verfügt hat (sog. „Double Spending").[41] Die dezentralen Rechner gleichen zu diesem Zweck die Transaktionshistorie einschließlich Zeitstempel ab: Sämtliche Transaktionen liegen in einem Pool gespeichert und werden im Netzwerk durch die Rechner dahingehend überprüft, ob eine neue Transaktion im Widerspruch zur bisherigen Historie liegt.[42] Sobald eine ausreichende Anzahl von Rechnern keine Unregelmäßigkeiten in der Transaktion feststellt, wird sie bestätigt.[43] Die bestätigten Transaktionen werden chronologisch und unveränderbar in der Blockchain hintereinander gespeichert, wohingegen die nicht bestätigten Transaktionen zurück in den Pool fallen.[44] **26**

36 Vgl. *Schulz*, c't 2017, Heft 23, 104; *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 2 Rn. 548; *Schrey/Thalhofer*, NJW 2017, 1431, 1432.

37 Vgl. *Schulz*, c't 2017, Heft 23, 104.

38 Vgl. *Schulz*, c't 2017, Heft 23, 104. Der dahinterliegende Ressourcenverbrauch ist zugleich auch Gegenstand von Kritik, vgl. Rn. 35.

39 Vgl. *Becher*, So funktioniert die Blockchain, PC-Welt 2018, https://www.pcwelt.de/a/so-funktioniert-die-blockchain,3389680 (zuletzt abgerufen am 29.9.2020).

40 Vgl. *Schulz*, c't 2017, Heft 23, 103; *Becher*, So funktioniert die Blockchain, PC-Welt, 2018, https://www.pcwelt.de/a/so-funktioniert-die-blockchain,3389680 (zuletzt abgerufen am 29.9.2020); *Simmchen*, MMR 2017, 162, 163; *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 2 Rn. 545; *Walter*, NJW 2019, 3609, 3612.

41 Vgl. *Schlund/Pongratz*, DStR 2018, 598, 600; *Walter*, NJW 2019, 3609, 3612.

42 Vgl. *Schlund/Pongratz*, DStR 2018, 598, 599.

43 Vgl. *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 2 Rn. 542; *Schrey/Thalhofer*, NJW 2017, 1431, 1432.

44 Vgl. *Schrey/Thalhofer*, NJW 2017, 1431, 1432.

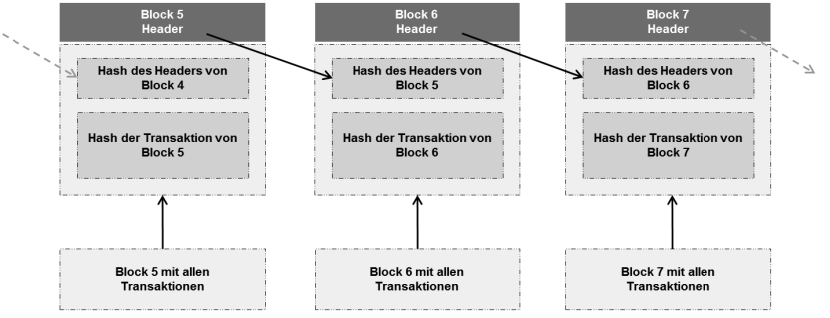

Abb. 1: Funktionsweise einer Blockchain
(in Anlehnung an *Schrey/Thalhofer*, NJW 2017, 1431, 1432).

27 Die dezentrale Struktur birgt ein geringes Fälschungsrisiko. Die Blockchain ist gegen nachträgliche Änderungen robust, da jeder Block den Hash des Vorgängers enthält, womit nachträgliche Manipulationen oder zufällige Änderungen unmittelbar auffallen.[45] Ein Eingriff in die Blockchain, etwa durch einen Hacker, ist praktisch wirkungslos: Da eine Vielzahl von Rechnern die vollständige Transaktionshistorie lokal speichert, würde eine gefälschte Blockchain von jedem teilnehmenden Rechner als solche erkannt.[46] Dies macht eine Fälschung entsprechend unattraktiv. Ein wirkungsvoller Eingriff könnte nur dann gelingen, wenn über 50 % der Rechnerleistung des jeweiligen Netzwerks beherrscht würde, um die gefälschte Transaktion zu bestätigen. Obgleich dies theoretisch möglich erscheint, dürfte dies praktisch gesehen einen zu großen Aufwand bedeuten: Eine beabsichtigte nachträgliche Änderung in einem Block setzt eine Neuberechnung der gesamten nachfolgenden Kette voraus, was bei weiter in der Historie zurückliegenden Blocks wenig verlockend erscheint.[47]

28 Technisch gesehen kann es vorkommen, dass von mehreren Minern berechnete Blöcke eingehen, die zwar unterschiedliche Vorgänger aufweisen, dennoch allesamt dieselbe Distanz zum letzten gemeinsamen Vorgänger haben (sog. „Fork“).[48] Die Blockchain teilt sich auf diese Weise in Zweige auf, wobei auf längere Sicht einer dieser Zweige sich durchsetzt, etwa weil in ihm die meiste Rechnerleistung liegt.[49] Kürzere Zweige sowie die in ihnen enthaltenen Transaktionen werden aus der Blockchain entfernt, womit eine langfristige Einflussmöglichkeit durch betrügerische Miner minimiert wird.[50]

45 Vgl. *Schulz*, c’t 2017, Heft 23, 103.
46 Vgl. *Schrey/Thalhofer*, NJW 2017, 1431, 1432.
47 Vgl. *Schulz*, c’t 2017, Heft 23, 103.
48 Vgl. *Schulz*, c’t 2017, Heft 23, 105.
49 Vgl. *Schulz*, c’t 2017, Heft 23, 105.
50 Vgl. *Schulz*, c’t 2017, Heft 23, 105.

Ein bedeutender Vorteil der Dezentralität ist, dass der Bedarf an einem Intermediär entfällt.[51] Essenzieller Bestandteil einer Wirtschaft ist, Vertrauen zwischen unbekannten Marktteilnehmern dergestalt zu schaffen, dass sie Vertrauen in die fragliche Transaktion entwickeln.[52] Hierfür kommt Intermediären bei herkömmlichen Transaktionen eine entscheidende Rolle zu. Blockchains benötigen keine zentral agierenden Intermediäre und lassen die entsprechenden Transaktionskosten sinken. Kam es also bislang stets auf Banken, Treuhänder oder Rechtsanwälte an, um Vertrauen zu generieren, nimmt dies die Blockchain-Technologie selbst wahr und wirkt auf diese Weise gestiegenen Transaktionskosten entgegen. **29**

2. Arten von Blockchains

Public Blockchains stellen öffentlich zugängliche Blockchains dar, auf die jedermann zugreifen kann.[53] Im Gegensatz zu Private Blockchains bestehen keine Zugriffsbeschränkungen. Einem unbegrenzten Personenkreis ist es damit möglich, sowohl Transaktionen an die Blockchain zu senden als auch solche zu validieren. **30**

Repräsentativ hierfür dürften insbesondere Kryptowährungen wie Bitcoin, Litecoin oder Ethereum sein. Bei Kryptowährungen handelt es sich um dezentralisierte, auf Open-Source-Verfahren und mathematischen Peer-to-Peer-Verfahren basierende virtuelle Währungen.[54] Ein Nutzer erhält eine individuelle Adresse, vergleichbar einer herkömmlichen Kontonummer, als ein von der Bitcoin-Software für den Nutzer generierter sog. Public Key.[55] Zusätzlich erhält der Nutzer einen Private Key und eine Wallet, wobei er durch die Kombination beider Keys den Zugang zur Wallet erhält.[56] Das Schlüsselpaar dient der Authentifizierung der Transaktion, indem der Private Key mit dem Public Key kryptographisch auf eine solche Weise verbunden wird, dass sie sich von anderen Nutzern anhand ihrer Public Keys überprüfen lässt.[57] **31**

Das kryptographische Element an dieser Vorgehensweise ist, dass anhand der vorbezeichneten Kombination auf drei mathematisch zusammenhängende Komponenten zurückgegriffen wird.[58] Ihre Prüfung erfolgt durch einen Abgleich der Transaktionshistorie und des Zeitstempels, um etwaige Widersprüche zwischen neuen und bisherigen Transaktionen zum Vorschein zu bringen. Die Besonder- **32**

51 Zur Rolle von Intermediären, vgl. Rn. 12 ff.
52 Zur Rolle von Reputation und Vertrauen, vgl. Rn. 16 ff.
53 Vgl. *Schrey/Thalhofer*, NJW 2017, 1431, 1433.
54 Vgl. *Willems*, CB 2016, 325.
55 Vgl. *Willems*, CB 2016, 325.
56 Vgl. *Willems*, CB 2016, 325.
57 Vgl. *Willems*, CB 2016, 325.
58 Vgl. *Zöllner*, BKR 2020, 117, 118.

heit liegt hier in der Konkurrenz zwischen den teilnehmenden Rechnern: Wem die schnellste Validierung gelingt, erhält eine Entlohnung in der validierten Währungseinheit, z. B. neue Bitcoin als Entlohnung.[59] Das Besondere an den Blockchains, wie z. B. bei Bitcoin, ist das Fehlen einer Intermediation oder Aufsicht. Das Vertrauen in die Währung basiert nicht auf der Steuerung durch eine Zentralbank oder auf der Existenz einer staatlichen Kontrolle, sondern allein auf den offengelegten Algorithmen.[60]

33 Eine Private Blockchain ist eine unter Genehmigungsvorbehalt stehende Blockchain. Sie funktioniert auf der Grundlage von Zugangskontrollen, die die am Netzwerk teilnehmenden Personen einschränken.[61] Ein Mitglied des Netzwerks wird nur, wer nach vorheriger Genehmigung oder Abstimmung durch die bereits existierenden Mitglieder als solches zugelassen wurde.[62] Es gibt eine oder mehrere kontrollierende Instanzen; Kenntnis von der Blockchain erhalten nur die an der Transaktion Beteiligten.[63] Dies erhöht die Sicherheit, zumal sich die Nutzer bei der Transaktion auf Dritte verlassen. Gleichwohl büßt dies an der Dezentralisierung ein. Private Blockchains eignen sich beispielsweise für den Einsatz zwischen Unternehmen, soweit sie in höherer Frequenz betriebliche Anwendungsfälle und gemeinsame Geschäftsprozesse haben.

34 Ungeachtet der Vorteile bei der Gewährung von Transaktionssicherheit weist eine Blockchain-Architektur auch Nachteile auf. Der Rechenaufwand für das Mining steigt, je größer die auf allen Rechnern des Netzwerks zu speichernde Blockchain wird.[64] Die Energiekosten dürften dann nicht im Verhältnis zu den herkömmlichen Transaktionskosten stehen, deren Umgehung ein wichtiger Gegenstand von Blockchains ist. Mit wachsenden Blockchains verläuft das Mining überdies schleppend und nimmt mehr Zeit in Anspruch.[65] Der vorerwähnten Zuschreibung als „disruptive" Technologie zum Trotz liegt die Vermutung nahe, dass der vorbeschriebene Grundaufbau auf längere Sicht dazu führt, dass Blockchains an Kapazitätsgrenzen geraten und wirtschaftlich unattraktiv werden.

---

59 Vgl. *Schlund/Pongratz*, DStR 2018, 598, 600; *Willems*, CB 2016, 325, 326.

60 Vgl. *Erbguth/Fasching*, ZD 2017, 560.

61 Vgl. *Sharma*, Public vs. Private Blockchain: A Comprehensive Comparison, https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/ (zuletzt abgerufen am 29.9.2020).

62 Vgl. *Sharma*, Public vs. Private Blockchain: A Comprehensive Comparison, https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/ (zuletzt abgerufen am 29.9.2020).

63 Vgl. *Sharma*, Public vs. Private Blockchain: A Comprehensive Comparison, https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/ (zuletzt abgerufen am 29.9.2020).

64 Vgl. *Schrey/Thalhofer*, NJW 2017, 1431, 1432.

65 Vgl. *Welzel/Kirstein/Jammeit*, Mythos Blockchain: Herausforderungen für den öffentlichen Sektor, S. 31.

IV. Token und ihr Vergleich zu bestehenden Konstrukten

1. Versuch einer Definition

Der Begriff „Token" ist weder Gegenstand einer gesetzlichen Definition noch kommt ihm eine einheitliche Terminierung in der Literatur zugute. Die BaFin erweist sich im Rahmen ihrer administrativen Praxis als richtungsweisend. Ihr zufolge stellen Token eine digitalisierte Form von Vermögenswerten dar, denen „eine bestimmte Funktion oder ein bestimmter Wert zugesprochen"[66] wird. In anderen Worten: Konzeptionell handelt es sich um einen digitalisierten Schuldschein für ein zugrunde liegendes Recht, der als individualisierter Eintrag in einer Datenbank existiert. Der Vertragsschluss zwischen Emittent und Erwerber erfolgt bei der „Übertragung" des Tokens, namentlich bei der Änderung der Berechtigung über den Datenbankeintrag.[67] Jener Vertrag gibt letztlich den Inhalt des entstehenden Rechts vor, das durch den Token repräsentiert wird. Aus dem Blickwinkel der finanzwirtschaftlichen Theorie handelt sich bei den Token um einen Finanzkontrakt, bei dem der Kapitalgeber im Gegenzug ein Versprechen auf zukünftige Leistungen, Zahlungen und/oder Mitsprache erhält. **35**

2. Ausgangssituation

Das Emittieren von ICOs stellt ein relativ junges Phänomen dar, das sich im Bereich der Blockchain-Technologie als eine Möglichkeit zur Kapitalaufnahme etabliert hat.[68] Die eingangs erläuterte Blockchain-Funktionalität erlaubt auch hier einen autonomen Vollzug sowie eine weitgehende Transaktionssicherheit, was einen entscheidenden Faktor bei der Entscheidung für dieses Finanzierungsmittel darstellen dürfte. Die Beschaffung des notwendigen Kapitals vollzieht sich dergestalt, dass ein Investor Kapital bereitstellt und hierfür ein virtuelles Äquivalent, namentlich den Token, erhält. **36**

Token als digitale Abbildung eines Werts oder einer Rechtsvermittlung sind im Rahmen eines ICO in der entsprechenden Blockchain abgelegt, wobei sie per öffentlichem Bieterverfahren veräußert werden.[69] Die Bezahlung erfolgt in Krypto- oder gesetzlicher Währung; der Preis bildet sich zunächst auf Vorgabe des Initiators nach einem „Take it or leave it"-Verfahren, im Anschluss daran durch **37**

66 Vgl. BaFin, Merkblatt Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token, WA 51-Wp 7100-2019/0011 und IF 1-AZB 1505-2019/0003, S. 1.

67 Vgl. *Kaulartz/Matzke*, NJW 2018, 3278.

68 Vgl. *Varmaz/Varmaz*, DIW 03.2018, S. 130; *Weitnauer*, BKR 2018, 231.

69 Vgl. *Klöhn/Parhofer/Resas*, ZBB 2018, 89, 93; *Hoche/Lerp*, in: Kunschke/Schaffelhuber, FinTech, Teil VI, Rn. 1.

Angebot und Nachfrage.[70] Das zugrunde liegende sog. White Paper dient der Darstellung des zu finanzierenden Projekts in seinen einzelnen Facetten, namentlich der Ziele des Projekts und des entsprechenden Fahrplans, der benötigten Technik und Ressourcen, der Teilnehmer, etwaiger Investoren sowie insbesondere des Finanzierungsmodells.[71] Im Unterschied zu einem IPO existieren keine gesetzlichen Vorgaben über Umfang oder Struktur des White Papers. Die autonome Ausführung erfolgt über sog. Smart Contracts. Bei Smart Contracts handelt es sich um in Blockchains implementierte Software, die zur Koordination der Vertragsabschlüsse zwischen den Parteien sowie zur Hinwirkung auf die Einhaltung der vereinbarten Pflichten eingesetzt werden.[72] Anhand einer „Wenn-Dann"-Logik, die sich beliebig vorab gestalten lässt, erfolgt eine Aktion, etwa das Emittieren von Token, erst nach Erfüllung vorbestimmter Bedingungen.

38 Vorteilhaft an dieser Vorgehensweise ist die nahezu unbegrenzte Erreichbarkeit potenzieller Förderer über das Internet. Gleichwohl birgt gerade dies auch hohe Risiken: Das Anlocken unerfahrener – und ggf. dem Informationsgefälle unterliegender – Investoren sowie die hohe Volatilität können hohe Verluste zum Ergebnis haben, zumal die begünstigte Anonymität häufig den Ruf der Umgehung geldwäscherechtlicher Vorgaben mit sich trägt. So sind ICOs in der Volksrepublik China vollständig verboten worden.[73] Die SEC lässt in den Vereinigten Staaten ebenfalls Skepsis durchblicken und stellt daher auf eine Einzelfallüberprüfung ab.[74] Auch die BaFin sah sich in ihren Verbraucherwarnungen veranlasst, die Bedeutung von Einzelfallüberprüfungen hervorzuheben.[75]

---

70 Vgl. *Klöhn/Parhofer/Resas*, ZBB 2018, 89, 95.

71 Vgl. *Varmaz/Varmaz*, DIW 03.2018, S. 132.

72 Vgl. *Glatz*, in: Breidenbach/Glatz, Rechtshandbuch Legal Tech, Teil IV, Rn. 46.

73 *Holtermann/Scheuer*, Handelsblatt v. 4.9.2017, https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/nein-zu-icos-chinesische-zentralbank-verbietet-krypto-boersengaenge/20279068.html?ticket=ST-2767702-D9plJIyRwo4ZadH0Jvrh-ap2 (zuletzt abgerufen am 29.9.2020).

74 Vgl. *Clayton*, Statement on Cryptocurrencies and Initial Coin Offerings, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 (zuletzt abgerufen am 29.9.2020). Erwähnenswert ist in diesem Zusammenhang auch der sog. Howey-Test, der in den Vereinigten Staaten bei der kapitalmarktrechtlichen Einordnung von Token herangezogen wird. Basierend auf einer Entscheidung des US Supreme Court aus dem Jahre 1946 (vgl. SEC v. W.J. Howey Co., 328 U.S. 293 (1946)) ermittelt dieser Test das Bestehen eines Kapitalanlagevertrages nach dem US Securities Act 1933 oder US Securities Exchange Act 1934. Der Howey-Test ist über viele Jahrzehnte eine Determinante der regulatorischen Aufsicht geblieben. Im Kern besagt der Test, dass ein Vertrag, eine Transaktion oder ein Schema, bei dem eine Person ihr Geld in ein gemeinsames Unternehmen investiert und dazu veranlasst wird, Gewinne ausschließlich aus den Bemühungen des Projektträgers oder einer dritten Partei zu erwarten, einen Kapitalanlagevertrag im Sinne des Securities Act 1933 darstellt.

75 BaFin, Verbraucherwarnung vom 9.11.2017.

3. Kategorien von Token

In der Literatur wird die Einordnung von Token breit diskutiert; ein klar definierter Rechtsrahmen scheint sich nur zögerlich zu etablieren. Zumindest lässt sich jedoch die nachfolgende Kategorisierung abzeichnen: Security Token, Utility Token, Currency Token und Hybride Token.[76] **39**

Security Token[77] weisen Merkmale auf, die mit denen einer Aktie oder einer anderweitigen Unternehmensbeteiligung vergleichbar sind. Es handelt sich um eine Investition, für die der jeweilige Investor im Gegenzug eine Gewinnbeteiligung oder mitgliedschaftliche Rechte erhält.[78] Dem Investor wird eine zukünftige Kapitalvermehrung versprochen, sei es in Form von Zinsen oder Dividenden.[79] Security Token spielen bei der Finanzierung insbesondere von Start-ups eine bedeutende Rolle, verkörpern sie doch einen künftigen Zahlungsanspruch in Abhängigkeit von der Geschäftsentwicklung des Anbieters. Ein Investor erwirbt Miteigentum an der Blockchain des Herausgebers und wird damit an ihrem Wachstum und dem ihres Netzwerks beteiligt.[80] **40**

Utility Token kennzeichnen sich dadurch, dass sie einen bestimmten Nutzwert für den Investor verkörpern. Sie ermöglichen den Zugang zu einem bestimmten Netzwerk, meist zu Produkten oder Dienstleistungen.[81] Die Kaufentscheidung des Investors wird begünstigt, da sich der Nutzen konkret darstellen lässt.[82] Bei der Erörterung von Utility Token wird häufig der Vergleich zu Gutscheinen oder Lizenzen gezogen.[83] **41**

Currency Token stellen ein digitales Wertaufbewahrungsmittel dar.[84] Ihrem Sinn und Zweck nach verkörpern sie Zahlungsmittel, mithin virtuelle Währungen. Sie repräsentieren den Betrag einer digitalen Währung, regelmäßig im Rahmen **42**

---

76 Vgl. etwa Blockchain Bundesverband, Regulierung von Token, 6.4.2018, S. 10 f.; *Fromberger/Haffke/Zimmermann*, BKR 2019, 377; *Zickgraf*, AG 2018, 293, 295; *Veil*, ZHR 2019, 346, 348.

77 Im Folgenden als Sammelbegriff für Security, Asset und Equity Token verwendet.

78 Vgl. *Hahn/Wons*, Initial Coin Offerings (ICO), S. 10.

79 Vgl. *Hoche/Lerp*, in: Kunschke/Schaffelhuber, FinTech, Teil VI, Rn. 11.

80 Vgl. *Hoche/Lerp*, in: Kunschke/Schaffelhuber, FinTech, Teil VI, Rn. 11.

81 Vgl. BaFin, Merkblatt Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token, WA 51-Wp 7100-2019/0011 und IF 1-AZB 1505-2019/0003, S. 5; *Hahn/Wons*, Initial Coin Offerings (ICO), S. 10. Abweichend KG Berlin, Urt. v. 25.9.2018, (4) 161 Ss 28/18 (35/18).

82 Vgl. *Hahn/Wons*, Initial Coin Offerings (ICO), S. 10.

83 Vgl. etwa *Weitnauer*, BKR 2018, 231, 232.

84 Vgl. BaFin, Merkblatt Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token, WA 51-Wp 7100-2019/0011 und IF 1-AZB 1505-2019/0003, S. 6.; *Hahn/Wons*, Initial Coin Offerings (ICO), S. 10.

einer Blockchain. Unter Currency Token fallen sämtliche Kryptowährungen, die die Nutzung als Zahlungsmittel oder Geldersatz bezwecken.[85]

43 Gelegentlich existieren Mischformen der vorbezeichneten Token-Arten, sog. Hybride. Token dieser Art weisen unterschiedliche Eigenschaften auf. Beispielsweise kann der Anbieter eines Utility Tokens den Gebrauch des Tokens auch als Zahlungsmittel zulassen.[86]

44 Sodann kann ein Token auch ein Investmentvermögen nach § 1 Abs. 1 KAGB darstellen. Vermittelt ein Token das Recht an einem Organismus, der auf der Grundlage einer vordefinierten Anlagestrategie Kapital einsammelt und sodann investiert und selbst kein operatives Unternehmen darstellt (beispielsweise Ertrag von Immobilien), finden die Vorschriften des KAGB Anwendung. Am bedeutendsten sind hierbei die Anlagebeschränkungen der §§ 192 ff., 219 KAGB, denen zufolge nur die abschließend genannten Wertpapierarten als Investitionsmöglichkeit dienen. Des Weiteren lässt sich ein Token subsidiär als Unternehmensbeteiligung nach § 1 Abs. 2 Nr. 1 VermAnlG, partiarisches Darlehen oder Nachrangdarlehen, § 1 Abs. 2 Nr. 3, 4 VermAnlG, Genussrecht, § 1 Abs. 2 Nr. 5 VermAnlG, oder sonstige Anlage, § 1 Abs. 2 Nr. 7 VermAnlG einordnen.

4. Rechtliche Einordnung

45 Unbeschadet der aktuellen Schwierigkeiten bei der rechtlichen Einordnung von Token in die Regelungsgefüge ist gleichwohl nicht zu schlussfolgern, dass ebendiese befreit von der Anwendbarkeit bestehender Gesetze wären. Eine abstrakte oder pauschalisierte Einordnung mag nicht durchführbar sein, aber die konkrete Ausgestaltung von Token lässt sich im Rahmen von Einzelfallüberprüfungen nach den nachfolgenden Maßstäben bewerten.

46 Die Einräumung von Gewinnbeteiligungen oder mitgliedschaftlichen Rechten drängt den Vergleich zu Wertpapieren auf. Nach § 2 Abs. 1 WpHG und § 2 Nr. 1 WpPG, geprägt durch Art. 4 Abs. 1 Nr. 44 MiFID II, ist ein Wertpapier dann zu bejahen, wenn die Merkmale Standardisierung, Handelbarkeit am Finanzmarkt sowie Übertragbarkeit vorhanden sind:

– Standardisiert ist ein Token dann, wenn mehrere Token dieselben Merkmale aufweisen und insoweit eine Austauschbarkeit eintritt. Die Austauschbarkeit lässt sich herstellen, indem eine Mehrzahl der Token in der Ausweisung des

85 Vgl. *Zickgraf*, AG 2018, 293, 296.

86 Vgl. BaFin, Merkblatt Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token, WA 51-Wp 7100-2019/0011 und IF 1-AZB 1505-2019/0003, S. 6.

Verpflichteten, der Laufzeit, der Art und des Umfangs der enthaltenen Rechte identisch ist.[87]
- Am Finanzmarkt handelbar ist ein Instrument dann, wenn es am organisierten Markt nach § 2 Abs. 11 WpHG teilnimmt oder über multilaterale Handelssysteme nach § 2 Abs. 21 WpHG gehandelt wird.
- Der Begriff der Übertragbarkeit knüpft an die technische Möglichkeit an, das Instrument von einem Nutzer auf den anderen zu übertragen, ohne dass die Übertragung Änderungen am rechtlichen oder technischen Gehalt bewirkt.

47 Ob Security Token als Wertpapiere zu qualifizieren sind, ist in der Literatur streitig. Eine Ansicht vertritt eine ablehnende Auffassung, weithin mit der Begründung, die mangelnde Möglichkeit eines gutgläubigen Erwerbs nach §§ 932 ff. BGB schließe eine Handelbarkeit am Finanzmarkt aus.[88] Der Imperativ für die kapitalmarktmäßige Handelbarkeit sei gerade der gutgläubige Erwerb.[89] Die Gutglaubensvorschriften setzten das Bestehen einer Sache nach § 90 BGB voraus, was mangels körperlicher Vergegenständlichung bei Token nicht zu erkennen sei.[90]

48 Dem gegenüber steht die vielfach vertretene Ansicht, der zufolge Security Token als Wertpapiere nach § 2 Abs. 1 WpHG einzuordnen seien, da eine Vergleichbarkeit mit gesetzlich vorgegebenen Wertpapieren bestehe.[91]

49 Letzterer Auffassung ist zu folgen. So hat auch die BaFin zu erkennen gegeben, dass sogar ein wie eine Vermögensanlage nach § 1 Abs. 2 VermAnlG konzipiertes Security Token als ein Wertpapier sui generis zu betrachten sei, soweit es in Form eines frei übertragbaren und am Finanzmarkt handelbaren Token digital verkörpert ist.[92] Gegen die ablehnende Auffassung spricht, dass die Transaktionssicherheit in der Blockchain eine ausreichende Sicherheit für den Handel auf dem Kapitalmarkt bietet. Die Eigentümerkette lässt sich nämlich durch die kryptografische Wiedergabe derart transparent abbilden, dass die Inhaberschaft mit Blick auf die einzelnen Token nachvollziehbar bleibt.[93] Darüber hinaus

87 Vgl. BaFin, Hinweise zu Finanzinstrumenten nach § 1 Abs. 11 Sätze 1 bis 5 KWG (Aktien, Vermögensanlagen, Schuldtitel, sonstige Rechte, Anteile an Investmentvermögen, Geldmarktinstrumente, Devisen, Rechnungseinheiten, Emissionszertifikate und Kryptowerte), geändert am 26.2.2020.

88 Vgl. etwa *Bialluch-von Allwörden/von Allwörden*, WM 2018, 2118.

89 Vgl. *von Ammon*, in: Siering/Izzo-Wagner, VermAnlG, § 1 Rn. 32.

90 Vgl. LG Konstanz, Urt. v. 10.5.1996, 1 S 292/95; *Wagner*, in: MüKo-BGB, § 823 Rn. 294; *Fritzsche*, in: BeckOK-BGB, § 903 Rn. 10.

91 Vgl. *Hahn/Wilkens*, ZBB 2019, 10; *Spindler*, WM 2018, 2109.

92 Vgl. BaFin, Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token, WA 51-Wp 7100-2019/0011 und IF 1-AZB 1505-2019/0003, S. 7.

93 Vgl. *Zickgraf*, AG 2018, 293, 298.

spricht für die Anwendung der aufsichtsrechtlichen Vorschriften, etwaige Anleger vor Informationssymmetrien bei der Ertrags- und Risikobewertung zu schützen.

50 Eine Standardisierung ist jedenfalls an einem Security Token daran zu erkennen, dass der jeweilige Transaktionsbericht auf der Blockchain einen sicheren Rückschluss auf eine bestimmte Adresse zulässt (Ausweisung des Verpflichteten) und insoweit den Nutzern erlaubt, die im Token verbrieften Rechte nachzuvollziehen (Zurkenntnisnahme der Laufzeit, der Art, des Umfangs). Überdies werden Security Token an sog. Kryptobörsen gehandelt, die organisierte Märkte darstellen dürften (Handelbarkeit am Finanzmarkt). Die Übertragbarkeit ist bei Bejahung der Handelbarkeit an einem Finanzmarkt grundsätzlich zu bejahen, Art. 2 Abs. 1 lit. c RL 2007/16/EG. Im Ergebnis lassen sich Security Token durchaus als Wertpapiere einstufen, soweit sie die vorgenannten Voraussetzungen erfüllen und ein Gewinnbeteiligungsrecht oder vergleichbare finanzielle Ansprüche vermitteln.

51 Erwähnenswert ist, dass – sofern man die Wertpapiereigenschaft im Einzelfall bejaht – auch eine Qualifizierung als Finanzinstrument nach § 1 Abs. 11 KWG gegeben ist.[94] Im Unterschied zu den Security Token dürften Utility Token nach wohl überwiegender Auffassung keine Wertpapiere darstellen. Vielmehr verkörpern sie bloß schuldrechtliche Ansprüche.[95]

52 Für die rechtliche Einordnung von Currency Token besteht mittlerweile ein langjähriger Katalog an Mitteilungen und Hinweisen durch die BaFin.[96] Currency Token erfüllen nicht die Merkmale eines Wertpapiers nach § 2 Abs. 1 WpHG, dürften aber regelmäßig Rechnungseinheiten nach § 1 Abs. 11 Satz 1 Nr. 7 KWG und damit Finanzinstrumente darstellen.[97] Daraus ergibt sich zwar keine Regulierung für die Ausgabe von Currency Token. Allerdings wird der Emittent – je nach Einzelfallprüfung – bei der Ausgabe und bei der Bewerbung entsprechende Erlaubnispflichten zu erfüllen haben. Soweit ein Markt gebildet wird, auf dem Currency Token gehandelt werden können, kann eine Erlaubnis der BaFin erforderlich sein. Der gewerbsmäßige Rücktausch von Currency Token in Euro steht namentlich grundsätzlich unter Erlaubnisvorbehalt nach § 32 Abs. 1 KWG.

---

94 Das KWG erhält im Übrigen durch die Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie eine Legaldefinition des Begriffs „Krypto Token“ in § 1 Abs. 1a Satz 3 ff. KWG n. F.

95 Vgl. *Spindler*, WM 2018, 2109.

96 Vgl. etwa BaFin, Viertuelle Währungen/Virtual Currency (VC), geändert am 28.4.2016; BaFin, Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, vom 19.12.2013.

97 Vgl. BaFin, Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token, WA 51-Wp 7100-2019/0011 und IF 1-AZB 1505-2019/0003, S. 6.

Die Gemeinsamkeit mit herkömmlichen Zahlungsmitteln besteht darin, dass auch Currency Token ihren Wert durch Angebot und Nachfrage erhalten. Unterscheidungsmerkmal ist jedoch, dass die digitale Währung einen Wert abbildet, der nicht von einer Zentralbank oder einer Behörde geschaffen wird.[98] Ihre Entstehung und ihr Ausbau wird demnach nicht von den Erwägungen einer Zentralbank gesteuert, sondern vorab von den Kenngrößen im digitalen Programmcode. Auch haben Currency Token keinen immanenten Wert; die Wertgewinnung wird allein durch das Vertrauen der Nutzer erreicht. Neben den geringen regulatorischen Kriterien spricht auch die Umsatzsteuerfreiheit für den Schritt zu Currency Token.[99] Für Investoren hingegen dürften Asset und Utility Token mehr Attraktivität aufweisen, da Currency Token lediglich als Zahlungsmittel dienen und daneben keinen zusätzlichen Zweck aufweisen. **53**

Eine pauschale Einordnung ist bei Hybriden nicht möglich. Wie auch bei Mischverträgen kommt es maßgeblich darauf an, worin im Einzelfall der Schwerpunkt der Leistung liegt. Für die jeweiligen Bestandteile können folglich unterschiedliche Vorschriften anwendbar sein. Soweit hybride Token entsprechende Merkmale aufweisen, können die Anforderungen des Wertpapierbegriffs erfüllt sein. **54**

5. Rechtsfolgen

Eine Rechtsfolge der Einstufung eines Tokens als Wertpapier ist die Prospektpflicht nach der Prospekt-VO. Namentlich hat der Initiator nach Art. 3 Prospekt-VO einen Prospekt für das öffentliche Angebot im Inland zu veröffentlichen. Formell und materiell hat der Prospekt den Anforderungen des Art. 6 Prospekt-VO Genüge zu leisten. Überdies ist eine vorherige Billigung durch die BaFin zwingend notwendig, Art. 20 Abs. 2 Prospekt-VO. Soweit eine Veröffentlichung im Internet stattfindet, ist eine grenzüberschreitende Veröffentlichung anwendbar, womit die weiteren Voraussetzungen des Art. 24 Abs. 1 Prospekt-VO gelten (Genehmigung durch die zuständige Behörde eines jeden Aufnahmestaats). Nicht zu unterschätzen ist das Risiko einer gesetzlichen Prospekthaftung nach § 22 WpPG bei fehlerhaften Prospekten oder das Risiko der Rückabwicklung nach § 24 WpPG bei einem Nichtnachkommen der vorbezeichneten Prospektpflichten. Ein Verstoß kann zuletzt auch eine Ordnungswidrigkeit darstellen, § 35 WpPG. **55**

Die Qualifizierung als Wertpapier hat des Weiteren zur Folge, dass aufgrund der Eigenschaft als Finanzinstrument nach § 1 Abs. 11 Nr. 1 bis 4 KWG auch das **56**

98 Vgl. BaFin, Virtuelle Währungen, https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html (zuletzt abgerufen am 29.9.2020).

99 Vgl. EuGH, Urt. v. 22.10.2015, C-264/14 – Hedqvist.

KWG Anwendung findet. Dies kann die Pflicht zur Einholung einer Erlaubnis durch die BaFin nach § 32 Abs. 1 KWG auslösen, etwa wenn die Ausgestaltung eines Tokens als Anlageberatung einzuordnen ist, §§ 1 Abs. 1a Satz 2 Nr. 1, 1a KWG.

57 Ebenfalls erlaubnispflichtig ist das Betreiben eines multilateralen Handelssystems. Namentlich ist für das Zusammenbringen von Interessen einer Vielzahl von Personen am Kauf und Verkauf von Finanzinstrumenten innerhalb eines Systems und nach festgelegten Bestimmungen dergestalt, dass Verträge über den Kauf der Finanzinstrumente die Folge sind, eine Voraberlaubnis der BaFin einzuholen, § 1 Abs. 1a Nr. 1b KWG. Betreiber von Kryptobörsen dürften als Adressaten dieser Vorschrift gelten, soweit sie Security Token oder Currency Token handeln.

58 Schließlich sind die strafrechtlichen Sanktionen aus §§ 54 ff. KWG in Betracht zu ziehen, wovon insbesondere § 54 Abs. 1 KWG den häufigsten Anwendungsfall darstellen dürfte. Demnach erhält Freiheitsstrafe von bis zu fünf Jahren oder Geldstrafe derjenige, der der Erlaubnispflicht nach § 32 Abs. 1 Satz 1 KWG nicht nachkommt.

59 Der Vollständigkeit halber seien regulatorische Vorgaben wie Informationspflichten nach der E-Commerce-Richtlinie, geldwäscherechtliche Identifizierungspflichten aus dem GwG sowie bilanzielle und steuerliche Pflichten beim Emittieren von Token erwähnt. Auch hier bedarf es der entsprechenden Einzelfallüberprüfung.

6. Zivilrecht

60 Aus zivilrechtlicher Sicht stellen Token weder Sachen noch Rechte dar. Die Verbriefung der Rechte stellt zwar eine Nähe zu Urkunden dar, allerdings mangelt es einem Token an einer Urkundeneigenschaft.[100] Das Term Sheet dürfte AGB darstellen, womit ein Emittent die Voraussetzungen der §§ 305 ff. BGB zu erfüllen hat. Sachenrechtliche Vorschriften finden dementsprechend auch keine Anwendung, womit auch ein gutgläubiger Erwerb nach §§ 932 ff. BGB nicht möglich ist. Auch kommt eine analoge Anwendung nicht in Betracht, da die absolute Geltungswirkung der Gutglaubensvorschriften ein essenzielles Prinzip des deutschen Zivilrechts darstellt.[101] In Fällen unberechtigten Erwerbs ist auf eine kondiktionsrechtliche Rückabwicklung nach §§ 812 ff. BGB zurückzugreifen.

61 Eine den (Form-)Anforderungen des deutschen Gesellschaftsrechts genügende Verbriefung von Gesellschafterrechten dürfte nur selten vorkommen. Gerade die

100 Vgl. *Kaulartz/Matzke*, NJW 2018, 3278.
101 Vgl. *Peters/Jacoby*, in: Staudinger, BGB, § 194 Rn. 19.

Formerfordernisse wie etwa die notarielle Form aus § 2 Abs. 1 GmbHG laufen dem entgegen. Im Ergebnis werden nur Personengesellschaften für diese Praxis in Frage kommen.

Das Konstituieren einer Schuldverschreibung geht ebenfalls fehl. Schuldverschreibungen ermöglichen die Wirksamkeit einer Forderung sogar bei der Unwirksamkeit des Begebungsvertrags, namentlich über den gutgläubigen Erwerb der Urkunde.[102] Der wesentliche Unterschied zu Token ist, dass Urkunden eine gesetzlich ausgeprägte Stellung als Rechtsscheinträger haben. Ein Token kann hingegen bei einem unwirksamen Begebungsvertrag keine Ansprüche an einen vermeintlich Berechtigten vermitteln, da sich regelmäßig mangels Hinterlegung jenes Vertrags in der Blockchain aus dem einzelnen Token selbst nicht unmittelbar ergibt, welche Rechte ihm innewohnen. Überdies mangelt es an dem Unterzeichnungserfordernis aus § 793 Abs. 2 BGB. **62**

7. Zwischenergebnis

Die bisherige Analyse zeigt auf, dass die unterschiedlichen Token-Arten unterschiedliche rechtliche Behandlungen mit sich ziehen. Eine Einzelfallprüfung lässt sich nicht umgehen. Auch dürfte feststehen, dass ein Großteil der rechtlichen Einordnung derzeit von etwaigen Einlassungen der BaFin abhängt. Obgleich ihre Auskünfte oder Hinweisschreiben hilfreiche Indikatoren liefern, bedarf es zur Herstellung von Rechtssicherheit der Initiative des Gesetzgebers, um Regelungsziele – sowohl auf (rechts-)politischer als auch auf legislativer Ebene – festzusetzen. **63**

V. Der aktuelle Kryptomarkt

1. Prozess der Notierung an einer Handelsplattform

Der Kryptowährungsmarkt ist ein relativ junger Markt, der nach dem White Paper von *Nakamoto* im Jahr 2008 entstand. Seit dem Jahr 2013 begann eine dynamische Entwicklung. Im Juni 2020 gab es rund 5600 verschiedene Kryptowährungen,[103] wobei die Anzahl je nach der Quelle variiert. Während manche Handelsplattformen ex post ihre Datenbank bereinigen, sobald eine Kryptowährung plattform-spezifische Kriterien nicht erfüllt, verbleiben dieselben Kryptowährung an anderen Handelsplattformen trotz eines minimalen Handelsvolumens. Die Gesamtmarktkapitalisierung aller Kryptowährungen beträgt aktuell 257 **64**

102 Vgl. *Habersack*, in: MüKo-BGB, § 793 Rn. 27 f.
103 Vgl. www.coinmarketcap.com (zuletzt abgerufen am 28.6.2020).

Mrd. US-Dollar.[104] Im Vergleich zu anderen Anlageformen ist der Betrag als gering einzustufen. SAP SE, als größter Vertreter im Deutschen Aktienmarktindex DAX, hat eine Marktkapitalisierung von 150 Mrd. US-Dollar.[105] Die mit Abstand bedeutendste Kryptowährung ist Bitcoin mit einem wertmäßigen Anteil von rund 65 % am Kryptowährungsmarkt, gefolgt von Ethereum mit 9,0 %, Tether mit 3,5 %, Ripple mit 3,1 % und Bitcoin Cash mit 1,5 %.[106]

65 Digitales Geld stellt kein neues Phänomen dar. Erste wissenschaftliche Abhandlungen gehen in die 1980er Jahre[107] zurück und bereits seit Anfang des Jahrtausends existiert das sog. E-Geld, das monetäre Werte in Form von Forderungen gegenüber dem Emittenten digital speichert.[108] Die eigentliche Neuheit an den Kryptowährungen und Token ist die Validierung und Dokumentation der Geschäftsvorfälle durch ein Open-Source-Konzept ohne zentrale Autorität.[109] Für die nachfolgende Analysen ist zu beachten, dass, wie bereits in Abschnitt IV (Rn. 39 ff.) herausgearbeitet, Kryptowährungen zwar den Namen tragen, aber zum überwiegenden Teil keine Pendants zu klassischen Zentralbankwährungen sind. Vielmehr stellt die Mehrheit der Kryptowährungen Utility Token dar, die dem Inhaber lediglich Anspruchs- oder Zugriffsrechte auf Dienstleistungen oder Netzwerke geben. Folglich gibt in der finanzwirtschaftlichen Forschung Einordnungsschwierigkeiten dieser neuartigen Produkte. Allmählich setzt es sich durch, Kryptowährungen als alleinstehende, neue Anlageklasse (auch: Assetklasse) anzusehen. Eine eigenständige Anlageklasse wird allgemein als eine Produktgruppe definiert, die

- keine Überschneidung mit anderen Anlageklassen bietet,
- genügend Variation innerhalb der Gruppe aufweist und
- eine geringe Korrelation zu anderen Assetklassen (bzw. deren Renditen) aufweist.[110]

66 Die Entwicklung des Kryptowährungsmarktes in US-Dollar ist in Abbildung 2 dargestellt. Insbesondere im Jahr 2017 erfuhr dieser einen starken, fast exponenziellen Anstieg der globalen Marktkapitalisierung. Der ungewöhnlich hohe Preisanstieg ging mit einer extensiven Berichterstattung einher, durch die viele Anleger auf die neue Anlageform aufmerksam wurden. Nach dem starken Preis-

104 Vgl. www.coinmarketcap.com (zuletzt abgerufen am 28.6.2020).
105 Vgl. https://www.finanzen.net/index/dax/marktkapitalisierung (zuletzt abgerufen am: 28.6.2020).
106 Vgl. www.coinmarketcap.com (zuletzt abgerufen am 28.6.2020).
107 Vgl. *Chaum*, in: Chaum/Rivest/Sherman, Advances in Cryptology, S. 199 f.
108 Vgl. www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/ueberwachung/e-geld-603588 (zuletzt abgerufen am 16.9.2020).
109 Vgl. *Härdle/Harvey/Reule*, Journal of Financial Econometrics, 2020, 182.
110 Nach *Sharpe*, Journal of Portfolio Management, 1992.

anstieg folgte ein starker Rückgang zu Beginn des Jahres 2018. Die hohe Nachfrage wurde häufig durch exorbitante Gewinnversprechen generiert, wobei viele Investoren das eingegangene Risiko vernachlässigten. Gerade bei Privatanlegern herrschte eine gewisse Unkenntnis der Funktionsweise dieses neu etablierten Marktes, der keiner Regulierung unterworfen war und auf dem zum Teil mit falschen Angaben in den White Papers der Verkauf von Token beworben wurde. Dies begünstigte Betrugsfälle, die dem Kryptowährungsmarkt geschadet und bis heute negativ belastet haben.

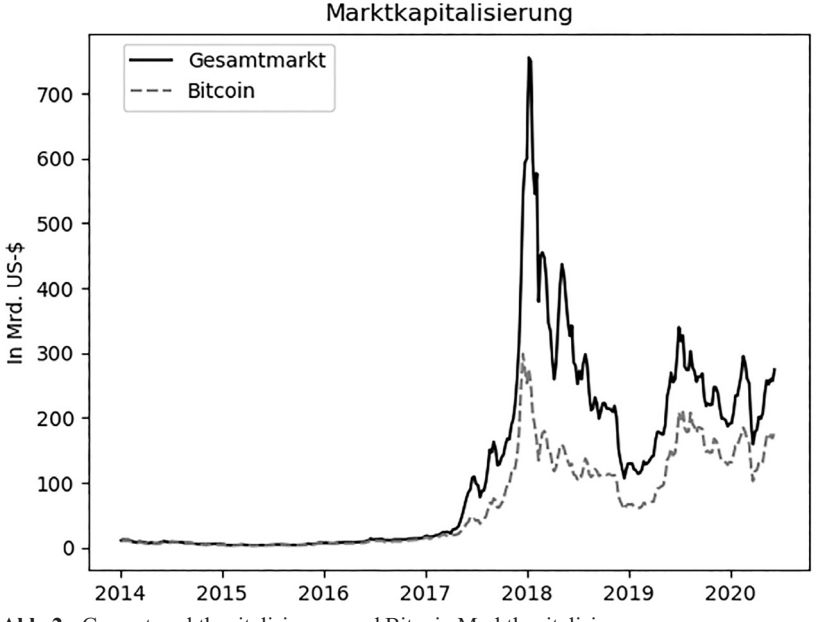

Abb. 2: Gesamtmarktkapitalisierung und Bitcoin Marktkapitalisierung (Daten: www.coingecko.com).

Die Mehrzahl neuer Kryptowährungen vor dem Jahr 2019 entstanden durch Initial Coin Offerings (ICOs). Dabei handelt es sich um eine projektbezogene Kapitalbeschaffung durch Ausgabe von Token. Basierend auf den Smart Contracts werden Token an Investoren mittels Bieterverfahren verkauft. Smart Contracts sind dabei Computerprotokolle, die Transaktionen zwischen dem Kryptoprojekt und den Investoren automatisieren.[111] Die Struktur und der Prozess eines ICO **67**

111 Vgl. auch die Darstellungen in Rn. 37.

ähnelt den klassischen Börsengängen auf den Aktienmärkten. Es wird allerdings durchgängig auf jeglichen Intermediär verzichtet. Daher sind im Prozess weder Anwälte, Wirtschaftsprüfer noch Banken beteiligt. Der Charme für Start-ups und zugleich die große Gefahr für die Anleger liegt damit in einem unregulierten und unbeaufsichtigten Prozess der Kapitalbeschaffung. Ob die schnelle Verbreitung von ICOs und ihr Erfolg durch die fehlende Regulierung oder durch andere Faktoren determiniert wird, ist Gegenstand der aktuellen Forschung.

68 Aktuell gibt es 5725 ICO-Projekte mit einem erzielten Gesamtfinanzierungsvolumen von 27 Mrd. US-$.[112] Von den angekündigten ICOs waren letztlich lediglich 32,6 % erfolgreich. Die restlichen Projekte, die durch die ICOs finanziert wurden, existieren nicht mehr. Die mittlere (mediane) Kapitalbeschaffung zwischen 2015 und 2018 liegt bei 15,1 (5,8) Mio. US-Dollar, wobei knapp 40 % des Gesamtfinanzierungsvolumens von lediglich 20 ICOs eingenommen wurden. Wurden im November 2018 insgesamt durch ICOs noch rund 400 Mio. US-Dollar an Risikokapital eingesammelt, waren es ein Jahr später lediglich 50 Mio. US-Dollar. Die durchschnittliche (mediane) Zeit vom Projektstart bis zum ICO lag bei 598 (312) Tagen und weiteren 93 (42) Tagen bis zur Notierung auf einer Kryptowährungsbörse.[113] Die Anzahl der ICO-Projekte ist im Zeitablauf gefallen und beläuft sich aktuell monatlich im einstelligen Bereich. Zum Jahresende 2019 gab es insgesamt 5711 angekündigte oder durchgeführte Projekte. Bis zum Juni 2020 kamen lediglich 14 Projekte hinzu. Der überwiegende Anteil der ICOs (87 %) wurde über die Ethereum-Plattform (ERC-20) aufgesetzt.[114] Nach den aktuellen Zahlen spielt die Kapitalbeschaffung mittels ICOs keine bedeutende Rolle mehr.

69 Eine Alternative zu den ICOs stellen sog. Initial Exchange Offerings (IEOs) dar. Hierbei werden ebenfalls meist Utility Token[115] aufgesetzt. Im Prozess von IEOs werden Projekte von einer Handelsplattform begleitet und betreut. Durch die Begleitung erhofft sich die Branche einen Qualitätszuwachs und Rückgewinnung von Vertrauen, das, wie im Abschnitt II (Rn. 16 ff.) erläutert, impliziter Bestandteil von Finanzkontrakten ist. Die Quantität der IEOs ist durch das Verfahren bedingt begrenzt. Aktuell sind rund 300 Projekte angekündigt.[116] Ein grundlegendes Problem ist auch hier die rechtliche Unsicherheit, die auch im Abschnitt IV (Rn. 45 ff.) thematisiert wird. Die amerikanische Finanzaufsichtsbehörde (SEC) veröffentlichte im Januar 2020 ein Schreiben, das vor Investitionen in IEOs

112 Vgl. www.icobench.com (zuletzt aufgerufen am 28.6.2020).
113 Vgl. *Momtaz*, PLOS ONE, 2020.
114 Vgl. https://icobench.com/reports/ICObench_ICO_Market_Analysis_November_2019.pdf (zuletzt abgerufen am 28.6.2020).
115 Zu den Utility Token vgl. Rn. 39 ff.
116 Vgl. https://www.icobench.com (zuletzt aufgerufen am 28.6.2020).

warnt. Speziell geht es um die Frage, ob IEOs unter die Regularien der Finanzaufsichtsbehörde fallen. Sollten IEOs, vereinzelt oder als Ganzes, als Wertpapiere (Security) eingestuft werden, so hätte der IEO von einer registrierten Börse (Security Exchange) stattfinden müssen. Die geforderten regulatorischen Anforderungen erfüllen die Handelsplattformen für Kryptowährungen aktuell nicht.[117] Für den Kryptowährungsmarkt wird es wichtig sein, einen Weg aus der rechtlichen Unsicherheit ohne die Aufgabe eigener Prinzipien der Dezentralität zu finden. Auch kann hier insbesondere auf die in Abschnitt II (Rn. 4 ff.) angesprochenen theoretischen Prinzipien der Finanzierungstheorie verwiesen werden. Eine Qualitätssicherung könnte mit IEOs Einzug erhalten, wenn die beteiligten Institutionen Signalling von Qualität gewähren können. Damit wäre jedoch eine Annäherung an die traditionelle Maklerfunktion von Finanzinstituten mit der Gefahr einer Zentralisierung verbunden.

2. Rentabilität von Investitionen in den Kryptomarkt

70 Im Jahr 2013 begannen die ersten Anbieter von Datenbanken systematisch Marktdaten von Kryptowährungen zu erfassen. Hierzu zählen vor allem der Preis, das Handelsvolumen sowie die Marktkapitalisierung. Viele Datenbankanbieter, ähnlich dem Hedgefonds-Phänomen Mitte der 1990er Jahre, haben die aus dem Markt ausscheidenden Token und Kryptowährungen bei der Berechnung historischer Renditen nicht berücksichtigt.[118] Gerade diese historische Performance wird häufig von Anlegern als Entscheidungsgrundlage für eine Investition zugrunde gelegt, auch wenn sie keine Prognose zukünftiger Entwicklungen erlaubt. Bekannt ist dieses Phänomen als Survivorship Bias, das zu einer optimistischen Einschätzung der Rentabilität führt. Denn bei der Berechnung der historischen Renditen werden nach der Datenbankbereinigung die gescheiterten Projekte nicht mehr berücksichtigt. Die Quantifizierung der Verzerrung ist schwierig, weil Datenbankanbieter unterschiedliche Kriterien für fehlgeschlagene Projekte anwenden. Eine Untersuchung von ICOs aus den Jahren 2015–2018 ergibt, dass 21 % aller Projekte von wenigstens einer der größten 26 Handelsplattformen gestrichen wurden, knapp 13 % sogar von allen.[119]

117 Vgl. https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_initialexchangeofferings (zuletzt abgerufen am 29.6.2020).

118 Beispielsweise durch Liquidationen, Insolvenzen oder Akquisitionen.

119 Vgl. *Momtaz*, PLOS ONE, 2020.

Tab. 1: Panel (a): Kennzahlen für monatliche Renditen für den Zeitraum 1.1.2014 bis 15.6.2020. Ethereum startet am 8.8.2015. Mean (%) bezeichnet die mittlere, Median (%) die mediane monatliche Rendite. Std (%) ist die Standardabweichung der Renditen, Total (%) die akkumulierte Rendite. EW bezeichnet Gleichgewichtet, VW eine Wertgewichtung nach Marktkapitalisierung. YTD steht für Year-to-Date. Panel (b): Renditen im Jahresverlauf der ausgewählten Kryptowährungen und Indizes (Daten: www.coingecko.com).

(a)						
Asset	Mean (%)	Median (%)	Std (%)	Min	Max	Total (%)
BTC	5,99	2,69	24,02	–35,60	72,54	1287,20
ETH	14,46	0,00	49,41	–54,52	218,19	16592,75
LTC	6,42	–2,34	39,54	–45,17	162,46	96,58
XRP	19,84	–6,48	110,85	–50,11	810,39	639,60
$Index_{EW}$	7,08	–0,31	38,25	–52,39	207,30	303,26
$Index_{VW}$	8,12	2,80	30,88	–43,44	141,10	3007,14

(b)						
Jahr	BTC	ETH	LTC	XRP	$Index_{EW}$	$Index_{VW}$
2014	–57,97	0,00	–88,82	–11,30	–83,99	–54,65
2015	51,44	–35,99	31,09	–75,17	75,05	32,70
2016	124,19	755,37	25,50	7,35	131,86	150,03
2017	1381,35	9570,58	5348,01	35047,83	6134,10	4001,50
2018	–74,33	–82,23	–86,82	–84,03	–93,13	–78,32
2019	90,05	–4,48	35,26	–46,97	–14,75	56,94
2020 (YTD)	34,50	85,78	9,95	5,06	70,10	48,00

71 Tabelle 1 fasst die wichtigsten Renditekennzahlen für den Kryptowährungsmarkt zusammen. Es werden die größten Kryptowährungen sowie zwei unterschiedlich gewichtete Indizes als Gesamtmarktrepräsentanten gegenübergestellt. Die Renditen der Indizes sind der einfache Mittelwert (EW: equally-weighted) sowie der nach anteiliger Marktkapitalisierung gewichtete Mittelwert (VW: value-weighted). Während der wertgewichtete Index stark von einzelnen sehr großen Kryptowährungen dominiert ist, sind bei dem gleichgewichteten Pendant kleine und häufig illiquide Kryptowährungen überrepräsentiert. Zur Abschätzung der Rentabilität werden in der Tabelle die gängigen deskriptiven Statistiken ausgegeben. Neben dem Mittelwert der Monatsrenditen wird auch der Median ausgewiesen, der robust gegen Ausreißer ist und eine unverzerrte Perspektive bietet. Die Standardabweichung (Volatilität) ist ein gängiges Risikomaß und gibt die durchschnittliche Abweichung vom Mittelwert an. Zur besseren Interpretation werden die Werte mit dem Aktienmarkt verglichen, der als risikoreich eingestuft werden kann.

An den Ergebnissen sind vor allem die negativen medianen Monatsrenditen in Panel (a) interessant. Lediglich Bitcoin sowie der wertgewichtete Marktindex weisen auch hier positive Werte auf. Daraus lässt sich schließen, dass vor allem Bitcoin der Treiber hinter dem wertgewichteten Marktindex ist, wohingegen Kryptowährungen mit geringer Marktkapitalisierung, wie aus dem gleichgewichteten Index sichtbar ist, sich schlechter entwickeln. Das liegt an der Wertgewichtung der Renditen, da der Marktanteil von Bitcoin ca. 65 % beträgt. Die hohe kumulierte Rendite (Spalte Total (%)) von Ethereum erklärt sich mit dem späten Start des Projektes (Juli 2015), womit die gesamte Kurshistorie in der aktuellen Analyse enthalten ist. Die insgesamt hohen monatlichen mittleren Renditen gehen einher mit einer hohen Standardabweichung (Volatilität). Ein Vergleich mit dem Aktienmarkt[120] verdeutlicht die Unterschiede. Im selbigen Zeitraum erwirtschaftete eine Anlage in einen weltweit gestreuten und börslich gehandelten Aktien-Indexfond (ETF)[121] eine mittlere (mediane) monatliche Rendite von 0,59 % (1,15 %) mit einer Standardabweichung von 2,35 %. Somit erscheinen die Aktienmärkte im Vergleich deutlich weniger riskant. Panel (b) der Tabelle zeichnet den Zeitverlauf der Renditen für ebenjene Kryptowährungen sowie beide Indizes. Im Krisenjahr 2018 verloren die Kryptowährungen und die Indizes einen Großteil ihres Marktwertes. Auch diese Verluste sind um ein Vielfaches höher als historische Verlustrenditen am Aktienmarkt. Hervorzuheben sind die Verzerrungen der Mittelwerte aus Panel (a) durch die extremen Renditen von 2017. Wie im Abschnitt II (Rn. 9) ausgeführt, beinhalten Kryptowährungen ein hohes Ausfall- und Qualitätsrisiko, das durch Informationsasymmetrien und Moral Hazard getrieben wird. Außerdem befinden sich Kryptowährungen auf einem rechtlich sehr unsicheren Terrain. Für die Übernahme dieses Risikos werden Investoren ebenfalls Prämien erwarten, die in Form von Preisnachlässen beim Verkauf von Token realisiert werden. **72**

3. Geografische Verteilung

Der Kryptowährungmarkt ist in verschiedenen Regionen der Welt unterschiedlich stark präsent. Das zeigt sich auch an dem Handelsvolumen der einzelnen Handelsplattformen. Das tägliche globale Handelsvolumen vervielfachte sich die vergangenen Jahre von täglich 0,99 Mrd. US-Dollar auf 7,4 Mrd. US-Dollar. Das ist gemessen an der Gesamtmarktkapitalisierung des Marktes ein hoher Betrag (aktuell: 257 Mrd. US-Dollar). Zur Einordnung: Die Deutsche Börse meldete für den Juni 2020 ein durchschnittliches tägliches Aktienhandelsvolumen an ihren Kassamärkten von knapp 6,7 Mrd. EUR bei einer vielfach höheren Markt- **73**

120 Als stellvertretend für den Aktienmarkt wurde ein weltweiter Aktien-ETF gewählt (MSCI World).

121 MSCI World.

kapitalisierung. Davon fallen zusammen rund 0,83 Mrd. EUR durch ETFs, ETCs und ETNs an. Alle Einzeltitel des deutschen Leitindex DAX kommen im selben Monat und Märkten gemeinsam auf ein durchschnittliches tägliches Handelsvolumen von 3,96 Mrd. EUR. Diese Zahlen unterliegen zwar auch Schwankungen, aber sie sind deutlich geringer im Vergleich zu den Kryptomärkten. Tabelle 2 zeigt den Anteil am durchschnittlichen täglichen Handelsvolumen, aggregiert nach Ländern und sortiert nach den höchsten Volumina des Jahres 2020. Insgesamt befinden sich die größten Plattformen im asiatischen Raum sowie an vereinzelten Offshore-Finanzplätzen. Diese acht Länder kommen für knapp 75 % des globalen medianen täglichen Handelsvolumens auf.

Tab. 2: Relativer Anteil am medianen täglichen Handelsvolumen eines Jahres, aggregiert auf Länderebene. YTD bezeichnet Year-to-Date (Daten: www.coingecko.com).

Jahr	Total (BTC/USD)	Seychellen	Hong-kong	Kaiman-inseln	Brit. Jgf. Inseln
2018	1,61 Mio./0,99 Mrd.	15,21 %	4,84 %	13,37 %	5,55 %
2019	5,22 Mio./4,13 Mrd.	13,39 %	9,60 %	10,98 %	3,23 %
2020 (YTD)	7,89 Mio./7,38 Mrd.	11,51 %	10,66 %	10,64 %	10,47 %

Jahr	China	Estland	Singapur	Belize	Nicht verfügbar
2018	12,57 %	0,81 %	4,86 %	11,56 %	5,23 %
2019	15,97 %	3,58 %	13,99 %	5,31 %	10,62 %
2020 (YTD)	9,35 %	9,01 %	7,80 %	4,65 %	9,64 %

74 Zu beachten ist, dass im Kryptowährungsmarkt verstärkt Wash Trading nachgewiesen wurde. Hierbei werden scheinbare Kauf- und Verkaufsorder platziert, um das Handelsvolumen künstlich zu vergrößern. Der Preisfindungsprozess bleibt davon unberührt, da sich das vermehrte Angebot und die Nachfrage gegenseitig aufheben, allerdings hat das zwei Nebeneffekte. Zum einen steigert es die Popularität einer Plattform und zum anderen könnten durch die anfallenden Transaktionsgebühren verdeckt Gefälligkeiten beglichen werden.[122] Aktuelle Untersuchungen gehen sogar davon aus, dass der überwiegende Teil des gemeldeten Handelsvolumens vieler Plattform auf Wash Trading zurückzuführen ist.[123]

122 Diese Art der Kompensationszahlung wurde u. a. im 2011 publik gewordenen Libor-Skandal angewendet.

123 Bekannt wurde das Phänomen in Kryptowährungen u. a. durch einen Report von Bitwise Asset Management vor der SEC im 19.3.2019, https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf (zuletzt abgerufen am 20.9.2020).

4. Geschäftsfelder

In der Abbildung 3 sind die aktuellen Kryptoprojekte in Kategorien und Geschäftsfeldern gruppiert, wobei die Einordnung vom Kryptoprojekt selbst vorgenommen werden und Mehrfachzuordnung möglich sind. Insgesamt liegen Informationen zu Kategorien und Geschäftsfeldern von 2.680 Kryptowährungen vor. Die am häufigsten selbst gewählte Kategorie ist die klassische Kryptowährung, gefolgt von den Geschäftsfeldern Finance/Banking, Business Platform sowie Business Services. An fünfter Stelle folgt die Kategorie Masternodes. Diese sind essenziell für anonymisierte Transaktionen (sog. Private Send), bei denen die Identität des Senders nicht mehr nachzuvollziehen ist, sowie eine instantane Abwicklung einer Transaktion (Instand Send). Weiterhin werden Smart Contracts häufig als Geschäftsfeld gewählt. Beispiele sind zum Beispiel Ethereum, EOS oder Cardano. Weitere Kategorien umfassen u. a. künstliche Intelligenz, Gesundheitswesen, Internet of Things oder auch Exchange Traded Funds (ETF). Insgesamt zeigt sich ein sehr heterogener Markt des Geschäftsfeldes von Kryptowährungen. **75**

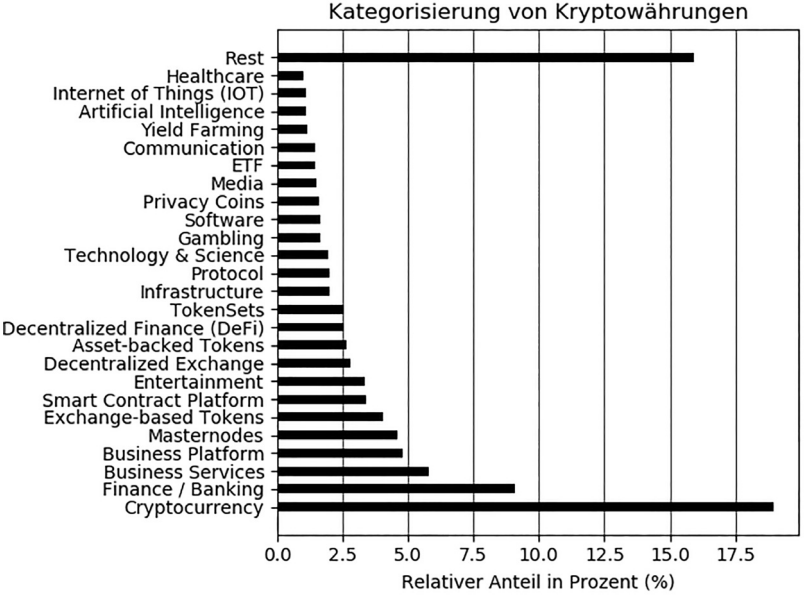

Abb. 3: Kategorisierung von 2.680 Kryptowährungen (Daten: www.coingecko.com).

76 Die Renditen der einzelnen Geschäftsfelder geben einen interessanten Einblick in den Kryptowährungsmarkt.[124] Lediglich acht Kategorien weisen positive durchschnittliche monatliche Renditen auf, die Standardabweichung ist im Vergleich zum Aktienmarkt überwiegend hoch bis sehr hoch. Bemerkenswert sind die überwiegend stark negativen totalen kumulierten Renditen (Spalte Total (%)). Eine totale Rendite von –100 % entspricht dabei einem Totalverlust des eingesetzten Kapitals. Demnach hat ein Großteil der Kryptowährungen in nahezu allen Geschäftsfeldern nahezu einen Totalverlust erlitten, was auf eine Marktbereinigung nach dem extremen Jahr 2017 hindeutet. Am besten schneiden Kryptowährungen in der Kategorie Masternodes mit einer totalen Rendite von 388 % und Smart Contract Platforms mit 137 % ab. Die Kategorie Asset-backed Token erlitt in dem Datensample lediglich ein Verlust von 5 %, was unter Einbezug der Corona-Pandemie und der starken Verwerfung an den Finanzmärkten plausibel ist. Gleichzeitig hat diese Kategorie mit ca. 10 % die geringste Volatilität, die aber deutlich höher als die monatliche Volatilität am Aktienmarkt ist.

Tab. 3: Renditen der einzelnen Kategorien von 2680 Kryptowährungen. Es werden deskriptive Statistiken von diskreten monatliche Rendite berichtet. Die Kategorien ETF und Yield Farming wurden aufgrund von zu wenig Datenpunkten entfernt (Daten: www.coingecko.com).

Kategorie	Mean (%)	Median (%)	Std (%)	Min (%)	Max (%)	Total (%)
Cryptocurrency	0,02	–7,11	32,51	–47,95	133,68	–96,63
Finance/Banking	–8,01	–13,24	25,92	–52,99	83,49	–98,39
Business Services	–5,90	–13,14	37,31	–47,40	160,13	–98,07
Business Platform	–4,02	–11,83	40,05	–50,88	184,97	–96,90
Masternodes	9,68	–5,13	46,10	–56,33	210,65	388,39
Exchange-based Token	0,96	–9,05	42,33	–46,58	195,22	–81,15
Smart Contract Platform	9,32	–6,86	49,63	–49,46	240,90	137,38
Entertainment	–7,61	–14,91	26,21	–45,13	82,72	–96,78
Decentralized Exchange	–5,45	–9,39	27,41	–46,75	94,12	–93,71
Asset-backed Tokens	0,27	-0,14	10,59	–21,66	15,37	–5,18
Decentralized Finance (DeFi)	6,39	–4,13	40,90	–54,65	128,96	–8,19
TokenSets	6,92	5,64	22,49	–24,34	35,67	39,19
Protocol	–5,28	–7,75	27,49	–47,19	98,68	–93,34
Infrastructure	–7,83	–10,64	28,81	–49,77	104,80	–97,75
Technology & Science	–8,06	–9,32	17,45	–45,91	30,55	–90,38

124 Für die nachfolgende empirische Analyse ist zu beachten, dass keine Liquiditätsfilter angewendet wurden. Die Zeitreihen sind durch Winsorizing um extreme Renditen bereinigt.

Kategorie	Mean (%)	Median (%)	Std (%)	Min (%)	Max (%)	Total (%)
Gambling	–11,11	–9,87	14,36	–41,73	11,76	–95,07
Software	–9,21	–11,50	24,43	–46,92	67,14	–98,18
Privacy Coins	9,36	–6,74	60,73	–55,10	319,51	–27,25
Media	–12,72	–11,52	19,31	–49,12	30,80	–98,46
Communication	–8,63	–10,05	21,35	–47,49	36,72	–95,87
Artificial Intelligence	–5,30	–9,42	24,92	–52,29	47,50	–87,22
Internet of Things (IOT)	–6,71	–10,44	23,22	–43,83	52,11	–93,62
Healthcare	–9,44	–13,09	22,03	–51,94	44,56	–95,90

5. Zugang zu den Handelsplattformen

Die Kryptoprojekte entscheiden selbst, an welcher und an wie vielen Handelsplattformen sie ihre Token notieren wollen. Der Zugang zur externen Finanzierung, vor allem wenn Finanzierungen mehrfach notwendig sind, wird erleichtert, wenn die Token an vielen Handelsplattformen in unterschiedlichen geographischen Märkten gehandelt werden können. Damit ist der Zugang von Investoren erleichtert und der Bekanntheitsgrad kann gesteigert werden. Die Verteilung der Notierungen von Kryptowährungen über die einzelnen Handelsplattformen ist dabei sehr heterogen. Für die nachfolgende empirische Analyse werden mehr als 250 Handelsplattformen einbezogen, für die Notierungen verzeichnet werden können. An den Handelsplattformen sind durchschnittlich 77 Einzelwährungen notiert, wobei im Median an jeder 26 Kryptowährungen gehandelt werden können. Abbildung 4 zeigt die Verteilung der Kryptowährungen über die Handelsplattformen, wobei die y-Achse in der logarithmierten Skalierung zur besseren Veranschaulichung ausgegeben wird. Die überwiegende Mehrheit der 4.800 in die Analyse einbezogenen Kryptowährungen kann an weniger als 50 Handelsplätzen gehandelt werden. Nur sehr wenige Kryptowährungen sind auf mehr als 100 Handelsplattformen notiert. Es ist anzunehmen, dass unter den Kryptowährungen mit Listung an wenigen Handelsplattformen viele bereits gescheiterte Projekte sind. Allerdings ist zu beachten, dass viele, gerade kleine Kryptoprojekte die hohen Kosten einer weiteren Listung scheuen dürften. Demgegenüber eröffnen Mehrfachlistungen auch neue Finanzierungsmöglichkeiten, wenn die Projekte eine Anschlussfinanzierung benötigen und Zugang zu einem großen Investorenkreis suchen. Inwieweit ein Zusammenhang zwischen der Anzahl der Notierungen und dem Erfolg des Projektes sowie den Renditen und dem Risiko einer Kryptowährung besteht, wird hier nicht weiter untersucht. In Anlehnung an die Literatur zu den Aktienrenditen ist anzunehmen, dass die Anzahl der Listungen positiv mit den Renditen und negativ mit dem Risiko bzw. der Ausfallwahrscheinlichkeit korreliert. Diese Annahme kann teilweise durch die besseren Performance und geringeren Volatilität des wertgewichteten Indizes abgeleitet werden. **77**

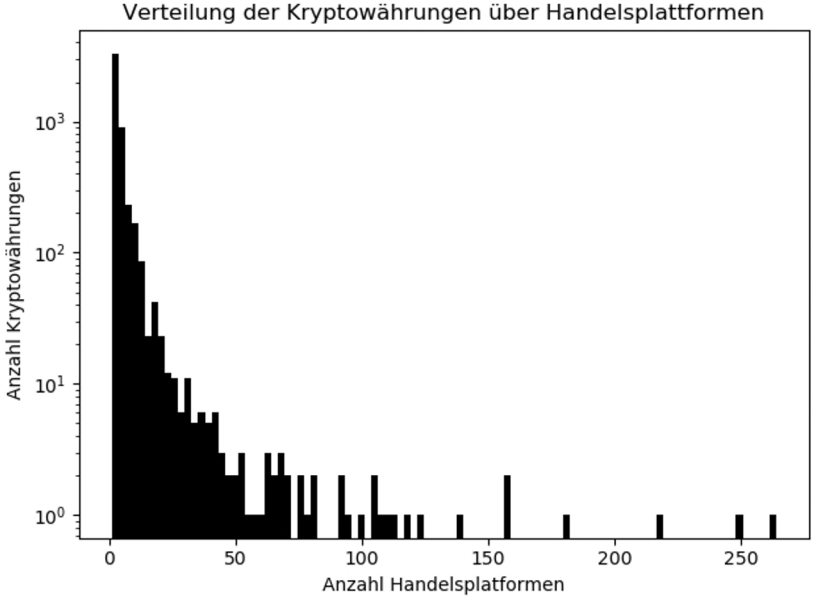

Abb. 4: Anzahl an Listungen auf Handelsplattformen für jede Kryptowährung. Die y-Achse wurde reskaliert (Daten: www.cryptocompare.com).

78 Der Kryptowährungsmarkt wird in der finanzwirtschaftlichen Forschung insgesamt als ein noch ineffizienter Markt angesehen. Markteffizienz bezieht sich hier vor allem auf Informationsasymmetrien und die Effizienzmarkthypothese. Die Effizienzmarkthypothese postuliert, etwas vereinfacht, dass alle verfügbaren Informationen von Investoren ausgewertet werden und durch ihre Markttransaktionen in den Marktpreisen jederzeit enthalten sind.[125] Das bedeutet allerdings nicht zwangsläufig, dass jeder einzelne Marktteilnehmer die gleiche Erwartung entwickeln muss, vielmehr ist die Gesamtheit rational.[126] Das ist möglich, wenn mindestens ein Marktteilnehmer rationale Erwartungen hat und der Markt kompetitiv ohne Zugangsbeschränkungen und vollkommen ist. Die Effizienz des Marktes hängt damit auch von der Liquidität des Marktes ab.[127] Ein vollkommener Markt zeichnet sich u. a. durch die Möglichkeit von Leerverkäufen aus, durch die Investoren Aktionen vornehmen können, wenn sie fallende Kurse von Kryptowährungen erwarten. Wenn die Leerverkäufe in einem Markt

125 Vgl. *Fama*, Journal of Finance, 1970.

126 Vgl. *Ramadan/Zeyad*, International Journal of Economics and Finance, 2015.

127 Untersuchungen speziell für Kryptowährungen, vgl. u. a. *Braunei/Mestel*, Finance Research Letters, 2019; *Wei*, Economic Letters, 2018; *Al-Yahyaee/Mensi/Ko/Yoon/Kang*, The North American Journal of Economics and Finance, 2020.

nicht möglich sind, dann handeln im Prinzip nur die Investoren, die positive Erwartungen entwickelt haben. In der Folge können sich übertriebene Preisentwicklungen realisieren. Kryptowährungsmärkte sind sehr heterogen bezüglich der Marktliquidität, weshalb viele Untersuchungen zeitweise und auch längerfristige Marktineffizienzen feststellen, und lassen bislang nur in sehr wenigen Fällen Leerverkäufe zu.[128]

Die Kryptowährungen können an mehreren Handelsplattformen gehandelt wer- **79**
den. Der Preis einer Kryptowährung zu einem Zeitpunkt ist, je nach ihrer Verbreitung, der gewichtete Mittelwert (Medianwert) von einigen wenigen bis zu mehreren Hundert Handelsplattformen. Daher lässt sich die Preisvarianz im Querschnitt der Handelsplattformen als eine Kennzahl für die Marktintegration und Markteffizienz heranziehen. In effizienten Märkten würde man erwarten, dass alle zum Zeitpunkt verfügbaren Informationen von den Marktteilnehmern ausgewertet und im Anschluss in die Marktpreise „hineingehandelt" werden. Signifikante Preisvarianzen dürften folglich zwischen unrestringierten Märkten nicht auftreten.

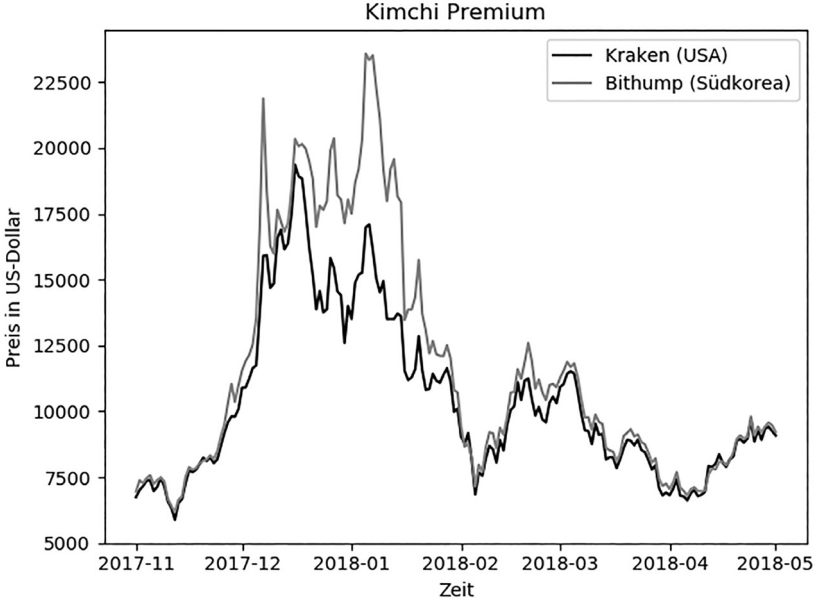

Abb. 5: Kimchi Premium. Unterschied im Bitcoin-Preis zwischen den USA (Exchange: Kraken) und Südkorea (Exchange: Bithump) im Jahreswechsel 2017/2018.

128 Vgl. u.A. *Tran/Leirvik*, Finance Research Letters, 2020; *Hu*, Finance Research Letters, 2019; *Zargar/Kumar*, Finance Research Letters, 2019; *Kristoufek/Vosvrda*, Physica A: Statistical Mechanics and its Applications, 2019.

80 Abbildung 5 zeigt exemplarisch die Preisdifferenz für Bitcoin zwischen den USA und Südkorea im Jahreswechsel 2017/2018. Diese betrug zeitweise mehrere tausend US-Dollar und hielt über Wochen an. Über den Zeitraum von Januar 2016 bis Februar 2018 übertraf der südkoreanische Bitcoin-Preis im Mittel um 4,73 % den Weltmarktpreis. Den Höchststand erreichte die Abweichung mit knapp 40 %.[129] Bekannt ist das Phänomen unter dem Begriff „Kimchi Premium".

81 In der Abbildung 6 werden die Standardabweichungen der Preise von drei führenden Kryptowährungen dargestellt. Hierfür wird zu jedem Zeitpunkt der Tagesschlusskurs von einem sehr breiten Querschnitt an Handelsplattformen gesammelt und ihre Standardabweichung berechnet. In effizienten Märkten sollte eine Kryptowährung an jeder Handelsplattforme den gleichen Wert und somit den gleichen Preis haben. Damit würde sich eine Standardabweichung der Preise von Null ergeben. Je höher die Standardabweichung der Preise ist, desto größer sind die Bedeutungsunterschiede zwischen den Märkten und Handelsplattformen. Wenn zwischen den Märkten keine regulatorischen oder sonstigen Restriktionen existieren, sollten Arbitrageure die Preise jederzeit in einem engen Korridor halten. Sollten dennoch Preisunterschiede existieren, könnten diese Rückschlüsse auf Marktineffizienzen erlauben.

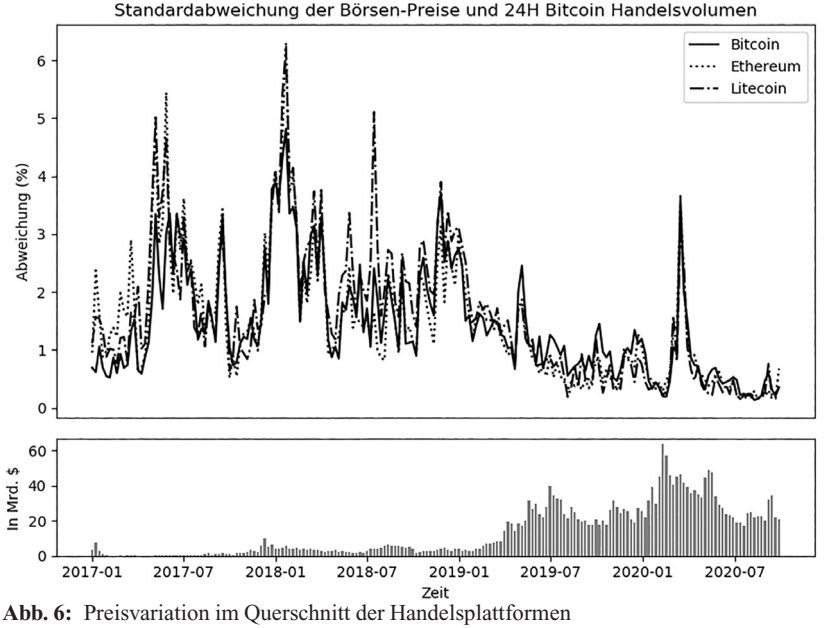

Abb. 6: Preisvariation im Querschnitt der Handelsplattformen (Daten: www.cryptocompare.com).

129 Vgl. *Choi/Lehar/Stauffer*, SSRN Electronic Journal, 2018.

Nach den dargestellten Ergebnissen in der Abbildung 6 zeigen sich für Bitcoin, Ethereum und Litecoin zum Teil starke Preisvarianzen zwischen den Handelsplattformen. So wies beispielsweise der Preis für Bitcoin zum Jahreswechsel 2017/2018 eine Standardabweichung von knapp 5% auf. Bei einem Bitcoin-Wert von mehr als Zehntausend Euro entspricht das einer durchschnittlichen Differenz von mehreren Hundert Euro. Die Entwicklung der Standardabweichungen ist für die drei Währungen nahezu identisch und ab dem Jahr 2019 stark abbauend. Lediglich die Verkündung der Lockdowns im März 2020, die durch die Corona-Pandemie bedingt waren, führte zu einer Ausweitung der Preisdifferenzen. Der Rückgang der Preisdifferenzen könnte als eine Erhöhung der Markteffizienz gedeutet werden, da scheinbar Arbitrageure durch den simultanen Handel an den Plattformen die Preise in ein relatives Gleichgewicht bringen. Denn der Rückgang der Preisdifferenzen impliziert gleichzeitig die Senkung von Gewinnmöglichkeiten für die Arbitrageure. **82**

In der akademischen Literatur finden sich Hinweise auf wiederkehrende und zum Teil über Tage und Wochen andauernde Preisabweichungen zwischen Handelsplattformen. In einer vielbeachteten Publikation werden vor allem Arbitragemöglichkeiten zwischen Ländern und Regionen dokumentiert. Während es innerhalb eines Landes (Region) typischerweise zu keinen nennenswerten Preisabweichungen von über 1% kommt, lag die durchschnittliche Preisdifferenz zwischen den USA und Europa (Japan) bei 3% (10%).[130] Allerdings scheinen sich die Märkte anzugleichen. Wie auch aus Abbildung 6 ersichtlich, sind Arbitragemöglichkeiten mit der Zeit seltener vorzufinden und/oder weniger lohnenswert. An dem Punkt, an dem Arbitragegewinne vollständig durch verbleibende Marktfriktionen aufgezehrt werden, spricht man von den Limits of Arbitrage.[131] **83**

VI. Zusammenfassung

In diesem Beitrag wird nach einer Kurzdarstellung der allgemeinen Finanzierungstheorie aufgezeigt, dass Token und Kryptowährungen vor allem eine neuartige Form der Zuteilung, Validierung und Dokumentation von Rechten und Pflichten aus einem Finanzvertrag sind. Dabei ist die Blockchain eine besondere Art von Ledger, mit dem die Dokumentation der Geschäftsvorfälle öffentlich und fälschungssicher gelingt und folglich die Probleme der unvollständigen Verträge im Hinblick auf eine fehlende vertrauenswürdige zentrale Institution abgemildert werden. Die Token in Verbindung mit Smart Contracts sind eine neuartige Technik, die finanziellen Verpflichtungen und Rechte aus einem Finanzvertrag ohne eine dritte Partei zu organisieren und zu steuern. Die grundsätzliche **84**

130 Vgl. *Markarov/Schoar*, Journal of Financial Economics, 2019.
131 Vgl. *Shleifer/Vishny*, The Journal of Finance, 2012.

Finanzierung bleibt jedoch bestehen: Kapitalgeber finanzieren die Projekte mit ihrem Geld und erhalten das Versprechen (aber keine Garantie) auf eine Entlohnung und/oder Mitsprache. Der rechtliche und empirische Überblick über den Kryptowährungsmarkt zeigt vor allem das juristische und ökonomische Risiko der Investition in derartige Projekte. Der Kryptowährungsmarkt kann am ehesten als ein sehr heterogener Markt ohne Regulierung beschrieben werden, auf dem eine Vielzahl von riskanten Projekten in ihren frühen Phasen finanziert wird. Das Risiko wird auch durch den hohen Anteil gescheiterter Projekte verdeutlicht, die sich insgesamt in sehr unterschiedlichen Geschäftsfeldern engagieren. Insgesamt sind Bestrebungen auf dem Kryptowährungsmarkt zu beobachten, eine Selbstregulierung zur Wahrung von Mindeststandards einzuführen.

Kapitel 2 Formen programmierbaren Geldes und Rolle der Zentralbank[1]

Literatur: *Adrian/Mancini-Griffoli*, The rise of digital money, 2019, IMF Note, no 19/001, July; *Armelius* et al., E-krona design models: pros, cons and trade-offs, 2020, Sveriges Riksbank Economic Review, June 2020; *Auer/Böhme*, The technology of retail central bank digital currency, 2020, BIS Quarterly Review March 2020, 85–100; *Auer* et al., Rise of the central bank digital currencies: drivers, approaches and technologies, 2020, BIS working paper No. 880, August 2020; *Auer* et al., Taking stock: ongoing retail CBDC projects, 2020, BIS Quarterly Review March 2020, 97–98; *Baeck/Elbeck*, Bitcoins as an investment or speculative vehicle? A first look, 2015, Appl. Econom. Lett., 22, 30–34; *Balz/Paulick*, Parallelwährungen jenseits der Finanzaufsicht: Haben Bitcoin und Libra eine Zukunft?, 2019, ifo Schnelldienst 17/2019, Volume 72, 13–16; *Balz/Diehl/Winter*, Digitales Geld: Welche Optionen hat Europa?, 2020, Zeitschrift für das gesamte Kreditwesen, Dezember 2020, 10–14; *Bank für Internationalen Zahlungsausgleich*, Distributed ledger technology in payment, clearing and settlement – An analytical framework, 2017, Bericht des Committee on Payments and Market Infrastructures; *Bindseil*, Tiered CBDC and the financial system, 2020, ECB working paper No. 2351, January 2020; *Böhme* et al., Bitcoin: Economics, technology and governance, 2015, Journal of Economic Perspectives 29 (2), 213–238; *Broadbent*, Central banks and digital currencies, 2016, Speech given at the London School of Economics, 2 March 2016; *Brühl*, Bitcoins, Blockchain und Distributed Ledgers – Funktionsweise, Marktentwicklungen und Zukunftsperspektiven, 2017, Wirtschaftsdienst, 97(2), 135–142; *Bundesbank*, Distributed-Ledger-Technologien im Zahlungsverkehr und in der Wertpapierabwicklung: Potentiale und Risiken, 2017, Monatsbericht September 2017, 35–50; *Bundesbank*, Krypto-Token im Zahlungsverkehr und in der Wertpapierabwicklung, 2019, Monatsbericht Juli 2019, 39–59; *Buterin*, The Search for a Stable Cryptocurrency, 2014, Ethereum Blog, November 11, 2014, https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/ (zuletzt abgerufen am 18.12.2020); *Carapella/Flemming*, Central Bank Digital Currency: A Literature Review, 2020, FEDS Notes, November 09, 2020, https://www.federalreserve.gov/econres/notes/feds-notes/central-bank-digital-currency-a-literature-review-20201109.htm (zuletzt abgerufen am 11.11.2020; *Central Bank of the Bahamas*, Project Sand Dollar: A Bahamas Payments System Modernisation Initiative, 2019; *De Filippi/Loveluck*, The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure, 2016, Internet Policy Review, Vol. 5, Issue 4, available at SSRN: https://ssrn.com/abstract=2852691; *Diehl*, Financial Market Infrastructures: The Backbone of Financial Systems, 2016, in: Diehl et al. (Hrsg.), Analyzing the Economics of Financial Market Infrastructures, 1–19; *Eastern Caribbean Central Bank*, ECCB Digital EC Currency Pilot. What you should know, 2019, https://www.eccbcentralbank.org/p/what-you-should-know-1 (zuletzt abgerufen am 19.12.2020); *ECB*, Report on a digital Euro, 2020, https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (zuletzt abgerufen am 19.12.2020); *Ethereum*, Ethereum Whitepaper, 2013, https://ethereum.org/en/whitepaper (zuletzt abgerufen am 16.12.2020); *Geiling*, Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain, 2016, BaFin Fachartikel; *Kahn*, How are payment accounts special?,

1 Der Text gibt die Meinung des Autors wieder und nicht notwendigerweise die Position der Deutschen Bundesbank oder des Eurosystems.

2016, Payments Innovation Symposium, Federal Reserve Bank of Chicago; *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf (zuletzt abgerufen am 14.7.2020); *Neyer*, The Future of Blockchain, 2017, Journal of Digital Banking, 2 (1), 74–94; *Raskin/Yermack*, Digital Currencies, Decentralized Ledgers, and the Future of Central Banking, 2016, NBER Working Paper No. 22238; *Roßbach*, Blockchain-Technologien und ihre Implikationen, 2016, Banking and Information Technology, 17(1), 54–69; *Selgin*, Synthetic commodity money, 2015, Journal of Financial Stability, 92–99; *Taleb*, Foreword, in: Ammous, The Bitcoin Standard: The Decentralized Alternative to Central Banking, 2018, XIII-XIV; *Thiele/Diehl*, Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten?, 2017, ifo Schnelldienst 22/2017, 70. Jahrgang, 23.11.2017, 3–6; *Weber*, Can Bitcoin compete with money?, 2014, Journal of Peer Production, Issue 4 (2014), available online at http://peerproduction.net/issues/issue-4-value-and-currency/invited-comments/can-bitcoincompete-with-money/; *Wu* et al., Does gold or Bitcoin hedge economic policy uncertainty?, 2019, Finance Research Letters (31), 171–178.

Übersicht

I. Grundlagen einer dezentralen Abwicklungstechnologie

1 Im Jahre 2008 wurde unter dem Namen *Satoshi Nakamoto* ein Papier mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System" veröffentlicht. Darin wird nicht nur ein neues dezentrales Zahlungsverkehrssystem auf Basis einer kryptographischen Technologie vorgeschlagen, sondern zugleich auch eine digitale Werteinheit, die zur Übertragung verwendet wird, der Bitcoin. Der Begriff wird zwar nur in der Überschrift verwendet, hat sich aber mittlerweile als Be-

zeichnung des tatsächlich entstandenen dezentralen Netzwerkes und des auf ihr umlaufenden Tokens durchgesetzt.

1. Ein neues Zahlungssystem

Im Fokus von *Nakamoto*, der bis heute seinen echten Namen nicht offengelegt hat, lag das neue Zahlungssystem, nicht die darin verwendete Werteinheit. So heißt es gleich zu Beginn: „What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[2] Das neue elektronische Zahlungssystem sollte also ohne Finanzintermediäre funktionieren, allein mittels sog. Peer-to-Peer-Transaktionen (P2P). Im gegenwärtigen Finanzsystem erfolgen Finanztransaktionen ganz überwiegend über Intermediäre, z. B. Zahlungsdienstleister und Finanzmarktinfrastrukturen.[3] **2**

Der Bedeutung und dem Design der verwendeten Werteinheit widmet das Papier wenig Aufmerksamkeit. Es wird festgelegt: „We define an electronic coin as a chain of digital signatures."[4] Ebenso wird in diesem grundlegenden Papier keinerlei Aussage über die mögliche oder zu erwartende Wertstabilität getätigt. Nach dem von *Nakamoto* vorgesehenen Mechanismus erhöht sich die Menge der geschaffenen Bitcoin im Laufe der Zeit mit abnehmender Geschwindigkeit und wird bei 21 Millionen Stück ihr Maximum erreichen. Diese absolute Mengenbegrenzung sowie die Verwendung von bergbautechnischen Begrifflichkeiten – die Dienstleister im Bitcoin-Netzwerk, die sich neue Bitcoin für bestimmte Leistungen zuschreiben dürfen, werden zum Beispiel „Miner" genannt – ließ den Bitcoin in der Betrachtung in die Nähe von Rohstoffen oder gar Gold rücken. Der bisweilen als „synthetic commodity" bezeichnete Coin[5] wurde empirisch als Wertaufbewahrungsmittel bzw. als Vehikel zur Portfoliodiversifizierung mit Gold verglichen.[6] **3**

Die Übertragung des Bitcoins erfolgt im Bitcoin-Netzwerk durch eine einfache Eintragung, dass ein Teil der einem Teilnehmer zugerechneten Bitcoin nun einem anderen Teilnehmer zugerechnet wird. Der Bitcoin wird in sog. Wallets gespeichert und nicht auf Konten verbucht. Er stellt keine Forderung oder Ver- **4**

2 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf (zuletzt abgerufen am 14.7.2020), S. 1.

3 Vgl. Bundesbank, Distributed-Ledger-Technologien im Zahlungsverkehr und in der Wertpapierabwicklung: Potentiale und Risiken, S. 39 ff.

4 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf (zuletzt abgerufen am 14.7.2020), S. 2.

5 *Selgin*, Synthetic commodity money, S. 92.

6 Vgl. *Selgin*, Synthetic commodity money, S. 92–99; *Baeck/Elbeck*, Bitcoins as an investment or speculative vehicle? A first look, S. 32; *Wu* et al., Does gold or Bitcoin hedge economic policy uncertainty?, S. 171.

bindlichkeit dar. Er existiert auch nicht als abgeschlossene digitale Einheit. Die Menge der einem Teilnehmer zugeschriebenen Bitcoin ergibt sich aus der Addition der in den gespeicherten Transaktionen ersichtlichen Übertragungen an ihn und der Subtraktion seiner eigenen Übertragungen.

5 Dieses Netzwerk funktioniert dezentral; bei Bitcoin auf Basis der sog. Blockchain-Technologie, die als Spezialform der Distributed-Ledger-Technologie (DLT) angesehen wird. Als Distributed Ledger (DL) oder Verteiltes Kontenbuch wird eine verteilte Datenbank bezeichnet, bei der die Teilnehmer im Netzwerk eine gemeinsame Schreib-, Lese- und Speicherberechtigung ausüben. Traditionellerweise dominieren in der Buchhaltung bislang zentrale Datenbanken. Lese- und teilweise auch Speicherrechte sind dabei üblicherweise ebenso für die Teilnehmer gegeben. Die Schreibrechte obliegen allerdings einer zentralen Einheit, zum Beispiel dem Betreiber eines Zahlungssystems. Der Betreiber, die zentrale Einheit, übernimmt in der Regel die Verantwortung für die Funktionsfähigkeit des Systems, für die sichere Speicherung und Verteilung der Daten, und er ist Ansprechpartner für regulative und aufsichtliche Belange. Ihm kommt eine besondere Vertrauensstellung zu, da er normalerweise auch die Zulassung der Teilnehmer zum Netzwerk regelt und deren systemkonformes Verhalten überwacht. Zudem hat er als einziger Schreibrechte. Da im traditionellen Finanzsystem üblicherweise Forderungen oder Wertpapiere auf Konten oder Depots übertragen werden, gibt es mindestens zwei Beteiligte bei Transaktionen, die deren korrekte Verbuchung überwachen. Die Korrektheit aller Salden ergibt sich, wenn alle bilateralen Salden, sprich alle Forderungen und Verbindlichkeiten der Teilnehmer gegenüber der zentralen Instanz korrekt sind.

6 In einem dezentralen System gibt es keine zentrale Instanz. Die DLT[7] erlaubt die fälschungssichere Übertragung digitalisierter Werte ohne zentrale Einheit oder Intermediär. Dies wird möglich durch die Dokumentation und Speicherung aller Transaktionen bei jedem Teilnehmer, meist in Form eines Hashes. Eine nachträgliche Fälschung historischer Transaktionen verändert den Hash in der Regel komplett und wird sofort von den Teilnehmern erkannt. Auf diese Weise kann das sog. „Double Spending Problem" vermieden werden. Darunter versteht man das Risiko, dass ein Teilnehmer Coins mehrfach überträgt. Vor Bitcoin war das „Double Spending Problem" der Grund, warum digital keine Werte, sondern „nur" Informationen übertragen werden konnten. Es ist nicht möglich, eine digi-

7 Zu den Grundlagen zu DLT und Blockchain siehe: Bank für Internationalen Zahlungsausgleich, Distributed ledger technology in payment, clearing and settlement – An analytical framework, 2017, Bericht des Committee on Payments and Market Infrastructures; *Roßbach*, Blockchain-Technologien und ihre Implikationen, Banking and Information Technology, 54–69; *Brühl*, Bitcoins, Blockchain und Distributed Ledgers – Funktionsweise, Marktentwicklungen und Zukunftsperspektiven, 135–142; sowie *Geiling*, Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain.

tale Kopie von einem digitalen Original zu unterscheiden. Seit Bitcoin können nun auch Werte zwischen Teilnehmern ohne Intermediär übertragen werden. Direkte Übertragungen von Teilnehmern an Teilnehmer, im Fachjargon „peer-to-peer" (P2P) sind nun auch digital möglich. P2P-Transaktionen gibt es im klassischen Finanzsystem nur bei der Übergabe von Inhaberpapieren, etwa bei der Bezahlung mit Bargeld.

Die Sicherung der Korrektheit der vorgeschlagenen Transaktionen in dezentralen Netzwerken erfordert eine Validierung und einen Konsensmechanismus, eine Art Abstimmungsprozess unter den Teilnehmern. Neue Transaktionsvorschläge müssen zunächst vom Netz oder von einer Teilmenge der Teilnehmer validiert werden, bevor sie in die Transaktionshistorie bzw. in die Blockchain aufgenommen werden. Durch den Konsensmechanismus wird die zeitliche Reihenfolge der zu verbuchenden Transaktionen festgelegt und ein einheitlicher Status der verteilten Datenbank bei allen Teilnehmern sichergestellt. Bei einigen Netzwerken können alle Teilnehmer sich an der Validierung und dem Konsensmechanismus beteiligen, bei anderen nur ausgewählte Teilnehmer. Je weniger Teilnehmer daran beteiligt sind, desto mehr nähert sich der Charakter des Netzwerkes einem zentralen Netzwerk. **7**

2. Offene und geschlossene Netzwerke

Eine wichtige Unterscheidung für die Art eines Netzwerkes ergibt sich aus der Regelung der Teilnahmeberechtigung am Netzwerk. In offenen, sog. „unpermissioned", Netzwerken gibt es keine formale Zulassungshürde. Alle Teilnehmer können sich ohne Beschränkung und oft auch mehrfach am Netz beteiligen. In zulassungsbeschränkten, sog. „permissioned", oder geschlossenen Netzwerken gibt es dagegen eine Entität, die über die Zulassung von Teilnehmern entscheidet. Dies bedeutet auch, dass die Teilnehmer zumindest gegenüber der zulassenden Stelle ihre Anonymität zumindest teilweise aufgeben müssen. Ohne überwachte Regeln zur Teilnahmeberechtigung sind Transaktionssysteme allerdings anfällig für illegale Transaktionen. Anonymität oder die sog. „Pseudoanonymität" der Teilnehmer läuft den Anforderungen der Bekämpfung von Geldwäsche und Terrorismusfinanzierung zuwider. In der Tat gibt es zahlreiche Beispiele für die Verwendung von Bitcoin zur Finanzierung illegaler Transaktionen oder zur Geldwäsche.[8] **8**

3. Vertrauen

Die Fähigkeit dezentraler Netze, mithilfe kryptographischer Verfahren Werte ohne Intermediär übertragen zu können, wird gelegentlich als vertrauenschaf- **9**

8 Vgl. *Böhme* et al., Bitcoin: Economics, Technology, and Governance, S. 222.

fende Funktion bezeichnet. Der Algorithmus der dezentralen Netzwerke schaffe Vertrauen, sodass die vertrauensbildende Wirkung von zentralen Einheiten nicht mehr benötigt werde. Allerdings bleibt diese vertrauenschaffende Wirkung der Algorithmen auf den virtuellen Bereich beschränkt. Die im Bitcoin-Netzwerk umlaufenden Coins sind nur virtuell, das heißt, sie haben keine Existenz außerhalb des digitalen Netzwerkes. Im Unterschied dazu verbrieft ein Wertpapier Ansprüche in der realen Welt. Es kann in tokenisierter Form via DLT übertragen werden, bedarf aber zur Verfügbarmachung auf der DLT eines Bindeglieds zwischen realer und digitaler Welt, zum Beispiel in Form eines Zentralverwahrers. Das heißt, an der Schnittstelle zwischen realer Welt und DLT bedarf es einer vertrauenswürdigen Instanz.[9] Der Übertrag eines Gutes kann zwar in der DLT dokumentiert werden, aber die reale Existenz des Gutes, seine Eigenschaften und möglicherweise auch die vorherigen Eigentumsverhältnisse wären damit noch nicht bestätigt. Der Anspruch der DLT, eine Übertragung ohne Vertrauen zu leisten, bleibt folglich auf den rein virtuellen Bereich ohne realen Bezug beschränkt.

4. Alternative Netzwerke und alternative Coins

10 Neben Bitcoin wurden zahlreiche weitere dezentrale Netzwerke geschaffen, die sich hinsichtlich der Algorithmen zur Validierung und Konsensfindung mehr oder weniger von Bitcoin unterscheiden. Viele dieser Netzwerke haben eigene Coins, sog. Krypto-Token geschaffen, sodass es angeblich zum Jahresende 2020 mehr als 8.000 verschiedene Krypto-Token gibt.[10] Das 2013 geschaffene Ethereum-Netzwerk mit dem Krypto-Token Ether gilt allgemein als das zweitgrößte dezentrale Netzwerk. Das Besondere an Ethereum ist, dass mit seiner Erfindung die Nutzung von sog. Smart Contracts möglich wurde.[11] Smart Contracts sind Computerprotokolle, die geschlossene Verträge automatisiert in Abhängigkeit von dem Eintreten vordefinierter Ereignisse ausführen. Sie ermöglichen die Vereinfachung von komplexen wiederkehrenden Vertragsabwicklungen zwischen mehreren Partnern. Damit gelten sie als Schlüsseltechnologie für die Reduktion von Transaktionskosten in einer arbeitsteiligen Volkswirtschaft. Der zweite große Vorteil der DLT ist die gemeinsame Datenhaltung der Beteiligten, wodurch unter anderem Abstimmungsprozesse bei komplexen arbeitsteiligen Wertschöpfungsketten entfallen können oder erheblich erleichtert werden.

---

9 Vgl. *Neyer*, The Future of Blockchain, 74–94.

10 Vgl. https://coinmarketcap.com/ (zuletzt abgerufen am 16.12.2020). Die Quelle kann als Indiz für die Marktentwicklung dienen. Die dort angegebenen Umsatzzahlen einzelner Kryptobörsen sowie der Marktkapitalisierung einzelner Krypto-Token sind jedoch nicht immer belastbar.

11 Vgl. Ethereum, Ethereum Whitepaper, 2013, https://ethereum.org/en/whitepaper (zuletzt abgerufen am 16.12.2020).

Die DLT hat daher anders als der Bitcoin oder andere Krypto-Token großes Interesse in real- und finanzwirtschaftlichen Unternehmen geweckt. Die ursprünglich für Bitcoin entwickelte DLT muss jedoch erheblich modifiziert werden, um sie an die Bedürfnisse der Wirtschaft anzupassen. So sind im bestehenden Rechtsrahmen zum Beispiel Identifizierbarkeit der Teilnehmer, Vertraulichkeit der Transaktionen gegenüber Dritten und absolute Finalität der Transaktionen unabdingbar. Darüber hinaus ist ein hoher Transaktionsdurchsatz notwendig. Mittlerweile sind viele DLT-Modifikationen von Softwarehäusern entwickelt worden, die zum Zwecke der realen Anwendung in der Regel mit zulassungsbeschränkten Netzwerken arbeiten und sehr gezielt auf die konkreten Bedürfnisse der Betreiber und Teilnehmer ausgerichtet sind. Bekannte Basisblockchains sind Corda, Hyperledger Fabric, Hyperledger Sawtooth, Digital Asset, um nur einige zu nennen, die in konkreten Projekten genutzt werden. **11**

II. Geld

Geld ist im ökonomischen Sinne alles, was die Geldfunktionen – Zahlungsmittel, Wertaufbewahrungsmittel und Recheneinheit – erfüllt. Dies hat sich im Zeitablauf stark gewandelt. Und mit der Erfindung der Krypto-Token gibt es nun auch virtuelle Dinge, die als Geld genutzt werden können. In der Tat gab und gibt es eine breite Debatte darüber, inwieweit Bitcoin oder andere Krypto-Token gegen Zentralbankgeld konkurrieren können bzw. was das für Zentralbanken bedeutet.[12] **12**

1. Geldfunktionen und Wertgrundlagen

Die wichtigsten Geldformen sind in Abb. 1 dargestellt. Manche Güter können als Geld genutzt werden und waren zum Teil historisch von großer Bedeutung. Dies können Verbrauchsgüter wie etwa Zigaretten oder Gebrauchsgüter wie Gold sein. Beide haben einen intrinsischen Wert, der sich aus dem Verbrauchs- oder Gebrauchswert ergibt. Es gibt also eine Nachfrage nach diesen Gütern unabhängig von ihrer Funktion als Geld. Dieser intrinsische Wert dient nicht zu- **13**

12 Vgl. beispielsweise *Weber*, Can Bitcoin compete with money?, 2014, Journal of Peer Production, Issue 4 (2014), available online at http://peerproduction.net/issues/issue-4-value-and-currency/invited-comments/can-bitcoincompete-with-money/; *Taleb*, in: Ammous, The Bitcoin Standard, Foreword, S. XIII–XIV; *Broadbent*, Central Banks and digital currencies, *Raskin/Yermack*, Digital Currencies, Decentralized Ledgers, and the Future of Central Banking; *Ludwin*, Why Central Banks Will Issue Digital Currency, 2016, Speech at the Federal Reserve Conference in Washington D.C., 1.6.2016, http://blog.chain.com/post/145509298356/why-central-banks-will-issue-digital-currency; *Thiele/Diehl*, Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten?

letzt als Wertanker für den Wert des Geldes. Wie stark dieser Wertanker wirkt, hängt von der Relation der Nachfrage nach diesem Gut als Gut und der Nachfrage nach dem Gut als Geld und der Substituierbarkeit ab. Die Stabilität des Geldwertes gemessen an einem allgemeinen repräsentativen Warenkorb kann per se nicht gewährleistet werden, da sich der Wert des Geldes am Wert eines Gutes orientiert. Nur wenn sich der Wert dieses Gutes synchron mit dem Wert eines repräsentativen Warenkorbes verändert, wäre Wertstabilität im Sinne einer Stabilität des Verbraucherpreisindexes erreicht.

Abb. 1: Geldfunktionen und Geldformen

14 Die gegenwärtig dominierende Form des Geldes sind dagegen Forderungen bzw. Verbindlichkeiten. Dabei unterscheidet man Verbindlichkeiten der Zentralbank, welche Zentralbankgeld begründen, von Verbindlichkeiten der Geschäftsbanken, welche Geschäftsbankengeld begründen. Beide haben an sich keinen intrinsischen Wert, sieht man vom Materialwert des Bargeldes einmal ab. Zentralbankgeld existiert in zwei Formen: als Bargeld in Noten und Münzen sowie als Guthaben auf Konten bei der Zentralbank. Letztere können üblicherweise nur Geschäftsbanken und einige wenige andere Institute halten. Geschäftsbankengeld existiert als Guthaben von Kunden auf Konten bei Geschäftsbanken. Dieses kann abgehoben und damit in Bargeld, also Zentralbankgeld konvertiert werden. Beide Geldformen sind also in einem Währungsraum nominal identisch. Im Euroraum lauten sie auf Euro. Geschäftsbanken unterliegen gleichwohl einem ungleich größeren Ausfallrisiko.

15 Zentralbanken dagegen gelten in den entwickelten Währungsräumen als ausfallsicher. Sie können nämlich eigenes Geld schaffen und daher in der Regel in eigener Währung nicht zahlungsunfähig werden. Hinter ihnen steht letztlich der Staat und das bestehende Rechtssystem. In den entwickelten Volkswirtschaften

mit einer grundsätzlich stabilitätsorientierten Geldpolitik gilt Zentralbankgeld als das ultimative Medium zur Erfüllung von Zahlungsforderungen. Es hat die Erfüllung durch Goldlieferung verdrängt. Der Wertanker für Zentralbankgeld ist das Vertrauen in die Zentralbank. Der Euro, d. h. Euro-Zentralbankgeld, wird von einer gesetzlich damit beauftragten Institution, der Europäischen Zentralbank und den nationalen Zentralbanken des Euroraums (Eurosystem) herausgegeben. Der Euro ist eine Verbindlichkeit des Eurosystems mit seinen Zentralbanken, darunter die Bundesbank. Euro-Zentralbankgeld gilt heute als das sicherste und zugleich wertstabilste Zahlungsmittel im Euroraum.

16 Die Geschäftsbanken spielen im Geldkreislauf eine wichtige Rolle. Sie bieten Einlagemöglichkeiten auf Konten an und versorgen die Wirtschaft mit Bargeld, das gegen Kontoguthaben dort abgehoben werden kann. Die Einlagen bei Geschäftsbanken sind heute der größte Teil der umlaufenden Geldmenge.[13] Sie sind aber praktisch genauso wertstabil wie Zentralbankgeld, weil sie eins zu eins in Bargeld umgewandelt werden können. Für die große Mehrheit der privaten Haushalte ist es unerheblich, ob es sich um Geschäftsbankengeld oder Zentralbankgeld handelt, zumal Einlagen bis zu 100.000 EUR von der Einlagensicherung gedeckt sind. Deshalb werden die meisten Zahlungen von Unternehmen und Haushalten in Geschäftsbankengeld abgewickelt, während Banken für ihre großen Übertragungen, etwa bei der Abwicklung von Wertpapiergeschäften, sicheres Zentralbankgeld in der Abwicklung bevorzugen.[14]

17 Krypto-Token, wie etwa der Bitcoin dagegen, haben keinen intrinsischen Wert. Sie werden praktisch ex nihilo geschaffen und repräsentieren weder ein Gebrauchs- noch ein Verbrauchsgut, noch haben sie einen zuverlässigen Emitten-

13 Im September 2020 beliefen sich in Deutschland die umlaufende Bargeldmenge auf 301,9 Mrd. EUR, die Guthaben der Monetären Finanzinstitute bei Zentralnotenbanken auf 887,4 Mrd. EUR und die Geldmenge M3 (ohne Bargeld) auf 3.398,6 Mrd. EUR. Vgl. Bundesbank, Statistische Fachreihe Saisonbereinigte Wirtschaftsdaten, November 2020; Bundesbank, Statistische Fachreihe Bankenstatistiken, November 2020 und Bundesbank, Zeitreihendatenbank Bargeldumlauf, 2020, https://www.bundesbank.de/dynamic/action/de/startseite/suche/statistiken/suche-im-zeitreihen-code/747632/titel suche-in-der-zeitreihendatenbank?query=Bargeldumlauf (zuletzt abgerufen am 1.12. 2020).

14 Die Zahlungsverkehrsstatistik weist für 2019 in der deutschen TARGET2-Komponente 48,2 Mio. Transaktionen in Zentralbankgeld im Wert von 209.082,3 Mrd. EUR aus. Insgesamt wurden aber bargeldlose Zahlungsinstrumente von Nicht-Zahlungsdienstleistern für 24.202,7 Mio. Transaktionen genutzt, übertrugen dabei aber „nur" 60.593,2 Mrd. EUR. Vgl. Bundesbank, Zahlungsverkehrs- und Wertpapierabwicklungsstatistiken, Statistische Fachreihe September 2020, https://www.bundesbank.de/de/statistiken/banken-und-andere-finanzielle-unternehmen/zahlungsverkehr/zahlungsverkehrs-und-wertpapierabwicklungsstatistiken-804046.

ten, der für sie haftet. Es fehlt praktisch jeglicher Wertanker. Dies dürfte ein Grund für die extrem hohe Volatilität des Wertes der meisten Krypto-Token gemessen am Preis in US-Dollar oder Euro sein. Der Wert der meisten Krypto-Token schwankt so stark, dass sie sich praktisch nicht zum Zahlungsmittel, zur Wertaufbewahrung oder als Recheneinheit eignen. In der Tat kommen Krypto-Token im gesamten Finanzsystem bislang nicht über eine Nischenfunktion in einigen dezentralen Netzwerken und eine Rolle als Spekulationsobjekt hinaus. Es gibt sehr wenige Händler, die Krypto-Token als Zahlungsmittel akzeptieren. Viele, die Bitcoin und andere Krypto-Token annehmen, tauschen diese aber unmittelbar wieder in eine stabile Währung, um ihre Werte zu sichern. Noch seltener werden sie als Recheneinheit etwa bei Preisangaben oder Wertaufstellungen verwendet. Im Gegenteil, der Preis des Bitcoins in US-Dollar dominiert die Berichterstattung und nicht etwa umgekehrt.

2. Zahlungsverkehr

18 Zur Stabilität des Geldes gehört auch eine sichere und effiziente Übertragungsmöglichkeit, also ein Zahlungssystem. Ohne dieses kann die Zahlungsmittelfunktion nicht erfüllt werden. In der traditionellen Finanzwirtschaft werden Zahlungen in einem gemischt öffentlich-privaten System unter Beteiligung von Finanzmarktinfrastrukturen und Finanzdienstleistern abgewickelt.[15] In den entwickelten Ländern betreiben Zentralbanken üblicherweise Individualzahlungsverkehrssysteme für die wertmäßig großen Transaktionen der Banken zur Abwicklung von Transaktionen in Zentralbankgeld. Dies sind meist sog. Real-Time-Gross-Settlement-Systeme (RTGS-Systeme), die Zahlungen in Echtzeit abwickeln. Im Euroraum betreibt das Eurosystem das RTGS-System TARGET2. Zahlungen in Geschäftsbankengeld werden dagegen in der Regel von privat betriebenen Clearinghäusern abgewickelt. Diese Clearinghäuser unterliegen der Zahlungsverkehrsaufsicht und sind zum Beispiel gehalten, ihren Spitzenausgleich in Zentralbankgeld abzuwickeln. Sie sind damit an die RTGS-Systeme angeschlossen. Daneben gibt es weitere private Formen des Übertrags von Geschäftsbankengeld zwischen den unterschiedlichen Finanzdienstleistern. Ebenso sind öffentliche und private Finanzmarktinfrastrukturen an der Abwicklung von Wertpapiergeschäften beteiligt. Soweit dies privat durchgeführt wird, unterliegt es aber der hoheitlichen Aufsicht. Es gibt also immer eine klare Betreiberverantwortung und eine öffentliche Beaufsichtigung.

15 Vgl. *Diehl*, in: Diehl et al., Analyzing the Economics of Financial Market Infrastructures, S. 28.

3. Unklare Governance in dezentralen Netzwerken

Die Verantwortung für dezentrale Netzwerke dagegen ist nicht auf einen eindeutigen Betreiber einschränkbar.[16] Üblicherweise werden dezentrale Netze als offener Code, also Open Source, bereitgestellt und dezentral weiterentwickelt. Die Entscheidung über die Annahme einer vorgeschlagenen Code-Änderung oder Ergänzung trifft idealiter die Gemeinschaft der Nutzer durch mehrheitliche Übernahme. In vielen Fällen haben nur Teile der jeweiligen Nutzergemeinschaft den neuen Code übernommen und das Netzwerk spaltete sich auf. Eines der Netzwerke behielt den alten Krypto-Token mit dem Namen, das andere gab sich einen neuen Namen und transferierte einen anderen Coin. Man sprach von den sog. AltCoins, eine Abkürzung für „alternative coins". Die Entscheidungsrechte bei dezentralen Netzwerken sind praktisch zwischen verschiedenen Stakeholdern – Nutzern, Entwicklern und Entwicklern von Anwendungen und evtl. weiteren – verteilt. Es gibt allerdings in der Regel eine Kerngruppe, die größeren Einfluss auf die Entwicklung des Netzwerkes ausübt, der über informale Beeinflussung hinausgeht. Dies ist leider für Außenstehende selten offensichtlich und nicht mit einer klaren Betreiberverantwortung zu vergleichen. Diese unklare Governance für den Betrieb des Netzwerkes erschwert nicht nur die Zulassung und Beaufsichtigung solcher Netzwerke, sie mindert naturgemäß auch das Vertrauen der breiten Öffentlichkeit. **19**

III. Bedarf an programmierbarem Geld

Durch die DLT kommen nun neue Anforderungen an Geld als Transaktionsmittel hinzu, die traditionelle Zahlungsmittel nicht oder nur bedingt erfüllen können. **20**

1. Programmierbarkeit von Zahlungen und von Geld

Mithilfe der DLT ist es möglich, sog. programmierbare Zahlungen zu nutzen. Programmierbare Zahlungen sind Überträge von Geld, bei denen Zeitpunkt, Betragshöhe und/oder Art des Übertrags nicht ad hoc beim Zahlungsvorgang, sondern durch vorab festgelegte Bedingungen bestimmt werden. Begrenzt geht das schon heute, etwa bei regelmäßigen Zahlungen per Dauerauftrag; hier werden Zahlungen zu bestimmten Kalenderterminen ausgelöst. In den dezentralen Netzwerken lassen sich allerdings komplexe Geschäftsprozesse automatisiert durch **21**

16 Vgl. *Böhme*, Bitcoin: Economics, Technology, and Governance; *De Filippi/Loveluck*, The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure, 2016, Internet Policy Review, Vol. 5, Issue 4, available at SRN: https://ssrn.com/abstract=2852691.

sog. Smart Contracts steuern. Um das auch geldseitig zu ermöglichen, bedarf es programmierbarer Zahlungen oder programmierbaren Geldes.

22 Bei programmierbarem Geld geht man davon aus, dass der digitalen Geldeinheit eine inhärente Logik durch den Nutzer beigegeben werden kann, die ihre Verwendung programmgesteuert einschränkt. Der digitale Coin verliert damit (temporär) seine universale Zahlungseignung. Er könnte zwischen Geschäftspartnern übertragen werden, aber erst nach Erfüllung vordefinierter Bedingungen einlösbar sein. Die Erfüllung der Bedingungen könnte jedes messbare Ereignis (zum Beispiel Erbringen einer Dienstleistung, Erreichen eines Bestimmungsortes, Ablauf einer Frist) sein. Der digitale Coin könnte gegebenenfalls Nachrichten senden, sodass der Nutzer bis zum tatsächlichen Eigentumsübergang am Coin den Verbleib und Status des Coins erfahren könnte. Weiterhin ist es denkbar, dass der Coin auch Nachrichten an den Empfänger überbringt, wodurch eine unternehmensübergreifende Prozessintegration möglich wird. Der Verkäufer erführe von der Bereitstellung des Coins und des unabdingbar programmierten Eigentumsüberganges an ihn bei Erfüllen der Leistungsversprechen. Nicht zuletzt könnten solche in programmierbaren Anwendungen gebundenen Coins das Risiko für beide Seiten deutlich reduzieren, stellen sie doch belastbare Sicherheiten dar, die auch bei der Liquiditäts- und Bonitätsbewertung der Beteiligten berücksichtigt werden könnten. Programmierbares Geld könnte in Verbindung mit der DLT zu einer nahezu vollständigen Synchronisierung von Güter- und Geldfluss führen.

23 Einige der beschriebenen Funktionen können auch ohne programmierbares Geld erfüllt werden, wenn digitales Geld in programmierbaren Zahlungsverfahren genutzt werden könnte. In dem Fall ist die Prozesslogik nicht in dem digitalen Coin integriert, er wird nur einer Prozesskette übergeben, die einer programmierten Logik folgt. Er müsste also lediglich tokenisiert sein.

2. Anwendungsfälle programmierbarer Zahlungen

24 Mittlerweile hat die Wirtschaft zahlreiche Anwendungsfälle für die Abwicklung von Geschäften mittels der DLT entwickelt, sodass ein Bedarf für programmierbare Zahlungen besteht. Dabei wird ein Vertrag zwischen den Vertragsparteien geschlossen und dann informationstechnisch zur automatisierten Abwicklung programmiert. Diese Abwicklung wird dann durch eingehende Signale, teilweise auch von Programmen oder Maschinen gesendet, gesteuert. Im Ergebnis sind also auch mehrere ineinander verwobene Automatismen denkbar, die mehrere Leistungsprozesse zum Beispiel mit Vor- und Endprodukt steuern. Je nach vertraglicher Vereinbarung löst also der Leistungsfluss einen entsprechenden Geldfluss aus.

Ein Beispiel sind Machine-to-machine-Zahlungen, bei denen Maschinen automatisch erbrachte Leistungen miteinander verrechnen und begleichen, natürlich letztlich auf Rechnung ihrer Besitzer. Also ein autonom fahrendes Fahrzeug tankt an einer Tankladesäule für Elektrizität und bezahlt selbständig mit digitalen Coins. Oder ein Zug eines Bahnunternehmens zahlt für den Stationshalt an einem Bahnhof der Deutschen Bahn an diese. Der ultimative Auslöser könnte jedes messbare Ereignis sein, der Veranlasser wäre eine geschäftsfähige Entität. Andere, aber ähnlich gelagerte Beispiele fallen unter Pay-per-Use-Modelle, bei denen die Begleichung eines Betrages in Abhängigkeit vom aktuellen Verbrauch erfolgt. Ein gemieteter Mähdrescher könnte zum Beispiel für jede genutzte Maschinenstunde direkt in digitalen Coins bezahlt werden. Die Anwendungsmöglichkeiten in den sehr arbeitsteilig geprägten modernen Volkswirtschaften sind mannigfaltig. **25**

Auch in der Finanzwirtschaft sollte ein Einsatz der DLT sinnvoll sein. Zum Beispiel ist eine automatisierte Abwicklung von Wertpapiergeschäften denkbar, bei der ein Smart Contract die Vertragsabwicklung als virtueller Treuhänder steuert. Von der Emission eines Finanzprodukts bis hin zum gesamten Lebenszyklus strukturierter Finanzprodukte einschließlich der notwendigen Kapitalmaßnahmen lassen sich alle Prozesse auch digital abbilden. Nicht zuletzt die klassische Delivery-versus-Payment-Abwicklung im Wertpapiergeschäft könnte ein Smart Contract übernehmen. Eine Übersicht der gegenwärtigen Anwendungsfälle der DLT im Finanzsektor zeigt Abb. 2. **26**

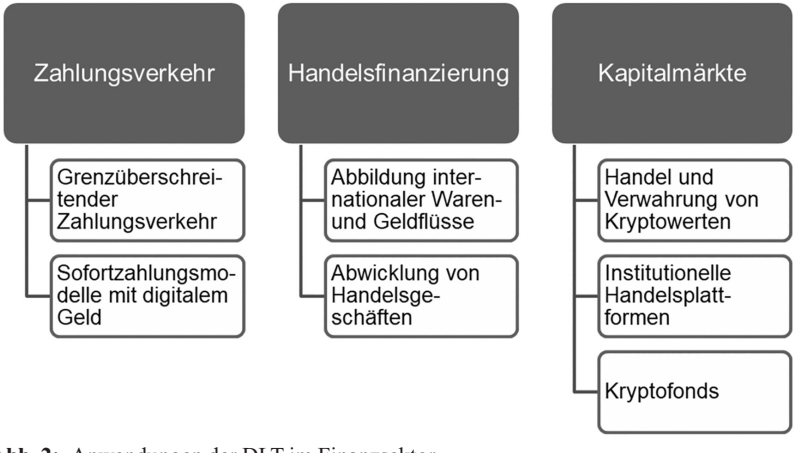

Abb. 2: Anwendungen der DLT im Finanzsektor

27 Die Möglichkeit zur Einbettung in programmierbare Anwendungen ist das eigentlich neue Merkmal des Geldes, das in dezentralen Netzwerken genutzt werden kann. Sie erst erlaubt die Nutzung der DLT für die vollständige Abwicklung von Geschäftsprozessen. Da in der öffentlichen Diskussion auch die digitale Ergänzung zu Bargeld unter digitales Geld subsumiert wird, wird die weitergehende Variante als programmierbares oder tokenisiertes Geld bezeichnet. Nur dieses kann in programmierbaren Prozessen verwendet werden, wäre also die weitergehende Innovation.

3. Krypto-Token

28 Einige der oben beschriebenen Krypto-Token ermöglichten als erstes die Zahlungsabwicklung in dezentralisierten Netzwerken in programmierbarer Form.[17] Bitcoin selbst gehört nicht dazu. Die weitergehende Form der DLT wurde erst mit Ethereum entwickelt. Daher gilt das Ethereum-Netzwerk als Testfeld für die Funktionalität von Smart Contracts aller Art. Allerdings erwiesen sich die klassischen Krypto-Token als zu wertinstabil für die Nutzung im Zahlungsverkehr und in weitergehenden Finanzgeschäften. Ein sehr volatiler Wertverlauf schränkte die Nutzbarkeit praktisch ein, weshalb gerade in längerfristig abzuwickelnden Vertragsbeziehungen auf die Zahlung in Krypto-Token verzichtet wird. Trotz zwischenzeitlicher Phasen reduzierter Volatilität bleibt das Problem der inhärenten Instabilität des Wertes der Krypto-Token bestehen, da sie über keinerlei Wertanker verfügen. Damit ist jede Wertbeimessung willkürlich. Hinzu kommt die unklare Governance und die weiterhin bestehende Möglichkeit, diese Krypto-Token anonym oder pseudoanonym zu verwenden. Ohne grundsätzliche Änderungen der Algorithmen und Transaktionsformen dürfte eine legale Verwendung als Zahlungsmittel ausgeschlossen bleiben.

4. Stablecoins

29 Um dem Manko der mangelnden Wertstabilität zu begegnen, wurden sog. Stablecoins[18] geschaffen. Sie entwickelten sich rasch zu einem signifikanten Marktsegment innerhalb der Welt der Krypto-Token.[19] Ziel war die Stabilisierung des Wertes. Für diese Stabilisierung gibt es potenziell drei Verfahren. Das erste ist

17 Vgl. Bundesbank, Krypto-Token im Zahlungsverkehr und in der Wertpapierabwicklung, S. 39–59; *Balz/Paulick*, Parallelwährungen jenseits der Finanzaufsicht: Haben Bitcoin und Libra eine Zukunft?, S. 13–16.

18 Vgl. *Buterin*, The Search for a Stable Cryptocurrency, 2014, Ethereum Blog, November 11, 2014, https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/ (zuletzt abgerufen am 18.12.2020).

19 Vgl. *Hileman*, The State of Stablecoins, 2018, available at SSRN: https://ssrn.com/abstract=3472568 or http://dx.doi.org/10.2139/ssrn.3472568.

die sog. algorithmische Stabilisierung, die einen Mechanismus vorsieht, nach dem der Wert des betreffenden Krypto-Tokens mehr oder weniger automatisch stabilisiert wird durch Markteingriffe. Im Kern läuft dies darauf hinaus, dass in Phasen steigender Bewertung Krypto-Token verkauft oder zusätzlich geschaffen werden, während in Schwächephasen Krypto-Token gekauft oder vom Markt genommen werden. Es bedarf dabei einer zahlungskräftigen Entität, die glaubhaft eine solche Preisstabilisierung auch durchsetzt. Ein Problem des Konzeptes liegt in der Frage, an welchem Maß die Wertstabilität gemessen wird. Ein schwerwiegenderes praktisches Problem war die Bestimmung des Mechanismus zur operativen Steuerung der Token-Menge, insbesondere die Finanzierung in Phasen schwacher Wertentwicklung.

30 Das zweite und dritte Stabilisierungsverfahren für Stablecoins lösten beide Probleme durch externe Wertorientierung. Der Wert des Tokens wurde gemessen am Wert anderer Objekte stabilisiert bzw. an diesen externen Wert gebunden. Damit das glaubwürdig war und operativ unterstützt werden konnte, sollten die Krypto-Token durch entsprechende Werte besichert werden. Im zweiten Verfahren erfolgte die Besicherung durch andere Krypto-Token, weshalb es Online-Verfahren genannt wurde. Im dritten Verfahren erfolgte die Bindung des Wertes an externe Werte, die nicht dezentral gehandelt wurden. Dies wird als Offline-Verfahren bezeichnet. Vorgeschlagen wurden Rohstoffe und Zentralbankwährungen. Auch die Besicherung erfolgte dann idealerweise durch einen Fonds der zugrunde gelegten Rohstoffe oder durch Zentralbankgeld. Die Stabilisierung war umso glaubwürdiger, je transparenter und unabhängiger vom Vertreiber des Krypto-Tokens die Besicherung erfolgte.

31 Allein das Offline-Verfahren hat sich in der Praxis durchgesetzt und dabei vor allem die Besicherung mit realem Geld. Dadurch orientieren sich Stablecoins zumeist am Wert einer Zentralbankwährung. Denkbar sind zwei Formen: einmal die Besicherung mit Geschäftsbankengeld und zum anderen die Besicherung mit Zentralbankgeld. Im ersten Fall besichert der Herausgeber der Stablecoins diese mit Einlagen bei Geschäftsbanken oder Schuldverschreibungen, die Forderungen an Geschäftsbanken darstellen. Auch im Falle der Besicherung durch Staatsanleihen bliebe der Stablecoin im Risiko auf dem Niveau von Geschäftsbankengeld. Seine Verwendung für die Abwicklung großer Beträge wäre risikobehaftet. Im zweiten Fall besichert der Herausgeber die Stablecoins mit Forderungen an eine Zentralbank. Dazu müsste der Herausgeber über ein Zentralbankkonto verfügen, auf dem ein Guthaben als Deckungsfonds gehalten wird. Ein solches Konstrukt ist derzeit noch nicht am Markt aktiv. Abgesehen von der konkreten Rechtskonstruktion, also den Verfügungsberechtigungen über das Guthaben, ist es umstritten, inwieweit ein so besicherter Stablecoin tatsächlich Eigenschaften des Zentralbankgeldes annehmen könnte oder ob er nicht doch Geschäftsbankengeld bliebe. Für die Zentralbanken birgt dieses Konstrukt das Re-

putationsrisiko, im Falle von operativen oder sonstigen Problemen mit in die Verantwortung gezogen zu werden. Zudem verlieren sie den direkten analytischen Zugriff auf wichtige Zahlungsvorgänge, die unter Umständen auch ein schnelles Eingreifen zur Sicherung der Systemliquidität erfordern können. Es droht die Gefahr, dass der systemrelevante Zahlungsverkehr in sog. synthetischem Zentralbankgeld[20] vor den Toren der Zentralbank erfolgt.

32 Unabhängig vom Netzwerk, in dem Stablecoins genutzt werden, sind mehrere Formen denkbar, in denen diese Form von Zahlungsmitteln rechtlich gestaltet werden kann, vorausgesetzt, dass die Stablecoins von einer verantwortlichen persönlichen oder juristischen Person herausgegeben werden. Nach derzeitigem europäischem Recht könnte es sich beim Herausgeber eines Stablecoins um ein E-Geld-Institut handeln. Dann müssten freilich die Rückzahlungsansprüche der Nutzer garantiert sein und weitere Forderungen der E-Geld-Richtlinie erfüllt werden. Es ist ebenso denkbar, dass Stablecoins als Geldmarktfonds organisiert werden, dann unterliegen sie dem entsprechenden Wertpapierrecht. Nicht zuletzt könnte das verwendete digitale Geld auch eine Verbindlichkeit für das emittierende Institut darstellen. Dann jedoch wäre der Emittent eine Bank, und es handelte sich um digitales Geschäftsbankengeld. Um die Herausgabe von Stablecoins in der Europäischen Union neu zu regeln, ist eine neue Verordnung zu „Markets in Crypto-assets" in Vorbereitung.[21] Stablecoins von dezentralen Netzwerken, die ohne Haftungs- und Rücknahmerechte begeben werden, sind dagegen im regulierten Finanzsektor als Zahlungsmittel nicht legalisierbar. Für die weitere Betrachtung der Einsetzbarkeit für programmierbare Zahlungen werden Stablecoins nur in der Form eines digitalen Geschäftsbankengeldes betrachtet.

IV. Optionen für das Angebot an programmierbaren Zahlungen

33 Um die Vorteile der neuen Abwicklungstechniken nutzbar zu machen, bedarf es also programmierbaren Geldes oder zumindest programmierbarer Zahlungsverfahren. Dafür stehen verschiedene Optionen zur Verfügung.[22] Tabelle 1 zeigt die Optionen im Überblick in einer Reihung mit zunehmender Beteiligung der Zentralbank daran. Im Folgenden wird als erstes eine Brückentechnologie zwischen dem neuen Geschäftsabwicklungssystem und dem konventionellen Zahlungsverkehr erörtert, die sog. Trigger-Anwendung. Die Krypto-Token oder Stable-

20 Vgl. *Adrian/Mancini-Griffoli*, The rise of digital money.

21 Vgl. https://ec.europa.eu/digital-single-market/en/legal-and-regulatory-framework-blockchain.

22 Vgl. *Balz/Diehl/Winter*, Digitales Geld: Welche Optionen hat Europa?

coins, die in dezentralen Netzwerken geschaffen werden, kommen nur in einer legalisierten Variante infrage, werden also unter digitalem Geschäftsbankengeld subsumiert. Hinzu kommt noch digitales Zentralbankgeld, und zwar entweder für einen begrenzten Nutzerkreis oder für jedermann.

Tab. 1: Optionen für programmierbare Zahlungen

Name	**Beispiel**	**Stabilität**	**Forderung**
Krypto-Token	Bitcoin, Ether	Extrem volatil	Nein
Stablecoin gedeckt in Geschäftsbankengeld	Tether, Projekt Diem	Bindung an echte Währung	Nein
Digitales Geschäftsbankengeld	JP Morgan Coin	Wie echte Währung	An Geschäftsbank
Trigger-Anwendung an Geschäftsbank	Diverse Projekte	Wie echte Währung	An Geschäftsbank
Stablecoin gedeckt in Zentralbankgeld	Noch nicht existent	Wie echte Währung	An Zentralbank?
Trigger-Anwendung an Zentralbank	Trigger-Projekt der Bundesbank	Echte Währung	An Zentralbank
Digitales Zentralbankengeld	Sand Dollar (Bahamas)	Echte Währung	An Zentralbank

1. Brückentechnologie zwischen DLT und konventionellem Zahlungsverkehr

Verschiedene Institutionen arbeiten daran, eine Brückentechnologie zu entwickeln, die zwischen einem Geschäftsabwicklungssystem auf Basis der DLT und dem konventionellen Zahlungssystem gebaut wird. Eine einheitliche Technik hat sich noch nicht durchgesetzt. Im Folgenden wird die von der Bundesbank favorisierte Abwicklung, die eine Verbindung zwischen DLT und TARGET2 schaffen soll, exemplarisch beschrieben. **34**

Bei einer DLT-basierten Abwicklung von Geschäften stehen im einfachsten Fall ein Asset Token, der das digitalisierte Gut repräsentiert, und ein Geld-Token zur Verfügung. In der Brückentechnologie wird der Geld-Token durch eine Zahlungsanweisung substituiert. Sobald alle Bedingungen für den Leistungs- oder Warenübergang erfüllt sind, blockiert der Smart Contract, der wie ein virtueller Treuhänder agiert, den Asset Token und initiiert („triggert“) eine Zahlung über den konventionellen Zahlungsverkehr. Wegen dieser Auslösefunktion wird die Technologie auch „Trigger-Anwendung“ genannt. Die Zahlungsanweisung wird direkt zu einem Netzwerk gesandt, das von einer Finanzmarktinfrastruktur betrieben wird (hier Bundesbank). In diesem Netzwerk sind die Banken der han- **35**

delnden Unternehmer vertreten und der Betreiber. Die Zahlungsanweisung wird von der Bank des Zahlungspflichtigen signiert und darauf im Zahlungssystem abgewickelt. Sobald der Geldübergang erfolgt ist, signiert der Betreiber des Zahlungssystems eine Zahlungsbestätigung und sendet diese an das auslösende Netzwerk der DLT-basierten Abwicklung zurück. Daraufhin wird der Asset Token an den Käufer gesandt und das Geschäft ist geld- und warenseitig abgewickelt. Der Geld-Token wird also durch eine tokenisierte signierte Zahlungsbestätigung ersetzt. Die geldseitige Abwicklung des Geschäftes kann entweder in Geschäftsbankengeld oder in Zentralbankgeld erfolgen. Im ersten Fall müsste die DLT mit einem Clearinghaus der Geschäftsbanken verbunden werden, im zweiten Fall mit TARGET2 oder TIPS (Target Instant Payment Settlement).

36 Diese Trigger-Anwendung dürfte sich vor allem für Abwicklungen von Großbeträgen eignen, da sie technische und organisatorische Voraussetzungen für die Beteiligten mit sich bringt. Die Beteiligten müssen Teilnehmer der virtuellen Netzwerke werden, also einen Knoten betreiben, und in der Lage sein, technische Nachrichten zu verarbeiten. Für den Zahlungsverkehr von Privathaushalten dürfte sich dieses Verfahren bestenfalls indirekt, also unter Einschaltung von Intermediären, eignen.

37 Trigger-Anwendungen ließen die bestehende Arbeitsteilung zwischen Zentralbank und Geschäftsbanken praktisch unverändert. Es könnte in Zentralbankgeld zu den derzeitigen Bedingungen abgewickelt werden, ohne tokenisiertes Zentralbankgeld zu schaffen. Insbesondere müsste der Zugang zu Zentralbankgeld nicht erweitert werden. Das bestehende Zahlungssystem könnte fast unverändert weiter genutzt werden, es müssten nur neue Schnittstellen programmiert werden. Der Zeit- und Ressourcenaufwand für die Entwicklung der Brückentechnologie wird daher im Vergleich zu neuen Netzwerken für digitale Geld-Token als relativ gering eingeschätzt.

2. Programmierbares Geschäftsbankengeld

38 Geschäftsbanken könnten für ihre Kunden Geld auch in tokenisierter Form zur Verfügung stellen. Dies könnte technisch analog zu den Netzwerken von Krypto-Token erfolgen, freilich mit belastbarer Betreiberverantwortung und einem Token, der als Verbindlichkeit der emittierenden Geschäftsbank gilt. Das Grundprinzip bliebe jedoch gleich.[23] Banken könnten diese neue Form von Geschäftsbankengeld, das auf die offizielle Währung lautet, im Tausch für Kontoguthaben

23 Vgl. *Ludwin*, Why Central Banks Will Issue Digital Currency, 2016, Speech at the Federal Reserve Conference in Washington D.C., 1.6.2016, http://blog.chain.com/post/145509298356/why-central-banks-will-issue-digital-currency. *Ludwin* erläutert darin, wie Geschäftsbanken digitales Geschäftsbankengeld schaffen könnten und wie Zentralbanken digitales Zentralbankgeld schaffen könnten.

und/oder Bargeld herausgeben. Einige Banken haben Prototypen von digitalem Geschäftsbankengeld entwickelt. Bekannt geworden ist der JP Morgen Coin, der allerdings nicht für die Nutzung durch Privathaushalte gedacht war. In einigen Jurisdiktionen betreiben private Konsortien Projekte zur Emission von privatem digitalen Geld.[24]

39 Rechtlich hätten die Kunden wie heute bei ihren Kontoguthaben eine Forderung gegenüber der herausgebenden Geschäftsbank. Darin liegt freilich das Problem, dass dies den Nutzen für Kunden einschränken könnte. Im konventionellen Zahlungsverkehr zahlt der Kunde einer Geschäftsbank aus seinem Konto und reduziert damit seine Forderungen an die Geschäftsbank seines Vertrauens. Der Begünstigte erhält eine Gutschrift auf seinem Konto, möglicherweise bei einer anderen Geschäftsbank, eben der Geschäftsbank seines Vertrauens. Dies wird ermöglicht durch die Einschaltung von Clearinghäusern, welche die verschiedenen Forderungen und Verbindlichkeiten der Geschäftsbanken miteinander verrechnen und die Zahlung des Spitzenbetrages von dem Nettoschuldner an den Nettogläubiger in Zentralbankgeld über ein RTGS-System veranlassen. Tokenisiertes Geschäftsbankengeld sollte allerdings auch zur direkten Nutzung für P2P-Transaktionen bzw. für Transaktionen zwischen Unternehmen und Privathaushalten nutzbar sein. Dabei erhielte aber der Zahlungsempfänger eine Forderung an eine Geschäftsbank, die nicht zwingend die Bank seines Vertrauens ist. Sofern es sich um größere Beträge handelt, die auch von der Einlagensicherung nicht erfasst sind, ist damit ein Risiko verbunden, das der Zahlungsempfänger vor dem Geschäft nicht eingehen wollte. Nur für den Fall, dass Zahlungspflichtiger und Zahlungsempfänger ihr Konto bei derselben Geschäftsbank führen, wäre das Risiko ausgeschaltet. In praktischer Hinsicht wäre jedoch tokenisiertes Geschäftsbankengeld von besonderem Nutzen, wenn Zahlungen mit diesem Token von allen Geschäftsbanken eines Währungsraums akzeptiert würden.

40 Für Privathaushalte und bei den üblichen kleineren Zahlbeträgen dürfte die bestehende Einlagenversicherung, die Kontoguthaben bis zu 100.000 EUR pro Institut absichert, ausreichend Sicherheit bieten. Generell könnte das Risiko durch ein System mit häufigem untertägigem Clearing und anschließendem Begleichen der Nettoforderung in Zentralbankgeld reduziert werden. Inwieweit eine Einbeziehung in die bisherigen Clearing-Strukturen sinnvoll ist, wäre nicht zuletzt unter Kosten- und Aufsichtsgesichtspunkten zu erörtern.[25] Es wäre auch

24 Vgl. *Auer* et al., Taking stock: ongoing retail CBDC projects. So gibt es in Westafrika eine eCFA-Initiative sowie auf den Marshall-Inseln, die formal keine Zentralbank haben, ebenso eine private Initiative.

25 Vgl. *Adrian*, Stablecoins, Central Bank Digital Currencies, and Cross-Border Payments: A New Look at the International Monetary System, 2019, Remarks by *Tobias Adrian* at the IMF-Swiss National Bank Conference, May 2019, https://www.imf.org/en/News/Articles/2019/05/13/sp051419-stablecoins-central-bank-digital-currencies-and-cross-border-payments (zuletzt abgerufen am 27.11.2020).

denkbar, dass die Geschäftsbanken eine rechtliche Konstruktion entwickeln, die es erlaubt, die mit dem Token verbundene Forderung nicht gegenüber einzelnen Geschäftsbanken geltend zu machen, sondern zum Beispiel gegenüber einer gemeinsamen rechtlichen Einheit. Dazu wäre die Gründung einer Zweckgesellschaft denkbar, ähnlich anderen Abwicklungsstrukturen, etwa bei Kartenzahlungen. Die entscheidende Herausforderung bei tokenisiertem Geschäftsbankengeld ist so gesehen der hohe Koordinationsaufwand, der damit für die Geschäftsbanken verbunden ist. Die Wettbewerber im Euroraum müssten sich zu einer neuartigen und weitreichenden Kooperation zusammenfinden. Die Hürde der notwendigen einheitlichen technischen Standards, um eine allgemeine Akzeptanz dieses neuen Geldtyps und eine breite Anwendbarkeit sicherzustellen, erscheint dagegen leichter überwindbar.

3. Programmierbares Zentralbankgeld

41 Zentralbankgeld unterscheidet sich von Geschäftsbankengeld dadurch, dass die Forderung gegenüber der ausfallsicheren Zentralbank besteht. Digitales, programmierbares Zentralbankgeld wäre neben Bargeld und Kontoguthaben von Geschäftsbanken bei der Zentralbank eine zusätzliche Form von Zentralbankgeld.

a) Begrifflichkeiten

42 In der allgemeinen Diskussion hat sich der Begriff Central Bank Digital Currency (CBDC) durchgesetzt, obwohl damit die Eigenschaften des neuen Geldtyps nicht klar umrissen sind. Digital sind die Guthaben bei Zentralbanken heute schon, und sie werden digital in RTGS-Systemen transferiert. Gemeint ist gleichwohl eine neue Geldform, die inspiriert ist von Krypto-Token und den Möglichkeiten der neuen Technologie. Teilweise orientieren sich die Entwickler an den Möglichkeiten der dezentralen Netzwerke und streben P2P-Übertragungen an, teilweise orientieren sie sich an den Chancen der DLT als Abwicklungstechnologie und streben Programmierbarkeit an. Eine weitere Unterscheidung ist die in tokenbasierten oder kontenbasierten Varianten.[26] Die Unterscheidung hat mit der Übertragung des Geldes zu tun. Bei Token, die man praktisch mit Inhaberpapieren vergleichen kann, muss die Echtheit des Tokens geprüft werden. Bei einem kontenbasierten System muss die Identität des Kontoinhabers bzw. desjenigen, der die Zahlung veranlasst, geprüft werden. Grundsätzlich bietet also eine tokenisierte Variante eher die Möglichkeit anonymer Transaktionen. Bei Nutzung der DLT ist allerdings die Anonymität nicht zwingend, da eine digitale Übertragung in einem Netzwerk digitale Spuren hinterlässt, kann die Ano-

26 Vgl. *Kahn*, How are payment accounts special?

nymität eines Tokens sehr wohl eingeschränkt werden, ist also nicht eins zu eins mit Bargeld zu vergleichen.

Analog zu Krypto-Token, die nicht durch Smart Contracts nutzbar sind, ist nicht jeder Token programmierbar. Die einfache Variante wäre tokenisiertes CBDC. Die weitergehende Variante, die auch die Nutzung der Möglichkeiten der neuen Technologie bietet, wäre dann programmierbares Zentralbankgeld bzw. digitales Zentralbankgeld in programmierbaren Zahlungsverfahren. Die bezogen auf die volkswirtschaftlichen Implikationen vermutlich wichtigste Unterscheidung ist die nach den Zugangsberechtigungen. Einmal wird über digitales Zentralbankgeld gesprochen, das nur einem begrenzten Kreis von Nutzern, meist sind die Institute gemeint, die auch heute Konten bei der Zentralbank führen dürfen, zur Verfügung stehen soll. Zum anderen wird über digitales Zentralbankgeld gesprochen, das allen heutigen Nutzern des Bargeldes – also Geschäftsbanken, Unternehmen und Privatpersonen – zur Verfügung stehen soll. Die erste Variante wird auch als Wholesale-CBDC, die zweite als Retail-CBDC bezeichnet. Gegenwärtig arbeiten mehrere Dutzend Zentralbanken an Projekten zur Erprobung bis hin zur Realisierung von digitalem Zentralbankgeld.[27] Eine kleine Gruppe testet dabei Modelle zur Emission von Wholesale-CBDC, die große Mehrheit testet Varianten zum Retail-CBDC. Einige testen beide Varianten. **43**

b) Wholesale-CBDC

Mit Wholesale-CBDC, bei dem digitales Zentralbankgeld nur einer begrenzten Nutzergruppe zur Verfügung gestellt wird, könnte die heutige Verwendung des Zentralbankgeldes weitgehend beibehalten werden. Daher gelten die volkswirtschaftlichen Implikationen als beherrschbar und überschaubar. Im gegenwärtigen Geldsystem gibt es leicht vereinfacht dargestellt drei Akteure: Zentralbank, Geschäftsbank, Nicht-Bank. Die Zentralbank emittiert Zentralbankengeld in barer und unbarer Form an die Geschäftsbanken. Die Geschäftsbanken nutzen Zentralbankgeld für die Transaktionen großer Beträge untereinander, zum Beispiel in der Abwicklung von Finanzmarkttransaktionen. Sie schöpfen Geschäftsbankengeld und bieten das Depositengeschäft für Nicht-Banken an. Nicht-Banken erhalten Kredite von Geschäftsbanken und können ihre Depositen in bar abheben. Bargeld ist die einzige Form des Zentralbankgeldes, das Nicht-Banken zur Verfügung steht. Den Geschäftsbanken sind die meisten Finanzgeschäfte vorbehalten, da sie einer entsprechenden Regulierung und Überwachung unterliegen. **44**

Die Emission von Wholesale-CBDC, das nur an Geschäftsbanken ausgegeben würde, ließe das Finanzsystem in seiner Grundkonstruktion unverändert. Aus **45**

27 Vgl. *Auer* et al., Rise of the central bank digital currencies: drivers, approaches and technologies; *Auer* et al., Taking stock: ongoing retail CBDC projects.

geldpolitischer und finanzstabilitätspolitischer Sicht sollten ceteris paribus keine signifikanten Risiken durch eine neue Geldform resultieren.

46 Der Begriff des Wholesale-Geschäftes wird jedoch in Geschäftsbankenkreisen anders verstanden als in der Zentralbank. In Geschäftsbanken ist der Wholesale-Begriff über das Geschäftsvolumen und die Art der Geschäfte eines Geschäftspartners definiert. Kunden, die größere Transaktionen abwickeln und Geschäfte tätigen, die ein stärker ausgebautes professionelles Finanzmanagement erfordern, werden als Wholesale-Kunden bezeichnet und anders behandelt. Privatleute und kleinere Unternehmen zählen dagegen zum Retail-Geschäft.

47 In der Tat gibt es zahlreiche Unternehmen, die formal Nicht-Banken sind, deren Finanztransaktionen aber hinsichtlich Volumen und Diversität die Aktivitäten einiger Banken deutlich übersteigen. Diese Unternehmen könnten im besonderen Maße von den Möglichkeiten der neuen Technologien profitieren, wären aber bei der Wholesale-Variante des digitalen Zentralbankgeldes ausgeschlossen. Sie könnten sich nur in Zusammenarbeit mit einer Bank an entsprechenden Abwicklungssystemen beteiligen. Daher ist zu überlegen, ob die Weitergabe von digitalem Zentralbankgeld durch Banken an Unternehmen in engen Grenzen erwogen werden könnte. Ob dies als eine neue technische Form von Geschäftsbankengeld geschehen würde, das nur teilweise von Zentralbankgeld gedeckt ist, oder vollgedeckt nur an bestimmte Nutzer weitergegeben würde, wären zwei zu prüfende Optionen. In jedem Fall müsste sichergestellt werden, dass dies keine negativen Auswirkungen auf die Geldpolitik hätte. Dabei könnte man sich an den Erfahrungen einiger Zentralbanken (auch der Bundesbank) orientieren, die auch in jüngerer Zeit Konten für bestimmte Wirtschaftsunternehmen, die nicht Banken waren, geführt haben.

48 Aus Zentralbanksicht hätte digitales Zentralbankgeld in der Wholesale-Variante den Vorteil, dass die Struktur des zweistufigen Bankensystems nicht grundsätzlich in Frage gestellt würde. Zu klären bliebe, in welcher Form die Banken Digitales Zentralbankgeld an welche Kunden weitergeben würden. Möglicherweise könnte die Weitergabe zunächst auf solche Unternehmen begrenzt werden, die es benötigen, um damit DLT-basierte Anwendungen friktionslos betreiben zu können.

c) Retail-CBDC

49 Unter Retail-CBDC wird digitales Zentralbankgeld verstanden, das für alle Wirtschaftssubjekte zur Verfügung steht. Bislang können die meisten Wirtschaftssubjekte Zentralbankgeld nur in Form des Bargeldes nutzen. Es mag sein, dass daher auch das Bestreben kommt, CBDC mit bargeldähnlichen Funktionalitäten auszustatten. Die Verwendung von Bargeld als Zahlungsmittel geht in den großen Volkswirtschaften tendenziell seit einigen Jahrzehnten zurück.

Selbst in den Ländern, die als intensivere Bargeldnutzer gelten, wie Deutschland oder Österreich, spielt Bargeld nur noch eine untergeordnete Rolle. Allein am Point of Sale, also an den Kassen des Handels, werden stückmäßig noch die meisten Transaktionen in bar abgewickelt. Wertmäßig ist das auch dort nicht mehr der Fall. Berücksichtigt man, dass die am Point of Sale abgewickelten Transaktionen gemessen an allen Transaktionen einer Volkswirtschaft eher weniger bedeutend sind, wird klar, dass die Bedeutung des Bargeldes eher gering ist. Gleichwohl kommt Bargeld eine hohe emotionale Bedeutung zu. Diese dürfte sich weniger aus der Eigenschaft des Zentralbankgeldes speisen, sondern mehr noch aus der Fähigkeit, mit Bargeld einfach, bequem und anonym bezahlen zu können. Die Unterscheidung zwischen Zentralbankgeld und Geschäftsbankengeld ist nur von handlungsleitender Bedeutung im Falle einer krisenhaften Zuspitzung im Finanzsektor, die zur Flucht in das Bargeld führen kann zulasten von Bankeinlagen. In manchen Ländern ist Bargeld von elektronischen Zahlungsmitteln soweit verdrängt worden, dass es regional nur erschwert noch zu beziehen ist bzw. nur unter Bedingungen angenommen wird. Daher wird als Motiv für CBDC oft genannt, den Bürgern auch bei abnehmender Bedeutung des Bargeldes eine Form von Zentralbankgeld anzubieten.

50 Auch die Diskussion im Euroraum konzentriert sich inzwischen wie in den meisten der bedeutenderen Währungsräume auf digitales Zentralbankgeld in der sog. Retail-Variante. Im Bericht der High Level Task Force des Eurosystems zum Digitalen Euro vom 2.10.2020 wurden die Fragen aufgeworfen, unter welchen Umständen und in welchen denkbaren Ausprägungen der Allgemeinheit digitales Zentralbankgeld angeboten werden könnte.[28] Dabei werden als mögliche Motivation auch solche Szenarien ins Feld geführt, die unter anderem das Ziel haben, für Bürgerinnen und Bürger den Zugang zu ausfallsicherem Zentralbankgeld sicherzustellen, sollte Bargeld kaum noch genutzt werden. Allerdings bekennt sich das Eurosystem weiterhin zur Ausgabe von Bargeld, solange eine Nachfrage danach existiert. Ein anderes Szenario begründet die Notwendigkeit einer europäischen Alternative zu privatwirtschaftlich angebotenen Stablecoins oder dem digitalen Zentralbankgeld anderer Zentralbanken. Angesichts dieser Szenarien ist es wichtig, dass das Eurosystem sich analytisch, technisch und organisatorisch mit der möglichen Emission digitalen Zentralbankgeldes befasst, um gegebenenfalls vorbereitet zu sein.

51 Die Sicherstellung des Zugangs zu Zentralbankgeld in Zeiten abnehmender Bargeldnutzung ist jedoch ein Ziel, das wenig zu tun hat mit den Möglichkeiten der neuen Technologien oder den Chancen programmierbarer Zahlungen an sich. Genau genommen ist es eher eine neue Variante der Debatte um Vollgeld, die

28 Vgl. ECB, Report on a digital Euro, 2020, https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (zuletzt abgerufen am 19.12.2020).

seit den 1930er Jahren geführt wird.[29] Einen einfachen Zugang zu digitalem Zentralbankgeld hätte man durch Kontoführung bei der Zentralbank auch vor DLT gewähren können. Bislang hat man sich grundsätzlich für das zweistufige Bankensystem mit einem beschränkten Zugang zu Zentralbankgeld in unbarer Form entschieden.

52 Digitales Zentralbankgeld als Retail-CBDC wäre unter allen Formen digitalen Geldes die weitestgehende Variante mit den mutmaßlich gravierendsten Implikationen.[30] Die Implikationen sind zu erwarten, wenn Retail-CBDC eine breite Verwendung im Zahlungsverkehr und möglicherweise auch in der Wertaufbewahrung erlangt und damit die heute dominierenden Einlagen bei Geschäftsbanken verdrängt. Eine hohe Akzeptanz ist naturgemäß das Ziel bei der Einführung einer neuen Geldform. Wenn sie der Bevölkerung auf breiter Basis Zugang zu Zentralbankgeld, gleichsam als Substitut für Bargeld, gewähren soll, muss sie auf breite Akzeptanz ausgelegt sein, also einfach und kommod in der Nutzung, technisch sicher und in den Kosten günstig, wenn nicht gar kostenlos für den gängigen funktionalen Bedarf der Privathaushalte. Einfach gesprochen: Retail-CBDC müsste so einfach und günstig wie Bargeld werden. Wenn das gelänge und gleichzeitig die technische Übertragung in einem von den Zentralbanken betriebenen oder beaufsichtigten Netzwerk mindestens so sicher erfolgte wie im heutigen Giro-System, dürfte sich Retail-CBDC als die überlegene Geldform am Markt durchsetzen. Die höhere Ausfallsicherheit als Geschäftsbankengeld weist es ohnehin auf. Der Schritt von der Nutzung des Retail-CBDC für Transaktionszwecke zur Nutzung als Wertaufbewahrungsmittel ist dann nicht weit. Daher kann in diesem Fall ceteris paribus mit einer weitreichenden Substitution heutiger Sicht- und Spareinlagen bei Geschäftsbanken durch Retail-CBDC gerechnet werden. Selbst die Bargeldhortung, die dem Diebstahl- und Verlustrisiko unterliegt, könnte teilweise zugunsten von Retail-CBDC aufgelöst werden.

53 Eine solche Substitution brächte erhebliche Veränderungen für den Finanzsektor mit sich. Wie genau es sich verändern würde, hängt nicht zuletzt von den Reaktionen und Handlungsoptionen der Finanzinstitute und der Zentralbank ab. Klar ist, dass praktisch alle wichtigen Retail-Geschäftsbereiche der Banken dramatische Veränderungen erfahren würden. Dies gilt naturgemäß zuerst für die Rolle der Finanzdienstleister im Zahlungsverkehr; darüber hinaus für das Einlagenge-

29 Vgl. *Hellwig*, Bargeld, Giralgeld, Vollgeld: Zur Diskussion um das Geldwesen nach der Finanzkrise, 2018, Vortrag auf dem Bargeldsymposium der Deutschen Bundesbank 14.2.2018, https://www.bundesbank.de/resource/blob/723728/1bad30182ce1b8b4162c37a736c33f8c/mL/bargeldsymposium-2018-hellwig-data.pdf (zuletzt abgerufen am 19.12.2020).

30 Vgl. zu den in der Literatur diskutierten Implikationen *Carapella/Flemming*, Central Bank Digital Currency: A Literature Review, 2020, FEDS Notes, November 09, 2020, https://www.federalreserve.gov/econres/notes/feds-notes/central-bank-digital-currency-a-literature-review-20201109.htm (zuletzt abgerufen am 11.11.2020).

schäft, bei dem die Banken gegen Retail-CBDC konkurrieren müssten. Die Art der Refinanzierung der Banken könnte sich ändern sowie auch die Refinanzierungskosten. Weiterhin wäre die Zentralbank direkt betroffen. Die geldpolitische Steuerung müsste umgestellt werden, wäre eventuell bei Retail-CBDC sogar direkter und wirkungsvoller. Die Auswirkungen auf die Finanzstabilität hängen von der neuen Bilanzstruktur der Geschäftsbanken ab. Im Falle einer Finanzkrise könnte die Existenz von Retail-CBDC allerdings einen potenziellen Bank-Run beschleunigen, da der Wechsel von Einlagen bei Geschäftsbanken zu Zentralbankgeld jederzeit und schneller möglich ist als heute mit Bargeld. Kurzum, Retail-CBDC könnte je nach Ausgestaltung umfassende Implikationen für das ganze Finanzsystem bewirken. Vor einer Einführung von Retail-CBDC müssen deshalb belastbare Analysen erfolgen. Es gilt zweierlei zu zeigen: erstens, dass und wie auch mit Retail-CBDC ein stabiles Gleichgewicht im Finanzsystem erreicht werden kann und zweitens, dass auch im Übergang von der gegenwärtigen Lage zum neuen Gleichgewicht keine unbeherrschbaren Risiken auftreten.

Parallel zu der Frage, ob und warum Retail-CBDC eingeführt werden sollte und wie die damit verbundenen Risiken zu beherrschen sind, ist zu prüfen, wie es ausgestaltet werden müsste, um attraktiv für die Nutzung in allen denkbaren Situationen des alltäglichen Zahlungsverkehrs zu sein, ohne die Funktionsfähigkeit des Finanzsektors signifikant zu beeinträchtigen und die Aktivität der Zentralbank über Gebühr, zulasten des Wettbewerbs und Geschäftsmodells privater Anbieter, auszuweiten.[31] **54**

Daneben stellen sich viele technische Fragen der Umsetzung, die derzeit in zahlreichen Experimenten erprobt werden. Dazu gehören neben der Wahl der technischen Basis die Fragen, ob token- oder kontenbasiert, ob verzinst oder unverzinst, wenn verzinst, ob potenziell auch negativ verzinst, ob kostenlos oder gebührenpflichtig, ob frei in der Nutzung oder beschränkt, ob nur für nationale oder auch für internationale Nutzung und so weiter. Praktisch alle diese Fragen sind noch offen, ihre Implikationen nicht voll erfasst.[32] **55**

Gerade die letzte Frage einer Emission von Retail-CBDC auch für die internationale Nutzung birgt in sich große Implikationen. Emittierte eine Zentralbank Retail-CBDC, das nur von Inländern genutzt werden dürfte, wäre es de facto für internationale Transaktionen nicht nutzbar und damit sogar weniger nutzbar als Bargeld. Gerade die Wirtschaft müsste angesichts des hohen Grades der internationalen Verflechtung auf eine internationale Nutzbarkeit bestehen. Wenn allerdings auch Personen anderer Währungsräume Retail-CBDC der heimischen Währung halten und nutzen dürfen, könnte dies mutatis mutandis ganz neue Dimensionen der Währungskonkurrenz einläuten. Eine einseitige Einführung von **56**

31 Vgl. *Auer* et al., Rise of the central bank digital currencies: drivers, approaches and technologies, 2020, BIS working paper No. 880, August 2020.

32 *Armelius* et al., E-krona design models: pros, cons and trade-offs.

attraktivem Retail-CBDC könnte zu einer starken Nachfrage nach heimischer Währung führen, also eine Aufwertung bewirken und die Bilanz der Zentralbank erheblich ausweiten. Ein intensiv diskutierter Aspekt ist die Frage nach Nutzungsbeschränkungen. Um die Auswirkungen auf den Finanzsektor gering zu halten, könnte man Nutzungsbeschränkungen einführen, sodass beispielsweise die Bürger nur eine bestimmte Summe an Retail-CBDC halten dürfen und darüber hinausgehende Beträge schlechter verzinst würden. Solche Nutzungsbeschränkungen sind denkbar.[33] Sie erinnern jedoch eher an ein stärker technokratisches Verständnis von Finanzen. Geld, dessen Nutzung in sich komplex ausgestaltet ist, dürfte zusätzliche Friktionen und Kosten verursachen, die wohlfahrtsmindernd wirken.

57 Die Beantwortung der Fragen zur Ausgestaltung wird erschwert durch die unklare Zielformulierung, ob es eher um Bargeldsubstitution, um Programmierbarkeit, um Tokenisierung, um P2P-Transaktionen, um Vollgeld oder um andere Ziele geht. Je nachdem, welches Ziel konkret mit CBDC erreicht werden soll, müssten andere Gestaltungsoptionen gewählt werden. Daher muss die Frage des „Wie" der Frage des „Warum" untergeordnet werden.

58 Konkret gibt es zwar eine Handvoll Retail-CBDC-Pilotprojekte, aber noch keine einheitliche Sicht auf die Gestaltungsvariationen.[34] Realisiert ist der Retail-CBDC allein auf den Bahamas mit dem Sand Dollar.[35] Die dortige Zentralbank verfolgt, ähnlich wie die Eastern Caribbean Central Bank mit einem ebenfalls sehr weit fortgeschrittenen Projekt,[36] das Ziel einer besseren Anbindung der heimischen Wirtschaft, die über viele kleine Inseln verstreut ist, an das internationale Finanzsystem. Unter den größeren Währungsräumen ragt das Pilotprojekt der People's Bank of China (PBoC) heraus.[37] Seit 2014 arbeitet eine Arbeitsgruppe der PBoC zusammen mit Experten des Privatsektors an einer digitalen Variante des Yuan. Ziel ist die vollständige Digitalisierung des Zahlungsverkehrs, die eine leichtere Überwachung und Steuerung des Finanzsektors und der gesamten Wirtschaft ermöglicht. Ziel sollte die Einführung zu den Olympischen Winterspielen im Jahr 2022 in Peking sein. Die lange Entwicklungsphase trotz intensi-

33 Zum Beispiel durch Limite oder eine gestaffelte Verzinsung. Vgl. *Auer* et al., Rise of the central bank digital currencies: drivers, approaches and technologies*; Bindseil*, Tiered CBDC and the financial system.

34 Vgl. *Auer/Böhme*, The technology of retail central bank digital currency.

35 Vgl. Central Bank of the Bahamas, Project Sand Dollar: A Bahamas Payments System Modernisation Initiative.

36 Vgl. Eastern Caribbean Central Bank, ECCB Digital EC Currency Pilot. What you should know, 2019, https://www.eccb-centralbank.org/p/what-you-should-know-1 (zuletzt abgerufen am 19.12.2020).

37 Vgl. Binance Research (Jinze & Etienne), First Look: China's Central Bank Digital Currency, 2019, Beitrag vom 28.8.2019, https://research.binance.com/analysis/china-cbdc (zuletzt abgerufen am 15.6.2020).

ver kombiniert staatlich-privater Bemühungen weist auf die hohe Komplexität der praktischen Umsetzung von Retail-CBDC hin.

V. Rolle der Zentralbank

Der bestehende Geldkreislauf ist eine Infrastruktur, die gemeinsam von öffentlichen und privaten Institutionen betrieben wird. Dabei beschränken sich die Zentralbanken mehr oder weniger auf den von ihnen als hoheitlich definierten Bereich. Eine neue Geldform könnte auch neue Infrastrukturen erfordern, sodass einige Rollen neu zu definieren sind, einige möglicherweise entfallen könnten und teilweise auch andere Rollen entstehen werden. **59**

Dezentrale Netzwerke sind anders strukturiert als das bisherige Finanzsystem mit Intermediären und zentral organisierten Finanzmarktinfrastrukturen. Allerdings entwickeln sich auch die dezentralen Netzwerke weiter. Mit den Weiterentwicklungen der DLT durch anwendungsorientierte Konsortien wie R3 oder durch Softwareunternehmen wird die rein dezentrale Struktur zugunsten von Hierarchien und funktionalen Differenzierungen zunehmend aufgelöst. In einer einfachen Variante kann man bereits fünf verschiedene Rollen im Netzwerk definieren: Betreiber des Netzwerkes, Emittent von Assets, Verwahrer von Assets, Produzent von Produkten, Beobachter.[38] Die ursprüngliche Idee, dass dezentrale Netzwerke eine reine P2P-Welt ohne jegliche Finanzintermediäre ermöglichen, wird vermutlich in der Reinform nicht umsetzbar sein. Gleichwohl werden zahlreiche Geschäftsprozesse sich verändern und neue entstehen, sodass auch bisherige funktionale Rollen entfallen können. **60**

Das bisherige Verhältnis zwischen öffentlichem Sektor und Privatsektor im Zahlungsverkehr könnte sich, insbesondere durch die Emission von Retail-CBDC, erheblich in Richtung einer Ausweitung der Rolle der Zentralbanken verschieben. Damit einher gingen vermutlich auch größere Risiken in der Zentralbankbilanz, die entsprechend abgesichert werden müssten. Hinzu kommen Implikationen für andere politische Ziele, etwa für die Umsetzung der Geldpolitik, für die Finanzstabilität oder, bei etwaigen Fehlfunktionen, Ausfällen oder Leistungseinschränkungen, für die Reputation der Zentralbanken. **61**

Für die konkrete Infrastruktur für Retail-CBDC werden drei Varianten diskutiert.[39] Erstens, ein einstufiges Modell, in dem die Zentralbank ein Netzwerk betreibt, an dem alle Wirtschaftssubjekte teilnehmen können. Dieses „Direct **62**

38 Vgl. *Ludwin*, Why Central Banks Will Issue Digital Currency, 2016, Speech at the Federal Reserve Conference in Washington D.C., 1.6.2016, http://blog.chain.com/post/145509298356/why-central-banks-will-issue-digital-currency.

39 Vgl. *Auer* et al., Rise of the central bank digital currencies: drivers, approaches and technologies.

CBDC" genannte Modell brächte den größten Aufgabenzuwachs für die Zentralbank. Das möglicherweise größere Vertrauen der Bürger in staatlich betriebene Systeme würde möglicherweise kompensiert durch die zu erwartende geringe Innovativität staatlicher Strukturen. Zudem erweisen sich private Anbieter in der Regel als überlegen bei der Gestaltung von nutzerfreundlichen Dienstleistungen. Deshalb wird, zweitens, auch „Hybrid CBDC" diskutiert. Dabei entstünde eine zweistufige Architektur, bei der die Zentralbank eine Rückfalllösung betreibt, die Nutzer aber auf Systemen privater Anbieter Retail-CBDC als Forderungen gegen die Zentralbank transferieren können. In einer dritten Variante, „Intermediated CBDC" genannt, betriebe die Zentralbank nur ein System für die Finanzdienstleister. Unternehmen und Privatkunden wären auf privat betriebene Systeme angewiesen. Auch dort würden Token transferiert, die Forderungen an die Zentralbank repräsentieren. Andere Lösungen, bei denen Geschäftsbanken Token herausgeben, die durch Zentralbankgeld besichert sind, werden allgemein nicht als CBDC interpretiert und fallen daher unter digitales Geschäftsbankengeld.

63 Geld soll vor allem stabil sein. Daher bleibt der Grundauftrag für die Zentralbank so aktuell wie eh und je. Neben der Bereitstellung von stabilem Geld hat daher das Eurosystem auch einen Sorgeauftrag für den Zahlungsverkehr, für seine Stabilität und Effizienz. Daher ist auch die Ausgestaltung der gesamten Infrastruktur zur Übertragung von Geld von direktem Interesse für die Zentralbank. Der Zahlungsverkehr und die Wertpapierabwicklung sind hochtechnische, komplexe Infrastrukturen, die höchsten Anforderungen an Ausfallsicherheit und Widerstandsfähigkeit genügen müssen. Probleme in der Transaktion mit digitalem Zentralbankgeld, selbst wenn sie in privaten Netzen auftreten, bergen auch für die Zentralbank Reputationsrisiken, die das Vertrauen in die Währung schwächen können. Daraus folgt nicht notwendigerweise, dass die Zentralbank alle Systeme selbst betreiben muss. Die Zentralbank sollte aber eine entscheidende Rolle beim Aufbau und Betrieb des Zahlungssystems für digitales Geld spielen. Bislang läuft Zentralbankgeld, abgesehen vom quantitativ weniger bedeutsamen Bargeld, ausschließlich in Zentralbanksystemen um. Sollte sich dies etwa bei der Einführung von digitalem Zentralbankgeld ändern, bestünde die Gefahr eines negativen Reputationseffektes im Falle von auftretenden Problemen in privaten Systemen. In jedem Fall wären erhebliche Überwachungs- und Eingriffsmöglichkeiten für die Zentralbank vorzusehen.

64 Es folgt auch ein Vorsichtsprinzip in der Gestaltung der neuen Infrastruktur nicht zuletzt aus technischen Gründen. Noch immer entwickeln sich dezentrale Netzwerke rapide weiter. Der Einsatz dezentraler Netzwerke für die Transaktionsvolumina, die den Erfordernissen einer modernen Volkswirtschaft entsprechen, muss noch immer als technisches Neuland gesehen werden. Der Aufbau von entsprechend verlässlichen dezentralen Netzwerken in der benötigten Dimension

mit der erforderlichen funktionalen Differenzierung dürfte erhebliche Zeit in Anspruch nehmen.

Operativ bietet sich möglicherweise das Lernen in kleinen Schritten an. Eine Trigger-Anwendung ließe das bestehende Zahlungssystem unverändert, ermöglichte aber den Einsatz der DLT als Abwicklungstechnik für komplexe Geschäftsfälle. Wholesale-CBDC hätte den Vorteil, dass das benötigte Netzwerk deutlich kleiner ausfallen könnte. Zudem handelten anfangs nur Profis mit digitalem Geld, sodass eine operative Grundkompetenz unterstellt werden könnte. Digitales Zentralbankgeld für jedermann, also Retail-CBDC, wäre in jeder Hinsicht die weitestgehende Option, birgt damit die größten Risiken und erfordert die umfassendste und längste Vorbereitung. **65**

Kapitel 3 Technische Grundlagen

Literatur: *Bitkom* (Hrsg.), Decentralized Finance (DeFi) – A new Fintech Revolution?, https://www.bitkom.org/Bitkom/Publikationen/Decentralized-Finance-A-new-Fintech-Revolution; *deloitte* (Hrsg.), Blockchain: A Technical Primer, https://www2.deloitte.com/us/en/insights/topics/emerging-technologies/blockchain-technical-primer.html; *deloitte* (Hrsg.), Blockchain and the future of financial infrastructure, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-blockchain-deloitte-summary.pdf; *Feige/Lapidot/Shamir*, Multiple Non-Interactive Zero Knowledge Proofs Under General Assumptions, SIAM J. Comput. 29(1) (1999), 1; *Hyperledger Fabric*, Open, Proven, Enterprise-grade DLT, https://www.hyperledger.org/wp-content/uploads/2020/03/hyperledger_fabric_whit epaper.pdf; *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bit coin.org/bitcoin.pdf (zuletzt abgerufen am 2.3.2021); *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin and cryptocurrency technologies: A comprehensive introduction, 2016; *OECD* (Hrsg.), The Tokenisation of Assets and Potential Implications for Financial Markets, https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implicatio ns-for-Financial-Markets.pdf; *Rivest/Shamir/Tauman Kalai*, How to leak a secret ASIACRYPT 2001, Volume 2248 of Lecture Notes in Computer Science, 552; *Sandner/Welpe/Tumasjan*, Die Zukunft ist dezentral: Wie die Blockchain Unternehmen und den Finanzsektor auf den Kopf stellen wird, 2020; *Shor*, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing 26/1997, 1484; *Valenta/Sandner*, Comparison of Ethereum, Hyperledger Fabric and Corda, FSBC Working Paper, 2017, https://philippsandner.medium.com/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6; *Voshmgir*, Token Economy: Wie das Web3 das Internet revolutioniert, 2. Aufl. 2020.

Übersicht

I. Einführung

Die Entstehung von Kryptowährungen und Token ist untrennbar mit der Entwicklung der Blockchain-Technologie – oder allgemeiner der „Distributed Leger Technology“ (DLT) – verbunden. **1**

Grundsätzlich gilt: Blockchain- bzw. Distributed Ledger Technology (die Unterschiede und Gemeinsamkeiten werden wir erläutern) ist die technische Basis für jede Form von Transaktionen in Kryptowährungen und Token. **2**

Seit die Bitcoin-Blockchain am 9. Januar 2009 startete, hat sich eine rasante Weiterentwicklung und Ausdifferenzierung der DLT/Blockchain-Technologie vollzogen. Es ist daher nicht ganz einfach, der Komplexität der realen Entwicklung gerecht zu werden und trotzdem die gemeinsamen Charakteristika herauszuarbeiten. **3**

In der Darstellung dieses Kapitels mussten wir also eine Auswahl der wesentlichen technologischen Plattformen und Elemente treffen, die natürlich immer nur eine subjektive sein kann. An vielen Stellen verweisen wir daher auf Dokumente und Publikationen zur weiteren Vertiefung. **4**

Das Thema DLT/Blockchain ist unter anderem deshalb so faszinierend, weil es so dynamisch ist. Die Technologie ermöglicht bestimmte Anwendungsfälle, aus denen dann Anregungen und Erweiterungen entstehen, die die Technologieentwicklung ihrerseits wieder zusätzlich befeuern. Eine positive Feedback-Schleife ist am Werk. Es ist absehbar, dass die DLT/Blockchain-Technologie mannigfaltige Anwendungen haben wird, für die sie derzeit aber noch nicht ausreichend mächtig oder ausgereift ist. Dieses Kapitel stellt also die Momentaufnahme einer äußerst dynamischen Entwicklung dar. **5**

Eine abschließende Bemerkung zum Sprachgebrauch: Die Gemeinschaft der Nutzer, Entwickler und Betreiber von DLT- oder Blockchain-Netzwerken ist in **6**

hohem Maße global. Die sich gerade herausbildende Terminologie ist daher vollständig angelsächsisch. Fachbegriffe werden in der Regel nicht übersetzt – nicht einmal ins Französische. Aus unserer Sicht sind außerdem viele Sprachschöpfungen unglücklich oder gar irreführend – siehe dazu z. B. unsere Bemerkungen zu den „Minern" in der Bitcoin-Blockchain. Da diese sich aber in der Literatur etabliert haben, werden wir dem herrschenden Sprachgebrauch folgen, bei der Einführung der Termini aber auf den entsprechenden Sachverhalt verweisen.

II. Grundlagen der Blockchain-Technologie am Beispiel Bitcoin

7 Kaum eine Technologie hat einen so präzise bestimmbaren Anfangspunkt wie die Blockchain-Technologie.[1]

8 Im Oktober 2008 wurde – unter dem Pseudonym *Satoshi Nakamoto* – das White Paper „Bitcoin: A Peer-to-Peer Electronic Cash System"[2] veröffentlicht, das alle grundlegenden Elemente der Blockchain-Technologie beschreibt – und dessen Lektüre wir jedem Interessierten nachdrücklich empfehlen. Am 9. Januar 2009 nahm dann das auf Basis dieses White Papers implementierte Netzwerk der Bitcoin-Blockchain seinen Dienst auf.

9 Wenngleich die Technologie in den folgenden Jahren eine schier unendliche Zahl von Weiterentwicklungen und Modifikationen erfahren hat, ist es sinnvoll, die Bitcoin-Blockchain zum Ausgangspunkt unserer Erläuterungen nehmen – um dann von dem so erreichten Verständnis aus die Bildung von Varianten und Erweiterungen zu beschreiben.

1. Die Grundidee der Bitcoin-Blockchain

10 Der Bitcoin-Blockchain liegt eine verblüffend einfache Idee zugrunde: Kann man nicht eine bestimmte Anzahl von Einheiten (Bitcoins) schaffen und für diese ein digitales Register (ein Buch, einen Ledger) führen, in das für jeden Bitcoin (und seine Untereinheiten) alle zugehörigen Transaktionen notiert werden, sodass immer klar ist, wer gerade wie viele Bitcoin besitzt?

11 Dieser Grundidee fügte *Nakamoto* noch eine Reihe von zusätzlichen Anforderungen hinzu:

---

1 Davon unbenommen ist, dass die Blockchain-Technologie natürlich viele über die letzten Jahrzehnte entwickelte Technologien einsetzt, vor allem im Bereich Netzwerke, Datenbanken und Kryptographie.

2 *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (zuletzt abgerufen am 2.3.2021).

1. Der Ledger soll in hohem Maße sicher sein, damit sich in ihm signifikante Werte speichern lassen.
2. Nicht eine zentrale Stelle soll den Ledger führen, sondern die Beteiligten sollen gemeinschaftlich die Führung und Sicherung des Ledgers übernehmen.
3. Wie beim Bargeld sollen anonyme Zahlungen möglich sein.

Es kann angenommen werden, dass die Grundidee eines von der Zivilgesellschaft (oder einer Untergruppe) geschaffenen und betriebenen Währungssystems stark durch die offensichtlichen Schwierigkeiten und Limitationen der Geschäfts- und Notenbanken in der Finanzkriese 2008/2009 befeuert wurde. **12**

Die wesentlichen Designkriterien der Bitcoin-Blockchain lassen sich aus den oben genannten Anforderungen ableiten: **13**

a) Redundanz

Zur Sicherheit des Ledgers trägt vor allem bei, dass dieser nicht an einer Stelle, sondern im Netzwerk der Bitcoin-Knoten („Bitcoin Nodes" oder oft auch einfach „Nodes") hochgradig redundant geführt wird: derzeit existiert der Bitcoin-Ledger (identisch) auf mehreren tausend Knoten. **14**

Bemerkung: Ursprünglich war intendiert, dass jeder Nutzer der Bitcoin-Blockchain auch einen Knoten betreiben sollte – somit die Idee eines von Nutzern selbst betriebenen Systems verwirklichend. Dieser Ansatz wurde aber mittlerweile aufgegeben: die meisten Nutzer der Bitcoin-Blockchain interagieren mit ihr über Dienstleister (z. B. über Wallet-Provider – siehe Rn. 167 ff.). **15**

b) Unveränderlichkeit/Block-für-Block-Ansatz

Die massive Redundanz der Knoten schützt vor Datenverlust und Manipulation. Sie ist aber auch die Ursache einer wesentlichen Herausforderung: Wie kann die Gleichheit und Integrität einer solch großen Anzahl von Ledger-Instanzen sichergestellt werden? **16**

Das hierzu wesentliche Lösungselement ist der (für die Blockchain namensgebende) Ansatz, den Datenbestand als Verkettung von Blöcken darzustellen und zwar so, dass das Netzwerk der Knoten eine Übereinstimmung nur hinsichtlich des jeweils neuen Blocks (bestehend aus den neu zu speichernden Transaktionen) erzielen muss und die vorausgehenden Blöcke als unveränderlich anzusehen sind. **17**

Blöcke fassen die Transaktionen, die innerhalb der sog. Blockzeit (bei Bitcoin: 10 Minuten) auftreten zusammen. Ein Bitcoin-Block enthält typischerweise ca. zweitausend Transaktionen, die in Summe ca. 1 Megabyte Datenvolumen ausmachen (1 Megabyte ist die Obergrenze der Block-Size). Naturgemäß ist es viel einfacher, im Netzwerk Einigkeit für die 1 Megabyte neue Daten zu erzielen als **18**

über den ganzen Datenbestand der Bitcoin-Blockchain (derzeit bei ca. 300 Gigabyte).

19 Die Unveränderlichkeit bestehender Blöcke wird wie folgt „erzwungen“: Jeder Block (außer dem erstem Block, dem sog. Genesis-Block) enthält als Teil seines Datenbestands einen Fingerabdruck des vorausgehenden Blocks. Technisch gesehen ist der Fingerabdruck als sog. Hash-Wert des Vorgängerblocks implementiert. Eine Änderung eines Blocks führte somit unweigerlich zu einem Mismatch mit seinem im Nachfolgeblock gespeicherten Fingerabdruck. Die auf den Knoten laufende Software würde einen solchen Datenbestand sofort als nicht integer erkennen und aussortieren.

c) Public-Private-Key-Kryptographie

20 Bitcoin nutzt – so wie alle anderen wichtigen Kryptowährungen auch – bestimmte kryptographische Verfahren, um Transaktionen zu sichern. Hierbei kommen die folgenden Elemente zum Einsatz:

- private Schlüssel (Private Keys),
- öffentliche Schlüssel (Public Keys),
- Bitcoin-Adressen (auch Wallet-Adressen oder Bitcoin-Wallet-Adressen genannt),
- digitale Signaturen.

21 In der Bitcoin-Blockchain wird die Gültigkeit von Transaktionen (und somit die Möglichkeit, über Bitcoin zu verfügen) durch digitale Schlüssel, Bitcoin-Adressen und digitale Signaturen nachgewiesen.

22 Die genannten Entitäten hängen wie folgt zusammen:

- Der **Private Key** entspricht einer Zufallszahl (mit 256 Byte Länge), die der Nutzer selbst wählen (oder besser noch: mit bestimmten Tools erzeugen) kann.
- Der **Public Key** wird aus dem Private Key durch Anwenden einer Falltür-Funktion[3] errechnet. Die Falltür-Funktion stellt sicher, dass der Aufwand, den private Key aus dem Public Key „zurückzurechnen“ astronomisch hoch wäre. Der Public Key wird erst in dem Moment benötigt (und somit auch erst sichtbar), wenn ein Nutzer über empfangene Bitcoin verfügen möchte (s. u.).
- Die Information, die der Sender zur Kennzeichnung des Adressaten wirklich benötigt, ist die **Bitcoin-Adresse** des Empfängers. Diese wird wieder durch Anwenden eines falltürartigen[4] Ansatzes aus dem **Public Key** ermittelt.

3 Es handelt sich um das auf der Multiplikation elliptischer Kurven basierende ECDSA-Verfahren (Elliptic Curve Digital Signature Algorithm).

4 Adresse = RIPEMD160 (SSHA256 (private key)), wobei SSHA256 und RIPEMD160 sog. Hashing-Algorithmen sind.

– Mit der **digitalen Signatur** (die aus den Transaktionsdaten und dem Private Key errechnet wird) kann ein Nutzer über die an seine Adresse gesendeten Bitcoin verfügen, da er dem Bitcoin-Netzwerk gegenüber nachweisen kann, dass er über den zur entsprechenden Bitcoin-Adresse zugehörigen **Private Key** verfügt – und zwar ohne, dass er den Private Key explizit zeigen muss (sichtbar wird nur die digitale Signatur).

Die digitalen Schlüssel und die Bitcoin-Adressen eines Benutzers sind also völlig unabhängig von der Bitcoin-Blockchain und können vom Benutzer ohne Bezugnahme auf die Blockchain erzeugt und verwaltet werden. Dies muss aus Sicherheitsgründen natürlich auch so sein. **23**

d) Konsensmechanismus

Auch wenn der „Block-für-Block-Mechanismus" den Gegenstand des Konsenses unter den Knoten auf die neuen Transaktionen reduziert (und somit deutlich vereinfacht), muss dieser Konsens zeitnah, effizient, fair und zuverlässig erreicht werden. **24**

Zunächst muss geklärt werden, dass die Transaktionen, die in den nächsten Block Eingang finden sollen **25**

– echte und erlaubte Transaktionen aus dem Netzwerk sind und
– den Regeln des Protokolls entsprechen.

Diese Überprüfung leistet die Knotensoftware, indem sie u. a. die oben erwähnten Signaturen der Transaktionen verifiziert. **26**

Des Weiteren muss verhindert werden, dass einzelne Knoten das Netzwerk mit neuen Blöcken überschwemmen (spammen) oder alternative Versionen der Blockchain (sog. „Forks"/Abzweigungen) erzeugen. So könnte beispielsweise ein Teilnehmer das Interesse haben, eine Version der Blockchain zu erzeugen, bei der er bestimmte in der Vergangenheit liegende Transaktionen gar nicht getätigt hätte (was ihm ein sog. „Double Spending" – ein doppeltes Ausgeben – von Bitcoins ermöglichen würde). **27**

Das in der Bitcoin-Blockchain zur Vermeidung solcher Aktionen implementierte Verfahren ist der sog. Proof-of-Work. Er stellt sicher, dass beim Festschreiben eines neuen Blocks eine signifikante Rechenarbeit geleistet werden muss. Im Detail funktioniert das Verfahren bei der Bitcoin-Blockchain wie folgt: **28**

Die Knoten stehen untereinander im Wettbewerb, wer von ihnen den nächsten Block für verbindlich erklären und somit der Blockchain hinzufügen kann. Damit sich dieser Wettbewerb lohnt, erhält der Knoten, der den Wettbewerb gewinnt, neu geschöpfte Bitcoin – derzeit 6,25 Bitcoin (ca. 70k US-Dollar) pro Block. **29**

30 Die Aufgabe, die im Wettbewerb gelöst werden soll, besteht darin, den Datenbestand des neu zu erzeugenden Blocks durch Hinzufügen weiterer frei wählbarer Bytes (der sog. Nonce) so zu ergänzen, dass der Hashwert des sich so ergebenden Datensatzes eine bestimmte Form annimmt (der Hashwert ergibt sich durch Anwenden einer Falltür-/Hashfunktion[5] auf den Datensatz).

31 Derzeit besteht die Aufgabe darin, die Nonce so zu wählen, dass in der Hexadezimaldarstellung[6] des Hashwerts die ersten 19 Stellen Null sein müssen. Da bei einem Hash-Algorithmus jede kleinste Veränderung im Input den Output völlig verändert, kann diese Aufgabe nur durch Ausprobieren gelöst werden. Im Durchschnitt müssen derzeit also 16^{19} = 75.557.863.725.914.323.419.136 Möglichkeiten ausprobiert werden, um eine Lösung zu finden. Die Schwierigkeit der Wettbewerbsaufgabe wird laufend der im Bitcoin-Netzwerk zur Verfügung stehenden Rechenperformance (der „Hash-Power") angepasst: Wird die Wettbewerbsaufgabe in tendenziell unter 10 Minuten gelöst, wird die Schwierigkeit erhöht, werden im Schnitt mehr als 10 Minuten gebraucht, wird sie reduziert. Auch diese Adjustierung hatte *Nakamoto* in seinem genialen Ansatz bereits vorgesehen.

32 Auf Basis der oben genannten Zahlen wird sofort klar, dass enorme Investitionen in Hardware und Energie zum Betreiben der Rechenzentren nötig sind, um die benötigte Rechenleistung zu erbringen. Dies hat dazu geführt, dass nicht mehr – wie ursprünglich intendiert – alle Knoten am Proof-of-Work-Prozess teilnehmen, sondern faktisch nur noch vergleichsweise wenige und zwar solche, die auf Basis hochspezialisierter Rechenzentren operieren.

33 Es ist nicht nur sehr aufwändig, die Wettbewerbsaufgabe im Proof-of-Work zu lösen, aus dem Wettbewerb gehen auch stochastisch verteilt immer andere Knoten als Sieger hervor. Dieses Zufallselement bei der Auswahl des Knotens, der den nächsten Block festschreiben darf, stellt eine zusätzliche Hürde für jeden potenziellen Angreifer auf die Integrität des Bitcoin-Netzwerks dar.

34 Da die Knoten im Wettbewerb des Proof-of-Work als Belohnung neu geschöpfte Bitcoin erhalten, hat sich für sie der Name „Miner" oder „Bitcoin-Miner" etabliert. Wir finden diese Nomenklatur sehr unglücklich, denn sie verdreht Ursache und Wirkung: Die Knoten erbringen die für die Bitcoin-Blockchain essenzielle Dienstleistung der Sicherung der Integrität der Blockchain und werden für diese Dienstleistung bezahlt. Das könnte statt mit neuen Bitcoin auch auf Basis einer Transaktionsgebühr geschehen (was derzeit sogar bereits teilweise der Fall ist). Außerdem ist die Anzahl der durch „Mining" hinzukommenden Bitcoins (der-

5 Es handelt sich um die Funktion SHA-256.

6 Zahlensystem zur Basis 16 – dargestellt durch die Ziffern 0…9 und die Buchstaben a…f; z. B. ist f4 die Hexadezimaldarstellung von 244.

zeit 900 pro Tag) im Vergleich zur bestehenden Basis (ca. 18,5 Mio.) kaum von Bedeutung.[7]

Verwandte Proof-of-Work-Verfahren werden übrigens seit den Neunzigerjahren genutzt, um Denial-of-Service (DoS) Attacken z. B. auf E-Mail-Server zu verhindern. **35**

Der Proof-of-Work ist in gewisser Weise der Dreh- und Angelpunkt der Bitcoin-Blockchain. Er schafft ein sehr hohes Maß an Sicherheit – allerdings zu sehr hohen Kosten. Wie wir sehen werden (siehe Rn. 94 ff.), gibt es mittlerweile andere Blockchain-Protokolle, die alternative Verfahren einsetzen. **36**

e) Open Source

Vertrauen in die Bitcoin-Blockchain setzt voraus, dass sich die Nutzer davon überzeugen können, dass die Knoten das Bitcoin-Regelwerk (das sog. Bitcoin-Protokoll) auch tatsächlich korrekt ausführen. Diese Überprüfung der Integrität der auf den Bitcoin-Knoten laufenden Software wird dadurch ermöglicht, dass sie „Open Source", also im Quellcode verfügbar ist. Jeder kann diesen Quellcode Zeile für Zeile lesen und sich vergewissern, dass er das intendierte Verhalten eines Bitcoin-Knotens korrekt umsetzt.[8] **37**

Die Überprüfung, dass die tatsächlich heruntergeladenen binären Releases (also des lauffähigen und somit auf dem Rechner ausgeführten Codes) ordnungsgemäß durch Compilieren des Quellcodes erzeugt wurden, wird anhand der in der FLOSS-Community[9] üblichen digitalen (und kryptographisch gesicherten) Signaturen vorgenommen. **38**

2. Eine Bitcoin-Transaktion

Das Zusammenspiel der im vorherigen Abschnitt erläuterten Elemente zeigen wir, indem wir einer Bitcoin-Transaktion folgen. **39**

1. Wir beginnen mit einem Teilnehmer A, der aus einer vorhergegangenen Transaktion über einen Bitcoin verfügt.
2. Teilnehmer A will diesen einen Bitcoin nun an Teilnehmer B senden und erstellt eine entsprechende neue Transaktion. Hierzu benötig er die **Bitcoin-Adresse** von B und seine eigenen **Public** und **Private Keys**; Letztere, um die Transaktion zu signieren.

---

7 Da die Prämie für das Mining eines Blocks ca. alle 4 Jahre (genau: alle 210.000 Blocks) halbiert wird, steigt die Zahl der existierenden Bitcoin auf max. 21 Mio. – wenn dieser Aspekt des Bitcoin-Protokolls nicht irgendwann geändert wird.

8 Die Open-Source-Community nutzt „github" als ihr gemeinsames Repository – dort liegt auch der Bitcoin-Quellcode und zwar unter https://github.com/bitcoin/bitcoin.

9 Free/Libre and Open Source Software Community.