



MASTER THESIS | MASTER'S THESIS

Titel | Title

Kryptowährung und Verbraucherschutz in der Europäischen Union und
Österreich

verfasst von | submitted by

Roholamin Alishahi

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt |
Degree programme code as it appears on the
student record sheet:

UA 992 548

Universitätslehrgang lt. Studienblatt |
Postgraduate programme as it appears on
the student record sheet:

Europäisches und Internationales Wirtschaftsrecht
(LL.M.)

Betreut von | Supervisor:

ao. Univ.-Prof. Mag. Dr. Siegfried Fina

Abstract (Deutsch)

Kryptowährungen haben in den vergangenen Jahren erheblich an wirtschaftlicher Bedeutung gewonnen und werden zunehmend auch von Verbraucher:innen genutzt. Gleichzeitig sind sie mit besonderen Risiken verbunden, darunter hohe Kursschwankungen, technische Sicherheitsprobleme, Informationsasymmetrien und rechtliche Unsicherheiten. Vor diesem Hintergrund gewinnt die Frage nach einem wirksamen Konsumentenschutz im Bereich von Kryptowährungen zunehmend an Bedeutung.

Ziel der Arbeit ist die Untersuchung der unions- und nationalrechtlichen Rechtsgrundlagen im Bereich von Kryptowährungen sowie deren Bewertung im Hinblick auf die Effektivität des Konsumentenschutzes. Dabei wird analysiert, ob die bestehenden rechtlichen Rahmenbedingungen einen ausreichenden Schutz von Verbraucher:innen gewährleisten oder ob weiterhin regulatorische Schutzlücken bestehen. Die Untersuchung zeigt, dass die bestehenden Rechtsgrundlagen zwar zu einer Verbesserung der Transparenz und Rechtssicherheit beitragen, jedoch nicht in allen Bereichen einen ausreichenden Schutz von Verbraucher:innen gewährleisten. Die Arbeit gelangt daher zu dem Ergebnis, dass weiterer gesetzgeberischer und aufsichtsrechtlicher Handlungsbedarf besteht.

Abstract (English)

Cryptocurrencies have gained significant economic importance in recent years and are increasingly used by consumers. At the same time, they are associated with specific risks, including price volatility, technical security issues, information asymmetries, and legal uncertainties. Against this background, the question of effective consumer protection in the field of cryptocurrencies has become increasingly relevant.

The objective of this thesis is to examine the European Union and Austrian legal frameworks governing cryptocurrencies and to assess their effectiveness in terms of consumer protection. The analysis evaluates whether the existing legal framework provides adequate protection for consumers or whether regulatory gaps continue to exist. The study demonstrates that current legal provisions contribute to greater transparency and legal certainty but do not ensure sufficient consumer protection in all areas. The thesis therefore concludes that further legislative and supervisory measures are necessary.

Inhaltsverzeichnis

Abstract (Deutsch)	2
Abstract (English)	3
Inhaltsverzeichnis	4
Abkürzungsverzeichnis	11
Kapitel 1 Einführung in die Thematik des Konsumentenschutzes bei Kryptowährungen	13
1.1 Problemstellung, Hintergrund und Aktualität von Kryptowährungen	13
1.2 Bedeutung von Kryptowerten und Konsumentenschutz	15
1.3 Regulatorische Unsicherheit und daraus resultierender Handlungsbedarf	18
1.4 Forschungsziel, Forschungsfragen und methodisches Vorgehen	20
1.5 Aufbau der Arbeit	22
Kapitel 2 Theoretische Grundlagen, Begriffsbestimmungen und ökonomisch- technische Einordnung.....	25
2.1 Philosophie des Geldes und Begriffsgrundlagen digitaler Vermögenswerte.....	25
2.1.1 Klassische Geldtheorien und ihre Herausforderungen im digitalen Kontext .	25
2.1.2 Geld als Rechtsinstitut und die Notwendigkeit der digitalen Rechtsdogmatik	26
2.1.3 Token, Blockchain und digitale Vermögensobjekte als neue Form der Wertrepräsentation	26
2.1.4 Dezentralität, Selbstorganisation und Governance als philosophische Herausforderung.....	27
2.1.5 Konsequenzen für die rechtliche Analyse.....	27
2.2 Definition und zentrale Konzepte von Kryptowährungen	27
2.2.1 Kryptowährungen als digitale, kryptografisch gesicherte Wertrepräsentationen	28
2.2.2 Token als Rechtssubstrate: Payment, Utility und Security-Token	28
2.2.3 Distributed Ledger Technology (DLT) und Blockchain	29
2.2.4 Smart Contracts und deren rechtliche Bedeutung	30
2.2.5 Konsensmechanismen: Proof-of-Work, Proof-of-Stake und Alternativen	30
2.2.6 Kryptowährungen als Vermögensobjekte im juristischen Sinne	30
2.2.7 Internationale Definitionen und regulatorische Uneinheitlichkeit	31
2.3 Technologische Grundlagen und Funktionsweise der Blockchain	31

2.3.1 Distributed-Ledger-Architektur als Grundlage digitaler Vermögenswerte.....	31
2.3.2 Kryptografische Sicherung und Schlüsselverwaltung.....	32
2.3.3 Konsensmechanismen und ihre Bedeutung für Sicherheit und Governance	33
2.3.4 Smart Contracts als automatisierte Rechtsfolgenmechanismen	33
2.3.5 Die Rolle zentraler Dienstleister in einem dezentralen System.....	34
2.4 Abgrenzung zu anderen digitalen Finanzinstrumenten und rechtliche Einordnung	34
2.4.1 Kryptowährungen versus elektronisches Geld (E-Geld)	35
2.4.2 Abgrenzung zu Stablecoins und Asset-Referenced Tokens	35
2.4.3 Abgrenzung zu tokenisierten Vermögenswerten (Security-Token)	36
2.4.4 Abgrenzung zu Non-Fungible Tokens (NFTs)	36
2.4.5 Abgrenzung zu CBDCs (Central Bank Digital Currencies)	36
2.4.6 Bedeutung der Abgrenzung für Eigentumsrecht, Verbraucherschutz und Aufsicht.....	37
Kapitel 3 Analyse der technologischen, ökonomischen und rechtlichen Risiken für Verbraucher:innen	40
3.1 Technologische Risiken von Kryptowerten	40
3.1.1 Verlust oder Kompromittierung kryptographischer Schlüssel	40
3.1.2 Cyberangriffe, Hacks und Sicherheitslücken	41
3.1.3 Technische Systemfehler, Protokollfehler und Smart-Contract-Risiken	42
3.1.4 Dezentralität, Validatorrisiken und Netzwerkangriffe.....	42
3.1.5 Irreversibilität und fehlende Transaktionskorrektur	43
3.1.6 Automatisierte Liquidationen und Marktmechanik	43
3.1.7 Verantwortungsdiffusion und fehlende Haftungsadressaten	44
3.2 Ökonomische Risiken von Kryptowerten	45
3.2.1 Extreme Volatilität und fehlende intrinsische Wertbasis.....	45
3.2.2 Marktmanipulation, Wash-Trading und fehlende Marktintegrität	46
3.2.3 Illiquide Märkte und strukturelle Liquiditätsrisiken	47
3.2.4 Stablecoin-Risiken und die Illusion der Preisstabilität.....	48
3.2.5 Systemische Risiken durch Interkonnektivität und Kaskadeneffekte	50
3.2.6 Kreditrisiken, Liquidationsspiralen und Überbesicherung	51
3.2.7 Informationsasymmetrien und Überforderung der Verbraucher:innen	51

3.3 Rechtliche Risiken von Kryptowerten	52
3.3.1 Rechtsunsicherheit über die rechtliche Einordnung („Legal Classification Risk“)	52
3.3.2 Vertragliche Risiken und AGB-Problematis bei Kryptodienstleistern	53
3.3.3 Eigentums- und Zuordnungsrisiken (Token Ownership Risk)	55
3.3.4 Rechtsdurchsetzungsprobleme (Enforcement Risk)	55
3.3.5 Insolvenzrisiken bei Kryptodienstleistern	57
3.3.6 Unklare Haftungsfragen und Verantwortungsdiffusion	58
3.3.7 Fehlende regulatorische Einbettung außerhalb zentraler Dienstleister	59
3.4 Risiken durch Marktstruktur und Intermediäre	59
3.4.1 Missbrauchsrisiken durch Eigenhandel, Interessenkonflikte und Intransparenz	60
3.4.2 Intransparenz und Informationsdefizite in Marktstrukturen	61
3.4.3 Unzureichende Marktüberwachung und fehlende Aufsichtsbefugnisse	62
3.5 MiCA aus verbraucherschutzrechtlicher Perspektive	62
3.5.1 Zielsetzung und normative Grundentscheidung	63
3.5.2 Informations- und Whitepaper-Pflichten als zentrale Verbraucherschutzinstrumente	63
3.5.3 Autorisierung und laufende Aufsicht von Krypto-Dienstleistern (CASPs)	64
3.5.4 Besondere Vorgaben für Asset-referenced Tokens und E-Geld-Token	65
3.5.5 Beschwerdeverfahren und Rechtsdurchsetzung	66
3.5.6 Marktintegrität und Schutz vor Marktmissbrauch	66
Kapitel 4 Unionsrechtlicher Rechtsrahmen mit Schwerpunkt auf der MiCA-Verordnung	68
4.1 Einbettung des österreichischen Rechtsrahmens in das Unionsrecht	68
4.1.1 MiCA als unionsrechtlicher Ordnungsrahmen mit unmittelbarer Relevanz für Österreich	69
4.1.2 Zusammenspiel mit AMLD5/FM-GwG, PSD2/ZaDiG 2018 und DSGVO	69
4.1.3 Nationale Umsetzungsschritte und Rolle der FMA	70
4.1.4 Spannungsverhältnis zwischen unionsrechtlicher Harmonisierung und nationale Rechtsordnungssystematik	71
4.2 Zivilrechtliche Qualifikation von Kryptowerten im österreichischen Recht	72
4.2.1 Sachbegriff des ABGB und Problem der Körperlichkeit	72

4.2.2 Modelle der zivilrechtlichen Einordnung in der österreichischen Literatur ...	73
4.2.3 Praktische Folgefragen: Eigentum, Übertragung, Sicherheiten, Erbrecht und Insolvenz	75
4.3 Aufsichtsrechtliche Einordnung und Regulierung von Kryptodienstleistungen in Österreich.....	77
4.3.1 Aufsichtsrechtliche Grundstruktur: Tätigkeitstypen und Abgrenzungsfragen	77
4.3.2 Geldwäscherechtliche Registrierung nach § 32a FM-GwG	78
4.3.3 Anwendbarkeit aufsichtsrechtlicher Spezialgesetze (BWG, WAG, ZaDiG)	79
4.3.4 Technologische Neutralität und Grenzen der Aufsichtspraxis (FMA)	80
4.4 Kapitalmarktrechtliche Einordnung und Anwendbarkeit des KMG und WAG 2018	81
4.4.1 Grundstruktur: Wann ist ein Kryptowert ein Finanzinstrument?	81
4.4.2 Security Token: Wann liegt ein „übertragbares Wertpapier“ vor?	82
4.4.3 Das Kapitalmarktgesetz (KMG): Prospektpflicht und ihre Grenzen	83
4.5 Steuerrechtlicher Rahmen für private Nutzer:innen	84
4.5.1 Entwicklung der Rechtslage: Von Spekulationsgeschäften zu Kapitaleinkünften.....	84
4.5.2 Systematik des § 27b EStG: Steuerbare Vorgänge, Steuersatz und Verlustverrechnung	85
4.5.3 Alt- und Neubestände, DeFi-Modelle und internationale Schnittstellen	86
4.5.4 Steuerrecht und Konsumentenschutz: Informationsdefizite, Komplexität und faktische Risiken	87
4.6 Datenschutzrechtliche Einordnung und Bedeutung der DSGVO für Verbraucher:innen.....	88
4.6.1 Grundanwendbarkeit der DSGVO auf Kryptowerte und Blockchain-Systeme	89
4.6.2 Verarbeitungssituationen im Kryptobereich und ihre datenschutzrechtlichen Implikationen.....	90
Kapitel 5 Nationale Umsetzung und österreichischer Rechtsrahmen	92
5.1 Einbettung von Kryptowerten in das österreichische Rechtssystem	92
5.2 Zentrale Rechtsquellen: FM-GwG, MiCA-VVG, KMG und weitere Normen	95
5.2.1 Finanzmarkt-Geldwäschegesetz (FM-GwG)	95
5.2.2 MiCA-Verordnung-Vollzugsgesetz (MiCA-VVG).....	96
5.2.3 Kapitalmarktgesetz 2019 (KMG 2019) und Prospektrecht	96

5.2.4 Weitere relevante Rechtsbereiche.....	97
5.3 Pflichten der Dienstleister und Aufsichtspraxis der FMA.....	98
5.3.1 Vom VASP-Regime zum CASP-Regime	98
5.3.2 Zulassungsvoraussetzungen und laufende Pflichten.....	99
5.3.3 Aufsichtsinstrumente und Eingriffsmöglichkeiten der FMA.....	100
5.4 Nationale Schutzlücken im österreichischen Kryptorecht	101
5.4.1 Fehlende zivilrechtliche Kodifikation der Rechtsnatur von Kryptowerten ...	101
5.4.2 Fehlende insolvenzrechtliche Absicherung	102
5.4.3 Kein Entschädigungssystem für Verluste.....	102
5.4.4 Unzureichende Haftungsregeln bei technischen Risiken	103
Kapitel 6 Internationaler Vergleich (USA, China, Japan)	104
6.1 Zielsetzung und Einordnung des internationalen Vergleichs	104
6.2 Regulierungsprofile in komparativer Perspektive.....	105
6.2.1 Vereinigte Staaten: Fragmentierte Zuständigkeit und ex-post-orientiertes Regulierungsmuster	106
6.2.2 China: Verbotsorientiertes Risikoblockademodell mit selektivem privatrechtlichen Eigentumsschutz	107
6.2.3 Japan: Integratives Lizenzmodell mit technischer Standardsetzung und Selbstregulierung.....	108
6.3 Strukturelle Vergleichsanalyse der untersuchten Regulierungsmodelle.....	109
6.3.1 Regulierungsphilosophie: Ex-post-Durchsetzung, Risikoblockade und präventive Lizenzierung	110
6.3.2 Institutionelle Architektur: Fragmentierung, Zentralisierung und funktionale Koordination	111
6.3.3 Vermögenszuordnung, Eigentumsstruktur und Insolvenzschutz	111
6.4 Normative Schlussfolgerungen für das unions- und österreichische Verbraucherschutzrecht	112
6.4.1 Erfordernis eines erweiterten, kohärenten Ex-ante-Schutzsystems.....	112
6.4.2 Kodifikation eines unionsweit einheitlichen Token-Eigentums- und Insolvenzschutzregimes	113
6.4.3 Stärkung der institutionellen Koordinationsmechanismen nach dem Vorbild funktionaler Modelle	114
6.4.4 Integration eines technologiebezogenen Risikorahmens in das europäische Aufsichtsmodell.....	114

6.4.5 Erforderlichkeit einer unionsweiten Reform des kollektiven Rechtsschutzes	115
Kapitel 7 Bewertung der Effektivität bestehender Schutzmechanismen.....	116
7.1 Systematische Ausgangslage des unionsrechtlichen Verbraucherschutzes im Bereich kryptobasierter Dienstleistungen	116
7.2 Struktur und systematische Funktion der unionsrechtlichen Verbraucherschutznormen im Bereich kryptobasierter Dienstleistungen	117
7.2.1 Verbraucherrechte-Richtlinie (CRD) im Kontext kryptobasierter Dienstleistungen	118
7.2.2 Richtlinie über unlautere Geschäftspraktiken (UCPD).....	119
7.3 Verhältnis zwischen MiCA und dem allgemeinen unionsrechtlichen Verbraucherschutzrecht	120
7.4 Unionsrechtliche Schutzdefizite im Lichte technischer und organisatorischer Risiken kryptobasierter Dienstleistungen	122
Kapitel 8 Reformvorschläge und normative Handlungsempfehlungen	125
8.1 Normativer Ausgangsrahmen und zentrale Erkenntnislinien	125
8.2 Zivilrechtliche Einordnung von Kryptovermögen im österreichischen Recht	127
8.2.1 Konsequenzen für den Eigentumsschutz	128
8.2.2 Konsequenzen für das Insolvenzrecht	129
8.3 Vertragsrechtliche Behandlung kryptobasierter Dienstleistungen im österreichischen Recht	129
8.3.1 Vertragstypologie und hybride Leistungsmodelle.....	130
8.3.2 Leistungsstörungen und Risikoverteilung.....	131
8.3.3 Intransparente Leistungsbeschreibungen	131
8.4 Haftung und Risikoallokation bei kryptobasierten Dienstleistungen	132
8.4.1 Ausgangspunkt: Haftungssystematik im österreichischen Recht	133
8.4.2 Haftung für technische Systemrisiken	133
8.4.3 Haftung für Verlust von Token (z. B. durch Hacks oder Fehltransaktionen) .	134
8.4.4 Haftung bei Staking-, Lending- und Protokollinteraktionen	135
8.4.5 Haftung bei Fehlberatung und Informationspflichtverletzungen	135
8.5 Reformbedarf und normative Handlungsoptionen für einen zukunftsfähigen Verbraucherschutz	136
8.5.1 Einführung eines gesetzlichen Sondervermögensregimes für Kryptowerte	136

8.5.2 Klarstellung der Rechtsnatur von Token durch eine gesetzliche Definition .	137
8.5.3 Mindeststandards für Verwahr-, Plattform- und Stakingdienste	137
8.5.4 Anpassung des FAGG und des KSchG an digitale, technisch irreversible Dienstleistungen.....	138
8.5.5 Stärkung der kollektiven Rechtsdurchsetzung im Kryptobereich	139
8.5.6 Institutionelle Weiterentwicklung des Kryptoverbraucherschutzes	140
8.5.7 Gesamtsynthese.....	141
Literaturverzeichnis.....	143

Abkürzungsverzeichnis

ABGB – Allgemeines bürgerliches Gesetzbuch

AEUV – Vertrag über die Arbeitsweise der Europäischen Union

AGB – Allgemeine Geschäftsbedingungen

AIFMG – Alternative-Investmentfonds-Manager-Gesetz

AMLD5 – Fünfte Geldwäscherichtlinie der Europäischen Union

AML – Anti-Money Laundering

ART – Asset-Referenced Token

BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht

BGB – Bürgerliches Gesetzbuch (Deutschland)

BIS – Bank for International Settlements

BGBI – Bundesgesetzblatt

BoJ – Bank of Japan

BTC – Bitcoin

BWG – Bankwesengesetz

CASP – Crypto-Asset Service Provider

CBDC – Central Bank Digital Currency

CCAF – Cambridge Centre for Alternative Finance

CFTC – Commodity Futures Trading Commission

CNIL – Commission nationale de l’informatique et des libertés

COM – Dokument der Europäischen Kommission

CRD – Consumer Rights Directive

CRS – Congressional Research Service

DAO – Decentralized Autonomous Organization

DeFi – Decentralized Finance

DLT – Distributed Ledger Technology

DSGVO – Datenschutz-Grundverordnung

EBA – European Banking Authority

ECB – European Central Bank

EDPB – European Data Protection Board

E-Geld – Elektronisches Geld

EMT – E-Geld-Token

ESA – European Supervisory Authorities

ESMA – European Securities and Markets Authority

EU – Europäische Union

EuGH – Gerichtshof der Europäischen Union

EUR – Euro

EZB – Europäische Zentralbank

FAGG – Fern- und Auswärtsgeschäfte-Gesetz

FATF – Financial Action Task Force

FEDS – Finance and Economics Discussion Series

FMA – Finanzmarktaufsichtsbehörde / Finanzmarktaufsicht

FM-GwG – Finanzmarkt-Geldwäschegesetz

FSA – Financial Services Agency

FSB – Financial Stability Board

FTX – Bezeichnung der Kryptohandelsplattform FTX

GDPR – General Data Protection Regulation

ICO – Initial Coin Offering

IDF – in der Fassung

IO – Insolvenzordnung

IMF – International Monetary Fund

iSd – im Sinne des / der

JFSA – Japan Financial Services Agency

KMG – Kapitalmarktgesetz

KMG 2019 – Kapitalmarktgesetz 2019

KSchG – Konsumentenschutzgesetz

KYC – Know Your Customer

KWG – Kreditwesengesetz (Deutschland)

MAR – Marktmissbrauchsverordnung

MiCA – Markets in Crypto-Assets Regulation / Verordnung über Märkte für Kryptowerte

MiCAR – Markets in Crypto-Assets Regulation

MiCA-VO – Verordnung über Märkte für Kryptowerte

MiCA-VO-E – Entwurf der Verordnung über Märkte für Kryptowerte

MiCA-VVG – MiCA-Verordnung-Vollzugsgesetz

MiFID II – Markets in Financial Instruments Directive II

MTF – Multilateral Trading Facility

NFT – Non-Fungible Token

Nr – Nummer

OeNB – Oesterreichische Nationalbank

OECD – Organisation for Economic Co-operation and Development / Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

OGH – Oberster Gerichtshof

OTC – Over the Counter

OTF – Organised Trading Facility

P2P – Peer-to-Peer

PDF – Portable Document Format

PoS – Proof of Stake

PoW – Proof of Work

PRC – People's Republic of China

Prospekt-VO – Prospektverordnung

PSD2 – Second Payment Services Directive / Zweite Zahlungsdiensterichtlinie

RL – Richtlinie

RIS – Rechtsinformationssystem des Bundes

RTGS – Real-Time Gross Settlement

RTS – Regulatory Technical Standards

SEC – Securities and Exchange Commission

Self-Custody – Eigenverwahrung kryptografischer Vermögenswerte

SRO – Self-Regulatory Organization

SWD – Staff Working Document

UCPD – Unfair Commercial Practices Directive

UWG – Gesetz gegen den unlauteren Wettbewerb

USD – US-Dollar

USDC – USD Coin

USDT – Tether USD

UST – TerraUSD

ua – unter anderem

VO – Verordnung

VASP – Virtual Asset Service Provider

VKrG – Verbraucherkreditgesetz

WAG 2018 – Wertpapieraufsichtsgesetz 2018

Whitepaper – Informationsdokument über ein Kryptoprojekt oder Kryptoangebot

ZaDiG 2018 – Zahlungsdienstegesetz 2018

Kapitel 1

Einführung in die Thematik des Konsumentenschutzes bei Kryptowährungen

1.1 Problemstellung, Hintergrund und Aktualität von Kryptowährungen

Die fortschreitende Digitalisierung des Finanzsystems hat in den vergangenen eineinhalb Jahrzehnten grundlegende Veränderungen in der Struktur, Funktionsweise und Regulierung wirtschaftlicher Austauschprozesse bewirkt. Kryptowährungen und andere digitale Vermögenswerte stellen dabei einen radikalen Bruch mit traditionellen Formen des Geldes und des Finanzverkehrs dar. Statt zentralisierter Institutionen wie Banken oder Zahlungsdienstleister ermöglichen sie Transaktionen über global vernetzte, kryptografisch abgesicherte und technisch dezentrale Systeme. Diese Dezentralität eröffnet zwar neue ökonomische Möglichkeiten, wirft jedoch erhebliche rechtliche Fragen auf, insbesondere im Hinblick auf den Schutz von Verbraucher:innen.¹

Historisch begann die Entwicklung mit der Veröffentlichung des Bitcoin-Whitepapers im Jahr 2008 und der ersten Transaktion im Januar 2009.² Was zunächst als experimentelles Open-Source-Projekt technikaffiner Gemeinschaften erschien, entwickelte sich binnen kurzer Zeit zu einem globalen Finanzmarkt mit zeitweise mehrtrillionenschwerer Marktkapitalisierung.³ Parallel zu dieser Entwicklung entstand ein breites Spektrum an Kryptowerten – darunter Zahlungstoken wie Bitcoin oder Litecoin, Stablecoins wie USDT oder USDC, Utility-Token, Security-Token sowie zunehmend komplexe dezentrale Finanzanwendungen (DeFi) und Non-Fungible Tokens (NFTs). Diese Produkte entziehen sich oftmals klaren rechtlichen Kategorien, da sie funktional an traditionelle Instrumente erinnern, technisch, aber unterschiedliche Risikoprofile und Governance-Strukturen aufweisen.⁴

Ein zentrales Strukturmerkmal digitaler Vermögenswerte ist ihre ausgeprägte Preisvolatilität. Die damalige Kurssprünge von Bitcoin – etwa der Höchststand im November 2021 von rund 69.000 USD und der anschließende Fall auf unter 20.000 USD im Jahr 2022 – verdeutlichen die damit einhergehenden spekulativen Risiken.⁵ Diese Volatilität ist nicht nur ein ökonomisches Phänomen, sondern hat erhebliche verbraucherschutzrechtliche Relevanz, da Einlagensicherungssysteme und traditionelle Absicherungsinstrumente auf diese Produkte nicht anwendbar sind.

¹ Vgl. Binder Grösswang (Hrsg), Digital Law 2. Aufl., 2020, S. 45 ff.

² Vgl. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

³ Vgl. Cambridge Centre for Alternative Finance, 2nd Global Cryptoasset Regulatory Landscape Study, 2024, S. 12–20.

⁴ Vgl. Binder Grösswang (Hrsg), Digital Law 2. Aufl. 2020, S. 45 f.

⁵ Vgl. Europäische Zentralbank, „Bitcoin’s last stand“, ECB-Blog, 30.11.2022.

Besonders gravierend manifestieren sich die Risiken im Bereich zentralisierter Dienstleister wie Kryptobörsen. Der Zusammenbruch der Handelsplattform FTX im Jahr 2022 stellt ein paradigmatisches Beispiel dar: Fehlende Trennung von Kunden- und Eigenvermögen, mangelhafte Governance, unzureichende Risikokontrollen sowie komplexe konzerninterne Verflechtungen führten dazu, dass Milliardenbeträge an Kundengeldern verloren gingen.⁶ Die Insolvenz hatte nicht nur ökonomische Auswirkungen, sondern legte auch offen, dass bestehende nationale und internationale Regulierungsbestimmungen häufig nicht ausreichen, um Verbraucher:innen vor betrügerischen oder fahrlässigen Praktiken zu schützen.

Internationale Organisationen wie der Financial Stability Board (FSB) und die Financial Action Task Force (FATF) warnen seit Jahren vor erheblichen regulatorischen Lücken, Inkonsistenzen zwischen Staaten und unzureichenden Mindeststandards für Risikomanagement, Markttransparenz und Verbraucherschutz.⁷ Parallel dazu zeigt eine Vielzahl rechtswissenschaftlicher Analysen – unter anderem aus Österreich und Deutschland (z.B. Kryptowerte im Privatrecht, Digital Law) –, dass Kryptowährungen und Blockchain-basierte Anwendungen in zentrale Schutzmechanismen des privaten und öffentlichen Rechts hineinwirken und diese vor neue dogmatische Herausforderungen stellen.⁸

Die Europäische Union hat mit der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA) einen wesentlichen Schritt unternommen, um regulatorische Fragmentierung zu überwinden. MiCA schafft erstmals unionsweite Vorgaben für Emittenten und Dienstleister, regelt Zulassungspflichten, Transparenzanforderungen, Wohlverhaltenspflichten und bestimmte Mindeststandards des Verbraucherschutzes.⁹ Dazu konkretisieren Regulatory Technical Standards der Europäischen Bankenaufsichtsbehörde (EBA) operative Anforderungen, insbesondere im Bereich der Beschwerdeverfahren und organisatorischen Sicherheiten.¹⁰

In Österreich werden Kryptowert-Dienstleistungen bislang vor allem durch das Finanzmarkt-Geldwäschegesetz (FM-GwG) und das Kapitalmarktgesetz (KMG) erfasst. Seit 2024/2025 übernimmt die Finanzmarktaufsicht (FMA) die vollständige Aufsicht über Krypto-Asset-Dienstleister gemäß MiCA. Dennoch bestehen insbesondere im Zivilrecht – etwa bei der Frage der Eigentumszuordnung, Verantwortlichkeit, Haftung, Rechtsdurchsetzung und

⁶ Vgl. KPMG, The Collapse of FTX (2022) S. 5–12.

⁷ Vgl. FSB, Thematic Review on Crypto-Asset Activities, 16.10.2025, S. 3–8; vgl. FATF, Updated Guidance on Virtual Assets, 2025.

⁸ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 33 f; vgl. Binder Grösswang (Hrsg), Digital Law, 2. Aufl. 2020, S. 1-11.

⁹ Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte 2023/1114 (MiCA), ABl. L 150/40 vom 09.06.2023.

¹⁰ Vgl. EBA, Draft RTS under MiCAR, 13.03.2024, S. 12–15.

Absonderungsfähigkeit – erhebliche Unsicherheiten, wie rechtswissenschaftliche Studien und praktische Fälle zeigen.¹¹

International ist das Bild heterogen: China hat große Teile der Kryptotätigkeiten untersagt, während Japan ein strenges Lizenzierungssystem mit starken Verbraucherschutzgarantien implementiert hat.¹² Die USA setzen hingegen stark auf ex-post-Durchsetzung durch Aufsichtsbehörden wie SEC (Securities and Exchange Commission) und CFTC (Commodity Futures Trading Commission), wodurch zentrale Rechtsfragen häufig erst im Wege von Enforcement-Maßnahmen geklärt werden.¹³ Diese Divergenzen verdeutlichen, dass Verbraucher:innen weltweit mit Produkten agieren, deren rechtliche Einbettung stark variiert – bei gleichzeitig globalem Marktzugang.

Vor diesem Hintergrund gewinnt die Frage an Bedeutung, inwieweit der unionsrechtliche und österreichische Rechtsrahmen geeignet ist, Verbraucher:innen im Umgang mit digitalen Vermögenswerten vor den spezifischen, neuartigen und häufig technisch determinierten Risiken zu schützen. Die Notwendigkeit eines kohärenten, technologiefesten und funktionsorientierten Verbraucherschutzes ist evident.

1.2 Bedeutung von Kryptowerten und Konsumentenschutz

Die ökonomische und rechtliche Bedeutung von Kryptowerten hat in den letzten Jahren stark zugenommen und umfasst heute weit mehr als ein rein technisches oder spekulatives Phänomen. Digitalisierte Vermögenswerte sind zunehmend in den Alltag von Verbraucher:innen eingedrungen und haben sich zu einem eigenständigen Segment des Finanzmarkts entwickelt. Nach aktuellen internationalen Erhebungen besitzen weltweit mehrere hundert Millionen von Menschen Kryptowährungen, nutzen diese regelmäßig für Investments, Zahlungen, DeFi-Anwendungen oder als Zugangsschlüssel zu digitalen Ökosystemen.¹⁴ Dieser schnelle Markteintritt führt dazu, dass Verbraucher:innen mit Strukturen konfrontiert sind, deren Funktionsweise sie oft nur in Grundzügen verstehen. Ein zentrales Problem entsteht dadurch, dass die Systeme — anders als klassische Finanzdienstleistungen — ohne zentrale Verwahrstellen, ohne staatlich gesicherte Intermediäre und ohne traditionelle Rechtsschutzmechanismen operieren.

Ein wesentlicher Aspekt der Bedeutung von Kryptowerten für Verbraucher:innen liegt in ihrer ökonomischen Attraktivität, die sich aus der Kombination von hoher Renditeerwartung,

¹¹ Vgl. OBLIN Rechtsanwälte, Regulierung virtueller Währungen in Österreich, 2020.

¹² Vgl. Reuters, China's top regulators ban crypto trading and mining, 24.09.2021; FSA Japan Examination of the Regulatory Systems Related to Cryptoassets, 2025.

¹³ Vgl. PwC, Global Crypto Regulation Report 2025, 2025, S. 8-9.

¹⁴ Vgl. Sumsub, Global Cryptocurrency Regulations 2024, 10.10.2024.

Marktdynamik und medialer Aufmerksamkeit ergibt. Kryptowährungen wie Bitcoin und Ethereum werden häufig als innovationsgetriebene Investitionsformen wahrgenommen, die Zugang zu zukunftsorientierten Märkten bieten.¹⁵ Diese Wahrnehmung schafft hohe Anreize — aber sie ist zugleich trügerisch. Das Fehlen eines intrinsischen Werts, die Abhängigkeit von Marktstimmung und technischen Netzwerkeffekten sowie eine ausgeprägte spekulative Komponente führen dazu, dass Verbraucher:innen Risiken eingehen, die sie häufig nicht ausreichend abschätzen können. Die Europäische Zentralbank weist darauf hin, dass die Preisvolatilität digitaler Vermögenswerte weit über der von Aktien, Rohstoffen oder Devisen liegt und Verbraucher:innen daher erheblichen Verlustgefahren ausgesetzt sind.¹⁶

Neben den ökonomischen Risiken kommen strukturelle Informationsdefizite hinzu. Kryptowert-Dienstleistungen sind hochkomplex; sie beruhen auf kryptografischen Verfahren, verteilten Netzwerken, dezentralen Protokollen und automatisierten Smart Contracts. Für juristische Laien sind diese Mechanismen kaum durchschaubar, was die Fähigkeit zur informierten Entscheidungsfindung erheblich beeinträchtigt. Diese Informationsasymmetrie wird durch intransparente Werbepraktiken, irreführende Versprechen und gezielte manipulative Kommunikation insbesondere über soziale Netzwerke verstärkt. Rechtswissenschaftliche Literatur betont, dass die mangelnde technische Kompetenz der Verbraucher:innen eine systematische Schutzlücke schafft, die weder klassische Aufklärungspflichten noch Markttransparenzregelungen vollständig schließen können.¹⁷

Die technologischen Risiken digitaler Vermögenswerte verschärfen die Gefährdungslage erheblich. Der Verlust eines privaten Schlüssels — der einzigen Möglichkeit, über einen Kryptowert zu verfügen — führt irreversibel zum Verlust des Vermögenswerts. Bei fehlerhaften oder kompromittierten Wallets, Software-Schwachstellen oder unzureichend geprüften Smart Contracts können Schäden eintreten, die technisch nicht rückgängig gemacht werden können.¹⁸ Besonders problematisch ist die Instabilität sogenannter Cross-Chain-Bridges, also Infrastrukturen, die den Austausch zwischen unterschiedlichen Blockchains ermöglichen. Diese gelten als besonders anfällig für Cyberangriffe und wurden bereits vielfach Ziel von Hackerangriffen mit Milliardenverlusten.¹⁹ Für Verbraucher:innen bedeutet dies, dass selbst bei Nutzung renommierter Plattformen ein erhebliches Sicherheitsrisiko bleibt.

¹⁵ Vgl. Cambridge Centre for Alternative Finance, 2nd Global Cryptoasset Regulatory Landscape Study, 2024, S. 11-12.

¹⁶ Vgl. Europäische Zentralbank, „Bitcoin’s last stand“, ECB-Blog, 30.11.2022.

¹⁷ Vgl. Cambridge Centre for Alternative Finance, 2nd Global Cryptoasset Regulatory Landscape Study, 2024.

¹⁸ Vgl. Weilingner/Miernicki in Kirchmayr-Schliesselberger/Klas/Miernicki/Rinderle-Ma/Weilingner, Kryptowährungen (2019) S. 96 f, 101, 33-35.

¹⁹ Vgl. OECD, Tokenisation of Assets, 2020, S. 45 ff.

Zentral für die verbraucherschutzrechtliche Bewertung ist zudem die zivilrechtliche Einordnung von Kryptowerten. Die Frage, ob Kryptowährungen als Sachen, Forderungen, sonstige Rechte oder sui-generis-Positionen zu qualifizieren sind, ist weder unionsrechtlich noch österreichisch abschließend geklärt. Vorhandenen Literaturen zeigen, dass unterschiedliche dogmatische Konstruktionen existieren, etwa als „unkörperliche Sachen“, als „digitale Vermögensrechte“ oder als „datumsbasierte Rechtspositionen“.²⁰ Diese Unsicherheit wirkt sich unmittelbar auf Eigentumsübertragung, Vertragspflichten, Sicherungsrechte und Insolvenzfestigkeit aus.

Besonders kritisch ist der Umgang mit Vermögen im Insolvenzfall von Kryptodienstleistern: Ob Verbraucher:innen Aussonderungsrechte geltend machen können oder nur einfache Insolvenzgläubiger sind, hängt von der rechtlichen Einordnung des verwahrten Kryptowerts ab, eine Frage, die in Österreich bislang nicht abschließend geregelt ist.²¹

Hinzu kommt die Governance-Problematik dezentraler Netzwerke. Obwohl Blockchain-Systeme technisch anscheinend transparent sind, ist die tatsächliche Entscheidungsgewalt häufig zentralisiert, etwa bei Entwicklerteams, dominanten Validatoren oder Mining-Pools.²² Diese Akteure kontrollieren Protokollupdates, können Konsensmechanismen beeinflussen und faktisch den Zugang zum Netzwerk steuern. Für Verbraucher:innen entsteht damit ein paradoxes Verhältnis: Einerseits suggeriert Dezentralität einen Wegfall von Intermediären, andererseits bestehen verdeckte Machtstrukturen, die die Sicherheit und Funktionalität des Netzwerks bestimmen jedoch ohne traditionelle Aufsicht, Haftung oder Governance-Mechanismen.

Ein besonders ausgeprägtes Risiko für Verbraucher:innen ist die Abhängigkeit von zentralen Dienstleistern, insbesondere Kryptobörsen und Verwahrstellen. Trotz des dezentralen Charakters der Technologie erfolgt der konkrete Erwerb, Handel und die Verwahrung digitaler Vermögenswerte in der Praxis weit überwiegend über zentral organisierte Handelsplattformen. Die Insolvenz von FTX hat eindrücklich gezeigt, dass unzureichende Corporate Governance, fehlende Trennung von Kunden- und Eigenvermögen, mangelhafte Compliance und fehlende Transparenz zu massiven Vermögensverlusten führen können.²³ Darüber hinaus erschweren internationale Struktur, Sitzverlagerungen und fehlende klare Zuständigkeiten eine effektive Rechtsdurchsetzung.

Aus ökonomischer Perspektive ist der Konsumentenschutz nicht nur eine individuelle Schutzmaßnahme, sondern eine systematische Voraussetzung für die Stabilität digitaler

²⁰ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 32 f.

²¹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 79, 102–104.

²² Vgl. ESMA, Decentralised Finance Report, 2023, S. 5 f.

²³ Vgl. Model Framework for Consumer Protection and Crypto-Exchanges Regulation, 2023, S 2-11.

Finanzmärkte. Ohne klare rechtliche Rahmenbedingungen entsteht ein fragiles Marktumfeld, in dem Verbraucher:innen hohe Risiken tragen, jedoch Anbieter in vielen Fällen nicht ausreichend reguliert oder beaufsichtigt werden. Internationale Vergleichsstudien belegen, dass Staaten mit kohärentem, technologiefestem Verbraucherschutz eine deutlich höhere Marktstabilität und Nutzervertrauen aufweisen.²⁴

Die MiCA-Verordnung stellt den ersten unionsweit einheitlichen Versuch dar, Verbraucher:innen im Kryptomarkt zu schützen. Allerdings ist sie in ihrer Schutzlogik begrenzt: Dezentrale Anwendungen bilden eine strukturelle Ausnahme, reine Peer-to-Peer-Transaktionen werden nicht erfasst, und zivilrechtliche Fragen, insbesondere Eigentum, Haftung, Irrtumsanfechtung und Rückabwicklung, bleiben weitgehend ungeregt.²⁵ Dadurch entsteht ein „Regulierungsschatten“, der genau jene Bereiche betrifft, in denen Verbraucher:innen am häufigsten Risiken ausgesetzt sind.

1.3 Regulatorische Unsicherheit und daraus resultierender Handlungsbedarf

Die Regulierung digitaler Vermögenswerte befindet sich weltweit in einem tiefgreifenden Transformationsprozess. Die rasante technologische Entwicklung, die globale Verfügbarkeit von Kryptowerten und die zunehmende Bedeutung dezentraler Finanzstrukturen haben dazu geführt, dass bestehende rechtliche Kategorien und Mechanismen vielfach überfordert oder unzureichend sind. Zahlreiche rechtswissenschaftliche Publikationen und internationale Berichte weisen darauf hin, dass die Rechtslage sowohl auf unionsrechtlicher als auch auf nationaler Ebene fragmentiert ist und strukturelle Schutzlücken aufweist, die insbesondere Verbraucher:innen betreffen.²⁶

Ein zentrales Problem besteht darin, dass Kryptowährungen — anders als traditionelle Finanzinstrumente — keiner universellen und kohärenten globalen Definition unterliegen. Staaten und internationale Organisationen verwenden unterschiedliche Terminologien („virtual assets“, „crypto-assets“, „digital property“, „digital commodities“), die jeweils unterschiedliche Rechtsfolgen auslösen.²⁷ Diese unterschiedliche rechtliche Qualifikation erschwert es nicht nur Verbraucher:innen, sondern auch Anbietern, die Reichweite ihrer Rechte und Pflichten einzuschätzen. Für grenzüberschreitende Sachverhalte, wie sie im Kryptomarkt alltäglich sind, führt dies zu erheblichen Rechtsunsicherheiten.

²⁴ Vgl. OECD, The Tokenisation of Assets and Potential Policy Implications, 2020, S. 8,11,41.

²⁵ Vgl. Verordnung (EU) 2023/1114 (MiCA), ABl. L 150/40 vom 09.06.2023.

²⁶ Vgl. Europäische Kommission, Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA) DE, KOM (2020), S. 19.

²⁷ Vgl. Cambridge Centre for Alternative Finance, 2nd Global Cryptoasset Regulatory Landscape Study, 2024, S. 28.

Die Europäische Union hat mit der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA) zwar einen wichtigen Schritt zur Harmonisierung gesetzt, doch umfasst dieser Rechtsrahmen nicht alle technologischen und ökonomischen Erscheinungsformen des Kryptomarkts. MiCA definiert Kryptowerte funktional und differenziert zwischen Asset-Referenced Tokens, E-Geld-Token und sonstigen Kryptowerten.²⁸ Diese Definitionen ermöglichen zwar eine systematische Regulierung zentraler Dienstleister, erfassen jedoch keine dezentralen Anwendungen (DeFi), keine reinen Peer-to-Peer-Transaktionen, keine dezentral organisierten Verwahrmechanismen (Self-Custody) und keine algorithmischen Stablecoins ohne identifizierbaren Emittenten.²⁹ Dadurch entsteht ein erheblicher Regulierungsbereich, der „im Schatten“ der MiCA verbleibt.

Hinzu kommt, dass MiCA primär ein aufsichtsrechtliches Instrument darstellt und kaum zivilrechtliche Fragestellungen adressiert. Fragen wie:

Wem „gehört“ ein Kryptowert zivilrechtlich? Welche Rechte bestehen bei Verlust privater Schlüssel? Wie erfolgt die Rückabwicklung fehlerhafter Transaktionen? Welche Ansprüche bestehen gegen Plattformen bei Cyberangriffen oder technischen Fehlern? Welche Vermögenszuordnung gilt im Insolvenzfall eines Dienstleisters? verbleiben weitgehend ungeregt.

Während einzelne Ansätze Kryptowährungen als „unkörperliche Sachen sui generis“ einordnen, argumentieren andere für eine rechtlich relevante Datenposition, ein obligatorisches Anspruchsrecht oder eine „technisch determinierte Vermögensposition“. Die fehlende dogmatische Einordnung verhindert die Entwicklung klarer Regeln für Eigentumsübertragung, Sicherungsrechte, Schadensersatz, vertragliche Pflichten und Insolvenzschutz.

Die österreichische Rechtslage illustriert diese Problematik besonders deutlich. Während das Finanzmarkt-Geldwäschegesetz (FM-GwG) und das Kapitalmarktgesetz (KMG) Kryptowert-Dienstleister adressieren, fehlt ein kohärenter zivilrechtlicher Rahmen, der Rechte und Pflichten aus dem Umgang mit Kryptowerte eindeutig regelt. Auch die FMA hat im Rahmen ihrer Auslegungshinweise wiederholt darauf hingewiesen, dass viele privatrechtliche Fragen ungelöst bleiben und im Streitfall nur analog oder über allgemeine Regeln des ABGB beantwortet werden können und oft mit erheblichen Unsicherheiten für Verbraucher:innen.

Die rechtswissenschaftliche Literatur spricht daher zunehmend von einer „regulatorischen Interdependenz“, bei den technischen, ökonomischen und rechtlichen Risiken miteinander verflochten sind und traditionelle normative Konzepte überfordern. Viele Regulierungsbehörden

²⁸ Vgl. Art. 3 Abs. 1 Nr. 5, 6 und 7 sowie Titel II–IV der Verordnung (EU) 2023/1114 (MiCA).

²⁹ Vgl. Erwägungsgrund 22 sowie Art. 3 Abs. 1 Nr. 5, 6 und Nr. 15–24. MiCA (Verordnung (EU) 2023/1114).

erkennen, dass bestehende Instrumente weder die technische Komplexität noch die global vernetzte Marktstruktur noch die fehlende institutionelle Verantwortlichkeit ausreichend erfassen.

In der Konsequenz entsteht ein struktureller Handlungsbedarf auf drei Ebenen:

Dogmatische Ebene: Entwicklung einer konsistenten zivilrechtlichen Einordnung digitaler Vermögenswerte, die Eigentum, Sicherheiten und Haftung klar regelt.

Regulatorische Ebene: Erweiterung bestehender Aufsichtsregime (MiCA, AML-Regime, PSD2) um dezentrale Strukturen, algorithmische Stablecoins, Peer-to-Peer-Transaktionen und hybride Governance-Modelle und andere relevante Punkte.

Institutionelle Ebene: Stärkung grenzüberschreitender Kooperationsmechanismen sowie Schaffung zentraler Anlaufstellen und Rechtsschutzinstrumente für Verbraucher:innen. Erst durch eine umfassende rechtliche, technische und institutionelle Weiterentwicklung kann ein nachhaltiges Verbraucherschutzniveau gewährleistet werden, das den Besonderheiten digitaler Vermögenswerte gerecht wird.

1.4 Forschungsziel, Forschungsfragen und methodisches Vorgehen

Die zunehmende Verbreitung digitaler Vermögenswerte und die damit verbundene Transformation des Finanzsystems stellen das bestehende Rechtsgefüge vor grundlegende Herausforderungen. Während traditionelle Finanzmärkte auf klar definierten Akteursstrukturen, institutionellen Verantwortlichkeiten und erprobten Aufsichtsmechanismen basieren, sind Kryptowährungen, Tokenisierungsvorgänge und dezentrale Systeme strukturell anders aufgebaut. Diese technologischen und ökonomischen Eigenheiten bedingen eine Rechtsentwicklung, die sich nicht lediglich an bestehende Kategorien anlehnt, sondern diese grundlegend neu denkt. Vor diesem Hintergrund verfolgt die vorliegende Arbeit das Ziel, die unionsrechtliche und österreichische Regulierung digitaler Vermögenswerte einer umfassenden Bewertung zu unterziehen und insbesondere deren Wirksamkeit im Hinblick auf den Verbraucherschutz zu analysieren.

Das zentrale Anliegen besteht darin, die bestehenden Schutzmechanismen für Verbraucher:innen im Bereich der Kryptowährungen systematisch zu untersuchen und normative Handlungsempfehlungen zu entwickeln. Dabei wird nicht nur auf die formelle Existenz regulatorischer Vorgaben abgestellt, sondern auch deren funktionale Wirksamkeit und praktische Umsetzbarkeit beurteilt. Schließlich ist Regulierung im digitalen Bereich nur dann effektiv, wenn sie in der Lage ist, tatsächliche Risiken zu reduzieren und gleichzeitig Innovationen nicht unnötig zu behindern.

Die wissenschaftliche Relevanz dieser Fragestellung ergibt sich aus mehreren Faktoren: Erstens bewegen sich Kryptowährungen häufig in regulatorischen Räumen, die bislang unzureichend erfasst sind oder in denen rechtliche Fragmentierung besteht. Zweitens zeigt die rechtswissenschaftliche Literatur, dass die zivilrechtliche Behandlung digitaler Vermögenswerte aus dieser Sicht, noch nicht ausreichend systematisiert ist.³⁰ Drittens verfügen Verbraucher:innen regelmäßig weder über die technische Expertise noch über die rechtliche Orientierung, die zur Einschätzung von Chancen und Risiken erforderlich wäre. Die fehlende Klarheit über Eigentumsrechte, Aufklärungspflichten, Rückabwicklungsmechanismen, Aufsichtsstrukturen und Haftungsfragen entspricht einem strukturellen Defizit, das zunehmend gesamtwirtschaftliche Dimensionen annimmt.³¹

Vor diesem Hintergrund ergeben sich die zentralen Forschungsfragen dieser Arbeit:

- (1) Welche technologischen, ökonomischen und rechtlichen Risiken entstehen für Verbraucher:innen im Umgang mit Kryptowährungen und digitalen Vermögenswerten?
- (2) Inwiefern bietet die MiCA-Verordnung ein angemessenes und technologiefestes Verbraucherschutzniveau?
- (3) Welche Schutzmechanismen gewährt der österreichische Rechtsrahmen, und wo bestehen strukturelle Lücken?
- (4) Welche Erkenntnisse liefert der internationale Rechtsvergleich (USA, China, Japan) für die Weiterentwicklung des Verbraucherschutzes im Kryptomarkt?
- (5) Welche normativen Vorschläge lassen sich entwickeln, um ein kohärentes und effektives Verbraucherschutzniveau zu gewährleisten?

Methodisches Vorgehen

Die vorliegende Untersuchung folgt einem methodisch mehrdimensionalen Ansatz, der juristische und ökonomische Perspektiven kombiniert und dabei dem besonderen interdisziplinären Charakter des Themas gerecht wird. Die Methodik umfasst vier zentrale Elemente:

(a) Rechtswissenschaftliche Analyse

Die Untersuchung beginnt mit einer systematischen Darstellung und Auslegung unionsrechtlicher Normen — insbesondere der MiCA-Verordnung, der PSD2, DSGVO und der einschlägigen Anforderungen der Geldwäscheprevention — sowie der österreichischen Normen, insbesondere FM-GwG, KMG und relevanter ABGB-Bestimmungen. Die Analyse erfolgt unter Einbeziehung aktueller Literatur wie Digital Law, Kryptowerte im Privatrecht,

³⁰ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2.Aufl. 2020, S. 45 ff.

³¹ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2.Aufl. 2020, S. 45 f.

Kryptowährungen, OBLIN-Kommentare, sowie der technischen Regulierungsstandards (RTS-Regulatory Technical Standard) der EBA (European Banking Authority) und auch zahlreiche andere Dokumente.

(b) Funktionsorientierte Betrachtung des Verbraucherschutzes

Im Gegensatz zu rein normativ systematischen Modellen berücksichtigt die Arbeit die „funktionale Wirksamkeit“ von Verbraucherschutznormen:

- Schützen sie Verbraucher:innen tatsächlich?
- Sind sie technisch umsetzbar?
- Werden neue Risiken adäquat berücksichtigt?

Diese Perspektive orientiert sich an internationalen Benchmarks wie dem FSB oder FATE.

(c) Rechtsvergleichende Analyse

Die Analyse vergleicht die europäische und österreichische Rechtslage mit jenen der USA, Chinas und Japans. Die Auswahl dieser Staaten basiert auf ihrer regulatorischen Diversität und ihrem globalen Einfluss. Dieser Vergleich ermöglicht, Best-Practice-Modelle zu identifizieren und strukturelle Schwächen des EU-Systems herauszuarbeiten.

(d) Normative Synthese

Abschließend werden die Ergebnisse der dogmatischen, funktionalen und rechtsvergleichenden Analyse gebündelt und in konkrete Reformvorschläge überführt. Diese Vorschläge sollen technologische Eigenschaften digitaler Vermögenswerte berücksichtigen und gleichzeitig rechtliche Kohärenz sicherstellen.

Die Verbindung dieser methodischen Ansätze ermöglicht eine umfassende Bearbeitung der Forschungsfragen und liefert die Grundlage für die Entwicklung eines gut ausgestatteten und zukunftsfähigen Verbraucherschutzrahmens im Bereich digitaler Vermögenswerte.

1.5 Aufbau der Arbeit

Die vorliegende Arbeit ist systematisch so aufgebaut, dass sie die komplexe, interdisziplinäre und vielfach noch ungeklärte Rechtsmaterie der digitalen Vermögenswerte Schritt für Schritt erschließt. Der Aufbau folgt einer wissenschaftlichen Logik, die sowohl der technischen Besonderheit als auch den juristischen Herausforderungen dieses Themas Rechnung trägt. Ziel ist es, die zentralen Fragestellungen nicht isoliert, sondern im Zusammenhang der technologischen Grundlagen, der ökonomischen Dynamiken, der unionsrechtlichen Regulierung, der nationalen Rechtslage und der internationalen Vergleichsmodelle zu analysieren.

Kapitel 2: Theoretische Grundlagen, Begriffsbestimmungen und ökonomisch-technische Einordnung

Kapitel 2 legt die begriffliche und theoretische Grundlage der vorliegenden Arbeit. Es analysiert die grundlegenden technischen Mechanismen von Blockchain-Systemen, Konsensverfahren, Token-Arten und Smart Contracts und ordnet diese in die bestehende Rechtsontologie ein. Dabei werden zentrale theoretische Ansätze aufgegriffen, die die Natur digitaler Vermögenswerte erläutern. Dieses Kapitel dient dazu, die terminologische und juristische Präzision sicherzustellen, dass ohne die eine vertiefte rechtliche Analyse nicht möglich wäre.

Kapitel 3: Analyse der technologischen, ökonomischen und rechtlichen Risiken für Verbraucher:innen

Kapitel 3 widmet sich der detaillierten Untersuchung der Risiken, denen Verbraucher:innen beim Umgang mit Kryptowährungen ausgesetzt sind. Dies umfasst Preisvolatilität, technologische Verwundbarkeiten, Smart-Contract-Risiken, Cyberangriffe, Funktionsstörungen dezentraler Protokolle, Intransparenz zentralisierter Dienstleister sowie Marktmissbrauch. Die Analyse erfolgt auf der Grundlage wissenschaftlicher Literatur, empirischer Studien, aktueller Marktberichte sowie rechtswissenschaftlicher Publikationen. Dieses Kapitel schafft die notwendige Grundlage, um die Effektivität bestehender Verbraucherschutzregime analysieren zu können.

Kapitel 4: Unionsrechtlicher Rechtsrahmen mit Schwerpunkt auf der MiCA-Verordnung

Kapitel 4 untersucht detailliert die Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA) sowie ihre flankierenden technischen Regulierungsstandards (EBA-RTS, ESMA-Standards). Die Analyse umfasst insbesondere die Zulassungsanforderungen für Emittenten und Dienstleister, organisatorische Pflichten, Verbraucherschutzmechanismen, Transparenzanforderungen, Regelungen zu Asset-Referenced Tokens und E-Geld-Token sowie die strukturellen Grenzen der Verordnung, insbesondere bezogen auf DeFi, algorithmische Stablecoins und P2P-Transaktionen. Dieses Kapitel zeigt, inwieweit MiCA in der Lage ist, die im vorherigen Kapitel identifizierten Risiken zu adressieren.

Kapitel 5: Nationale Umsetzung und österreichischer Rechtsrahmen

Kapitel 5 behandelt das österreichische Recht und seine Schnittstellen zur MiCA-Verordnung. Zentrale Regelungswerke wie das FM-GwG, das KMG, steuerrechtliche Bestimmungen, insolvenzrechtliche Normen sowie die Rechtsprechung und Verwaltungspraxis der FMA werden analysiert. Die Untersuchung zeigt, inwieweit das österreichische Recht Verbraucher:innen schützt oder ob - wie zahlreiche juristische Autoren betonen - strukturelle Lücken bestehen,

etwa bei Eigentumszuordnung, Rückabwicklung fehlerhafter Transaktionen oder der Insolvenzfestigkeit digitaler Vermögenswerte.

Kapitel 6: Internationaler Vergleich (USA, China, Japan)

Kapitel 6 dient der rechtsvergleichenden Betrachtung und analysiert drei sehr unterschiedliche Regulierungsmodelle:

USA: Auf die effektive Durchsetzung ausgerichtet, durch SEC/CFTC geprägt, ohne kohärenten legislativ definierten Rechtsrahmen;

China: Restriktiv, mit umfassenden Verboten für Handel und Mining, stärker staatlich motivierte Risikoreduktion;

Japan: Hochreguliert, technologiefest, Verbraucherschutzorientiert, mit klaren Verwahrungsvorschriften und Vermögenstrennung.

Der Vergleich dient der Analyse, welche Elemente internationaler Regulierungsansätze als Vorbild dienen können und welche Risiken unterschiedliche Regulierungsmodelle hervorbringen.

Kapitel 7: Bewertung der Effektivität bestehender Schutzmechanismen

Kapitel 7 bündelt die Ergebnisse der bisherigen Untersuchung und prüft, inwieweit die derzeitigen unionsrechtlichen und nationalen Schutzmechanismen geeignet sind, die identifizierten Risiken zu adressieren. Die Bewertung erfolgt anhand funktionaler Kriterien wie Rechtssicherheit, Durchsetzbarkeit, Transparenz, Verantwortungszuordnung, technologische Anschlussfähigkeit und institutionelle Leistungsfähigkeit. Dabei werden sowohl normative als auch praktische Aspekte berücksichtigt, etwa die Rechtsdurchsetzung bei internationalen Sachverhalten, technische Implementierbarkeit oder Lücken in der zivilrechtlichen Haftung.

Kapitel 8: Reformvorschläge und normative Handlungsempfehlungen

Das abschließende Kapitel 8 entwickelt konkrete Reformoptionen und Empfehlungen für eine zukunftsfähige Regulierung digitaler Vermögenswerte. Diese Vorschläge basieren auf der Verbindung dogmatischer Erkenntnisse, empirischer Analysen und internationaler Vergleichsergebnisse. Die Empfehlungen betreffen unter anderem Klarstellungen zur rechtlichen Einordnung digitaler Vermögensobjekte, notwendige Ergänzungen der MiCA-Verordnung, Anpassungen des österreichischen Zivil- und Aufsichtsrechts sowie institutionelle Entwicklungen im Bereich des Verbraucherschutzes.

Der systematische Aufbau gewährleistet somit, dass jede Ebene der Analyse auf klar definierten Grundlagen basiert und gleichzeitig die Komplexität der Materie berücksichtigt. Dies ermöglicht eine differenzierte, wissenschaftlich fundierte und praxisrelevante Untersuchung der Rechtslage digitaler Vermögenswerte im Kontext des Verbraucherschutzes.

Kapitel 2

Theoretische Grundlagen, Begriffsbestimmungen und ökonomisch-technische Einordnung

2.1 Philosophie des Geldes und Begriffsgrundlagen digitaler Vermögenswerte

Die Auseinandersetzung mit Kryptowährungen und digitalen Vermögenswerten setzt zwingend ein grundlegendes Verständnis der Natur des Geldes voraus. Die Frage, was Geld ist und welche Funktionen es erfüllt, gehört zu den ältesten und zugleich umstrittensten Themen ökonomischer und rechtsphilosophischer Diskussionen.³² Eine präzise begriffliche Grundlage ist unverzichtbar, besonderes bei digitalen Vermögenswerten die traditionellen Kategorien des Geldes kritisch hinterfragen und zugleich neue Formen der Wertrepräsentation schaffen. Die Besonderheit besteht darin, dass Kryptowährungen weder durch staatliche Anordnung geschaffen noch zwingend durch materielle oder institutionelle Deckung gestützt sind. Damit werden etablierte rechtliche und philosophische Grundannahmen in Frage gestellt, die in der bisherigen Geldtheorie als selbstverständlich galten.

2.1.1 Klassische Geldtheorien und ihre Herausforderungen im digitalen Kontext

Traditionelle Geldtheorien verstehen Geld als ein soziales oder rechtliches Konstrukt, das bestimmte Funktionen erfüllt: Tauschmittel, Recheneinheit und Wertaufbewahrungsmittel.³³ Die Chartalistische Theorie (Knapp, Innes) betont die Rolle des Staates bei der Schaffung und Konstitution von Geld, das in erster Linie durch Steuerforderungen und hoheitliche Akzeptanz fixiert wird.³⁴ Die Kreditgeldtheorie begreift Geld als Ergebnis wechselseitiger Verrechnung, als Versprechen und Forderung innerhalb eines rechtlich strukturierten Schuldverhältnisses.³⁵ Kryptowährungen wie Bitcoin stehen außerhalb dieses Systems: Sie entstehen nicht durch staatliche Normsetzung, nicht durch Banken oder Kreditbeziehungen, sondern durch algorithmische Konsensmechanismen. Sie sind weder gesetzliche Zahlungsmittel noch durch staatliche Accept-or-Pay-Regime geschützt. Damit widersprechen sie der chartalistischen Grundannahme, wonach Geld seine Geltung durch hoheitliche Autorität erlangt.³⁶ Gleichzeitig bestätigt die rasante globale Verbreitung von Kryptowerten die These moderner sozialkonstruktivistischer Ansätze (Searle, Lawson), denen zufolge wirtschaftliche Institutionen

³² Vgl. Kraemer, Klaus / Brugger, Florian (Hrsg.), Schlüsselwerke der Wirtschaftssoziologie, 2. Aufl., Wiesbaden 2021, S. 69–74. (Philosophie des Geldes von Georg Simmel).

³³ Vgl. Bundesrat Schweiz, Bericht des Bundesrates zu virtuellen Währungen, 2018, S. 7.

³⁴ Vgl. Innes, Alfred Mitchell, what is Money? 1913, S. 4 ff.

³⁵ Vgl. Lawson, Social Positioning and the Nature of Money, 2016, S. 963, 986; vgl. Jakelja, Geoffrey Ingham, The Nature of Money, in: Schlüsselwerke der Wirtschaftssoziologie, 2. Aufl. 2021, S. 457–458.

³⁶ Vgl. Schweizer Bundesrat, DLT-Bericht 2018, S. 17 f., 37; vgl. Lawson, Social Positioning and the Nature of Money 2016, S. 978 f.; vgl. Ingham, in: Schlüsselwerke der Wirtschaftssoziologie 2021, S. 459 f.

- einschließlich Geld - durch kollektive Akzeptanz und geteilte Bedeutung konstituiert werden.³⁷ Digitale Vermögenswerte demonstrieren, dass selbst in Abwesenheit staatlichen Zwangs neue Formen ökonomischer Realität entstehen können, sofern eine hinreichende Menge an Marktteilnehmer:innen das zugrunde liegende Symbolsystem akzeptiert.

2.1.2 Geld als Rechtsinstitut und die Notwendigkeit der digitalen Rechtsdogmatik

Moderne rechtswissenschaftliche Literatur versteht Geld zunehmend als **Rechtsinstitut**, dessen Geltungsgrund und Funktionsweise durch rechtliche Normen, institutionelle Rahmenbedingungen und soziale Praktiken bestimmt werden.³⁸ Kryptowährungen werfen die Frage auf, ob digitale Werte in die bestehenden geldrechtlichen Kategorien eingeordnet werden können oder ist dafür eine eigenständige rechtliche Einordnung erforderlich.

Aufgrund ihrer nichthaptischen Existenz und fehlender zentraler Herausgeber entsprechen sie keiner klassischen Vermögenskategorie des ABGB. Dieses rechtliche Spannungsfeld ist für den Verbraucherschutz von besonderer Bedeutung: Nur mit einer klaren Qualifikation lassen sich Eigentum, Besitzschutz, Übertragung, Sicherheiten und Insolvenzfestigkeit juristisch solide regeln.³⁹

2.1.3 Token, Blockchain und digitale Vermögensobjekte als neue Form der Wertrepräsentation

Blockchain-basierte Vermögenswerte funktionieren nicht als physische Güter, sondern als kryptografisch gesicherte Datenpositionen, deren Inhaberschaft durch den Besitz kryptografischer Schlüssel bestimmt wird.⁴⁰ Diese Struktur führt dazu, dass die Verfügungsmacht über digitale Werte nicht durch staatliche Register, sondern durch mathematische Operationen erzeugt wird.

Die rechtliche Konsequenz besteht darin, dass der Zugang zu einem digitalen Vermögenswert gleichzeitig, ein technischer Akt (Schlüsselinhalt), ein ökonomischer Akt (Vermögenssträgerschaft) und ein rechtlich hochrelevanter Akt (Inhalt einer vermögensrechtlichen Position) ist. Damit entsteht eine neue Art von Rechtsobjekt, das weder als reine Information noch als klassisches Wirtschaftsgut verstanden werden kann.

³⁷ Vgl. Lawson, Social Positioning and the Nature of Money 2016, S. 970 f.

³⁸ Vgl. Kryptowerte im Privatrecht, S. 16; sowie Smit/Buekens/du Plessis, What Is Money? An Alternative to Searle's Institutional Facts, S. 1-6.

³⁹ Vgl. Schweizer Bundesrat, Rechtliche Grundlagen der Distributed-Ledger-Technologie 2018, S. 52 f., 62–66, 68 f.

⁴⁰ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 115, 124, 132; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 52.

2.1.4 Dezentralität, Selbstorganisation und Governance als philosophische Herausforderung

Die Dezentralität der Blockchain stellt eine grundlegende Herausforderung für traditionelle ökonomische und juristische Ordnungen dar. In klassischen Finanzsystemen existieren klare institutionelle Verantwortlichkeiten: Zentralbanken, Aufsichtsbehörden, Intermediäre. In dezentralen Netzwerken dagegen verteilen sich Validierung, Regelsetzung und Governance auf eine Vielzahl oft anonymer Akteure.⁴¹

Philosophisch gesehen rührt dies an die Frage, ob normative Ordnungen ohne zentrale Autorität funktionieren können oder ob Dezentralität selbst eine neue Form digitaler Institutionalisierung darstellt. Lawson beschreibt dies als neue Entwicklungen „sozialer Positionierungssysteme“, die durch technische Regeln statt durch gesetzliche Normen entstehen.⁴² Im Kontext des Verbraucherschutzes führt dies zu erheblichen Problemen: Dezentralität erschwert Rechtsschutz, Verantwortlichkeitszuordnung und Durchsetzung.

2.1.5 Konsequenzen für die rechtliche Analyse

Aus diesen Überlegungen ergeben sich mehrere zentrale Erkenntnisse, die die Grundlage der weiteren Kapitel bilden:

Kryptowerte sind keine bloße technische Erscheinung, sondern ein neues rechtliches Phänomen, das bestehende Kategorien überdehnt.

Die klassische Geldtheorie reicht nicht aus, um digitale Vermögenswerte zu beschreiben; eine erweiterte rechtlich-philosophische Perspektive ist notwendig. Digitale Vermögenswerte erfordern eine Neubewertung bestehender Eigentumskonzepte, da Inhaberschaft, Verfügung, Verlust, technisch, ökonomisch und rechtlich voneinander abweichen.

Fehlende Verantwortlichkeit und Dezentralisierung stellen das bestehende Verbraucherschutzrecht vor strukturelle Grenzen.

Die Entwicklung einer technologiefesten Rechtsdogmatik ist zwingend erforderlich, um Regulierung, Haftung, Eigentum und Insolvenzrecht konsistent zu gestalten.

2.2 Definition und zentrale Konzepte von Kryptowährungen

Die genaue Definition von Kryptowährungen und digitalen Vermögenswerten ist ein grundlegender Ausgangspunkt für jede rechtswissenschaftliche Untersuchung in diesem Bereich. Die Vielfalt der Erscheinungsformen, die schnelle technologische Weiterentwicklung

⁴¹ Vgl. Schweizer Bundesrat, DLT-Bericht 2018, S. 54 f; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 271 f.

⁴² Vgl. Smit/Buekens/du Plessis, What Is Money? An Alternative to Searle's Institutional Facts, S. 14; vgl. Lawson, Social Positioning and the Nature of Money, S. 963 f.

sowie das Fehlen kohärenter gesetzlicher Definitionen in zahlreichen Rechtsordnungen führen dazu, dass Begriffe wie „Kryptowährung“, „Token“, „digitale Vermögenswerte“, „Krypto-Assets“ oder „virtuelle Währungen“ weder einheitlich verwendet noch eindeutig voneinander abgrenzbar sind.⁴³ Für eine juristische Analyse - insbesondere im Hinblick auf Verbraucherschutz, Aufsichtspflichten, Haftungsfragen und zivilrechtliche Einordnung - ist jedoch eine klare, funktionsorientierte und zugleich technologisch präzise Begriffsbestimmung unerlässlich.

2.2.1 Kryptowährungen als digitale, kryptografisch gesicherte Wertrepräsentationen

In der ökonomischen und technischen Literatur werden Kryptowährungen häufig als „kryptografisch gesicherte digitale Werteinheiten“ beschrieben, die über ein verteiltes Netzwerk (Distributed Ledger Technology, DLT) übertragen und gespeichert werden und deren Integrität durch Konsensmechanismen gewährleistet wird.⁴⁴ Diese Definition hebt drei konstituierende Elemente hervor:

Digitalität: Kryptowährungen existieren ausschließlich in Form von Datenstrukturen und besitzen keine körperliche Komponente.

Kryptografische Sicherung: Jede Transaktion wird durch mathematische Verfahren verifiziert und gegen Manipulation geschützt.

Dezentrale Konsensbildung: Die Validierung erfolgt nicht durch eine zentrale Instanz, sondern durch ein Netzwerk unabhängiger Rechner (Nodes, Validatoren, Miner).

Diese Merkmale unterscheiden Kryptowährungen strukturell von staatlichen Währungen (FIAT-Geld), elektronischem Geld und sonstigen digitalen Kontoeinträgen, die stets auf institutioneller Autorität, Zentralbankmandat oder Kontenführung basieren.⁴⁵

2.2.2 Token als Rechtssubstrate: Payment, Utility und Security-Token

Die juristische Literatur differenziert zunehmend zwischen verschiedenen Token-Arten, um deren rechtliche Behandlung präziser bestimmen zu können.⁴⁶ Die wichtigsten Kategorien sind:

⁴³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 16.

⁴⁴ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 35; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 54 f.

⁴⁵ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 55; vgl. Smit/Buekens/du Plessis, What Is Money? 2011, S. 17, 19.

⁴⁶ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 26 f; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. 2020, S. 47 f.

(a) Zahlungstoken („Payment Token“): Token wie Bitcoin oder Litecoin, deren primäre Funktion in der Abwicklung von Zahlungen oder im Werttransfer liegt. Sie fungieren nicht als gesetzliche Zahlungsmittel, können aber vertraglich, als Zahlungsmittel vereinbart werden.⁴⁷

(b) Utility-Token: Token, die Nutzungsrechte oder den Zugang zu digitalen Dienstleistungen gewähren (z. B. Zugang zu einer Softwareplattform). Ihr Wert leitet sich aus dem zugrunde liegenden Ökosystem ab.⁴⁸

(c) Security-Token („Investment Token“): Token, die Kapitalmarktrechtlich relevante Positionen repräsentieren, wie etwa Gewinnbeteiligungen oder schuldrechtliche Ansprüche. Sie fallen häufig unter bestehendes Wertpapier oder Kapitalmarktgesetze.⁴⁹ Diese Einteilung orientiert sich an der Funktion und nicht an der rechtlichen Einordnung. MiCA knüpft an ähnliche Kategorien an, differenziert aber insbesondere zwischen: Asset-referenced tokens, E-Geld-Token, anderen Kryptowerten und schließt bestimmte Bereiche (z. B. NFTs oder DeFi-Protokolle ohne Verantwortliche) ausdrücklich aus.⁵⁰

2.2.3 Distributed Ledger Technology (DLT) und Blockchain

DLT umfasst digitale Systeme, in denen Datensätze über mehrere Knoten verteilt gespeichert werden. Die bekannteste Form ist die Blockchain, eine sequenzielle Kette kryptografisch verknüpfter Datenblöcke.⁵¹

Blockchain zeichnet sich aus durch:

Unveränderlichkeit (Immutability), Pseudoanonymität und Fehlen einer zentralen Behörde. Diese Struktur ermöglicht die Verwaltung von Vermögenswerten ohne zentrale Register. Zivilrechtlich führt diese „Registerlosigkeit“ dazu, dass Eigentum nicht über klassische Besitzkonzepte übertragen wird, sondern über die Verfügungsmacht eines kryptografischen Schlüssels.⁵²

⁴⁷ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 89.

⁴⁸ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 88 f; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24, 31.

⁴⁹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 49; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 21.

⁵⁰ Vgl. MiCA-Vorschlag, ErwGr. S. 18-22.

⁵¹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 18 f; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 43–46.

⁵² Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 24; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 217.

2.2.4 Smart Contracts und deren rechtliche Bedeutung

Smart Contracts sind automatisierte Code-Strukturen, die Vertragsbedingungen selbstständig durchsetzen. Sie sind nicht notwendigerweise „Verträge“ im zivilrechtlichen Sinn, können aber rechtsgeschäftliche Funktionen übernehmen.⁵³

Ihre Besonderheiten sind:

Automatisierung, Irreversibilität, Abhängigkeit vom Code und fehleranfällige Implementierung.

Für den Verbraucherschutz ergeben sich daraus zentrale Probleme:

Fehler im Code führen zu unwiderruflichen Transaktionen, Rechtsdurchsetzung wird erschwert und Verantwortlichkeiten sind unklar (Entwickler? Betreiber? Nutzer?).

2.2.5 Konsensmechanismen: Proof-of-Work, Proof-of-Stake und Alternativen

Der Konsensmechanismus bestimmt, wie Transaktionen verifiziert werden. Die beiden wichtigsten Modelle sind:

Proof-of-Work (PoW): hoher Energieverbrauch, aber technologisch ausgereift (z. B. Bitcoin).

Proof-of-Stake (PoS): energieeffizienter, aber anfälliger für Machtkonzentration (z. B. Ethereum seit „The Merge“).⁵⁴

Diese Mechanismen haben Auswirkungen auf Verbraucherschutz (Manipulationsrisiken), Machtverteilung (Governance) Nachhaltigkeit und Rechtspolitik.

2.2.6 Kryptowährungen als Vermögensobjekte im juristischen Sinne

Zivilrechtlich sind Kryptowährungen schwer einzuordnen. Keine der klassischen Kategorien des ABGB (Sachen, Forderungen, Immaterialgüter, Rechte) passt vollständig.⁵⁵

Die wichtigsten Ansätze sind:

Kryptowerte als unkörperliche Sachen: das problematisch wegen fehlender Körperlichkeit.

Kryptowerte als Datenrechte: problematisch wegen mangelnder Eigentumskonformität

Kryptowerte als sui-generis-Vermögensrechte: derzeit am ehesten geeignet.

Diese Einordnung ist maßgeblich für: Eigentum und Besitzschutz, Übertragung, Absonderungsrechte, Haftung und Insolvenzfestigkeit⁵⁶

Die Rechtswissenschaft arbeitet aktiv daran, digitale Vermögenswerte als eigenständige Kategorie zu etablieren, doch ein Konsens ist noch nicht erreicht.

⁵³ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 85 f; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 60–62.

⁵⁴ Vgl. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, S. 3 f; vgl. Ethereum Foundation, The Merge – Proof-of-Stake Documentation, Version vom 14.09.2022.

⁵⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 79 f.

⁵⁶ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 35, 107.

2.2.7 Internationale Definitionen und regulatorische Uneinheitlichkeit

Die internationale Regulierungslandschaft ist heterogen:

FSB spricht von „crypto-asset activities“.

FATF verwendet „virtual assets“.

OECD spricht von „crypto-assets“.

USA unterscheiden zwischen „commodities“, „securities“ und „digital property“.

China betrachtet Kryptowährungen nicht als Vermögensrechte, sondern als verbotene Spekulationsobjekte.⁵⁷

Japan definiert Kryptoassets gesetzlich präzise und streng Verbraucherschutzorientiert.

Diese Divergenzen erschweren die Rechtsanwendung und unterstreichen den Bedarf nach klaren, technologiefesten Definitionen. Die Vielzahl an technischen, ökonomischen und rechtlichen Eigenschaften zeigt, dass Kryptowährungen weder einheitlich definierbar noch unter bestehende Vermögenskategorien eindeutig einordbar sind.

Für die rechtliche Analyse gilt daher das, Begriffe müssen funktional und technologisch präzise gefasst werden, damit Haftung, Eigentum, Aufsicht, Verbraucherschutz und Insolvenzrecht sinnvoll geregelt werden können.

2.3 Technologische Grundlagen und Funktionsweise der Blockchain

Die Analyse der technologischen Grundlagen ist unverzichtbar, um die rechtliche Struktur digitaler Vermögenswerte und die Verbraucherschutzproblematik in späteren Kapiteln hinreichend präzise zu erfassen. Kryptowährungen basieren auf technischen Mechanismen, deren Funktionsweise die rechtliche Bewertung in fundamentaler Weise beeinflusst. Die Blockchain-Technologie bildet dabei das Kernstück, da sie sowohl die Existenz digitaler Vermögenswerte als auch ihre Übertragbarkeit, Sicherheit und Dezentralisierung ermöglicht.⁵⁸

Ohne ein klares Verständnis dieser technologischen Parameter bleiben zentrale juristische Fragen wie etwa Eigentum, Haftung, Verantwortlichkeit, Risikoverteilung und Insolvenzfestigkeit, die notwendig sind, unvollständig.

2.3.1 Distributed-Ledger-Architektur als Grundlage digitaler Vermögenswerte

Distributed-Ledger-Technologien (DLT) bezeichnen Systeme, in denen Daten über ein Netzwerk verteilt gespeichert werden, ohne dass eine zentrale Behörde existiert, die Transaktionen

⁵⁷ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets 2020, S. 11–12, 23, 54 f; vgl. McDermott, Megan, The Crypto Quandary: Is Bankruptcy Ready?, Northwestern University Law Review 2021, S. 1921–1923.

⁵⁸ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 17–19; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 14, 23, 74.

validiert oder Register führt.⁵⁹ Die Blockchain ist die prominenteste Form der DLT und unterscheidet sich durch ihre sequenzielle, blockweise Struktur sowie die kryptografische Verknüpfung dieser Blöcke. Jeder Block enthält Transaktionen, einen Zeitstempel und einen kryptografischen Hash des vorherigen Blocks, wodurch eine unveränderbare Kette entsteht. Die dezentrale Struktur führt dazu, dass kein einzelner Akteur Kontrolle über das System hat. Diese Eigenschaft, häufig als „Trustless Environment“ beschrieben, bildet aus technologischer Sicht ein Sicherheitsmerkmal, führt aus rechtlicher Perspektive jedoch zu Problemen der Verantwortlichkeitszuordnung.⁶⁰ Wenn Transaktionen nicht von einer Institution, sondern durch das Netzwerk validiert werden, stellt sich die Frage, welche Instanz im Fehlerfall haftet oder wem Fehlfunktionen zugerechnet werden können — eine der zentralen Herausforderungen im Verbraucherschutz. Ein wesentliches Merkmal der Blockchain ist ihre **Unveränderlichkeit (Immutability)**. Sobald Daten gespeichert und durch Konsensmechanismen bestätigt wurden, können sie nur durch extreme technische Eingriffe (z. B. 51%-Attacken) verändert werden.⁶¹ Dies schafft hohe Sicherheit, führt aber zu rechtlich relevanten Konsequenzen da Fehlerhafte Transaktionen können technisch nicht rückgängig gemacht werden, Irrtümer, Manipulationen oder Codefehler entfalten sofort rechtliche Bedeutung und Rückabwicklungsmechanismen, wie sie im Zivilrecht üblich sind, existieren technisch nicht. Die Rechtswissenschaft betont, dass diese Immutabilität nicht mit dem zivilrechtlichen Konzept der Nichtigkeit, Irrtumsanfechtung oder Restitution vereinbar ist und besondere gesetzgeberische Lösungsmodelle erforderlich macht.⁶²

2.3.2 Kryptografische Sicherung und Schlüsselverwaltung

Kryptografische Verfahren, insbesondere Hashfunktionen und asymmetrische Verschlüsselung, gewährleisten die Integrität der Transaktionen und die Authentizität der digitalen Vermögenswerte. Jeder Nutzer besitzt einen privaten Schlüssel, der ihm die Verfügung über die jeweilige Tokenposition ermöglicht.⁶³ Die Rechtsrelevanz ergibt sich aus dem Umstand, dass der private Schlüssel die einzige Verfügungsmacht darstellt, der Verlust des Schlüssels einem vollständigen Vermögensverlust gleichkommt und die Zuordnung des Vermögenswerts

⁵⁹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 17–19; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 43–46.

⁶⁰ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 17–18; vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets 2020, S. 14; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 14, 46.

⁶¹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 17–19; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 52 f.

⁶² Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 2, 38, 62, 74.

⁶³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 44; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 32.

technisch, nicht rechtlich definiert ist. Die Literatur sieht dieses Konzept im Spannungsverhältnis zu traditionellen Eigentumsvorstellungen, in der Besitz und Verfügungsmacht rechtlich, nicht rein technisch bestimmt werden.⁶⁴

2.3.3 Konsensmechanismen und ihre Bedeutung für Sicherheit und Governance

Blockchain-Systeme validieren Transaktionen durch Konsensverfahren, wobei die beiden wichtigsten Modelle Proof-of-Work (PoW) und Proof-of-Stake (PoS) sind.

(a) Proof-of-Work (PoW) beruht auf rechenintensiven mathematischen Aufgaben, die Durchsetzbarkeit und Sicherheit durch „Arbeitsnachweise“ gewährleisten.⁶⁵

Juristisch relevant sind: hohe Energiekosten (regulatorische Nachhaltigkeit), mögliche Konzentration großer Mining-Pools und begrenzte Skalierbarkeit.

(b) Proof-of-Stake (PoS) hängt die Stimm- und Validierungsmacht vom gehaltenen Vermögen („Stake“) ab. PoS ist energieeffizient, aber anfälliger für Machtkonzentration, da große Vermögensträger erhebliche Entscheidungshoheit erlangen können.⁶⁶

Das führt zu strukturellen Steuerungsproblemen, z.B. faktische Zentralisierung, Einfluss großer Validatoren und mögliche Marktmanipulation. Diese Mechanismen bestimmen die Sicherheit, Robustheit und Haftungszuordnung der Netzwerke, was im Verbraucherschutz wesentlich ist.

2.3.4 Smart Contracts als automatisierte Rechtsfolgenmechanismen

Smart Contracts bestehen aus Programmcode, der -sobald ausgelöst- automatisch Vertragselemente ausführt. Sie sind keine Verträge im rechtlichen Sinn, können aber vertragliche Wirkungen entfalten.⁶⁷ Die zentrale Problematik liegt in:

Automatisierung ohne menschliche Kontrolle, fehlender Fehlerkorrektur, Unvereinbarkeit mit klassischen Vertragsdogmen (etwa Willenserklärung, Irrtum) und unklarer Verantwortlichkeit bei Fehlfunktionen. Die Literatur betont, dass Smart Contracts ein „hybrides Rechtsobjekt“ bilden, das technisches und rechtliches Verhalten verbindet.⁶⁸

folgende Sicherheitsrisiken sind als Beispiel relevant:

(a) Codefehler: Fehler im Programmcode können ausgenutzt werden und zu erheblichen Vermögensverlusten führen.⁶⁹

⁶⁴ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 32; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 52.

⁶⁵ Vgl. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, S. 3 f.

⁶⁶ Vgl. Ethereum Foundation, The Merge – Proof-of-Stake Documentation, Version vom 15.09.2022

⁶⁷ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 85–86.

⁶⁸ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 85; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 60–62.

⁶⁹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 32; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 290.

(b) Oracles: Smart Contracts benötigen externe Datenquellen („Oracles“), die manipulierbar sind. Diese externe Abhängigkeit widerspricht der Vorstellung technischer Autonomie.⁷⁰

(c) Cross-Chain-Bridges: Interoperabilität zwischen Blockchains erhöht Angriffsflächen und gilt als einer der größten Risikofaktoren im DeFi-Bereich.⁷¹

Für den Verbraucherschutz bedeutet dies, dass selbst bei technisch korrekter Nutzung erhebliche Risiken bestehen, die weder vorhersehbar noch rechtlich eindeutig rückabwickelbar sind.

2.3.5 Die Rolle zentraler Dienstleister in einem dezentralen System

Obwohl Blockchains technisch dezentral aufgebaut sind, agieren in der Praxis zentrale Akteure: Kryptobörsen, Verwahrer („Custodians“), Wallet-Anbieter, Entwicklerteams und große Validatoren und Mining-Pools. Diese Akteure übernehmen faktisch Aufgaben, die einer zentralen Infrastruktur entsprechen, ohne jedoch unter klassischen Aufsichtsstrukturen zu stehen.⁷² Dies führt zu einer strukturellen Diskrepanz zwischen technologischer Dezentralität und faktischer Zentralisierung, mit erheblichen Konsequenzen für Haftung, Verbraucherschutz und Aufsicht.

2.4 Abgrenzung zu anderen digitalen Finanzinstrumenten und rechtliche Einordnung

Die zunehmende Digitalisierung der Finanzmärkte hat zu einer Vielzahl neuer digitaler Produkte geführt, deren Gemeinsamkeiten und Unterschiede zu Kryptowährungen nicht immer auf den ersten Blick erkennbar sind. Für die rechtliche Analyse ist eine präzise Abgrenzung unerlässlich, da die verschiedenen Instrument Typen unterschiedlichen aufsichtsrechtlichen, steuerrechtlichen, zivilrechtlichen und haftungsrechtlichen Behandlungsschemata unterliegen.⁷³ Im Kern geht es um die Frage, wie Kryptowährungen in Relation zu anderen digitalen Wertrepräsentationen wie elektronischem Geld, digitalen Zahlungssystemen, tokenisierten Vermögenswerten, NFTs oder Stablecoins, einzuordnen sind und welche Konsequenzen sich daraus für den Verbraucherschutz ergeben.

⁷⁰ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 85–86; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 208.

⁷¹ Vgl. Chainalysis, Crypto Crime Report 2022, S. 18 f.

⁷² Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 28–30; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 49.

⁷³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 21–25; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 20–22; vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets 2020, S. 11–12.

2.4.1 Kryptowährungen versus elektronisches Geld (E-Geld)

Ein verbreiteter Irrtum besteht darin, Kryptowährungen als Form von „elektronischem Geld“ im Sinne der E-Geld-Richtlinie (Richtlinie 2009/110/EG) zu betrachten. Rechtlich unterscheiden sich beide Konzepte jedoch grundlegend:

E-Geld stellt eine geldwerte Forderung gegenüber dem Emittenten dar, ist gedeckt durch echte Gelder, wird von lizenzierten E-Geld-Instituten ausgegeben, ist gesetzlich reguliert und beaufsichtigt und gewährleistet Rücktauschbarkeit zum Nennwert. Kryptowährungen stellen keine Forderungen gegenüber einem Emittenten dar, sind nicht durch staatliche Zahlungsmittel gedeckt, werden durch Konsensmechanismen erzeugt, unterliegen keinem Rücktauschanspruch und existieren unabhängig von zentralen Intermediären.⁷⁴ Die MiCA-Verordnung unterscheidet daher strikt zwischen E-Geld-Token und „sonstigen Kryptowerten“ (Art. 3 Abs. 1 Nr. 7 MiCA).⁷⁵ Diese Trennung ist für Verbraucher:innen entscheidend, da der Schutzmechanismus für E-Geld erheblich stärker ausgeprägt ist als jener für Kryptowährungen.

2.4.2 Abgrenzung zu Stablecoins und Asset-Referenced Tokens

Stablecoins versuchen, die Volatilität klassischer Kryptowährungen zu minimieren, indem sie den Wert an Vermögensreserven (z. B. US-Dollar, Staatsanleihen, Rohstoffe) koppeln.⁷⁶ MiCA, E-Geld-Token (EMT): Dabei handelt es sich um Kryptowerte, deren Wert an eine gesetzliche Währung gebunden ist. Sie unterliegen strengen regulatorischen Anforderungen und gewähren grundsätzlich Rücktauschansprüche. Asset-Referenced Tokens (ART): Diese basieren auf einem Korb von Vermögenswerten. Sie weisen eine besondere Relevanz für den Verbraucherschutz auf, da sie mit komplexen Risiko- und Bewertungsstrukturen verbunden sind. Die Risiken ergeben sich aus Intransparenz der Reserven, Emittentenrisiko, Betriebsrisiko, Liquiditätsproblemen und mangelnder Governance.

Der Zusammenbruch des Stablecoin UST im Jahr 2022 zeigte, dass algorithmische Stablecoins besonders instabil sind und erhebliche Vermögensverluste verursachen können.⁷⁷ Für Verbraucher:innen besteht damit ein strukturelles Risiko, das herkömmliche Geldformen nicht aufweisen.

⁷⁴ Vgl. RL 2009/110/EG über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, Art. 2 Nr. 2; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 17–20; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 14–20.

⁷⁵ Art. 3 Abs. 1 Nr. 5 und Nr. 7 Verordnung (EU) 2023/1114 (MiCA).

⁷⁶ Art. 3 Abs. 1 Nr. 6 und Nr. 7 Verordnung (EU) 2023/1114 (MiCA).

⁷⁷ Vgl. zu Risiken von Stablecoins und zur Instabilität algorithmischer Modelle: Badev/Watsky, Interconnected DeFi: vgl. Ripple Effects from the Terra Collapse, Federal Reserve Board FEDS 2023-044, 2023, insb. S. 3, 8 f., 19.

2.4.3 Abgrenzung zu tokenisierten Vermögenswerten (Security-Token)

Tokenisierte Vermögenswerte repräsentieren reale oder rechtliche Positionen wie etwa Forderungen, Gewinnansprüche oder Eigentumsrechte.⁷⁸

Sie unterscheiden sich von Kryptowährungen in wesentlichen Punkten:

Kryptowährungen sind originäre digitale Vermögenswerte (primäre Digitalisierung).

Tokenisierung bildet bestehende Rechte ab (sekundäre Digitalisierung).

Tokenisierte Wertpapiere unterliegen klassischem Kapitalmarktrecht (Prospektpflicht, MiFID II).

So werden Kryptowährungen nur dann unter Kapitalmarktrecht fallen, wenn sie Investmentfunktionen erfüllen.⁷⁹ Diese Unterscheidung ist zentral, da Verbraucherschutz bei Security-Token über etablierte Mechanismen erfolgt, während Kryptowährungen überwiegend neue Rechtsfragen aufwerfen.

2.4.4 Abgrenzung zu Non-Fungible Tokens (NFTs)

NFTs sind einzigartige, nicht austauschbare Token, die oft digitale Kunstwerke, Musikdateien, virtuelle Immobilien oder Sammlerstücke repräsentieren.⁸⁰

rechtlich unterscheiden sie sich dadurch, dass NFTs repräsentieren individuelle Rechte, keine fungiblen Einheiten, sind nicht notwendigerweise „Kryptowährungen“ und dessen Wert und Rechtsnatur hängen vom **zugrunde liegenden Asset** ab.⁸¹ MiCA schließt NFTs grundsätzlich vom Anwendungsbereich aus, sofern sie tatsächlich nicht-fungibel sind.⁸²

2.4.5 Abgrenzung zu CBDCs (Central Bank Digital Currencies)

Central Bank Digital Currencies (CBDCs) stellen staatlich herausgegebene digitale Zentralbankwährungen dar und bilden die digitale Weiterentwicklung bestehender staatlicher Geldsysteme. Im Gegensatz zu dezentralen Kryptowährungen werden sie von Zentralbanken emittiert und unterliegen der staatlichen Geldordnung sowie den bestehenden institutionellen und regulatorischen Strukturen. Zu ihren wesentlichen Merkmalen zählt insbesondere ihre Funktion als gesetzliches Zahlungsmittel, wodurch sie innerhalb der jeweiligen Rechtsordnung grundsätzlich zur Erfüllung von Zahlungspflichten eingesetzt werden können. Darüber hinaus besteht eine staatliche Haftungs- und Vertrauensgrundlage, da die Emission unmittelbar durch öffentliche Institutionen erfolgt. Die Geldschöpfung bleibt weiterhin Ausdruck hoheitlicher Kompetenz und unterliegt somit den geldpolitischen Steuerungsmechanismen der jeweiligen

⁷⁸ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 11 ff.

⁷⁹ OECD, Tokenisation of Assets, 2020, S. 11 f; vgl. Schweizer Bundesrat, DLT-Bericht, 2018, S. 148 f; vgl. Binder Grosswang, Digital Law, 2. Aufl. 2020, S. 61.

⁸⁰ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 22 f.

⁸¹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 22 f., S. 38 f.

⁸² Vgl. ErwGr 10 Verordnung (EU) 2023/1114 (MiCA), ABL. L 150/42.

Zentralbanken. Zudem verfügen CBDCs über eine klare rechtliche Einordnung innerhalb des bestehenden Finanz- und Währungssystems und werden durch institutionelle Aufsichtsstrukturen überwacht, etwa durch die Europäische Zentralbank (EZB), die Oesterreichische Nationalbank (OeNB), die Federal Reserve System (FED) oder andere Zentralbanken. Im Gegensatz dazu sind Kryptowährungen grundsätzlich nicht staatlich legitimiert, verfügen regelmäßig nicht über den Status eines gesetzlichen Zahlungsmittels und werden nicht durch staatliche oder reale Vermögenswerte gedeckt. Darüber hinaus weisen sie aufgrund ihrer dezentralen Struktur, hoher Volatilität, fehlender zentraler Haftungsmechanismen sowie technischer und regulatorischer Unsicherheiten ein deutlich erhöhtes Risikopotenzial auf, was insbesondere aus Sicht des Verbraucherschutzes von erheblicher Bedeutung ist. Die Abgrenzung ist entscheidend, da Verbraucher:innen häufig „digitale Währungen“ verwechseln, obwohl ihre Rechtsfolgen fundamental unterschiedlich sind.⁸³

2.4.6 Bedeutung der Abgrenzung für Eigentumsrecht, Verbraucherschutz und Aufsicht

Die eindeutige Abgrenzung und rechtliche Einordnung digitaler Instrumente besitzen nicht nur theoretische Bedeutung, sondern entfaltet unmittelbare praktische Auswirkungen auf verschiedene verbraucherschutzrechtliche und vermögensrechtliche Fragestellungen. Von besonderer Relevanz ist dabei insbesondere die Eigentums- und Vermögenszuordnung, da die rechtliche Qualifikation eines digitalen Vermögenswertes maßgeblich bestimmt, welche Rechte Verbraucherinnen und Verbrauchern im Einzelfall zustehen. Die jeweilige Einordnung beeinflusst insbesondere die Frage, ob Ansprüche auf Aussonderung im Insolvenzfall, Rückabwicklungsansprüche oder Schadenersatzansprüche geltend gemacht werden können.⁸⁴ Dies ist vor allem bei Insolvenzverfahren von Kryptodienstleistern, Verwahrstellen oder Plattformbetreibern von erheblicher Bedeutung, da die Zuordnung der Vermögenswerte darüber entscheidet, ob Verbraucher auf die Herausgabe bestimmter Vermögenswerte Anspruch haben oder lediglich als allgemeine Gläubiger behandelt werden. Die rechtliche Qualifikation digitaler Vermögenswerte wirkt sich daher unmittelbar auf die Reichweite des Vermögensschutzes und die tatsächliche Durchsetzbarkeit verbraucherschützender Ansprüche aus.

Die rechtliche Einordnung digitaler Instrumente besitzt darüber hinaus erhebliche Bedeutung für das Aufsichtsrecht, da die jeweilige Qualifikation bestimmt, welchem regulatorischen Regime ein digitales Produkt unterliegt und welche Pflichten für Emittenten, Dienstleister und

⁸³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 33 f; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 54 f.

⁸⁴ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 6, 34, 104, 309.

Marktteilnehmer entstehen. Kryptowährungen unterfallen grundsätzlich dem Anwendungsbereich der Verordnung über Märkte für Kryptowerte (MiCA), die Unionsweit einheitliche Vorgaben für Emission, Transparenz, Zulassung und Aufsicht von Kryptowerten vorsieht. Demgegenüber unterliegen tokenisierte Wertpapiere, sofern sie die Merkmale klassischer Finanzinstrumente erfüllen, regelmäßig den bestehenden kapitalmarktrechtlichen Regelungen, insbesondere der Richtlinie über Märkte für Finanzinstrumente (MiFID II) sowie den prospektrechtlichen Vorschriften. E-Geld wird hingegen weiterhin durch die unionsrechtlichen Bestimmungen des E-Geld-Rechts erfasst und unterliegt den entsprechenden regulatorischen Anforderungen. Stablecoins, insbesondere in Form von E-Geld-Token (EMT) und Asset-Referenced Tokens (ART), werden zwar grundsätzlich durch die MiCA-Verordnung reguliert, unterliegen jedoch zusätzlich erweiterten Anforderungen und besonderen Emittentenpflichten, etwa hinsichtlich Reserven, Governance-Strukturen, Transparenz und Rücktauschmechanismen. Eine gesonderte Betrachtung erfordern schließlich Non-Fungible Tokens (NFTs), da ihre regulatorische Einordnung nicht einheitlich erfolgt, sondern maßgeblich von ihrer konkreten Funktion, wirtschaftlichen Ausgestaltung und tatsächlichen Verwendung abhängt. Dadurch kann ihre rechtliche Behandlung im Einzelfall erheblich variieren.⁸⁵

Auch im Bereich der Haftung kommt der rechtlichen Einordnung digitaler Instrumente erhebliche Bedeutung zu, da die Frage nach dem Haftungssubjekt und der Durchsetzbarkeit von Ansprüchen wesentlich von der jeweiligen Ausgestaltung des Instruments abhängt. Bei E-Geld besteht grundsätzlich eine klare Verantwortungsstruktur, da der Emittent als identifizierbarer und regulierter Akteur auftritt und daher für die Erfüllung der gesetzlichen Verpflichtungen sowie für mögliche Ansprüche der Nutzer haftet. Bei tokenisierten Vermögenswerten kann die Haftung je nach Struktur sowohl den Emittenten als auch beteiligte Dienstleister erfassen, insbesondere wenn diese Funktionen im Bereich der Verwahrung, Emission, Vermittlung oder Verwaltung übernehmen. Demgegenüber gestaltet sich die Haftungsfrage bei Kryptowährungen häufig deutlich komplexer. Aufgrund ihrer dezentralen Struktur, des Fehlens zentraler Emittenten sowie grenzüberschreitender und teilweise anonymer Marktstrukturen ist eine eindeutige Zuordnung von Verantwortlichkeiten vielfach erschwert oder die praktische Durchsetzung von Ansprüchen nur eingeschränkt möglich. Dies stellt insbesondere aus Sicht des Verbraucherschutzes ein erhebliches Problem dar. Bei Non-Fungible Tokens (NFTs) ist die Haftung wiederum vom jeweiligen Einzelfall abhängig und richtet sich insbesondere nach der zugrunde liegenden vertraglichen Ausgestaltung, den mit dem Token verbundenen Rechten sowie der jeweiligen

⁸⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 23,31; vgl. MiCA-VO, Erwägungsgrund 10 und Art. 48 Abs. 2; vgl. Richtlinie 2009/110/EG (E-Geld-RL).

digitalen oder physischen Ressource, auf die sich der NFT bezieht. Die Haftungsverteilung kann daher je nach Struktur und Funktion des Tokens unterschiedlich ausgestaltet sein.⁸⁶

⁸⁶ Vgl. MiCA-VO, Art. 14 und Art. 47; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 23 f; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 54 f.

Kapitel 3

Analyse der technologischen, ökonomischen und rechtlichen Risiken für Verbraucher:innen

3.1 Technologische Risiken von Kryptowerten

Die technologische Architektur von Kryptowerten bildet den Kern ihres Funktionsversprechens, gleichzeitig aber auch den Ursprung zahlreicher Risiken, die sich grundlegend von traditionellen Finanzinstrumenten unterscheiden. Während klassische Finanzsysteme auf zentralisierten Infrastrukturen, regulierten Intermediären und etablierten Haftungs- und Zuweisungsregeln beruhen, sind Kryptowerte typischerweise durch dezentrale Netzwerke, kryptographische Verfahren und autonome technische Prozesse geprägt. Diese Struktur führt zu einer Verschiebung der Risikosphären vom regulierten Intermediär hin zum Endnutzer, wobei die rechtlichen Anknüpfungspunkte häufig unklar oder fehlend sind.⁸⁷

Technologische Risiken betreffen nicht nur die Funktionsfähigkeit einzelner Protokolle, sondern die Infrastruktur als Ganzes: kryptographische Schlüssel, Blockchain-Validierung, Smart Contracts, Protokoll-Upgrades, Interoperabilität sowie Sicherheitsmechanismen gegen Cyberangriffe. Hinzu kommen Risiken der Irreversibilität von Transaktionen, der Abhängigkeit von einzelnen Softwareimplementierungen und der Unsicherheit bezüglich der Verantwortlichkeit im Schadensfall. Diese Risiken wirken unmittelbar auf Verbraucher:innen, da sie in der Regel keine institutionelle Absicherung (z. B. Einlagensicherung oder Haftungsübernahme durch Intermediäre) besitzen.⁸⁸

3.1.1 Verlust oder Kompromittierung kryptographischer Schlüssel

Kryptowerte basieren auf Public-Key-Kryptographie: Der Besitz eines privaten Schlüssels konstituiert faktisch die volle Verfügungsmacht über den Token.⁸⁹ Der Verlust, Diebstahl oder die Kompromittierung dieses Schlüssels führt unmittelbar und unwiderruflich zum Verlust der Vermögenswerte. Anders als im klassischen Zahlungsverkehr, in dem Banken Rückbuchungen, Sperren und Ersatzleistungen ermöglichen, existiert bei Kryptowerten kein zentraler Akteur, der Transaktionen stoppen oder rückgängig machen kann.⁹⁰

⁸⁷ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 19-21, 31 f., 83; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 33, 5-7.

⁸⁸ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 19-21., 31-33; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 59-65.

⁸⁹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 19-21; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 58-60.

⁹⁰ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 32 f; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 244, 340 f; Richtlinie (EU) 2015/2366, Art. 69-74.

Die Literatur bewertet die ausschließliche Schlüsselabhängigkeit als „Single Point of Failure“, der besonders für Kleinanleger:innen ein strukturelles Risiko darstellt. Zudem ist aus zivilrechtlicher Perspektive problematisch, dass der Schlüsselverlust keinen Tatbestand eines anerkannten Eigentumsschutzes erfüllt. Das österreichische Sachenrecht schützt nur körperliche Sachen, während der Verlust eines privaten Schlüssels rechtlich eher einer verlorenen Zugangsinformation als einem enteignungsgleichen Eingriff entspricht.⁹¹ Für Verbraucher:innen entsteht ein rechtsfreier Raum, da weder klassische Gewährleistung noch Schadenersatz greifen, wenn der Verlust technisch, aber nicht rechtswidrig verursacht wurde.

3.1.2 Cyberangriffe, Hacks und Sicherheitslücken

Kryptowerte sind regelmäßig Ziel hochkomplexer Cyberangriffe, die insbesondere Börsen, Wallet-Anbieter und Smart-Contract-Systeme betreffen. Wissenschaftliche Untersuchungen belegen Fälle, in denen Millionenbeträge durch Angriffe auf Smart Contracts, Cross-Chain-Bridges oder fehlerhafte Multi-Sig-Implementierungen verloren gingen.⁹² Die dezentrale Natur solcher Systeme erschwert die Verantwortlichkeitszuweisung, weil klassische Haftungsadressaten wie Verwahrer, Zahlungsdienstleister oder Intermediäre häufig fehlen. Solche Angriffe weisen eine besondere verbraucherschutzrechtliche Relevanz auf, da im Gegensatz zum klassischen Finanzsystem regelmäßig keine Einlagensicherung greift und Verbraucher daher häufig keinen vergleichbaren Schutzmechanismen unterliegen. Zudem besteht vielfach keine zwingende gesetzliche Verpflichtung zur Kompensation eingetretener Verluste, wodurch betroffene Nutzer das Risiko finanzieller Schäden oftmals selbst tragen müssen. Erschwerend kommt hinzu, dass die Zuweisung von Verantwortlichkeiten in vielen Fällen unklar bleibt, da häufig nicht eindeutig festgestellt werden kann, ob die Verantwortung beim zugrunde liegenden Protokoll, beim Betreiber einer Handelsplattform oder Börse oder letztlich beim Nutzer selbst liegt. Diese Unsicherheiten können die Durchsetzung von Ansprüchen zusätzlich erschweren und verstärken die verbraucherschutzrechtlichen Herausforderungen im Bereich digitaler Vermögenswerte. Selbst bei zentralisierten Plattformen bleibt die Rechtslage unsicher: Viele Anbieter schließen die Haftung vertraglich nahezu vollständig aus, während die technische Infrastruktur häufig außerhalb klassischer Finanzmarktregulierung liegt.⁹³

⁹¹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 31 f; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 58-60., 244 f., 340 f.

⁹² Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 31-33; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2.Aufl. 2020, S. 26.

⁹³ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 31-33, 150-151; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 59-65, 340-341; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2.Aufl. 2020, S. 43.

3.1.3 Technische Systemfehler, Protokollfehler und Smart-Contract-Risiken

Kryptowerte beruhen häufig auf Smart Contracts – autonomen, selbst ausführenden Programmcodes. Fehler im Code können schwerwiegende wirtschaftliche Schäden verursachen, etwa wenn Sicherheitslücken Liquidationen auslösen, Vermögenswerte irreversibel eingefroren werden oder Angreifer fehlerhafte Logik ausnutzen.⁹⁴

Juristisch problematisch ist, dass die Verantwortlichkeit für fehlerhafte Smart Contracts unklar bleibt. Auch hier Entwickler:innen haften häufig nicht, da ihre Tätigkeit nicht als Werkvertrag klassifiziert wird und Betreiber vermeiden Verantwortlichkeit durch

Dezentralisierungsbehauptungen. Andererseits haben Nutzer:innen, keine Ansprüche aus Gewährleistung, weil der „Code“ kein Produkt im zivilrechtlichen Sinn darstellt.⁹⁵

Das führt dazu, dass Verbraucher:innen strukturell ohne Rechtsschutz bleiben, selbst wenn die Ursache des Schadens klar einem Softwarefehler zugeordnet werden kann.

3.1.4 Dezentralität, Validatorrisiken und Netzwerkangriffe

Blockchain-Netzwerke basieren auf dezentralen Validierungsmechanismen, durch welche Transaktionen überprüft, bestätigt und dauerhaft in der Blockchain gespeichert werden. Hierfür kommen insbesondere Konsensverfahren wie Proof-of-Work (PoW) und Proof-of-Stake (PoS) zum Einsatz. Diese Mechanismen dienen grundsätzlich dem Schutz vor Manipulationen und sollen die Integrität sowie Sicherheit des Netzwerks gewährleisten. Gleichzeitig führen sie jedoch zu neuen technischen und Verbraucherschutzrechtlich relevanten Risiken. Dazu zählen insbesondere sogenannte 51%-Angriffe, bei denen eine Gruppe von Validatoren oder Miner die Mehrheit der Validierungsleistung kontrolliert und dadurch potenziell Einfluss auf die Verarbeitung und Bestätigung von Transaktionen ausüben kann. Ein weiteres Risiko stellen Reorganisationen von Blöcken („Reorgs“) dar, bei denen bereits bestätigte Blöcke nachträglich verändert oder überschrieben werden können, wodurch Transaktionen rückwirkend betroffen sein können. Darüber hinaus bestehen im Bereich von Proof-of-Stake-Systemen sogenannte Slashing-Risiken. Dabei können Teilnehmerinnen und Teilnehmer, die Vermögenswerte im Rahmen des Stakings bereitstellen, Teile ihrer hinterlegten Werte verlieren, wenn Fehlverhalten festgestellt wird oder technische bzw. netzwerkbezogene Probleme auftreten. Diese Risiken verdeutlichen, dass die technische Absicherung dezentraler Systeme zwar Sicherheitsvorteile schafft, gleichzeitig jedoch neue Gefährdungslagen hervorbringt, die insbesondere aus Sicht

⁹⁴ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 24, 33, 85–86; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 61, 340–341.

⁹⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 58–65, 340–341; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 31–33, 85–86, 150–151.

des Verbraucherschutzes von erheblicher Bedeutung sind.⁹⁶ Diese Risiken haben unmittelbare finanzielle Auswirkungen auf Verbraucher:innen, die häufig weder deren technische Funktionsweise noch deren juristische Bedeutung verstehen. Da bei dezentralen Systemen kein Betreiber existiert, können typische Rechtsbehelfe – Unterlassung, Schadenersatz, Gewährleistung – nicht effektiv geltend gemacht werden.

3.1.5 Irreversibilität und fehlende Transaktionskorrektur

In klassischen Zahlungssystemen existieren rechtliche und technische Mechanismen zur Fehlerkorrektur (z. B. § 39 ZaDiG 2018, Widerruf oder Rückbuchungen). Bei Kryptowerten sind Transaktionen grundsätzlich irreversibel.⁹⁷ Irrtümer, Betrug oder Fehlbuchungen können technisch nicht rückgängig gemacht werden, sofern nicht ein außergewöhnlicher Netzwerk-Rollback vorgenommen wird — ein Prozess, der extrem selten, technisch riskant und rechtlich ungeklärt ist. Die Irreversibilität führt dazu, dass Kleinanleger:innen vollständig auf Eigenverantwortung verwiesen werden, ohne flankierende Schutzmechanismen.⁹⁸

3.1.6 Automatisierte Liquidationen und Marktmechanik

In zahlreichen dezentralen Finanzprotokollen (DeFi) erfolgt die Absicherung von Krediten und sonstigen Finanztransaktionen durch automatisierte Mechanismen, die auf Smart Contracts basieren. Dabei werden hinterlegte Sicherheiten laufend überwacht und mit vorgegebenen Schwellenwerten verglichen. Sinkt der Wert der Sicherheiten unter ein bestimmtes Niveau, wird die betreffende Position automatisch und ohne weiteres menschliches Eingreifen liquidiert, um die Stabilität des Protokolls und die Absicherung der Forderungen zu gewährleisten. Für Verbraucherinnen und Verbraucher können sich daraus jedoch erhebliche Risiken ergeben. Insbesondere besteht regelmäßig keine Möglichkeit einer nachträglichen Intervention oder Einflussnahme, da die Liquidation unmittelbar durch den zugrunde liegenden Programmcode ausgelöst wird. Darüber hinaus besteht vielfach keine Verpflichtung des Protokolls zur vorherigen Warnung oder Benachrichtigung, sodass betroffene Nutzer häufig erst nach Durchführung der Liquidation Kenntnis vom Verlust ihrer Position erhalten. Gleichzeitig finden klassische verbraucherschützende Mechanismen vielfach keine oder nur eingeschränkte Anwendung. Dies betrifft insbesondere Informations- und Transparenzpflichten, wie sie etwa im österreichischen Konsumentenschutzrecht oder im Zahlungsdiensterecht vorgesehen sind.

⁹⁶ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 19–21, 31–33, 85–86; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 52.

⁹⁷ Vgl. Richtlinie (EU) 2015/2366 (PSD2), Art. 71–74; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 33; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 340–341.

⁹⁸ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 31–33; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 52, 59–65, 340–341.

Dadurch entstehen Schutzlücken, da traditionelle Instrumente des Verbraucherschutzes vielfach auf zentrale Vertragspartner und klar identifizierbare Verantwortliche ausgerichtet sind, während diese Strukturen im Bereich dezentraler Finanzprotokolle häufig fehlen.⁹⁹ Diese automatische Marktmechanik ist ein inhärentes technologisches Risiko, das in traditionellen Finanzsystemen durch eingreifbare Intermediäre abgedeckt wird.

3.1.7 Verantwortungsdiffusion und fehlende Haftungsadressaten

Ein wesentliches technologisches und zugleich verbraucherschutzrechtlich relevantes Risiko dezentraler Systeme liegt in der fehlenden Bestimmbarkeit eines eindeutigen Haftungsadressaten. Im Gegensatz zum traditionellen Finanzsystem, in dem die Verantwortlichkeiten regelmäßig klar zugeordnet sind und Haftungsträger wie Banken, Depotbanken oder Zahlungsdienstleister eindeutig identifiziert werden können, entstehen im Bereich dezentraler Technologien häufig erhebliche Verantwortlichkeitslücken. Dies ist insbesondere darauf zurückzuführen, dass die zugrunde liegenden Strukturen oftmals ohne zentrale Steuerungsinstanz organisiert sind und die beteiligten Akteure unterschiedliche Rollen übernehmen. So berufen sich Protokollentwickler häufig darauf, keine unmittelbare Kontrolle über den laufenden Betrieb des Systems auszuüben und daher nicht für dessen spätere Nutzung oder Fehlfunktionen verantwortlich zu sein. Validatoren übernehmen zwar Aufgaben im Bereich der Netzwerkvalidierung und Transaktionsbestätigung, weisen jedoch regelmäßig jede unmittelbare Haftung gegenüber Nutzerinnen und Nutzern zurück. Hinzu kommt, dass Dezentrale Autonome Organisationen (DAO) häufig grenzüberschreitend und ohne klassische Organisationsstruktur agieren, wodurch ihre Einordnung in nationale Rechtsordnungen sowie die Zuweisung rechtlicher Verantwortung zusätzlich erschwert wird. Gleichzeitig begrenzen Kryptobörsen und Plattformbetreiber ihre Haftung vielfach durch Allgemeine Geschäftsbedingungen auf ein Mindestmaß. Diese Verantwortungsdiffusion führt dazu, dass Verbraucher im Schadensfall häufig keinen eindeutig identifizierbaren Anspruchsgegner vorfinden, wodurch die Durchsetzung von Ersatz- oder Schutzansprüchen erheblich erschwert werden kann.¹⁰⁰

⁹⁹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 31–33, 150–151; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 59–65; Richtlinie (EU) 2015/2366 (PSD2), Art. 38–47, 51–58, 71–74.

¹⁰⁰ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 59–65, 340–341; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 31–33, 85–86, 150–151; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. 2020, S. 43.

3.2 Ökonomische Risiken von Kryptowerten

Ökonomische Risiken betreffen jene Eigenschaften von Kryptowerten, die aufgrund ihrer Marktstrukturen, Preisbildungsmechanismen, Liquiditätsverhältnisse und makroökonomischen Wechselwirkungen ein besonderes Gefährdungspotenzial für Verbraucher:innen darstellen. Diese Risiken unterscheiden sich fundamental von klassischen Finanzinstrumenten, weil Kryptowerte weder über eine intrinsische Wertbasis noch über etablierte Stabilitätsmechanismen verfügen.¹⁰¹ Anders als traditionelle Finanzmärkte, die durch institutionelle Stabilitätsanker wie Zentralbanken, Bankenaufsicht, Einlagensicherungssysteme und Marktinfrastrukturbetreiber stabilisiert werden, weisen Kryptomärkte überwiegend keine vergleichbaren Schutzmechanismen auf. Ihr Verhalten wird zudem durch algorithmische Mechanismen, Netzwerkeffekte und spekulative Marktpsychologie geprägt. Ökonomische Risiken entstehen daher nicht nur durch externe Schocks, sondern bereits aus der Struktur des Systems selbst.¹⁰²

3.2.1 Extreme Volatilität und fehlende intrinsische Wertbasis

Kryptowerte weisen eine außergewöhnlich hohe Volatilität auf, die weit über jene traditioneller Anlageformen hinausgeht. Studien zeigen, dass Preisschwankungen tägliche Ausschläge von mehreren Prozentpunkten aufweisen können, während in Stressphasen Kurseinbrüche über 40%, innerhalb weniger Tage auftreten können.¹⁰³ Die ökonomische Ursache liegt darin, dass Kryptowerte überwiegend kein zugrunde liegendes Cash-Flow-Modell (dividends, interest) besitzen.¹⁰⁴ Ihr Wert basiert primär auf Erwartungen über zukünftige Nachfrage und kollektive Marktsentiments – Elemente, die besonders anfällig für spekulative Blasen und plötzliche Korrekturen sind.

Für Verbraucherinnen und Verbraucher ergeben sich daraus erhebliche Risiken, da die hohe Dynamik und Volatilität von Kryptomärkten die Vorhersehbarkeit von Preisentwicklungen deutlich einschränken kann. Dies führt häufig zu einer unzureichenden Prognostizierbarkeit der

¹⁰¹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24–25, 98–101, 147–150; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. 2020, S. 45–46; vgl. Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), Erwägungsgründe 26–29.

¹⁰² Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 150–151; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24–25, 98–101; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. 2020, S. 28–29; vgl. Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), Erwägungsgründe 5–8, 26–29.

¹⁰³ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. 2020, S. 45–46; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24–25; vgl. Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), Erwägungsgründe 5–8, 26–29.

¹⁰⁴ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 37–38, 105–107; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. 2020, S. 45–46; vgl. Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), Erwägungsgründe 5–10.

Marktentwicklung und erhöht die Gefahr erheblicher finanzieller Verluste, insbesondere im Zuge plötzlicher Marktkorrekturen oder starker Kursschwankungen. Erschwerend kommt hinzu, dass Kryptomärkte vielfach nicht durch klassische fundamentale Werte oder institutionelle Stabilisierungsmechanismen abgesichert werden, wodurch marktinterne Ausgleichs- und Stabilisierungseffekte häufig fehlen. Zusätzlich kann es durch algorithmisch gesteuerte Verkaufsmechanismen, automatisierte Liquidationen oder andere technisch ausgelöste Marktprozesse zu einer weiteren Verstärkung von Kursbewegungen und Verlusten kommen. Aus juristischer Sicht ist dabei besonders relevant, dass eine hohe Marktvolatilität grundsätzlich keinen klassischen Produktmangel darstellt. Wertschwankungen und Marktrisiken werden regelmäßig dem allgemeinen Investitionsrisiko zugeordnet und lösen daher grundsätzlich keine Gewährleistungsansprüche aus, wodurch Verbraucher in vielen Fällen keinen entsprechenden Ausgleichsanspruch geltend machen können.¹⁰⁵ Verbraucher:innen tragen dieses Risiko allein, selbst wenn sie die tatsächliche Volatilität mangels Fachkenntnis nicht einschätzen konnten.

3.2.2 Marktmanipulation, Wash-Trading und fehlende Marktintegrität

Kryptomärkte weisen aufgrund ihrer dezentralen Struktur, der teilweise begrenzten Regulierung sowie der hohen Markttransparenz und Geschwindigkeit eine erhöhte Anfälligkeit für Marktmanipulationen auf. Besonders relevant sind dabei verschiedene Formen manipulativer Marktpraktiken. Dazu zählt insbesondere Wash-Trading, bei dem durch Eigengeschäfte oder Scheingeschäfte künstlich Handelsvolumen erzeugt wird, um Marktaktivität und Liquidität vorzutäuschen. Ebenso bedeutsam ist Spoofing, bei dem Marktteilnehmer durch das Platzieren und anschließende Zurückziehen von Kauf- oder Verkaufsaufträgen irreführende Signale über Angebot und Nachfrage erzeugen und dadurch Marktteilnehmer beeinflussen können. Darüber hinaus treten sogenannte Pump-and-Dump-Schemata auf, bei denen Vermögenswerte durch koordinierte Maßnahmen oder gezielte Informationsverbreitung künstlich im Wert gesteigert werden, um anschließend unter Gewinnmitnahme wieder veräußert zu werden. Weitere Risiken ergeben sich durch Insiderhandel, bei dem nicht öffentlich verfügbare Informationen zur Erlangung von Marktvorteilen genutzt werden, sowie durch koordiniertes Gruppenverhalten in sozialen Netzwerken, bei dem Marktbewegungen gemeinschaftlich beeinflusst oder verstärkt werden. Diese Mechanismen können erhebliche Auswirkungen auf Markttransparenz, Preisbildung und Verbraucherinteressen haben und sind daher aus

¹⁰⁵ Vgl. Andrade/Sharman/Xiao/Newall, Safer Gambling and Consumer Protection Failings Among 40 Frequently Used Crypto-Gambling Services, 2022, S. 552; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. 2020, S. 45–46; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24–25, 59–65, 98–101, 340–341; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 33, 85–86.

verbraucherschutzrechtlicher Sicht von besonderer Bedeutung.¹⁰⁶ Im Vergleich zu geregelten Finanzmärkten, die insbesondere durch Regelwerke wie die Marktmissbrauchsverordnung (MAR) und die Richtlinie über Märkte für Finanzinstrumente (MiFID II) erfasst werden, bestehen im Bereich der Kryptomärkte weiterhin erhebliche regulatorische Unterschiede. In vielen Rechtsordnungen fehlt es nach wie vor an umfassenden behördlichen Aufsichtsstrukturen, verbindlichen Meldepflichten, wirksamen Marktüberwachungs- und Surveillance-Systemen sowie an klar definierten und einheitlichen Verhaltensregeln für Marktteilnehmer. Dadurch können Marktmanipulationen, missbräuchliche Handelspraktiken oder Interessenkonflikte oftmals nur eingeschränkt erkannt oder verhindert werden. Selbst größere Kryptobörsen und Handelsplattformen verfügen teilweise lediglich über begrenzte interne Kontroll- und Überwachungsmechanismen, wodurch zusätzliche Risiken hinsichtlich Marktintegrität, Transparenz und Verbraucherschutz entstehen können. Diese regulatorischen Unterschiede verdeutlichen, dass Kryptomärkte im Vergleich zu traditionellen Finanzmärkten vielfach noch nicht über gleichwertige Schutz- und Kontrollstrukturen verfügen.¹⁰⁷ Rechtlich entsteht eine massive Schutzlücke und Marktmanipulation ist zwar in vielen Jurisdiktionen verboten, aber aufgrund fehlender Markttransparenz kaum nachweisbar.¹⁰⁸ Für geschädigte Kleinanleger:innen existiert praktisch kein Durchsetzungsweg für Schadenersatz, weil Täter anonym agieren und Transaktionen weltweit verteilt sind.¹⁰⁹

3.2.3 Illiquide Märkte und strukturelle Liquiditätsrisiken

Viele Kryptowerte weisen geringe Markttiefe auf. Selbst bei bekanntem Token entstehen Liquiditätsengpässe in Stressphasen, die massive Preissprünge verursachen.¹¹⁰ Ursache hierfür ist, dass bereits, vergleichsweise geringe Veränderungen von Angebot oder Nachfrage erhebliche Auswirkungen auf die Preisbildung entfalten können. Die strukturellen Liquiditätsrisiken der Kryptomärkte werden dabei durch mehrere ökonomischen Faktoren verstärkt. Von besonderer Bedeutung ist die Konzentration des Handels auf wenige große Handelsplattformen, wodurch Marktliquidität und Handelsvolumen teilweise von einzelnen Infrastrukturen abhängig werden. Hinzu kommt die zunehmende Bedeutung algorithmischer Market-Maker (Automated Market Maker – AMM), die Liquidität automatisiert bereitstellen und dadurch Handelsprozesse ermöglichen, gleichzeitig jedoch Liquidität teilweise künstlich

¹⁰⁶ Vgl. IMF, Global Financial Stability Report, October 2021, S. 47–53; Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2.Aufl. 2020, S. 45–46; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24–25; MiCA-VO-E, ErwGr. 5–8.

¹⁰⁷ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 59–65, 340–341.

¹⁰⁸ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2.Aufl. 2020, S. 45–46.

¹⁰⁹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 59–65.

¹¹⁰ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2.Aufl. 2020, S. 45–46.

erzeugen und von algorithmischen Parametern abhängig machen. Eine weitere zentrale Rolle spielen Stablecoins, die vielfach als faktische Liquiditätsbasis innerhalb des Kryptomarktes dienen und zahlreiche Handels- und Finanzierungsprozesse ermöglichen. Dadurch entstehen zusätzliche Abhängigkeiten von deren Stabilität und Verfügbarkeit. Ergänzend werden die Märkte durch hohe Kapitalzuflüsse kurzfristig orientierter und spekulativer Investitionen beeinflusst, wodurch Volatilität und Liquiditätsrisiken zusätzlich verstärkt werden können. Diese Faktoren führen dazu, dass Kryptomärkte insbesondere in Krisen- und Stresssituationen eine erhöhte Anfälligkeit für Marktstörungen und abrupte Wertveränderungen aufweisen.¹¹¹ Für Verbraucherinnen und Verbraucher kann eine geringe Marktliquidität erhebliche wirtschaftliche Risiken mit sich bringen. Von besonderer Bedeutung sind dabei Slippage-Risiken, bei denen eine Differenz zwischen dem erwarteten Ausführungspreis einer Order und dem tatsächlich realisierten Preis entsteht. Solche Abweichungen treten insbesondere in Phasen geringer Liquidität oder hoher Marktvolatilität auf und können zu unerwarteten finanziellen Nachteilen führen. Darüber hinaus besteht das Risiko von Verlusten infolge einer fehlenden oder nur teilweisen Ausführung von Handelsaufträgen, wenn nicht ausreichend Marktliquidität vorhanden ist. Erschwerend kommen mögliche Preisverwerfungen hinzu, bei denen bereits, vergleichsweise geringe Handelsvolumina erhebliche Preisbewegungen auslösen können. Zusätzlich kann ein rascher Abzug von Liquidität zu Marktunsicherheit und verstärkten Reaktionen der Marktteilnehmer führen, wodurch Marktpaniken und weitere Preisrückgänge begünstigt werden können. Diese Faktoren verdeutlichen, dass Liquiditätsrisiken im Kryptomarkt erhebliche Auswirkungen auf die wirtschaftliche Position und den Schutz von Verbraucherinnen und Verbrauchern haben können.¹¹² In traditionellen Märkten existieren Liquiditätsreserven, Stabilisierungsmechanismen und Market-Maker-Pflichten aber in Kryptomärkten fehlen solche Vorgaben. Rechtlich stellt Illiquidität ebenfalls keinen Produktmangel dar. Zudem existiert keine Pflicht der Plattformbetreiber, Mindestliquidität sicherzustellen, sodass Verbraucher:innen das Risiko einer Nichtausführung voll tragen.¹¹³

3.2.4 Stablecoin-Risiken und die Illusion der Preisstabilität

Stablecoins verfolgen das Ziel, innerhalb der Kryptomärkte Preisstabilität zu schaffen und Wertschwankungen klassischer Kryptowährungen zu reduzieren. Sie sollen Nutzern eine stabile Werteinheit für Handels-, Zahlungs- und Liquiditätszwecke bereitstellen. Empirische

¹¹¹ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2.Aufl. 2020, S. 45–46.

¹¹² Ebd.

¹¹³ Ebd.

Untersuchungen und Marktentwicklungen zeigen jedoch, dass diese Stabilität vielfach nur eingeschränkt erreicht wird und auch Stablecoins erheblichen Risiken unterliegen können.¹¹⁴ Grundsätzlich lassen sich drei zentrale Kategorien unterscheiden. Fiat-gedeckte Stablecoins (etwa USDC oder USDT) stützen ihren Wert auf Reserven in gesetzlichen Währungen oder vergleichbaren Vermögenswerten. Krypto-gedeckte Stablecoins, wie etwa DAI, basieren hingegen auf hinterlegten Kryptowerten als Sicherheiten. Daneben existieren algorithmische Stablecoins, beispielsweise TerraUSD oder FRAX, die ihre Preisstabilität durch algorithmische Steuerungsmechanismen und Marktanreize aufrechterhalten sollen. Jeder dieser Kategorien weist eigene Risikostrukturen auf. Bei fiat-gedekten Stablecoins bestehen insbesondere Risiken hinsichtlich der tatsächlichen Deckung und Transparenz der Reserven. Unzureichende oder nicht ausreichend überprüfbare Reserven, mögliche Insolvenzrisiken des Emittenten sowie fehlende oder eingeschränkte Prüf- und Offenlegungspflichten können die Stabilität des Systems beeinträchtigen. Krypto-gedeckte Stablecoins unterliegen demgegenüber den Wertschwankungen der hinterlegten Sicherheiten, wodurch starke Marktbewegungen die Stabilität unmittelbar beeinflussen können. Besonders risikobehaftet gelten algorithmische Stablecoins, da deren Stabilitätsmechanismen häufig auf komplexen Marktanreizen beruhen und systemische Instabilitäten hervorrufen können. Dies zeigte insbesondere der Zusammenbruch von TerraUSD, bei dem die angestrebte Preisbindung nicht aufrechterhalten werden konnte und erhebliche Marktverluste entstanden. Die Entwicklung verdeutlicht, dass die angenommene Preisstabilität von Stablecoins nicht uneingeschränkt gewährleistet ist und aus verbraucherschutzrechtlicher Sicht erhebliche Risiken bestehen können.¹¹⁵

Aus juristischer Sicht sind die mit Stablecoins verbundenen Risiken erheblich. Ein wesentliches Problem besteht darin, dass die zugrunde liegenden Reserven häufig nicht insolvenzgeschützt ausgestaltet sind. Verbraucherinnen und Verbraucher verfügen im Insolvenzfall vielfach über keinen Aussonderungsanspruch und können daher lediglich, als allgemeine Gläubiger behandelt werden. Zusätzlich bestehen außerhalb der Europäischen Union häufig keine einheitlichen Prospekt- und Offenlegungspflichten, wodurch Transparenzdefizite und zusätzliche Verbraucherschutzrisiken entstehen können.¹¹⁶

Selbst bei 1:1 gedeckten Stablecoins gibt es hinsichtlich Liquidität, Reserven Qualität und Transparenz, massive Unterschiede, die für Kleinanleger:innen kaum erkennbar sind.

¹¹⁴ Vgl. OECD, The Tokenisation of Assets and Potential Implications, 2020, S. 14–16.

¹¹⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24 f; vgl. ErwGr 26 Verordnung (EU) 2023/1114 (MiCA).

¹¹⁶ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 72–74, 97–99; vgl. Art. 4 ff. Verordnung (EU) 2023/1114 (MiCA).

3.2.5 Systemische Risiken durch Interkonnektivität und Kaskadeneffekte

Kryptomärkte sind durch eine hohe Interkonnektivität und starke wechselseitige Abhängigkeiten zwischen den einzelnen Marktteilnehmern und Infrastrukturen geprägt. Börsen halten häufig erhebliche Bestände an Stablecoins und nutzen diese als zentrale Liquiditäts- und Handelsbasis. Gleichzeitig stützen sich zahlreiche DeFi-Protokolle auf die Liquiditätsbereitstellung durch Automated Market Maker (AMM) und entsprechende Liquiditätspools. Hinzu kommt, dass Kredit- und Finanzierungsplattformen durch automatisierte Mechanismen potenzielle Kaskadeneffekte auslösen können, die Marktbewegungen zusätzlich verstärken. Darüber hinaus verbinden Cross-Chain-Bridges unterschiedliche Blockchain-Ökosysteme miteinander und schaffen dadurch weitere technische und wirtschaftliche Abhängigkeiten zwischen verschiedenen Netzwerken. Diese enge Verflechtung kann die Übertragung von Risiken innerhalb des Kryptomarktes zusätzlich begünstigen.¹¹⁷ Diese Struktur führt dazu, dass der Ausfall eines einzigen Protokolls oder Emittenten ganze Marktsegmente destabilisieren kann. Studien zeigen, dass mehrere Großausfälle (Terra/LUNA, Celsius, FTX) nicht isolierte Ereignisse waren, sondern systemische Schocks erzeugten.¹¹⁸

Für Verbraucherinnen und Verbraucher führt diese starke Interkonnektivität zu erheblichen Risiken, da selbst ohne eigenes Fehlverhalten ein Gesamtverlust von Vermögenswerten eintreten kann, wenn verbundene Marktstrukturen oder Plattformen ausfallen. Gleichzeitig wird die Möglichkeit einer wirksamen Risikodiversifikation eingeschränkt, da die enge Vernetzung der Marktteilnehmer und Systeme Risiken über verschiedene Plattformen, Protokolle und Vermögenswerte hinweg übertragen kann. Aus rechtlicher Sicht wird das Systemrisiko im Kryptobereich bislang nur eingeschränkt erfasst. Zwar erkennt die MiCA-Verordnung die Problematik grundsätzlich an und schafft erste regulatorische Ansätze, jedoch bleiben wesentliche Bereiche wie DeFi-Strukturen, algorithmische Stablecoins sowie zahlreiche Offshore-Plattformen weiterhin außerhalb oder nur teilweise innerhalb des regulatorischen Anwendungsbereichs. Dadurch bestehen weiterhin erhebliche Schutz- und Regulierungslücken.¹¹⁹

¹¹⁷ Vgl. International Monetary Fund, Global Financial Stability Report – Crypto Ecosystem and Financial Stability, October 2021, S. 65–73.

¹¹⁸ Vgl. BIS, The crypto ecosystem: key elements and risks (Report to be submitted ahead of the July 2023 G20 FMCBG meeting), Juli 2023, S. 8.

¹¹⁹ Vgl. Bank for International Settlements, The crypto ecosystem: key elements and risks, Juli 2023, S. 8–9, 14; vgl. Art. 2 Abs. 4 sowie ErwGr 22, 23 und 26 Verordnung (EU) 2023/1114 (MiCA).

3.2.6 Kreditrisiken, Liquidationsspiralen und Überbesicherung

Viele Kryptokredite erfordern eine **Überbesicherung** (z. B. 150 %), um die Volatilität der Sicherheiten zu kompensieren.¹²⁰

Ökonomisch kann die Überbesicherung von Kryptokrediten erhebliche Folgewirkungen auslösen. Insbesondere können automatische Liquidationen, Margin-Call-Kaskaden sowie Preisverzerrungen infolge von Zwangsverkäufen auftreten, die in weiterer Folge zur Destabilisierung einzelner Marktsegmente oder ganzer DeFi-Ökosysteme beitragen können. Das Risiko automatisierter Liquidationen besitzt dabei besondere Bedeutung, da bereits geringe Kursbewegungen ausreichen können, um eine Kette weiterer Liquidationen auszulösen. Die dadurch ausgelösten Zwangsverkäufe erhöhen den Verkaufsdruck zusätzlich und können zu einem überproportionalen Wertverlust der hinterlegten Sicherheiten führen. Dies verstärkt Marktbewegungen und kann die Stabilität des Gesamtsystems zusätzlich beeinträchtigen.¹²¹ Rechtlich handelt es sich bei diesen automatisierten Prozessen weder um Kreditverträge im klassischen Sinn noch um Verbraucherkreditgeschäfte, sodass die Schutzvorschriften des VKrG (Verbraucherkreditgesetz) oder der PSD2 (Payment Services Directive) regelmäßig nicht greifen.

3.2.7 Informationsasymmetrien und Überforderung der Verbraucher:innen

Ein wesentliches ökonomisches Risiko im Kryptobereich besteht in ausgeprägten Informationsasymmetrien zwischen den Marktteilnehmern. Insbesondere Protokollbetreiber, Entwickler und große Marktteilnehmer („Whales“) verfügen häufig über strukturelle Informationsvorteile, die ihnen einen besseren Zugang zu technischen, wirtschaftlichen und marktbezogenen Informationen ermöglichen. Demgegenüber fehlt vielen Kleinanlegerinnen und Kleinanlegern oftmals der Zugang zu vertieften technischen Analysen, Risikomodellen und komplexen Bewertungsmechanismen, wodurch die Einschätzung tatsächlicher Risiken erschwert wird. Zusätzlich ersetzen Whitepaper regelmäßig keine regulierten Prospekte und unterliegen vielfach nicht denselben Transparenz-, Prüf- und Offenlegungsanforderungen wie klassische Kapitalmarktinformationen. Dadurch können Informationsdefizite entstehen, die die Entscheidungsgrundlage von Verbraucherinnen und Verbrauchern erheblich beeinträchtigen.¹²² Wissenschaftliche Untersuchungen zeigen, dass ein Großteil der Kleinanleger:innen technische Risiken, Liquiditätsmechanismen oder Protokollabhängigkeiten nicht versteht.¹²³

¹²⁰ Vgl. Bank for International Settlements, The crypto ecosystem: key elements and risks, Juli 2023, S. 11.

¹²¹ Vgl. Bank for International Settlements, The crypto ecosystem: key elements and risks, Juli 2023, S. 11–12, 14.

¹²² Vgl. Bank for International Settlements, The crypto ecosystem: key elements and risks, Juli 2023, S. 6–8; Vgl. Art. 4 Abs. 1 sowie ErwGr 22 Verordnung (EU) 2023/1114 (MiCA).

¹²³ Vgl. OECD, The Tokenisation of Assets and Potential Implications, 2020, S. 29,41; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 83.

Juristisch führt dies zu strukturellen Nachteilen: Da Kryptowert-Angebote häufig nicht prospektpflichtig sind, fehlen standardisierte Offenlegungspflichten, wie sie im Kapitalmarktrecht (MiFID II, Prospekt-VO) vorgesehen sind.¹²⁴

3.3 Rechtliche Risiken von Kryptowerten

Rechtliche Risiken ergeben sich aus der besonderen Stellung von Kryptowerten zwischen Technik, Finanzmarktregulierung und allgemeinem Zivilrecht. Da Kryptowerte keine einheitliche rechtliche Kategorie darstellen und ihre technische Struktur traditionelle Rechtsfiguren herausfordert, entstehen Unsicherheiten in Bezug auf Eigentum, Vertragspflichten, Haftung, Insolvenz und regulatorische Zuordnung. Diese Risiken wirken besonders stark auf Verbraucher:innen, die ohne regulierte Intermediäre und ohne etablierte Rechtsmittel in einem Umfeld agieren, das von hoher Komplexität und rechtlicher Fragmentierung geprägt ist. Während sich traditionelle Vermögensrechte in klaren dogmatischen Kategorien bewegen (insbesondere Eigentum, Forderungen, Wertpapiere), entziehen sich Kryptowerte diesen Strukturen teilweise oder vollständig. Die fehlende Einbettung in das klassische Sachen und Schuldrecht führt dazu, dass alltägliche Vorgänge wie Erwerb, Verlust, Übertragung, Verwahrung, Insolvenz, Rechtsdurchsetzung, rechtlich ungeklärt oder widersprüchlich bleiben. Dies schafft Rechtsunsicherheit auf Seiten der Verbraucher:innen, verringert die Vorhersehbarkeit von Rechtsfolgen und erhöht die Gefahr irreparabler Vermögensverluste.¹²⁵

3.3.1 Rechtsunsicherheit über die rechtliche Einordnung („Legal Classification Risk“)

Ein zentrales rechtliches Risiko liegt in der fehlenden einheitlichen Einordnung von Kryptowerten. Die Qualifikation kann je nach Zweck, Struktur und Rechtsordnung variieren: Kryptowerte können als digitale Repräsentationen von Rechten, als Forderungen, als unkörperliche Sachen oder als reine technische Daten betrachtet werden.¹²⁶

In Österreich und Deutschland ist die Einordnung besonders diffizil, weil das Sachenrecht ausschließlich körperliche Sachen kennt. Ein Token ist jedoch weder körperlich noch ein klassisches Forderungsrecht; vielmehr handelt es sich um eine „technische Zuordnungsmöglichkeit“, deren Verfügungsmacht auf kryptographischer Kontrolle beruht.¹²⁷ Die Folge ist eine erhebliche Rechtsunsicherheit hinsichtlich der vermögensrechtlichen Einordnung digitaler Vermögenswerte. Dies betrifft insbesondere den Eigentumsschutz, da

¹²⁴ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 97–99.

¹²⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 17–23, 603–623, 658 ff.

¹²⁶ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 41–43, 249–251, 270 f; vgl. Binder Grosswang (Hrsg.), Digital Law, 2. Aufl. 2020, S. 19 f; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 149.

¹²⁷ Vgl. § 285 ABGB; § 90 BGB.

Kryptowerte vielfach nicht dem klassischen Eigentumsbegriff unterfallen. Ebenso bestehen Unsicherheiten im Zusammenhang mit dem Übertragungsvorgang, da weder ein körperlicher Besitz noch eine traditionelle Übergabe im sachenrechtlichen Sinn vorliegt. Darüber hinaus gestaltet sich ein gutgläubiger Erwerb regelmäßig problematisch oder ist nach klassischen sachenrechtlichen Strukturen nicht ohne weiteres möglich. Auch der sachenrechtliche Schutz vor Eingriffen kann nur eingeschränkt greifen, da traditionelle Schutzmechanismen grundsätzlich an das Vorliegen einer Sache anknüpfen und daher auf digitale Vermögenswerte nicht ohne Weiteres anwendbar sind. Diese Einordnungsprobleme führen zu erheblichen rechtlichen Unsicherheiten, insbesondere im Bereich des Vermögens- und Verbraucherschutzes.¹²⁸ Rechtswissenschaftliche Literatur weist darauf hin, dass die Zuordnung von Verfügungsgewalt via Private Key ein „rechtlich fiktives Besitzkonstrukt“ darstellt, jedoch kein sachenrechtliches Besitzrecht begründet.¹²⁹ Verbraucher:innen sind dadurch rechtlich schlechter gestellt als bei allen traditionellen Vermögensformen.

3.3.2 Vertragliche Risiken und AGB-Problematik bei Kryptodienstleistern

Verbraucher:innen nutzen häufig zentrale Intermediäre wie Kryptobörsen oder Wallet-Provider. Die Rechtsbeziehungen basieren nahezu ausnahmslos auf Allgemeinen Geschäftsbedingungen (AGB), die Haftung, Verwahrung, Pflichten und Rechte der Nutzer:innen regeln.¹³⁰

Typische rechtliche Risiken:

- 1. Zusätzliche rechtliche Unsicherheiten ergeben sich aus den unklaren Eigentumsverhältnissen bei Kryptobörsen und Verwahrstrukturen.** Viele Plattformen behandeln von Nutzer:innen und Nutzern eingezahlte Kryptowerte nicht als individuell zugeordnete Vermögenswerte, sondern lediglich als Anspruch auf Herausgabe gegenüber der Plattform. Dadurch kann die individuelle Zuordnung der Vermögenswerte erschwert werden. Im Insolvenzfall besteht daher das Risiko, dass Verbraucher:innen und Verbraucher lediglich über einen schuldrechtlichen Anspruch gegenüber dem Insolvenzschuldner verfügen und kein unmittelbarer Zugriff auf die eingezahlten Vermögenswerte möglich ist. Dies kann die Rechtsposition der Nutzer erheblich schwächen und den Vermögensschutz einschränken.¹³¹
- 2. Umfassende Haftungsausschlüsse in Allgemeinen Geschäftsbedingungen (AGB) führen häufig dazu, dass Anbieter ihre Verantwortlichkeit für zahlreiche Risiken des Kryptobereichs weitgehend begrenzen oder ausschließen.** Dies betrifft insbesondere Schäden infolge von

¹²⁸ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 217–218, 252, 297–303, 336–338.

¹²⁹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 217–218, 336–338.

¹³⁰ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 63, 69, 78.

¹³¹ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 72–74; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 205.

Hacks und Cyberangriffen, Verlusten privater Schlüssel (Private Keys), technischen Ausfällen, Systemfehlern sowie Netzwerküberlastungen. Für Verbraucherinnen und Verbraucher kann dies erhebliche Auswirkungen haben, da im Schadensfall die Durchsetzung von Ersatzansprüchen erschwert oder teilweise ausgeschlossen sein kann.¹³²

Solche Klauseln sind oft überraschend und für Verbraucher:innen nachteilig, aber mangels klarer Regulierung kaum angreifbar.

3. Weitere rechtliche Unsicherheiten ergeben sich aus Rechtswahlklauseln, die von Kryptobörsen und Plattformbetreibern häufig zugunsten ausländischer Rechtsordnungen verwendet werden. Dabei wird die Anwendbarkeit des Rechts bestimmter Staaten oder Offshore-Jurisdiktionen, etwa der Cayman Islands, von Singapur oder der Vereinigte Staaten, vereinbart. Für Verbraucherinnen und Verbraucher kann dies erhebliche praktische Schwierigkeiten verursachen, da die Durchsetzung von Ansprüchen in Österreich oder innerhalb der Europäischen Union erschwert und teilweise nur mit erheblichem Aufwand möglich sein kann. Dadurch entstehen zusätzliche Hürden im Bereich des Rechtsschutzes und der Anspruchsdurchsetzung.¹³³

4. Weitere verbraucherschutzrechtliche Risiken ergeben sich aus einseitigen Änderungen der Geschäftsbedingungen, die von vielen Kryptoplattformen und Dienstleistern vertraglich vorbehalten werden. Häufig behalten sich Anbieter das Recht vor, AGB, Gebührenstrukturen, Verwahrbedingungen oder Risikohinweise ohne ausdrückliche Zustimmung der Nutzerinnen und Nutzer anzupassen. Dadurch entsteht aus juristischer Sicht eine strukturelle Ungleichgewichtslage, da Kryptodienstleister die Vertragsbedingungen vielfach weitgehend selbst gestalten und verändern können. Gleichzeitig greifen traditionelle verbraucherschützende Mechanismen, insbesondere Anforderungen an Transparenz, faire Vertragsbedingungen und der Schutz vor missbräuchlichen Vertragsklauseln, im Kryptobereich teilweise nur eingeschränkt oder werden durch grenzüberschreitende und digitale Strukturen erschwert. Dies kann die Rechtsposition von Verbraucherinnen und Verbrauchern zusätzlich schwächen.¹³⁴

¹³² Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 17, 19 ff, 24, 31; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 30–32 (Ziff. 2.5.2).

¹³³ Vgl. Binance, Terms of Use, Governing Law (Cayman Islands); vgl. OKX, Terms of Use, Governing Law (Singapore); vgl. Coinbase, User Agreement, Governing Law (USA), jeweils abrufbar auf den Websites der Anbieter (abgerufen am 13.06.2026); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24, 31; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 30–32.

¹³⁴ Vgl. Binance, Terms of Use, Abschnitt „Changes to Terms“; vgl. Coinbase, User Agreement, Abschnitt „Modification of Agreement“, jeweils abrufbar auf den Websites der Anbieter (abgerufen am 13.06.2026); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 24, 31; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 30–32.

3.3.3 Eigentums- und Zuordnungsrisiken (Token Ownership Risk)

Ein besonders gravierendes rechtliches Risiko liegt in der ungeklärten Frage, was ein Verbraucher „besitzt“, wenn er einen Token hält.

Kein Eigentum im Sachenrecht: Kryptowerte stellen nach österreichischem, deutschem und schweizerischem Recht keine körperlichen Sachen dar und unterfallen daher nicht unmittelbar dem klassischen sachenrechtlichen Eigentumsbegriff; allerdings werden in Rechtsprechung und Literatur zunehmend eigentumsähnliche Zuordnungsmodelle diskutiert.¹³⁵

Kein Besitzschutz: Besitz setzt körperliche Sachherrschaft voraus; Private Keys erfüllen dieses Kriterium nicht. Keine dingliche Wirkung der Übertragung: Die Übertragung von Kryptowerten erfolgt regelmäßig technisch durch Transaktionen innerhalb der Blockchain, jedoch nicht im Sinne einer klassischen rechtsgeschäftlichen Übereignung nach sachenrechtlichen Grundsätzen. Dadurch entstehen erhebliche rechtliche Unsicherheiten hinsichtlich der vermögensrechtlichen Zuordnung und des Rechtsschutzes. Insbesondere besteht regelmäßig kein gutgläubiger Erwerb nach traditionellen sachenrechtlichen Strukturen, da die hierfür erforderlichen Voraussetzungen vielfach nicht vorliegen. Ebenso fehlt es an einer klassischen Publizitätswirkung, da keine körperliche Übergabe oder vergleichbare Publizitätsmechanismen bestehen. Darüber hinaus greift keine Eigentumsvermutung im herkömmlichen Sinn, wodurch die Zuordnung und Berechtigung an digitalen Vermögenswerten erschwert werden kann. Dies führt zu Unsicherheiten hinsichtlich der Frage, wer tatsächlich zur Verfügung über die betreffenden Kryptowerte berechtigt ist und welche Rechtswirkungen mit der Übertragung verbunden sind.¹³⁶ Rechtsfolgen für Verbraucher:innen : Bei Verlust von Token (z. B. durch Hack, Fehler, falsche Adresse) besteht kein sachenrechtlicher Rückforderungsanspruch. Auch Unterlassungs- oder Bereicherungsansprüche scheitern, wenn der Angreifer anonym ist oder außerhalb der Gerichtsbarkeit sitzt.¹³⁷ Der Verbraucher trägt das Risiko des Verlustes vollständig selbst, unabhängig von Verschulden oder Täterschaft.

3.3.4 Rechtsdurchsetzungsprobleme (Enforcement Risk)

Selbst bei eindeutigem Betrug oder rechtswidrigem Verhalten stehen Verbraucher:innen erheblichen Durchsetzungsproblemen gegenüber:

1. Ein weiteres wesentliches Problem stellt die Anonymität beziehungsweise Pseudonymität der Beteiligten dar. Blockchain-Transaktionen erfolgen regelmäßig unter Verwendung

¹³⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 26–28, 29–31, 33; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 102–105.

¹³⁶ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 134, 195, 200, 205, 337.

¹³⁷ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 27, 29–31, 33, 200; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 30–32.

kryptografischer Adressen und sind daher nicht unmittelbar einer bestimmten natürlichen oder juristischen Person zuordenbar. Dadurch kann die Identifikation von Tätern oder verantwortlichen Personen erheblich erschwert oder in einzelnen Fällen praktisch unmöglich werden. Dies wirkt sich insbesondere auf die Durchsetzung zivilrechtlicher Ansprüche sowie auf die strafrechtliche Verfolgung und den Verbraucherschutz aus.¹³⁸

2. Ein weiteres Problem besteht in der fehlenden internationalen Zuständigkeit und grenzüberschreitenden Durchsetzbarkeit von Ansprüchen. Viele Kryptoplattformen und Dienstleister operieren über Drittstaaten oder Offshore-Jurisdiktionen, wodurch Gerichtsstand und anwendbares Recht häufig außerhalb der Europäischen Union liegen. Für Verbraucherinnen und Verbraucher kann dies erhebliche Schwierigkeiten bei der gerichtlichen Durchsetzung von Ansprüchen verursachen, da Verfahren im Ausland mit zusätzlichen rechtlichen, organisatorischen und finanziellen Hürden verbunden sein können.¹³⁹

3. Ein weiteres wesentliches Problem besteht in den fehlenden Eingriffsmöglichkeiten innerhalb dezentraler Systeme. Regelmäßig existiert keine zentrale Instanz, die Transaktionen nachträglich rückgängig machen, Vermögenswerte einfrieren oder fehlerhafte Übertragungen korrigieren könnte. Dadurch kann selbst bei eindeutigen Rechtsverletzungen, etwa infolge von Betrug, Fehlüberweisungen oder unbefugten Zugriffen, die Wiederherstellung des ursprünglichen Vermögenszustands erheblich erschwert oder praktisch unmöglich werden. Dies führt zu zusätzlichen Herausforderungen im Bereich des Vermögens- und Verbraucherschutzes.¹⁴⁰

4. Ein weiteres Hindernis stellen die Kosten der Rechtsverfolgung dar. Grenzüberschreitende Verfahren und internationale Klagen sind häufig mit erheblichen finanziellen und organisatorischen Aufwendungen verbunden, wobei die entstehenden Kosten nicht selten über den tatsächlich eingetretenen Schadenssummen liegen können. In der Praxis führt dies dazu, dass Verbraucherinnen und Verbraucher häufig auf die Durchsetzung ihrer Ansprüche verzichten. Dadurch wird das rechtliche Risiko zusätzlich verstärkt, da bestehende Rechte zwar grundsätzlich vorhanden sein können, ihre tatsächliche Durchsetzung jedoch oftmals an praktischen und wirtschaftlichen Hürden scheitert.¹⁴¹

¹³⁸ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 26-32.

¹³⁹ Vgl. Binance, Terms of Use, Governing Law (Cayman Islands); vgl. OKX, Terms of Use, Governing Law (Singapore); vgl. Coinbase, User Agreement, Governing Law (USA), jeweils abrufbar auf den Websites der Anbieter (abgerufen am 13.06.2026); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 31.

¹⁴⁰ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 18-19, 30-32.

¹⁴¹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 200-201; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 30-32; vgl. OECD, Consumer Data Rights and Competition, 2020, S. 18-20.

3.3.5 Insolvenzzrisiken bei Kryptodienstleistern

Insolvenzzrisiken sind eines der zentralen rechtlichen Risiken für Verbraucher:innen.

1. Fehlende Sondervermögenstrennung: Von besonderer Bedeutung ist dabei die fehlende Trennung zwischen Kundenvermögen und Unternehmensvermögen. Bei zahlreichen Kryptoplattformen und Verwahrdienstleistern werden die von Nutzerinnen und Nutzern eingebrachten Kryptowerte nicht als gesondertes Vermögen geführt, sondern teilweise gemeinsam mit den Vermögenswerten des Unternehmens verwaltet. Im Insolvenzfall kann dies dazu führen, dass Verbraucher:innen nicht als gesondert berechnete Inhaber ihrer Vermögenswerte behandelt werden, sondern lediglich die Stellung ungesicherter Gläubiger einnehmen. Dadurch kann die Durchsetzung von Ansprüchen erheblich erschwert und der Vermögensschutz deutlich eingeschränkt werden.¹⁴²

2. Keine Aussonderungsrechte: Ein weiteres wesentliches Insolvenzzisiko besteht im Fehlen von Aussonderungsrechten. Aufgrund der fehlenden klassischen sachenrechtlichen Einordnung digitaler Vermögenswerte besteht vielfach kein Aussonderungsanspruch, wie er etwa bei traditionellen Wertpapieren oder Depotvermögen vorgesehen ist. Dadurch können Verbraucher:innen im Insolvenzfall häufig keinen unmittelbaren Zugriff auf ihre eingebrachten Kryptowerte geltend machen und werden unter Umständen lediglich als allgemeine Gläubiger behandelt. Dies kann die Rechtsposition der Betroffenen erheblich schwächen und den Vermögensschutz einschränken.¹⁴³

3. Beispielhafte Fälle: Wie die Insolvenzen von FTX, Celsius Network und Voyager Digital verdeutlichen die praktischen Auswirkungen dieser Risiken. Die Analysen dieser Insolvenzverfahren zeigen, dass Verbraucher:innen häufig nur geringe Insolvenzquoten erhielten. Zudem wurden die eingebrachten Kryptowerte teilweise, wie Unternehmensvermögen behandelt, wodurch die Rechtsposition der Nutzer zusätzlich geschwächt wurde. Erschwerend kam hinzu, dass zahlreiche Plattformen umfassende Haftungsausschlüsse in ihren Allgemeinen Geschäftsbedingungen vorgesehen hatten, wodurch die Durchsetzung von Ansprüchen zusätzlich erschwert wurde.¹⁴⁴

4. Fehlende europäische Harmonisierung: Vor Inkrafttreten der MiCA-Verordnung existierte innerhalb der Europäischen Union keine einheitliche Regelung hinsichtlich der Verwahrungs- und Schutzpflichten für Kryptowerte. Dadurch bestanden erhebliche Unterschiede zwischen

¹⁴² Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 246–252; vgl. FDIC, The FDIC’s Investigation of Voyager Digital, 2023, S. 7–10.

¹⁴³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 246–252.

¹⁴⁴ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 246–249; vgl. KPMG, The Collapse of FTX, (2022), S. 5–12; vgl. FDIC, The FDIC’s Investigation of Voyager Digital, (2023), S. 7–10; vgl. OECD, Consumer Data Rights and Competition, (2020), S. 18–20.

den nationalen Rechtsordnungen und Aufsichtssystemen. Auch nach Einführung der MiCA-Verordnung verbleiben weiterhin Regelungslücken, da insbesondere DeFi-Protokolle sowie Non-Custodial-Wallets grundsätzlich nicht oder nur eingeschränkt vom Anwendungsbereich erfasst werden. Dadurch bestehen weiterhin Bereiche mit begrenzter regulatorischer Erfassung und verbraucherschutzrechtlichen Unsicherheiten.¹⁴⁵

Verbraucher:innen tragen folglich ein vollständiges Insolvenz- und Vermögenszuordnungsrisiko.

3.3.6 Unklare Haftungsfragen und Verantwortungsdiffusion

Kryptosysteme führen zu einer Aufsplitterung von Verantwortlichkeiten, da die einzelnen Funktionen regelmäßig auf unterschiedliche Akteure verteilt werden. So entwickeln Entwickler:innen die zugrunde liegende Software, Börsen und Plattformbetreiber führen Transaktionen und Handelsvorgänge aus, Validatoren übernehmen die Bestätigung und Validierung von Blöcken, Dezentrale Autonome Organisationen (DAO) treffen organisatorische oder protokollbezogene Entscheidungen und Nutzer:innen verwalten ihre privaten Schlüssel eigenverantwortlich. Diese funktionale Verteilung erschwert die Zuweisung rechtlicher Verantwortung erheblich. Im Schadensfall bleibt daher häufig unklar, welcher Akteur als Haftungssubjekt heranzuziehen ist. In der Literatur wird dies teilweise als „haftungsrechtliche Fragmentierung“ bezeichnet, da die Aufteilung der Verantwortlichkeiten die Voraussetzungen klassischer Anspruchsgrundlagen – insbesondere aus Vertrag, Delikt oder Produzentenhaftung – häufig nur eingeschränkt erfüllt und dadurch die Durchsetzung von Ansprüchen erschwert wird.¹⁴⁶

Die haftungsrechtliche Fragmentierung führt zu mehreren zentralen Problemen im Bereich der Verantwortungszuweisung. So besteht regelmäßig keine klassische Produzentenhaftung für Open-Source-Software, da Entwickler häufig keinen unmittelbaren Betreiberstatus innehaben und ihre Programme dezentral zur Verfügung gestellt werden. Ebenso wird eine Haftung von Validatoren vielfach abgelehnt, da diese grundsätzlich lediglich Validierungs- und Bestätigungsfunktionen innerhalb des Netzwerks übernehmen. Hinzu kommt das Fehlen einer Organhaftung bei Dezentralen Autonomen Organisationen (DAO), da diese häufig keine klassische Organisationsstruktur mit eindeutig zuordenbaren Organen aufweisen. Darüber hinaus bestehen bei dezentralen Protokollen ohne identifizierbaren Betreiber vielfach keine unmittelbaren vertraglichen Beziehungen, wodurch auch vertragliche Pflichten und

¹⁴⁵ Vgl. Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM (2020) 593 final; vgl. Art. 2, 3 und 75 ff. Verordnung (EU) 2023/1114 (MiCA); vgl. ESMA, Advice on Crypto-Assets, (2022).

¹⁴⁶ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 28–29, 86–87; Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 569–571.

entsprechende Haftungsgrundlagen nur eingeschränkt bestehen. Diese Umstände erschweren die Bestimmung eines Haftungssubjekts und können die Durchsetzung von Ansprüchen erheblich beeinträchtigen.¹⁴⁷

Für Verbraucher:innen bedeutet dies ein systemisches Rechtsschutzdefizit: selbst bei eindeutigem technischem Fehler oder Organisationsversagen gibt es keinen haftbaren Rechtsträger.

3.3.7 Fehlende regulatorische Einbettung außerhalb zentraler Dienstleister

Die MiCA-Verordnung schafft erstmals einheitliche regulatorische Pflichten für zentrale Kryptodienstleister (Crypto-Asset Service Providers – CASPs) und stärkt dadurch die Aufsicht sowie den Verbraucherschutz innerhalb des regulierten Bereichs. Dennoch verbleiben weiterhin wesentliche Teile des Kryptomarktes außerhalb oder nur eingeschränkt innerhalb des regulatorischen Anwendungsbereichs. Dies betrifft insbesondere DeFi-Protokolle, Dezentrale Autonome Organisationen (DAO), Open-Source-Infrastrukturen, Cross-Chain-Bridges sowie Non-Custodial-Wallets. Für diese Bereiche bestehen weiterhin erhebliche Regelungs- und Schutzlücken, da zentrale Verantwortungsstrukturen und klassische Aufsichtsmechanismen häufig fehlen.¹⁴⁸ Gerade diese Bereiche sind technologisch am komplexesten und rechtlich am unklarsten, sodass Verbraucher:innen dort besonders schutzlos sind.

3.4 Risiken durch Marktstruktur und Intermediäre

Die Marktstruktur des Kryptosektors unterscheidet sich fundamental von traditionellen Finanzmärkten. Im Gegensatz zu regulierten Finanzsystemen, die durch Intermediäre mit klar definierten Aufgaben und Pflichten – etwa Banken, Wertpapierfirmen, Zentralverwahrer oder Zahlungsdienstleister – geprägt sind, operieren Kryptomärkte innerhalb eines hybriden Systems aus zentralisierten Plattformen, dezentralen Protokollen, nebeneinander bestehenden technischen Infrastrukturen sowie global verteilten Marktteilnehmern. Diese Struktur führt zu einer wesentlich komplexeren Organisations- und Verantwortungsordnung und erschwert die eindeutige Zuordnung rechtlicher Pflichten sowie die Anwendung traditioneller Regulierungs- und Verbraucherschutzmechanismen.¹⁴⁹

Diese Struktur erzeugt erhebliche Risiken für Verbraucher:innen, weil Zuordnungs-, Transparenz- und Verantwortlichkeitsfragen unklar bleiben und wesentliche

¹⁴⁷ Vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 28–29, 86–87, 150; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 569–570.

¹⁴⁸ Vgl. Art. 2, 3, 59 ff. und 75 ff. Verordnung (EU) 2023/1114 (MiCA); vgl. ESMA, Advice on Crypto-Assets, (2022); vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 28–29, 86–87.

¹⁴⁹ Vgl. OECD, Consumer Data Rights and Competition, (2020), S. 7–11; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 24–26, 28–29, 86–87.

Schutzmechanismen fehlen, die in traditionellen Märkten selbstverständlich sind. Die Besonderheit des Kryptomarktes liegt darin, dass Marktstruktur- und Intermediäris Risiken unmittelbar mit technologischen, rechtlichen und ökonomischen Risiken verwoben sind. Dies führt zu einem Umfeld, in dem Verbraucher:innen nicht nur durch Marktvolatilität, sondern durch strukturell bedingte Systemschwächen gefährdet sind.¹⁵⁰

3.4.1 Missbrauchsrisiken durch Eigenhandel, Interessenkonflikte und Intransparenz

Kryptobörsen übernehmen häufig mehrere Funktionen gleichzeitig und vereinen unterschiedliche Rollen innerhalb einer einzigen Plattformstruktur. Sie agieren nicht nur als Handelsplatz für den Kauf und Verkauf von Kryptowerten, sondern übernehmen vielfach zugleich Aufgaben der Verwahrung von Vermögenswerten. Darüber hinaus treten sie teilweise als Market-Maker auf, emittieren eigene Token, stellen Kredit- und Finanzierungsleistungen bereit und fungieren zusätzlich als Liquiditätsanbieter. Diese Mehrfachfunktion kann zu Interessenkonflikten sowie zu erhöhten Risiken im Bereich der Marktintegrität, Transparenz und des Verbraucherschutzes führen.¹⁵¹ Diese vertikale Integration würde in traditionellen Finanzmärkten als inakzeptabler Interessenkonflikt gelten.

Typische Risiken für Verbraucher:innen:

a) Eigenhandel gegen Kund:innen : Ohne Marktmissbrauchsaufsicht besteht das Risiko, dass Börsen interne Informationen nutzen, um gegen ihre Kunden zu handeln.

b) Intransparente Orderausführung: Viele Kryptoplattformen weisen weiterhin Transparenzdefizite hinsichtlich ihrer Handels- und Preisbildungsmechanismen auf. Häufig wird nicht offengelegt, ob Handelsaufträge intern ausgeführt oder internalisiert werden, nach welchen Kriterien Preise und Kursstellungen berechnet werden oder ob zusätzliche Spread-Aufschläge und indirekte Kosten erhoben werden. Diese fehlende Transparenz kann die Nachvollziehbarkeit von Handelsvorgängen erschweren und die Informationslage von Verbraucher:innen und Verbrauchern erheblich beeinträchtigen.¹⁵²

c) Listing-Risiken: Kryptobörsen verfügen regelmäßig über einen weitreichenden Entscheidungsspielraum hinsichtlich der Auswahl und Listung von Token. Dabei entscheiden die Plattformen häufig eigenständig, welche Kryptowerte zum Handel zugelassen werden. Gleichzeitig bestehen Hinweise darauf, dass einzelne Projekte Gebühren oder sonstige Leistungen für Listings erbringen, ohne dass diese Vorgänge oder mögliche wirtschaftliche

¹⁵⁰ Vgl. OECD, Consumer Data Rights and Competition , (2020), S. 7–12, 18–20; vgl. Schweizer Bundesrat, DLT-Bericht (2018), S. 15–17, 24–29, 86–87; vgl. ErwGr 1–3 Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final.

¹⁵¹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 540, 550–556.

¹⁵² Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 544–548, 558–562.

Interessen stets offengelegt werden. Dies kann zu Transparenzdefiziten und potenziellen Interessenkonflikten führen.¹⁵³

d) Fehlende Best Execution-Regeln

Die im traditionellen Finanzmarkt geltenden Grundsätze der MiFID II, insbesondere die Verpflichtung zur bestmöglichen Ausführung von Aufträgen (Best Execution), finden im Kryptobereich vielfach keine oder nur eingeschränkte Anwendung. Dadurch bestehen für Kryptodienstleister regelmäßig keine vergleichbaren Verpflichtungen hinsichtlich Ausführungsqualität, Preisgestaltung oder Transparenz. Verbraucher:innen erhalten daher häufig nicht denselben Schutzstandard, wie er Kundinnen und Kunden im klassischen Wertpapiermarkt zur Verfügung steht.¹⁵⁴

3.4.2 Intransparenz und Informationsdefizite in Marktstrukturen

Ein strukturelles Risiko liegt darin, dass Kryptomärkte keine regulierten Marktinfrastrukturen wie geregelte Märkte, MTFs (Multilateral Trading Facility) oder OTFs (Organized Trading Facility) kennen.¹⁵⁵ Für Verbraucher:innen ergeben sich daraus erhebliche Herausforderungen im Bereich der Markttransparenz und Nachvollziehbarkeit. Häufig bestehen keine umfassenden Meldepflichten sowie nur eingeschränkte Handelsüberwachungsmechanismen, wodurch Marktaktivitäten und mögliche Unregelmäßigkeiten nur begrenzt nachvollzogen werden können. Hinzu kommt eine fehlende Transparenz hinsichtlich Orderbücher und Handelsdaten, wodurch Preisbildung und Ausführungsprozesse oftmals nur eingeschränkt überprüfbar sind. Darüber hinaus existiert regelmäßig kein einheitlicher Referenzmarkt, sodass erhebliche Preis- und Kursabweichungen zwischen verschiedenen Handelsplattformen auftreten können. Dies erschwert Verbraucher:innen die Bewertung von Marktpreisen und erhöht die Informationsasymmetrien innerhalb des Kryptomarktes.¹⁵⁶

Preisfindung ist nicht reguliert, sondern erfolgt durch Plattform-Aggregatoren. Dies unterscheidet sich fundamental von traditionellen Märkten, in denen Börsen strengen Transparenzvorgaben unterliegen.

¹⁵³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 544–548.

¹⁵⁴ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 544–548; Art 27 Richtlinie 2014/65/EU (MiFID II).

¹⁵⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 544–548; Art 4 Abs 1 Z 21–23 Richtlinie 2014/65/EU (MiFID II).

¹⁵⁶ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 544–548, 558–562; Art 4 Abs 1 Z 21–23, Art 26, Art 27 Richtlinie 2014/65/EU (MiFID II).

3.4.3 Unzureichende Marktüberwachung und fehlende Aufsichtsbefugnisse

Im Unterschied zu traditionellen Finanzmärkten verfügen Kryptomärkte vielfach nicht über vergleichbare Marktüberwachungs- und Kontrollmechanismen. Häufig fehlen Systeme zur Überwachung von Marktmissbrauch, verbindliche Transaktionsmeldepflichten, Positionslimits zur Begrenzung von Marktkonzentrationen sowie Transparenzpflichten für außerbörsliche Geschäfte (Over-the-Counter – OTC), die außerhalb regulierter Handelsplattformen erfolgen.¹⁵⁷ Dies führt dazu, dass Marktmanipulationen häufig nur eingeschränkt erkannt oder verfolgt werden, Insiderhandel vielfach unentdeckt bleibt und die Preisbildung nur begrenzt transparent und nachvollziehbar ist. Verbraucher:innen verfügen daher oftmals nicht über vergleichbare Schutzmechanismen wie Kund:innen im traditionellen Wertpapiermarkt. Zwar schafft die MiCA-Verordnung erstmals regulatorische Pflichten und Aufsichtsvorgaben für zentrale Kryptodienstleister, jedoch verbleiben DeFi-Strukturen sowie zahlreiche Offshore-Börsen und grenzüberschreitende Plattformen weiterhin außerhalb oder nur eingeschränkt innerhalb des regulatorischen Anwendungsbereichs. Dadurch bestehen weiterhin erhebliche Aufsichts- und Verbraucherschutzlücken.

3.5 MiCA aus verbraucherschutzrechtlicher Perspektive

Die Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA) ist die erste unionsweit einheitliche Kodifikation, die den bislang weitgehend unregulierten Kryptomarkt in ein kohärentes Regime überführt und ausdrücklich ein hohes Schutzniveau für Kleinanleger:innen und sonstige Nutzer:innen zum Ziel erklärt.¹⁵⁸ MiCA versteht Verbraucherschutz dabei nicht als isoliertes Spezialthema, sondern als Querschnittsziel: Schutzvorgaben finden sich in den allgemeinen Bestimmungen, in den Kapiteln über Emittenten von Kryptowertearten (insbesondere Asset-referenced Tokens und E-Geld-Token) sowie im Abschnitt über Kryptodienstleister (CASPs) und in den Marktmissbrauchsregeln.¹⁵⁹

In den vorangegangenen Kapiteln und Abschnitten wurden sowohl die Systematik der MiCA-Verordnung im Überblick als auch die konkreten Gefährdungen für Verbraucherinnen und Verbraucher dargestellt. Aufbauend darauf richtet sich der Fokus nun auf die verbraucherschutzrechtliche Funktion der MiCA-Instrumente. Im Mittelpunkt steht dabei die Analyse, in welchem Umfang MiCA die zuvor herausgearbeiteten technologischen,

¹⁵⁷ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 544–548, 558–562; Art. 20–22, 26, 57 Richtlinie 2014/65/EU (MiFID II).

¹⁵⁸ ErwGr 1, 2, 5, 6, 8–10, 16, 67 sowie Art. 1, 4–7, 59–76 Verordnung (EU) 2023/1114 (MiCA).

¹⁵⁹ Vgl. Art. 1 Abs. 1, 15–36, 43–55, 59–76 und 80–92 sowie ErwGr 5, 8 und 9 Verordnung (EU) 2023/1114 (MiCA).

ökonomischen, informationsbezogenen und organisatorischen Risiken adressiert und auf welche regulatorischen Mechanismen sie sich hierbei stützt.

3.5.1 Zielsetzung und normative Grundentscheidung

In den Erwägungsgründen hebt die MiCA-Verordnung hervor, dass das Fehlen eines einheitlichen unionsweiten Rechtsrahmens für Kryptowerte das Vertrauen der Nutzer:innen beeinträchtigen und gleichzeitig zu Marktfragmentierungen, regulatorischer Arbitrage sowie zu unterschiedlichen Schutzniveaus innerhalb der Europäischen Union führen kann. Vor diesem Hintergrund verfolgt die Verordnung das Ziel, ein harmonisiertes Regelwerk für Kryptowerte zu schaffen. Dieses soll einerseits Rechtsklarheit und Rechtssicherheit für Emittent:innen und Kryptodienstleister schaffen und andererseits Wettbewerbsverzerrungen infolge nationaler Sonderregelungen begrenzen. Gleichzeitig soll die Verordnung ein hohes Schutzniveau für Inhaber:innen von Kryptowerten sicherstellen und dadurch zur Stärkung des Vertrauens sowie zur Stabilisierung des Kryptomarktes beitragen.¹⁶⁰

Der Verbraucherschutz wird im Rahmen der MiCA-Verordnung primär durch präventive Regulierungsinstrumente ausgestaltet. Im Mittelpunkt stehen dabei insbesondere standardisierte Informationspflichten, die Transparenz und Nachvollziehbarkeit für Nutzer:innen schaffen sollen. Ergänzend sieht die Verordnung Zulassungs- und Organisationsanforderungen für Emittent:innen und Kryptodienstleister vor, um Mindeststandards hinsichtlich Struktur, Governance und Aufsicht sicherzustellen. Hinzu treten Verhaltensregeln, die ein ordnungsgemäßes Marktverhalten fördern sollen, sowie Marktmissbrauchsverbote, die Manipulationen und missbräuchliche Praktiken begrenzen sollen. Darüber hinaus werden Beschwerde- und Aufsichtsmechanismen vorgesehen, um die Durchsetzung regulatorischer Vorgaben und den Schutz der Nutzer:innen zu stärken.¹⁶¹ Ein explizites System ex-post finanzieller Kompensation (etwa Einlagensicherung oder Anlegerentschädigung) enthält MiCA demgegenüber nicht;

3.5.2 Informations- und Whitepaper-Pflichten als zentrale Verbraucherschutzinstrumente

Ein zentrales Element des MiCA-Verbraucherschutzes ist die Pflicht zur Veröffentlichung eines Krypto-Asset-Whitepapers für öffentliche Angebote und Börsenlistings von Kryptowerte, die in den Anwendungsbereich fallen.¹⁶² Das Whitepaper soll den Informationsvorsprung der Emittenten begrenzen und Anleger:innen eine fundierte Entscheidung ermöglichen.

¹⁶⁰ ErwGr 1, 2, 5, 6, 8–10 Verordnung (EU) 2023/1114 (MiCA).

¹⁶¹ Art. 4–7, 19, 51, 59–63, 66–70, 71–75, 80–92, 94–111 Verordnung (EU) 2023/1114 (MiCA).

¹⁶² Art. 4 Abs. 1, Art. 5–7 sowie ErwGr 5, 8 und 9 Verordnung (EU) 2023/1114 (MiCA).

MiCA schreibt hierfür Mindestinhalte vor, darunter insbesondere:

Angaben zur Identität des Emittenten bzw. Anbieters,
eine Beschreibung des Projekts und der mit den aufgenommenen Mitteln verfolgten Zwecke,
eine Darstellung der Rechte der Inhaber (z. B. Rückzahlungsrechte, Stimmrechte, Gewinnbeteiligungen),
eine klare und ehrliche Beschreibung der wesentlichen Risiken,
bei bestimmtem Token auch Informationen zu Umwelt- und Klimawirkungen des Konsensmechanismus.¹⁶³

Zugleich unterwirft MiCA-Marketingkommunikation eigenständigen Anforderungen: Werbung muss klar als solche erkennbar, mit dem Whitepaper konsistent, nicht irreführend und für Kleinanleger:innen verständlich sein.¹⁶⁴ Damit werden typische Muster des Krypto-Marketings – aggressive Renditeversprechen, selektive Herausstellung von Chancen bei gleichzeitiger Verdeckung der Risiken – erstmals unionsweit reguliert.

3.5.3 Autorisierung und laufende Aufsicht von Krypto-Dienstleistern (CASPs)

Ein zweiter zentraler Verbraucherschutzpfeiler ist die Zulassungspflicht für Krypto-Dienstleister (Crypto-Asset Service Provider – CASPs). Dienste wie Handel, Verwahrung, Betrieb von Handelsplattformen oder Beratung dürfen künftig grundsätzlich nur von zugelassenen Unternehmen erbracht werden, die:

bestimmte Eigenmittelanforderungen erfüllen,
eine geeignete Geschäftsorganisation vorhalten,
über Leitungsorgane mit ausreichender fachlicher Eignung und Zuverlässigkeit verfügen,
interne Kontroll- und Risikomanagementsysteme implementieren,
Interessenkonflikte identifizieren und steuern.¹⁶⁵

Für Verbraucher:innen bedeutet die MiCA-Verordnung erstmals die Schaffung eines Mindestmaßes an institutioneller Verlässlichkeit, das sich teilweise an den Schutzmechanismen regulierter Finanzdienstleistungen orientiert.

Von besonderer Bedeutung sind dabei insbesondere die Verwahr- und Vermögenstrennungsregeln, wonach Crypto-Asset Service Provider (CASPs) verpflichtet sind, Kundengelder und eigene Vermögenswerte getrennt zu halten und organisatorische Maßnahmen zu treffen, damit Kundentoken nicht für unternehmenseigene Zwecke verwendet

¹⁶³ Art. 5 Abs. 1 lit. a–f, j sowie Art. 6 Abs. 2 Verordnung (EU) 2023/1114 (MiCA); ErwGr 67 Verordnung (EU) 2023/1114 (MiCA).

¹⁶⁴ Art. 6 Abs. 2, Art. 7 Abs. 1 und 2 sowie ErwGr 5, 8 und 67 Verordnung (EU) 2023/1114 (MiCA).

¹⁶⁵ Art. 59, 61–62, 67, 72 sowie Art. 94–111 Verordnung (EU) 2023/1114 (MiCA).

werden. Dadurch soll der Schutz der Vermögenswerte von Nutzer:innen verbessert und das Risiko von Vermischungen reduziert werden.¹⁶⁶

Ergänzend sieht die Verordnung Best-Execution- und Transparenzpflichten vor. Bei der Ausführung von Dienstleistungen müssen angemessene Maßnahmen getroffen werden, um für Kund:innen den bestmöglichen Ausführungspreis zu erreichen. Gleichzeitig bestehen Verpflichtungen zur Offenlegung von Gebühren, Kosten und weiteren relevanten Informationen, um Transparenz und Nachvollziehbarkeit für Verbraucher:innen zu stärken.¹⁶⁷

3.5.4 Besondere Vorgaben für Asset-referenced Tokens und E-Geld-Token

Für Asset-referenced Tokens (ARTs) und E-Geld-Token (EMTs) sieht MiCA ein besonders dichtes Regime vor, das ausdrücklich auf die Risiken für breite Nutzerkreise abstellt. Der Gesetzgeber geht davon aus, dass gerade stabile oder als stabil wahrgenommene Token in großem Umfang von Verbraucher:innen als Wertaufbewahrungs- oder Zahlungsmittel verwendet werden können und damit zusätzliche Gefahren für Finanzstabilität und Zahlungsverkehr entstehen.¹⁶⁸

Zu den verbraucherschutzrelevanten Elementen zählen insbesondere:

Reserve- und Deckungsanforderungen: Emittenten müssen das Token vollständig oder in einem definierten Verhältnis mit hochwertigen, liquiden Vermögenswerten unterlegen und klare Regeln für die Verwaltung dieser Reserven einhalten.¹⁶⁹

Rückzahlungsrechte: Halter von EMTs haben grundsätzlich einen Anspruch auf Rückzahlung zum Nennwert in der Referenzwährung; bei ARTs sind Rücknahme- und Rückzahlungsmechanismen festzulegen und offenzulegen.¹⁷⁰

Zusätzliche Governance- und Liquiditätsstandards für „signifikante“ Token, die aufgrund ihrer Größe oder Reichweite als systemisch relevant eingestuft werden können.¹⁷¹

Diese Regelungen sollen verhindern, dass Verbraucher:innen durch den Zusammenbruch vermeintlich stabiler Token – wie in der Vergangenheit bei einzelnen „Stablecoin“-Projekten – unvorbereitet Vermögensverluste erleiden.

¹⁶⁶ Vgl. Art. 59–63, Art. 61 Abs. 1 und 2, Art. 67 Abs. 8 sowie ErwGr 5, 8 und 9 Verordnung (EU) 2023/1114 (MiCA).

¹⁶⁷ Vgl. Art. 66 Abs. 3 und Art. 67 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

¹⁶⁸ Vgl. ErwGr 9, 22, 24, 26–28, 60 sowie Art. 15–36 und 43–55 Verordnung (EU) 2023/1114 (MiCA).

¹⁶⁹ Vgl. Art. 30–34, Art. 31, Art. 45–47 sowie ErwGr 26–28 und 60 Verordnung (EU) 2023/1114 (MiCA).

¹⁷⁰ Vgl. Art. 44 Abs. 1, Art. 16 Abs. 1 lit. d, Art. 29 Abs. 1 lit. b sowie ErwGr 22, 24 und 26 Verordnung (EU) 2023/1114 (MiCA).

¹⁷¹ Vgl. Art. 35, 36, 43, 45 und 56 sowie ErwGr 26–28 und 60 Verordnung (EU) 2023/1114 (MiCA).

3.5.5 Beschwerdeverfahren und Rechtsdurchsetzung

Ein wesentlicher Bestandteil eines funktionsfähigen Verbraucherschutzes ist die Möglichkeit, Beschwerden effektiv vorzubringen und behördlich prüfen zu lassen. MiCA sieht hierfür eine mehrschichtige Struktur vor:

Interne Beschwerden bei Emittenten von ARTs und EMTs:

Emittent:innen sind verpflichtet, Verfahren zur schnellen, fairen und kostenfreien Bearbeitung von Beschwerden von Tokeninhaber:innen vorzuhalten. Dadurch soll sichergestellt werden, dass Verbraucher:innen ihre Anliegen und Beschwerden effektiv geltend machen können. Diese Anforderungen werden zusätzlich durch delegierte Rechtsakte sowie Regulatory Technical Standards (RTS) der Europäische Bankenaufsichtsbehörde weiter konkretisiert. Dabei werden insbesondere Vorgaben zu Verfahrensabläufen, Bearbeitungs- und Vorhaltefristen sowie Dokumentationspflichten festgelegt, um eine einheitliche und nachvollziehbare Beschwerdebearbeitung sicherzustellen.¹⁷²

Beschwerdeverfahren bei CASPs:

Für Krypto-Dienstleister normiert MiCA eigenständige Pflichten zur Beschwerdebearbeitung (insbesondere in Art. 71 MiCA). CASPs müssen Kunden ermöglichen, Beschwerden unentgeltlich einzureichen; sie haben strukturierte, nachvollziehbare Verfahren vorzuhalten und die Ergebnisse transparent mitzuteilen.¹⁷³

Beschwerden bei Aufsichtsbehörden:

MiCA verpflichtet die zuständigen nationalen Behörden, Verfahren einzurichten, über die Verbraucher:innen, aber auch Verbraucherverbände, mutmaßliche Verstöße gegen MiCA anzeigen können. Die Behörden müssen hierzu leicht zugängliche Kanäle bereitstellen und ESMA bzw. EBA über ihre Verfahren informieren.¹⁷⁴

Damit reagiert MiCA auf ein zentrales Defizit der bisherigen Kryptomärkte, in denen Verbraucher:innen bei Konflikten mit Plattformen häufig ohne wirksame Anlaufstelle blieben.

3.5.6 Marktintegrität und Schutz vor Marktmissbrauch

Da sich viele Verbraucherrisiken aus manipulativer Preisbildung, Insiderhandel und missbräuchlicher Marktkommunikation ergeben, erweitert MiCA das unionsrechtliche Marktmissbrauchsregime auf Kryptowerte, die zum Handel auf einer Handelsplattform zugelassen sind oder für die ein Zulassungsantrag gestellt wurde.¹⁷⁵

¹⁷² Vgl. Art. 31 Abs. 1 lit. h und Abs. 4, Art. 46 Abs. 1 lit. h und Abs. 4, Art. 94–111 sowie ErwGr 5, 8 und 9 Verordnung (EU) 2023/1114 (MiCA).

¹⁷³ Vgl. Art. 71 Abs. 1–3 sowie ErwGr 5, 8 und 9 Verordnung (EU) 2023/1114 (MiCA).

¹⁷⁴ Vgl. Art. 108 Abs. 1–3 sowie Art. 94–111 Verordnung (EU) 2023/1114 (MiCA).

¹⁷⁵ Vgl. Art. 80–92 sowie ErwGr 5, 9 und 67 Verordnung (EU) 2023/1114 (MiCA).

Die Verordnung enthält ein eigenständiges Set von Verboten, u. a.:

Verbot des Insiderhandels,

Verbot der unrechtmäßigen Offenlegung von Insiderinformationen,

Verbot von Marktmanipulation, inklusive manipulativer Orders, Fake-Volumen und irreführender Signale, auch durch Nutzung sozialer Medien und algorithmischer Tools.¹⁷⁶

Krypto-Dienstleister, die Handelsplattformen betreiben, müssen Systeme und Verfahren zur Überwachung und Meldung von Marktmissbrauch implementieren. Dies dient mittelbar dem Schutz von Kleinanleger:innen, indem extreme Kursverwerfungen, künstliche Preisblasen oder koordinierte Verkaufswellen zumindest leichter erkannt und sanktioniert werden können.

¹⁷⁶ Art. 80–92, insb. Art. 87–89 sowie ErwGr 5, 9 und 67 Verordnung (EU) 2023/1114 (MiCA).

Kapitel 4

Unionsrechtlicher Rechtsrahmen mit Schwerpunkt auf der MiCA-Verordnung

4.1 Einbettung des österreichischen Rechtsrahmens in das Unionsrecht

Die österreichische Rechtsordnung begegnet Kryptowerten nicht isoliert, sondern innerhalb eines mehrstufigen Regelungsgefüges, das maßgeblich durch das Unionsrecht geprägt wird. Ausgangspunkt bildet dabei ein Top-down geprägtes Zusammenspiel zwischen unionsrechtlichen und nationalen Regelungsebenen. Auf europäischer Ebene schaffen insbesondere die MiCA-Verordnung, die Geldwäscherichtlinien, insbesondere die Fünfte Geldwäscherichtlinie (AMLD5), die Zahlungsdiensterichtlinie (PSD2), die Datenschutz-Grundverordnung (DSGVO) sowie weitere sektorspezifische Aufsichtsregelungen den rechtlichen Rahmen für den Umgang mit Kryptowerten. Auf nationaler Ebene werden diese unionsrechtlichen Vorgaben in die bestehende österreichische Rechtsordnung integriert und in die Systematik des Allgemeinen Bürgerlichen Gesetzbuches (ABGB) sowie in kapitalmarkt-, finanzmarkt- und aufsichtsrechtliche Spezialregelungen eingebettet. Dazu zählen insbesondere das Finanzmarkt-Geldwäschegesetz (FM-GwG), das Zahlungsdienstegesetz 2018 (ZaDiG 2018), das Kapitalmarktgesetz (KMG) sowie steuerrechtliche Vorschriften. Dadurch entsteht ein mehrschichtiges Regelungssystem, das sowohl unionsrechtliche als auch nationale Elemente miteinander verbindet.¹⁷⁷

Für den Verbraucherschutz bedeutet dies, dass Österreich nicht frei darin ist, ein vollständig eigenständiges Regelungssystem für Kryptowerte zu entwickeln, sondern die unionsrechtlichen Vorgaben in ein kohärentes nationales Rechts- und Schutzsystem zu integrieren hat.

Gleichzeitig verbleiben den Mitgliedstaaten weiterhin Gestaltungsspielräume. Die Europäische Union legt insbesondere Mindeststandards, grundlegende Strukturen und regulatorische Rahmenbedingungen fest, während die konkrete Ausgestaltung, der Vollzug sowie ergänzende Schutzmechanismen weitgehend in der Verantwortung der einzelnen Mitgliedstaaten verbleiben. Dadurch entsteht ein Zusammenspiel aus unionsrechtlicher Harmonisierung und nationaler Umsetzung, das auch für den österreichischen Verbraucherschutz im Kryptobereich von zentraler Bedeutung ist.¹⁷⁸

¹⁷⁷ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 5–9; Vgl. ErwGr 1 und 7 Verordnung (EU) 2023/1114 (MiCA); Vgl. ErwGr 8 Richtlinie (EU) 2018/843; ErwGr 6 Richtlinie (EU) 2015/2366; ErwGr 15 Verordnung (EU) 2016/679 (DSGVO).

¹⁷⁸ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 1-23; Verordnung (EU) 2023/1114, ErwGr 7, 10.

4.1.1 MiCA als unionsrechtlicher Ordnungsrahmen mit unmittelbarer Relevanz für Österreich

Mit der Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCA) wird erstmals ein **unmittelbar anwendbares** unionsrechtliches Regelwerk geschaffen, das Emittenten und Dienstleister im Bereich von Krypto-Assets umfassend adressiert.¹⁷⁹ MiCA definiert Kategorien von Kryptowerte (u. a. Asset-referenced Tokens, E-Geld-Token, sonstige Kryptowerte), normiert Zulassungs- und Organisationspflichten für Kryptowerte-Dienstleister (CASPs) und enthält Transparenz-, Verhaltens- und Marktmissbrauchsregeln.¹⁸⁰

Für Österreich hat dies zwei zentrale Konsequenzen:

Vorrang und unmittelbare Geltung: MiCA gilt als Verordnung ohne Umsetzungsakt direkt im innerstaatlichen Recht; nationale Normen dürfen weder hinter das unionsrechtlich geforderte Schutzniveau zurückfallen noch in Widerspruch zu MiCA treten.¹⁸¹

Transformationsdruck auf bestehende Strukturen: österreichische Spezialregelungen zu „virtuellen Währungen“ – etwa im FM-GwG – müssen an die unionsrechtlichen Begriffe und Kategorien angepasst werden. Die FMA hat bereits hervorgehoben, dass nach § 32a FM-GwG registrierte „Dienstleister in Bezug auf virtuelle Währungen“ schrittweise in das MiCA-Regime überführt und künftig, als Kryptowerte-Dienstleister beaufsichtigt werden.¹⁸²

Damit verschiebt sich der Fokus von einer bislang primär geldwäscherechtlich motivierten Erfassung hin zu einem integrierten Finanzmarktaufsichtsregime, in dem Verbraucherschutz, Marktintegrität und Finanzstabilität gemeinsam adressiert werden.

4.1.2 Zusammenspiel mit AMLD5/FM-GwG, PSD2/ZaDiG 2018 und DSGVO

Die MiCA-Verordnung steht nicht isoliert, sondern ergänzt bestehende unionsrechtliche Regelungsinstrumente, die in Österreich bereits umgesetzt wurden. Von besonderer Bedeutung ist dabei die Fünfte Geldwäscherichtlinie (AMLD5), welche virtuelle Währungen sowie Dienstleister im Zusammenhang mit virtuellen Währungen als Verpflichtete im Bereich des Geldwäscherechts erfasst. Österreich hat diese Vorgaben durch das Finanzmarkt-Geldwäschegesetz (FM-GwG) umgesetzt und bereits vor Inkrafttreten der MiCA-Verordnung eine Registrierungspflicht für Wallet-Provider und Umtauschplattformen eingeführt. Für Verbraucher:innen führt dies zu einem Mindestmaß an Identifizierungs-, Sorgfalts- und

¹⁷⁹ Vgl. Art. 1 Abs. 1, Art. 2 Abs. 1, Art. 3 Abs. 1 Z 6 und 15 sowie ErwGr 1 und 7 Verordnung (EU) 2023/1114 (MiCA), vgl. Art 288 AEUV.

¹⁸⁰ Vgl. Art. 2 Abs. 4, Art. 3 Abs. 1, Art. 4–5, Art. 48–49, Art. 53–59, Art. 60–67, Art. 66–72 sowie Art. 86–92 Verordnung (EU) 2023/1114 (MiCA).

¹⁸¹ Vgl. Art 288 Abs 2 AEUV; Vgl. Art. 1 Abs. 1 sowie ErwGr 1 und 7 Verordnung (EU) 2023/1114 (MiCA).

¹⁸² Vgl. Art. 1 Abs. 1, Art. 3 Abs. 1, Art. 53–54 sowie Art. 143–145 Verordnung (EU) 2023/1114 (MiCA); vgl. § 2 Z 21, § 32a FM-GwG.

Kontrollpflichten, insbesondere im Bereich der Kundenidentifikation und Geldwäscheprävention. Gleichzeitig begründen diese Regelungen jedoch keinen unmittelbaren materiellen Schutz bei Vermögensverlusten, technischen Fehlfunktionen oder sonstigen Risiken der Kryptodienstleistungen, sodass verbraucherrechtliche Schutzlücken weiterhin bestehen können.¹⁸³

Die Zahlungsdiensterichtlinie (PSD2) regelt klassische Zahlungsdienste und wurde in Österreich durch das Zahlungsdiensteegesetz 2018 (ZaDiG 2018) umgesetzt. PSD2 bringt u. a. starke Kundenauthentifizierung, Haftungsregeln bei nicht autorisierten Zahlungsvorgängen und Transparenzanforderungen für Entgelte.¹⁸⁴ Diese Schutzmechanismen greifen jedoch nur, wenn ein Dienst tatsächlich als Zahlungsdienst im Sinne von PSD2/ZaDiG 2018 qualifiziert werden kann; reine Kryptotransaktionen fallen nach derzeitiger Judikatur des OGH nicht darunter.¹⁸⁵

Die Datenschutz-Grundverordnung (DSGVO) findet Anwendung auf personenbezogene Daten, die bei der Nutzung von Kryptodiensten verarbeitet werden (z. B. Identitätsdaten, Transaktionshistorien, KYC-Daten). Sie adressiert Informationspflichten, Rechte der Betroffenen und Sicherheitsanforderungen, ist jedoch nicht auf die speziellen Vermögens- und Haftungsrisiken von Kryptowerte zugeschnitten.¹⁸⁶

In Summe entsteht ein Regelungsverbund, in dem MiCA die bisher sektorale Regulierung ergänzt: FM-GwG bleibt für Geldwäscheprävention zuständig, PSD2/ZaDiG 2018 für klassische Zahlungsdienste, DSGVO für den Datenschutz. Für Verbraucher:innen ist die Systematik jedoch schwer durchschaubar, da der Anwendungsbereich der einzelnen Instrumente von der rechtlichen Einordnung des jeweiligen Geschäftsmodells abhängt.

4.1.3 Nationale Umsetzungsschritte und Rolle der FMA

Auch wenn die MiCA-Verordnung als Verordnung unmittelbar gilt, erfordert sie dennoch innerstaatliche Begleitgesetzgebung. Insbesondere müssen die Zuständigkeiten der Finanzmarktaufsicht (FMA) klar zugewiesen werden. Darüber hinaus sind die Aufsichtsbefugnisse, insbesondere Auskunfts- und Prüfungsrechte sowie Eingriffsbefugnisse,

¹⁸³ Vgl. Richtlinie (EU) 2018/843, Art 1 Z 2 lit d, Art 2 Abs 1 Z 3 lit g; vgl. § 2 Z 21, Z 22 sowie § 32a FM-GwG; vgl. §§ 5–10 FM-GwG; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 5–9.

¹⁸⁴ Vgl. Richtlinie (EU) 2015/2366, Art 1 Abs 1, Art 4 Z 3, 5, 6, Art 44, 45, 52, Art 73, 74, Art 97; vgl. §§ 1, 2, 32–36, 68–71 ZaDiG 2018.

¹⁸⁵ Vgl. Richtlinie (EU) 2015/2366, Art 1 Abs 1, Art 4 Z 3, Anhang I; vgl. §§ 1, 2 ZaDiG 2018; OGH 4.11.2020, 4 Ob 95/20x; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 215–218.

¹⁸⁶ Vgl. Art. 2 Abs. 1, 4 Z 1, 12–14, 15–22 und 32 sowie ErwGr 15 Verordnung (EU) 2016/679 (DSGVO); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 6–10.

an das neue Regime anzupassen. Zusätzlich müssen Sanktionsrahmen für Verstöße gegen die MiCA-Pflichten festgelegt werden.¹⁸⁷

Die bereits bestehende Registrierungspflicht nach § 32a FM-GwG und die Aufsichtserfahrung der FMA über Dienstleister in Bezug auf virtuelle Währungen bilden den institutionellen Ausgangspunkt. Österreich hat bislang auf ein eigenständiges Kryptogesetz verzichtet und kryptobezogene Tätigkeiten über bestehende finanzmarkt- und geldwäscherechtliche Regelwerke erfasst.¹⁸⁸

Mit dem Inkrafttreten von MiCA wandelt sich dieses Modell zu einem hybriden System: MiCA bildet den primären Ordnungsrahmen für Emittenten und Dienstleister; nationale Normen wie FM-GwG, ZaDiG 2018, WAG 2018, KMG und ABGB fungieren als Flankierung und Ausfüllungslast, insbesondere im Bereich Haftung, Vertrag, Insolvenz und Steuerrecht.

4.1.4 Spannungsverhältnis zwischen unionsrechtlicher Harmonisierung und nationale Rechtsordnungssystematik

Die Einbettung des österreichischen Rechtsrahmens in das unionsrechtliche Gefüge ist nicht spannungsfrei. Einerseits verlangt MiCA eine weitgehende Harmonisierung zentraler Begriffe, Kategorien und Aufsichtspflichten; andererseits beruht das österreichische Zivilrecht weiterhin auf dem traditionellen Sachen- und Schuldrecht des ABGB, das digitale Vermögensobjekte ursprünglich nicht im Blick hatte.¹⁸⁹

Bei der zivilrechtlichen Qualifikation von Kryptowerten zeigt sich dieses Spannungsverhältnis besonders deutlich: Die MiCA-Verordnung arbeitet mit unionsrechtlichen Funktionskategorien, während österreichische Autor:innen weiterhin eine rechtlich und systematisch konsistente Einordnung von Kryptowerten als Vermögensobjekte sui generis anstreben.¹⁹⁰

Bei der Abgrenzung von Zahlungsdiensten und Kryptodienstleistungen zeigt sich das Spannungsverhältnis ebenfalls deutlich: Auf unionsrechtlicher Ebene bestehen PSD2 und MiCA nebeneinander, wobei die nationale Anwendung sicherstellen muss, dass weder Überregulierung noch Unterregulierung entsteht und Verbraucher:innen nicht in Regelungslücken geraten.¹⁹¹

¹⁸⁷ Vgl. Art 149–153, Verordnung (EU) 2023/1114 (MiCA).

¹⁸⁸ Vgl. §§ 2 Z 21, 2 Z 22, 32a FM-GwG; Richtlinie (EU) 2018/843 (AMLD5).

¹⁸⁹ Vgl. Art 1 Abs 1, Art 3, ErwGr 1 und 7 Verordnung (EU) 2023/1114 (MiCA); vgl. ABGB §§ 285 ff, §§ 859 ff; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 3–6, 15–20, 23–27.

¹⁹⁰ Vgl. Art 3, Art 4–5, Art 48–49, Art 53 ff Verordnung (EU) 2023/1114 (MiCA); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 3–6, 15–18, 22–27, 30–35.

¹⁹¹ Vgl. Art 1 Abs 1, Art 4 Z 3, Anhang I Richtlinie (EU) 2015/2366; vgl. Art 1 Abs 1 und 2, ErwGr 1, 7, 9–11. Verordnung (EU) 2023/1114 (MiCA).

Bei der Aufteilung der Aufsichts Kompetenzen zeigt sich dieses Spannungsverhältnis ebenfalls: Die Finanzmarktaufsicht (FMA) ist in ein europäisches Aufsichtsnetzwerk, insbesondere unter Einbindung von ESMA und EBA, eingebettet, bleibt jedoch weiterhin für den konkreten nationalen Vollzug und die praktische Aufsichtstätigkeit verantwortlich.¹⁹²

Für den Verbraucherschutz bedeutet dies, dass die Effektivität der unionsrechtlichen Instrumente in hohem Maß davon abhängt, wie konsequent und kohärent der österreichische Gesetzgeber die systematische Verknüpfung herstellt und wie die FMA ihre Aufsichtspraxis ausrichtet.

4.2 Zivilrechtliche Qualifikation von Kryptowerten im österreichischen Recht

Die Frage, wie Kryptowerte zivilrechtlich einzuordnen sind, besitzt für den Verbraucherschutz zentrale Bedeutung. Von der rechtlichen Qualifikation hängen wesentliche Rechtsfolgen ab. Dies betrifft insbesondere die Frage, ob und in welcher Form Eigentum an Token besteht und wie dieses geschützt wird, wie eine wirksame Übertragung oder Bestellung von Sicherheiten erfolgen kann sowie wie Kryptowerte im Erb- und Insolvenzrecht behandelt werden. Davon hängt letztlich auch ab, ob Verbraucher:innen ihre Rechtsposition im Streitfall eindeutig bestimmen, beziffern und wirksam durchsetzen können.¹⁹³

4.2.1 Sachbegriff des ABGB und Problem der Körperlichkeit

Ausgangspunkt ist der Sachbegriff des § 285 ABGB, wonach Sachen „alles, was von der Person unterschieden ist und zum Gebrauche der Menschen dient“, sind. Das ABGB baut dabei traditionell auf dem Leitbild der körperlichen Sache auf; § 292 ABGB stellt ausdrücklich auf die Körperlichkeit ab. Klassische Beispiele sind körperliche Gegenstände wie Geldscheine, Wertpapierurkunden oder bewegliche Sachen.

Kryptowerte – etwa Bitcoin, Ether oder andere Token – sind hingegen rein digitale Einheiten, die als Datensätze in einem verteilten Register (Blockchain) existieren. Sie werden durch kryptografische Verfahren gesichert und sind technisch nur über private Schlüssel disponibel. Eine physische Verkörperung fehlt, soweit nicht ausnahmsweise ein Token mit einer Urkunde verbunden ist (z. B. verbriefte Security Tokens).¹⁹⁴

¹⁹² Vgl. Art. 84–86, 149 Abs. 1, 150 Abs. 1 und 2 sowie 151 Verordnung (EU) 2023/1114 (MiCA).

¹⁹³ Vgl. §§ 285 ff., 353 ff., 426 ff., 447 ff. und 531 ff. ABGB sowie §§ 1 und 3 IO; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 1–6, 15–20, 22–27, 30–35, 36–42, 45–50, 60–65, 66–72 und 73–78.

¹⁹⁴ Vgl. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008); vgl. § 285 ABGB; vgl. Art. 2 Abs. 2 lit. a Verordnung (EU) 2023/1114 (MiCA); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 2–4, 6–15, 22–27, 30–35 und 40–50.

Die österreichische Literatur hat daraus zunächst geschlossen, dass Kryptowerte nicht ohne Weiteres als körperliche Sachen qualifiziert werden können.¹⁹⁵ Stattdessen rückt zunehmend die Frage in den Vordergrund, ob der Sachbegriff des ABGB technologieneutral verstanden und auf rein digitale, aber exklusiv beherrschbare Vermögenspositionen ausgedehnt werden kann und dass Kryptowerte zwar keine körperliche Substanz haben, aber wesentliche sachrechtliche Merkmale aufweisen. Exklusivität, Beherrschbarkeit durch den Inhaber des privaten Schlüssels und Eignung als Gegenstand von Verkehrsgeschäften.¹⁹⁶ In der Literatur wird teilweise diskutiert, ob Werteinheiten bei funktionsorientierter Betrachtung sachrechtlichen Kategorien angenähert werden könnten. Die herrschende Lehre lehnt jedoch eine Qualifikation als Sache iSd § 285 ABGB ab und plädiert vielmehr für eine eigenständige vermögensrechtliche Einordnung.¹⁹⁷

4.2.2 Modelle der zivilrechtlichen Einordnung in der österreichischen Literatur

In der österreichischen Diskussion haben sich mehrere Einordnungsmodelle herausgebildet, die sich teilweise überschneiden. Dazu zählt insbesondere der Ansatz der registerbasierten Vermögensobjekte bzw. Werteinheiten. Danach werden Kryptowerte als digital erzeugte und in einem Register geführte Vermögensobjekte verstanden. Sie sind von der Person zu unterscheiden, erfüllen wirtschaftliche Funktionen – insbesondere im Bereich Zahlung, Anlage und Zugang zu Protokollen – und weisen aufgrund ihrer blockchainbasierten Struktur eine exklusive Beherrschbarkeit auf.¹⁹⁸ Eigentum und Besitz würden danach nicht an eine körperliche Urkunde anknüpfen, sondern an die faktische Kontrolle über den privaten Schlüssel sowie an den Eintrag im jeweiligen Register.¹⁹⁹

In der Literatur wird teilweise erwogen, Kryptowerte trotz fehlender Körperlichkeit als sachrechtsnahe Vermögensobjekte zu behandeln und einzelne sachrechtliche Instrumente analog anzuwenden; die herrschende Lehre lehnt jedoch eine Gleichstellung mit Sachen iSd § 285 ABGB ab.²⁰⁰

Ein weiterer Ansatz ordnet Kryptowerte als sonstige Vermögenswerte-Rechte bzw. Rechte sui generis ein. Dabei wird stärker auf den Rechtscharakter der zugrunde liegenden Position abgestellt. Nach dieser Auffassung werden Kryptowerte nicht primär als Vermögensobjekte verstanden, sondern als eigenständige Vermögenswerte Rechtspositionen, die aufgrund ihrer

¹⁹⁵ Vgl. § 285 ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 22–27 und 30–32.

¹⁹⁶ Vgl. § 285 ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 9–15, 22–42.

¹⁹⁷ Vgl. § 285 ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 22–40.

¹⁹⁸ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 1–6 und 15–40.

¹⁹⁹ Vgl. §§ 285 und 309 ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 9–15 und 22–36.

²⁰⁰ Vgl. § 285 ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 28–40.

besonderen Eigenschaften keiner klassischen Kategorie vollständig zugeordnet werden können.²⁰¹

Im Vordergrund steht die Überlegung, dass die Rechtsordnung hier eine neue Kategorie anerkennen muss, die weder vollständig im Sachenrecht noch im Forderungsrecht aufgeht.²⁰²

Kryptowerte erscheinen dann als rechtlich geschützte Machtposition, die auf der Kombination aus technischer Kontrolle (privater Schlüssel) und sozialer Akzeptanz (Markt) beruht.²⁰³

in weiterer Einordnungsansatz sind forderungsbasierte Modelle. Diese werden insbesondere für bestimmte Tokenarten vertreten, etwa bei zentral ausgegebenen Stablecoins oder Plattform-Token mit Rückzahlungsansprüchen. Nach diesem Ansatz wird der Token nicht als eigenständiges Vermögensobjekt betrachtet, sondern als schuldrechtliche Position, wobei der Token eine Forderung gegenüber einem Emittenten verkörpert. Dadurch steht nicht der Token selbst, sondern das zugrunde liegende Forderungsverhältnis im Mittelpunkt der rechtlichen Einordnung.²⁰⁴ Dieses Modell passt gut zu Asset-Backed- oder E-Geld-Token, weniger hingegen zu dezentral generierten Kryptos wie Bitcoin, bei denen es keinen identifizierbaren Schuldner gibt.²⁰⁵

Ein weiterer Ansatz betrifft die Analogie zu Wertpapieren und Wertrechten. In der Literatur wird unter Bezugnahme auf ausländische Regelungsmodelle – insbesondere das deutsche Gesetz über elektronische Wertpapiere (eWpG) – diskutiert, ob und inwieweit Kryptowerte funktional in eine registerbasierte Wertpapierordnung eingeordnet werden können. Ausgangspunkt dieser Überlegung ist, dass der Registereintrag die Funktionen übernehmen könnte, die bei klassischen Wertpapieren durch die körperliche Urkunde erfüllt werden. Insbesondere wird angenommen, dass der Registereintrag die Beweis- und Legitimationsfunktion der traditionellen Urkunde ersetzen kann. Dadurch wird eine funktionale Annäherung zwischen Kryptowerten und elektronisch geführten Wertrechten diskutiert.²⁰⁶ Gemeinsam ist diesen Ansätzen, dass sie Kryptowerte als wirtschaftlich relevante und exklusiv zuordenbare Vermögenspositionen anerkennen, die Gegenstand von Übertragung, Belastung und Zwangsvollstreckung sein können. Unterschiede bestehen jedoch hinsichtlich ihrer rechtlichen Einordnung und

²⁰¹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 15–18, 22–27 und 37–45.

²⁰² Vgl. § 285 ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 15–18, 22–27 und 37–45.

²⁰³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 9–15, 28–30, 37–45 und 73–78; vgl. Lawson, The Social Positioning of Nature (2016), S. 98–105 und 112–118; vgl. Stanford Encyclopedia of Philosophy, Philosophy of Money and Finance, Abschnitt „Money as a social institution“.

²⁰⁴ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 15–18 und 46–55; vgl. Art. 3 Abs. 1 Z 6 und 7, Art. 36, Art. 37 sowie Art. 43 Verordnung (EU) 2023/1114 (MiCA).

²⁰⁵ Vgl. Art. 3 Abs. 1 Z 6 und 7, Art. 36, 37 und 43 Verordnung (EU) 2023/1114 (MiCA); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 9–12, 15–18, 22–27 und 46–55; vgl. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

²⁰⁶ Vgl. §§ 2, 4 und 6 eWpG (DE); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 52–64.

Systemzuordnung. Gerade diese Uneinheitlichkeit wirkt sich unmittelbar auf die Rechtsposition von Konsument:innen aus, da von der jeweiligen Einordnung wesentliche Fragen des Vermögensschutzes, der Durchsetzbarkeit von Ansprüchen sowie der Behandlung im Insolvenz- und Vollstreckungsrecht abhängen können.²⁰⁷

4.2.3 Praktische Folgefragen: Eigentum, Übertragung, Sicherheiten, Erbrecht und Insolvenz

Die rechtliche Unsicherheit bleibt nicht auf theoretische Fragestellungen beschränkt, sondern prägt zentrale Lebens- und Anwendungsbereiche von Konsument:innen im Umgang mit Kryptowerten. Sie wirkt sich insbesondere auf die praktische Handhabung, den Vermögensschutz sowie die Durchsetzung von Rechten im Zusammenhang mit Kryptowerte aus.²⁰⁸

a) Eigentum, Besitz und Schutz bei Eingriffen

Wenn Kryptowerte als Sachen iSd § 285 ABGB verstanden werden, stellt sich die Frage, wie Eigentum und Besitz daran konkret aussehen: Nach dem sachrechtlichen Ansatz knüpft Eigentum an die Zuordnung im Register und die faktische Kontrolle über den privaten Schlüssel an. Wer den Schlüssel exklusiv kontrolliert, soll – vergleichbar einem Inhaberpapier – als Eigentümer gelten.²⁰⁹ Besitzschutzinstrumente (§§ 339 ff ABGB) lassen sich nur eingeschränkt übertragen, weil kein körperlicher Besitz vorliegt. Die Literatur argumentiert daher mit einer funktionalen Beherrschbarkeit, die der klassischen Gewahrsame nahekommt.

Für Verbraucher:innen ist vor allem relevant, wie die Rechtsordnung auf unbefugte Zugriffe reagiert (Diebstahl von Schlüsseln, Hacking, unautorisierte Dispositionen durch Dienstleister). Ohne klare Eigentumskonzept bleibt oft unklar, ob ein dinglicher Herausgabeanspruch besteht oder lediglich schuldrechtliche Ansprüche (z. B. gegen die Plattform) geltend gemacht werden können.²¹⁰

b) Übertragung und dingliche Sicherheiten

Die technische Übertragung von Kryptos erfolgt durch Signatur und Eintrag in der Blockchain. Rechtlich stellt sich die Frage, ob diese Transaktion einer Übereignung (mit Modus), oder einer Abtretung (Zession) oder einem eigenständigen Verfügungstypus über digitale Registerwerte entspricht.²¹¹

²⁰⁷ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 3–6, 9–30, 36–50, 66–78.

²⁰⁸ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 1–6, 22–27, 36–50, 60–65, 635, 651–657.

²⁰⁹ Vgl. § 285 ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 28–40 und 61–64.

²¹⁰ Vgl. § 366 sowie §§ 1293 ff. und 859 ff. ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 22–27, 37–82.

²¹¹ Vgl. §§ 380 ff., 426 ff. und 1392 ff. ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 6–9, 15–18, 28–45, 46–50 und 61–64; vgl. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

In der Literatur wird teilweise eine analoge Anwendung sachenrechtlicher Regelungen auf werteinheitenbasierte Kryptowerte vertreten. Danach wird angenommen, dass die On-Chain-Transaktion funktional die Rolle des Modus bei der Übertragung übernehmen kann. Darüber hinaus wird diskutiert, ob Pfandrechte durch eine besondere Kennzeichnung oder einen Pfandvermerk im Register begründet werden können. Ebenso werden Sicherungsabtretungen und Eigentumsvorbehalte grundsätzlich als möglich angesehen, sofern die Anforderungen an Publizität und Bestimmtheit gewahrt bleiben.²¹²

Für Konsument:innen ist dies vor allem bei Krediten relevant, die durch Kryptos besichert werden, und bei der Frage, ob im Insolvenzfall von Plattformen ein abgesondertes Sicherungsrecht besteht oder den Token in die Masse fallen. Ohne ausdrückliche gesetzliche Regelung bleibt hier ein erhebliches Rechtsrisiko.

c) Erbrechtliche Zuordnung

Stirbt der Inhaber eines Wallets, stellt sich die Frage, ob und wie Kryptowerte in die Verlassenschaft fallen. Unabhängig von der rechtlichen Einordnung kann die faktische Durchsetzbarkeit erheblich beeinträchtigt sein, wenn Zugangsdaten fehlen oder nicht auffindbar sind: Nach herrschender Auffassung gehören Kryptowerte als Vermögensobjekte grundsätzlich zum Nachlass. Praktisch scheitert die Durchsetzung aber häufig daran, dass Zugangsdaten fehlen oder vernichtet wurden. Dann besteht zwar ein erbrechtlicher Anspruch, der Vermögenswert ist aber faktisch verloren. Mangels spezifischer gesetzlicher Vorgaben stellt sich die Frage, ob im Umgang mit Kryptowerten besondere Dokumentations- oder Vorsorgemaßnahmen – etwa testamentarische Anordnungen – sinnvoll sind. Für Erben kann daraus die Situation entstehen, dass sie zwar rechtlich berechtigt, faktisch jedoch mangels Zugangsdaten nicht verfügungsbefugt sind. dieses Spannungsverhältnis ist insbesondere für Kleinanleger:innen schwer nachvollziehbar.

d) Insolvenzrechtliche Einordnung

Besonders gravierend sind die Folgen im Insolvenzfall von Dienstleistern (Börsen, Verwahrer, Lending-Plattformen): Ist die Verwahrung als Fremdverwahrung ausgestaltet und werden Kryptowerte eindeutig einem Kunden zugeordnet, spricht vieles dafür, sie als Sondervermögen zu behandeln; dann fallen sie nicht in die Masse. Fehlt eine klare Trennung oder werden Kryptos in Sammelwallets ohne hinreichende Dokumentation gehalten, besteht das Risiko, dass sie als Teil des Vermögens der Schuldnerin behandelt werden und Konsument:innen nur Quotenansprüche als Insolvenzgläubiger zustehen.²¹³

²¹² Vgl. §§ 380 ff. und 426 ff. ABGB; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 28–55 und 61–64.

²¹³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 651–653 und 657.

Gerade die Erfahrungen mit prominenten Börseninsolvenzen (auch außerhalb Österreichs) zeigen, wie schwierig es für Kund:innen ist, ihre Stellung einzuordnen: Weder das ABGB noch die österreichische Insolvenzordnung enthalten bisher spezifische Regeln zur Behandlung von Kryptovermögen. Die rechtliche Unklarheit schlägt damit direkt in ein praktisches Vollzugsrisiko für Verbraucher:innen um.

4.3 Aufsichtsrechtliche Einordnung und Regulierung von Kryptodienstleistungen in Österreich

Die aufsichtsrechtliche Behandlung von Kryptodienstleistungen in Österreich ist durch ein Zusammenspiel verschiedener unions- und nationalrechtlicher Regelungsebenen sowie der Aufsichtspraxis der Finanzmarktaufsicht geprägt.

Auch wenn die MiCA-Verordnung künftig einen einheitlichen europäischen Ordnungsrahmen bereitstellt, basiert das österreichische System bis zu ihrem vollständigen Wirksamwerden weiterhin auf einer funktionalen Betrachtungsweise. Kryptodienstleistungen werden jeweils danach eingeordnet, ob der konkrete Dienst einer bereits regulierten Tätigkeit des Finanzmarktrechts entspricht. Diese Einordnung hat unmittelbare Konsequenzen für Konsument:innen, weil davon abhängt, ob Schutzmechanismen wie Risikohinweise, Organisationspflichten, Vermögenstrennung, Prüfpflichten und Haftungsregime greifen.²¹⁴ Im Folgenden wird dieser komplexe Rechtsrahmen systematisch dargestellt, einschließlich nationaler Besonderheiten und jener Stellen, an denen das österreichische Aufsichtsrecht strukturelle Lücken aufweist, die trotz geldwäscherechtlicher Registrierung bestehen bleiben.

4.3.1 Aufsichtsrechtliche Grundstruktur: Tätigkeitstypen und Abgrenzungsfragen

Österreich verfolgt im Gegensatz zu Deutschland kein eigenes „Kryptogesetz“, sondern ordnet Tätigkeiten funktionsbezogen zu. Das bedeutet, Es wird nicht die Technologie reguliert, sondern ausschließlich des wirtschaftlichen Verhaltens des Dienstleisters.²¹⁵

Die zentrale Frage lautet daher: Ist die konkrete Dienstleistung einem bestehenden Tatbestand im BWG, WAG 2018, ZaDiG 2018 oder FM-GwG zuzuordnen?

Dies führt zu vier Grundkategorien:

(1) Kryptoverwahrung und Wallet-Management: Die Verwahrung fremder Kryptowerte wird in Österreich bislang nicht als Bankgeschäft qualifiziert. Dies unterscheidet sich von der deutschen Rechtslage, die mit dem „Kryptoverwahrgeschäft“ nach § 1 Abs. 1a Nr. 6 KWG einen

²¹⁴ Vgl. Art. 1 Abs. 1, Art. 2 Abs. 4, Art. 3 Abs. 1, Art. 59 ff. sowie ErwGr 5, 8, 9 und 22 Verordnung (EU) 2023/1114 (MiCA); vgl. FMA, Informationen zu MiCA und Kryptowerte-Dienstleistern.

²¹⁵ Vgl. Art. 2 Abs. 4 und Art. 3 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); vgl. FM-GwG; vgl. ZaDiG 2018; vgl. WAG 2018; vgl. FMA, Informationen zu MiCA und Kryptowerte-Dienstleistern.

eigenen aufsichtsrechtlichen Tatbestand vorsieht. Daraus folgt, dass in Österreich grundsätzlich keine Konzessionspflicht nach dem Bankwesengesetz (BWG) besteht, sondern lediglich eine geldwäscherechtliche Registrierungspflicht gemäß § 32a FM-GwG vorgesehen ist.²¹⁶

(2) Kryptohandel (Brokerage, OTC, Plattformgeschäft): Kryptohandel (Brokerage, OTC, Plattformgeschäft): Handelsplattformen, die Kryptowerte gegen Fiatwährungen oder andere Kryptowerte tauschen, unterliegen grundsätzlich keiner Zulassungspflicht nach dem WAG 2018, solange kein Finanzinstrument im Sinne des § 1 Z 7 WAG 2018 vorliegt. Eine aufsichtsrechtliche Konzessionspflicht entsteht daher regelmäßig erst bei sogenannten Security Token, sofern diese als übertragbare Wertpapiere qualifiziert werden können.²¹⁷

(3) Tauschdienste (Fiat ↔ Crypto): Dienstleistungen im Zusammenhang mit dem Tausch von Fiatwährungen gegen Kryptowerte werden von § 32a FM-GwG erfasst, unterliegen jedoch grundsätzlich nicht dem Zahlungsdiensterecht des ZaDiG 2018, da Kryptowerte nicht als „Geldbeträge“ im Sinne der entsprechenden Regelungen qualifiziert werden. Daraus folgt insbesondere, dass die Haftungsregelungen der PSD2 beziehungsweise des ZaDiG 2018 bei Fehlüberweisungen regelmäßig keine Anwendung finden.²¹⁸

(4) Staking, Lending, Custodial Services: Diese Tätigkeiten sind in Österreich bislang nicht ausdrücklich reguliert, sofern sie nicht als Veranlagungsgeschäft, Kreditgeschäft oder Wertpapierdienstleistung qualifiziert werden. Dadurch besteht bis zum vollständigen Wirksamwerden der MiCA-CASP-Regelungen eine strukturelle Regulierungslücke. Die funktionale Zuordnung der einzelnen Geschäftsmodelle führt insgesamt zu einem „Patchwork-Regime“ (zersplittertes Regelungssystem), das für Verbraucher:innen häufig nur schwer nachvollziehbar ist und abhängig von der jeweiligen Ausgestaltung des Dienstes sehr unterschiedliche Schutzniveaus gewährleistet.²¹⁹

4.3.2 Geldwäscherechtliche Registrierung nach § 32a FM-GwG

Seit dem Jahr 2020 unterliegen Anbieter:innen von Dienstleistungen im Zusammenhang mit virtuellen Währungen einer Registrierungspflicht gemäß § 32a FM-GwG. Erfasst werden insbesondere Wallet-Provider, Tauschdienste, Betreiber:innen von Krypto-Handelsplattformen,

²¹⁶ Vgl. § 1 Abs. 1a Nr. 6 KWG (DE); vgl. § 1 BWG; vgl. § 32a FM-GwG; vgl. Art. 3 Abs. 1 Z 17 und Art. 59 ff. Verordnung (EU) 2023/1114 (MiCA); vgl. FMA, Informationen zu MiCA und Kryptowerte-Dienstleistern.

²¹⁷ Vgl. § 1 Z 7 WAG 2018; vgl. Art. 2 Abs. 4, Art. 3 Abs. 1 Z 5 und 6 sowie ErwGr 9, 22 und 24 Verordnung (EU) 2023/1114 (MiCA).

²¹⁸ Vgl. § 32a FM-GwG; vgl. § 3 Abs. 2 ZaDiG 2018; vgl. Art. 2 Abs. 2 lit. c Richtlinie (EU) 2015/2366 (PSD2); vgl. Art. 2 Abs. 4 sowie ErwGr 8 und 9 Verordnung (EU) 2023/1114 (MiCA).

²¹⁹ Vgl. § 1 BWG; vgl. § 1 Z 7 WAG 2018; vgl. KMG 2019; vgl. Art. 3 Abs. 1 Z 16–18, Art. 59 ff. sowie ErwGr 8, 9 und 22 Verordnung (EU) 2023/1114 (MiCA).

Anbieter:innen von Übertragungsdiensten sowie Custody- beziehungsweise Verwahrdienstleister:innen. Die Registrierung dient vor allem der Einbindung dieser Dienstleister in die geldwäscherechtlichen Kontroll- und Sorgfaltspflichten.²²⁰

Wichtig für Verbraucher:innen ist jedoch, was **nicht** durch die Registrierung gewährleistet wird:

Keine aufsichtsrechtlichen Kapitalanforderungen,

keine Vorgaben zur Risikotrennung,

keine IT-Sicherheitsstandards,

keine Governance- oder Compliance-Pflichten,

keine Kostenregulierung,

keine Haftungsregeln,

keine laufende prudenzielle Aufsicht durch die FMA.²²¹

Die Registrierung dient ausschließlich der Geldwäscheprävention, nicht dem Verbraucherschutz.

Für viele Konsument:innen entsteht damit ein falscher Eindruck von Sicherheit, denn die Registrierung erweckt den Anschein einer behördlichen „Zulassung“, obwohl sie lediglich eine formelle Erfassung ohne materielle Überprüfung des Geschäftsmodells darstellt.²²²

4.3.3 Anwendbarkeit aufsichtsrechtlicher Spezialgesetze (BWG, WAG, ZaDiG)

Die Aufsichtsrelevanz hängt davon ab, ob Kryptowerte Finanzinstrumente, Einlagen, E-Geld, Zahlungsinstrumente oder Veranlagungen darstellen.²²³

(1) Bankwesengesetz (BWG): Bitcoin, Ethereum und vergleichbare Kryptowerte gelten grundsätzlich weder als Einlagen noch als E-Geld, da ihnen insbesondere ein Rechtsanspruch auf Auszahlung gegenüber einem Emittenten fehlt. Daraus folgt, dass zentrale Schutzmechanismen des Bankwesengesetzes regelmäßig keine Anwendung finden. Dies betrifft insbesondere die Einlagensicherung, den Kundengeldschutz sowie die Organisations- und Sorgfaltspflichten nach § 39 BWG.²²⁴

(2) Wertpapieraufsichtsgesetz 2018 (WAG 2018): Nur sogenannte Security Token können als übertragbare Wertpapiere im Sinne des Art. 4 Abs. 1 Nr. 44 MiFID II beziehungsweise § 1 Z 7 WAG 2018 qualifiziert werden. Reine Utility- oder Payment-Token unterliegen demgegenüber

²²⁰ Vgl. § 32a sowie § 2 Z 21 lit. b FM-GwG.

²²¹ Vgl. § 32a FM-GwG; vgl. § 1 BWG; vgl. § 1 Z 7 WAG 2018.

²²² Ebd.

²²³ Vgl. § 1 BWG; vgl. § 1 Z 7 WAG 2018; vgl. § 1 ZaDiG 2018; vgl. § 1 KMG 2019.

²²⁴ Vgl. § 1, § 39 BWG sowie § 1 ZaDiG 2018.

grundsätzlich keiner wertpapieraufsichtsrechtlichen Regulierung und lösen daher regelmäßig keine Aufsichtspflichten nach dem WAG 2018 aus.²²⁵

(3) ZaDiG 2018 (PSD2-Umsetzung): Bitcoin gilt nicht als „Geldbetrag“ im Sinne des ZaDiG 2018. Der OGH entschied daher, dass Krypto-Zahlungen keine Zahlungsvorgänge im Sinne des ZaDiG 2018 darstellen. Daraus folgt, dass zentrale Schutzmechanismen des Zahlungsdiensterechts regelmäßig keine Anwendung finden. Dies betrifft insbesondere Rückerstattungspflichten, Fristenkontrollen, Sorgfaltspflichten von Dienstleistern sowie Haftungsregelungen bei Fehlüberweisungen.²²⁶ Für Verbraucher:innen stellt dies eine der größten Schutzlücken im Kryptobereich dar. Fehlübertragungen, Hacking-Vorfälle oder Fehlbedienungen führen – anders als im klassischen Giro- und Zahlungsverkehr – regelmäßig zu keinen vergleichbaren Ansprüchen gegenüber einem Dienstleister. Dadurch fehlen vielfach Rückerstattungs-, Haftungs- oder Korrekturmechanismen, wie sie im traditionellen Zahlungsdiensterecht vorgesehen sind.

4.3.4 Technologische Neutralität und Grenzen der Aufsichtspraxis (FMA)

Die FMA wendet eine technisch neutrale Auslegung an und beurteilt jedes Geschäftsmodell nach seiner wirtschaftlichen Funktion.²²⁷

Dabei zeigt sich jedoch, dass sich zahlreiche Kryptoprojekte einer eindeutigen rechtlichen Zuordnung entziehen. Häufig werden Dienstleistungen zudem bewusst so strukturiert, dass keine aufsichtsrechtliche Konzessionspflicht ausgelöst wird, was als „regulatory arbitrage“ bezeichnet wird. Zusätzlich bestehen im Bereich des Decentralized Finance (DeFi) erhebliche Aufsichtsprobleme, da aufgrund fehlender oder schwer identifizierbarer Rechtsträger vielfach keine klassische Beaufsichtigung möglich ist. Darüber hinaus prüft die FMA in vielen Fällen nicht die Bonität, Governance-Struktur, Reservedeckung oder Liquiditätslage der Anbieter:innen, wodurch aus Sicht des Verbraucherschutzes weiterhin erhebliche Risiken bestehen können.²²⁸ Die Aufsichtslücken werden durch die FMA selbst als Problem anerkannt, insbesondere im Hinblick auf fehlende Vermögenstrennung, Insolvenzrisiken, Intransparenz der Geschäftsmodelle und Interessenkonflikte.

²²⁵ Vgl. Art. 4 Abs. 1 Nr. 44 MiFID II; vgl. § 1 Z 7 WAG 2018.

²²⁶ Vgl. OGH 26.1.2021, 4 Ob 95/20x; vgl. § 3 ZaDiG 2018; vgl. Art. 2 Abs. 2 lit. c Richtlinie (EU) 2015/2366 (PSD2).

²²⁷ Vgl. § 1 BWG; vgl. § 1 Z 7 WAG 2018; vgl. § 1 ZaDiG 2018; vgl. § 32a FM-GwG.

²²⁸ Vgl. § 32a FM-GwG; vgl. Art. 59 ff. Verordnung (EU) 2023/1114 (MiCA).

4.4 Kapitalmarktrechtliche Einordnung und Anwendbarkeit des KMG und WAG 2018

Die kapitalmarktrechtliche Analyse ist für den Verbraucherschutz besonders relevant, weil sie bestimmt, ob ein Angebot von Kryptowerten den strengen Informations-, Transparenz- und Wohlverhaltenspflichten unterliegt, die für traditionelle Finanzprodukte gelten. In Österreich hängt dies maßgeblich davon ab, ob ein Kryptowert als Finanzinstrument im Sinne des WAG 2018 einzuordnen ist oder ob ein öffentliches Angebot nach dem Kapitalmarktgesetz (KMG) vorliegt. Die Einordnung entscheidet darüber, ob Anleger:innen durch prospektrechtliche Offenlegungspflichten, Beratungs- und Eignungsprüfungen, Best-Execution-Vorgaben sowie Compliance-Mechanismen geschützt sind.²²⁹

Da Kryptowerte jedoch sehr heterogen sind und technisch wie ökonomisch unterschiedlich funktionieren, stellt sich die Frage, welche Token-Typen überhaupt in den Anwendungsbereich des Kapitalmarktrechts fallen. Die Analyse zeigt, dass der überwiegende Teil der am Markt befindlichen Token, wird kapitalmarktrechtlich nicht erfasst, was erhebliche Schutzlücken erzeugt.²³⁰

4.4.1 Grundstruktur: Wann ist ein Kryptowert ein Finanzinstrument?

Das Wertpapieraufsichtsgesetz 2018 (WAG 2018) setzt die MiFID II in Österreich um und definiert in § 1 Z 7 WAG 2018 den Begriff der Finanzinstrumente. Maßgeblich ist dabei, ob ein Token funktional einem bestimmten Finanzinstrumententyp entspricht. Dazu zählen insbesondere übertragbare Wertpapiere, Geldmarktinstrumente, Anteile an Organismen für gemeinsame Anlagen sowie finanzielle Differenzgeschäfte oder derivative Finanzinstrumente. Ein bloßer Blockchain-Eintrag erfüllt diese Voraussetzungen jedoch grundsätzlich nicht. Aus diesem Grund fällt die überwiegende Mehrheit der Kryptowerte nicht in den Anwendungsbereich des WAG 2018.²³¹

Die österreichische Literatur sowie die Aufsichtspraxis unterscheiden regelmäßig zwischen drei zentralen Token-Kategorien.

(1) Payment Token: Dazu zählen insbesondere Kryptowährungen wie Bitcoin, Litecoin oder Monero. Diese Tokens dienen primär der Wertübertragung und Zahlungsfunktion, verbriefen jedoch grundsätzlich keine darüberhinausgehenden Rechte. Sie werden daher regelmäßig nicht als Finanzinstrumente qualifiziert.

²²⁹ Vgl. § 1 KMG 2019; vgl. § 1 Z 7 sowie §§ 47 ff. WAG 2018.

²³⁰ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 21 und 715; vgl. Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final, S. 13.

²³¹ Vgl. § 1 Z 7 WAG 2018; vgl. Art. 4 Abs. 1 Nr. 44 MiFID II; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 700–705 und 714–716.

(2) Utility Token: Diese Tokens gewähren typischerweise Zugang zu bestimmten Softwarefunktionen, Plattformdiensten oder Protokollrechten. Sie verkörpern vor allem Nutzungs- und Zugangsrechte, begründen jedoch grundsätzlich keine finanziellen Ansprüche gegenüber einem Emittenten. Auch sie gelten daher regelmäßig nicht als Finanzinstrumente.

(3) Security- beziehungsweise Investment-Token: Hierbei handelt es sich um Tokens, die etwa Dividenden-, Zins-, Rückzahlungs- oder Gewinnbeteiligungsrechte vermitteln können. Solche Tokens können als Finanzinstrumente qualifiziert werden, wenn sie wirtschaftlich einer Aktie, Anleihe oder einem strukturierten Finanzprodukt entsprechen.²³²

Nur Kategorie 3 löst kapitalmarktrechtliche Pflichten aus.

4.4.2 Security Token: Wann liegt ein „übertragbares Wertpapier“ vor?

Ein Token gilt als „übertragbares Wertpapier“, wenn er folgende Merkmale erfüllt: Verbriefung wirtschaftlicher Rechte (z. B. Zins, Rückzahlung, Gewinnbeteiligung), Übertragbarkeit an den Kapitalmärkten, Gleichartigkeit der Einheiten (fungibility) und Marktfähigkeit.²³³

Damit können tokenisierte Anleihen, tokenisierte Beteiligungen oder tokenisierte Genussrechte als Finanzinstrumente qualifiziert werden, selbst wenn ihre Ausgabe über eine Blockchain erfolgt. Die Finanzmarktaufsicht (FMA) beurteilt diese Qualifikation im Einzelfall und stellt dabei insbesondere auf die wirtschaftliche Funktion des jeweiligen Tokens ab. Maßgeblich ist unter anderem, ob ein Rückzahlungsversprechen besteht, ob Ertrags- oder Gewinnansprüche eingeräumt werden, ob das eingesammelte Kapital der Finanzierung eines Projekts dient sowie ob der Token übertragbar ist und auf Handelsplattformen gehandelt wird. Liegt ein Security Token vor, greifen automatisch verschiedene kapitalmarkt- und aufsichtsrechtliche Pflichten. Dazu zählen insbesondere die Prospektpflicht nach dem KMG, Wohlverhaltenspflichten nach dem WAG 2018, verschärfte Anforderungen an die Anlageberatung, Regelungen zum Interessenkonfliktmanagement sowie Produktüberwachungs- und Governancepflichten. Diese Anforderungen dienen dem Schutz der Anleger:innen und entsprechen den Schutzstandards des traditionellen Kapitalmarktrechts.²³⁴ Das Problem ist, dass der Großteil der Krypto-Angebote erfüllt diese Kriterien nicht und bleibt daher außerhalb des kapitalmarktrechtlichen Schutzsystems.

²³² Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 22 f., 712 f., 715 f.

²³³ Art. 4 Abs. 1 Nr. 44 MiFID II; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 712–716.

²³⁴ Vgl. Art. 4 Abs. 1 Nr. 44 sowie ErwGr 2 und 71 MiFID II; vgl. § 1 KMG 2019; vgl. §§ 38 ff. WAG 2018; vgl. Art. 16 Abs. 3 MiFID II; vgl. Delegierte Richtlinie (EU) 2017/593.

4.4.3 Das Kapitalmarktgesetz (KMG): Prospektpflicht und ihre Grenzen

Das Kapitalmarktgesetz (KMG) normiert die Prospektpflicht für öffentliche Angebote von Wertpapieren und Veranlagungen. Im Zusammenhang mit Kryptowerten stellt sich daher die Frage, ob bestimmte Kryptoangebote in den Anwendungsbereich des KMG fallen können.

(A) KMG 2019 – „Veranlagungen“ (§ 1 Z 3 KMG): Auch wenn ein Token nicht als Wertpapier qualifiziert wird, kann er dennoch eine Veranlagung im Sinne des KMG darstellen. Dies ist insbesondere dann möglich, wenn Kapital von Anleger:innen eingesetzt wird, dieses Kapital der Finanzierung einer unternehmerischen Tätigkeit dient, Anleger:innen eine wirtschaftliche Gewinnerwartung haben und das wirtschaftliche Risiko im Wesentlichen beim Emittenten oder Projektträger verbleibt. Unter diesen Voraussetzungen können auch bestimmte Kryptoprojekte oder Tokenmodelle der kapitalmarktrechtlichen Prospektpflicht unterliegen. Einige ICOs (Initial Coin Offerings) erfüllen diese Kriterien – allerdings nur jene, die tatsächlich der Kapitalaufnahme für ein Projekt dienen und eine Renditechance vermitteln.²³⁵

(B) Grenzen der Prospektpflicht: Viele Tokenmodelle werden bewusst so ausgestaltet, dass sie nicht unter die klassischen kapitalmarktrechtlichen Prospektpflichten fallen. Dies geschieht insbesondere dadurch, dass kein Rückzahlungsanspruch vorgesehen wird, das wirtschaftliche Risiko vollständig auf die Investor:innen verlagert wird, keine bestimmte Rendite oder Gewinnbeteiligung zugesagt wird und der Token formal lediglich als reines Nutzungs- oder Zugangsrecht (Utility Token) ausgestaltet beziehungsweise deklariert wird. Dadurch können sich bestimmte Kryptoprojekte der Anwendung kapitalmarktrechtlicher Schutzmechanismen entziehen.²³⁶

(C) Folge für Verbraucher:innen: Token, die keiner Prospektpflicht unterliegen, werden regelmäßig keiner behördlichen Prüfung unterzogen und enthalten häufig keine standardisierten Mindestangaben zu Risiken, Kosten oder zur wirtschaftlichen Struktur des Projekts. Dadurch verbleiben Anleger:innen oftmals ohne einen klaren und strukturierten Informationsrahmen für ihre Investitionsentscheidung. Dies steht in deutlichem Gegensatz zu traditionellen Kapitalmarktprodukten, bei denen Prospekte umfassende Informationen über Risiken, Kosten,

²³⁵ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. (2020), S. 46 f; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 69 f.

²³⁶ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. (2020), S. 62; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 21.

Emittent:innen, Geschäftsmodelle und wirtschaftliche Hintergründe enthalten müssen, um Transparenz und Anlegerschutz sicherzustellen.²³⁷

4.5 Steuerrechtlicher Rahmen für private Nutzer:innen

Für Verbraucher:innen ist die steuerliche Behandlung von Kryptowerten von erheblicher Bedeutung, da sie maßgeblich bestimmt, ob und in welchem Umfang Kursgewinne und laufende Erträge der Einkommensteuer unterliegen. Mit der Einführung des § 27b EStG 1988 hat der österreichische Gesetzgeber seit 1. März 2022 einen eigenständigen steuerlichen Rahmen geschaffen, der Einkünfte aus Kryptowerten ausdrücklich erfasst und grundsätzlich den Einkünften aus Kapitalvermögen zuordnet.²³⁸

4.5.1 Entwicklung der Rechtslage: Von Spekulationsgeschäften zu Kapitaleinkünften

Bis zur Steuerreform 2022 wurden Gewinne aus privaten Kryptogeschäften in Österreich im Regelfall als **Spekulationseinkünfte** behandelt. Maßgeblich war, ob zwischen Anschaffung und Veräußerung eine bestimmte Frist (Spekulationsfrist) überschritten wurde; bei längerem Haltedauer konnte Steuerfreiheit eintreten.²³⁹ In der Praxis bedeutete dies für Verbraucher:innen, dass insbesondere kurzfristige Veräußerungsgeschäfte mit Kryptowerten steuerpflichtig waren, während ein längerfristiges „Hodln“ nach Ablauf bestimmter Fristen unter Umständen steuerfreie Gewinne ermöglichen konnte. Die steuerliche Behandlung hing dabei vielfach vom jeweiligen Zeitpunkt der Anschaffung und Veräußerung sowie von den konkreten Umständen des Einzelfalls ab. Mit der Einführung des § 27b EStG verfolgte der Gesetzgeber das Ziel, die Besteuerung von Kryptowerten systematisch in das Regime der Kapitaleinkünfte einzugliedern und dadurch eine einheitlichere steuerliche Behandlung zu schaffen. Seit dem 1. März 2022 gelten Einkünfte aus Kryptowährungen grundsätzlich als Einkünfte aus Kapitalvermögen. Sie unterliegen damit regelmäßig einem besonderen Steuersatz von 27,5 % und sind von der Progression des übrigen Einkommens grundsätzlich getrennt.²⁴⁰ Gleichzeitig wurden **Übergangsregeln** für vor dem 1. März 2021 erworbene Bestände („Altvermögen“) geschaffen, um rückwirkende Belastungen zu vermeiden und bereits getroffene Dispositionen zu schützen. Unter bestimmten Voraussetzungen bleiben Veräußerungsgewinne aus diesen Altbeständen auch nach 2022 steuerfrei.²⁴¹

²³⁷ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), Digital Law, 2. Aufl. (2020), S. 61; vgl. Schweizer Bundesrat, Rechtliche Grundlagen der Distributed-Ledger-Technologie und Blockchain in der Schweiz (2018), S. 129.

²³⁸ Vgl. § 27b EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022).

²³⁹ Vgl. § 31 Abs. 1 EStG 1988 idF vor BGBl. I Nr. 10/2022.

²⁴⁰ Vgl. § 27b EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022).

²⁴¹ Ebd.

Damit erkennt das österreichische Steuerrecht Kryptowerte ausdrücklich als steuerlich relevante Vermögenswerte an und differenziert zugleich zwischen Alt- und Neubestand. Für Konsument:innen bedeutet dies eine formale Klarstellung – allerdings um den Preis erheblich gesteigerter Komplexität.

4.5.2 Systematik des § 27b EStG: Steuerbare Vorgänge, Steuersatz und Verlustverrechnung

§ 27b EStG enthält ein eigenständiges Regelwerk für die Besteuerung von Kryptowerten.

Kernpunkte sind:²⁴²

a) Steuergegenstand und Einordnung: Kryptowerte werden steuerlich als „Kryptowährungen“ erfasst und den Einkünften aus Kapitalvermögen zugeordnet. Damit unterliegen sowohl Veräußerungsgewinne als auch bestimmte laufende Erträge (z. B. aus Lending oder Staking) dem Sondersteuersatz von 27,5 %.²⁴³

b) Steuerbare Realisationstatbestände: Steuerlich relevante Vorgänge sind insbesondere der Tausch von Kryptowerten gegen gesetzliche Zahlungsmittel, etwa Euro oder US-Dollar, sowie der Tausch von Kryptowerten gegen sonstige Wirtschaftsgüter oder Dienstleistungen, beispielsweise bei der Bezahlung eines Kaufs mit Bitcoin. Darüber hinaus kann auch die entgeltliche Überlassung von Kryptowerten, etwa im Rahmen von Lending-, Staking- oder vergleichbaren Modellen, steuerlich relevant sein. Gleiches gilt für die Rückzahlung bestimmter tokenisierter Forderungen, sofern dadurch steuerpflichtige Einkünfte oder Wertveränderungen realisiert werden.²⁴⁴ Demgegenüber gilt der Tausch einer Kryptowährung gegen eine andere (z. B. BTC → ETH) nach der gesetzlichen Konzeption grundsätzlich nicht als steuerlicher Realisationstatbestand; die Steuerpflicht tritt erst beim „Ausstieg“ in Fiat oder andere Wirtschaftsgüter ein.²⁴⁵

c) Steuersatz und Erhebungsform: Einkünfte aus Kryptowerten unterliegen grundsätzlich einem fixen Steuersatz von 27,5 %, der dem allgemeinen Kapitalertragsteuersatz entspricht. Soweit inländische Dienstleister:innen oder Emittent:innen als Abzugsverpflichtete tätig werden, kann die Besteuerung im Wege der Kapitalertragsteuer (KESt) erfolgen, wodurch die Steuer grundsätzlich bereits abgegolten wird. In vielen praktischen Konstellationen – insbesondere bei der Nutzung ausländischer Börsen, Plattformen oder Wallets – besteht jedoch keine entsprechende Abzugsverpflichtung. In diesen Fällen müssen die Einkünfte im Rahmen

²⁴² Vgl. § 27b EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022).

²⁴³ Ebd.

²⁴⁴ Vgl. § 27b EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022); vgl. ErlRV zum Ökosozialen Steuerreformgesetz 2022, BGBl. I Nr. 10/2022.

²⁴⁵ Ebd.

der Einkommensteuerveranlagung eigenständig erklärt und in der Steuererklärung angegeben werden.²⁴⁶

d) Verlustverrechnung: Seit 1. März 2022 können Verluste aus Kryptogeschäften mit anderen Einkünften aus Kapitalvermögen, die dem Sondersteuersatz unterliegen, gegengerechnet werden. Dies gilt etwa für Verluste aus der Veräußerung oder aus der Verwertung wertlos gewordener Bestände.²⁴⁷

Für Verbraucher:innen ist dies ambivalent: Einerseits ermöglicht die Verlustverrechnung eine Nettoentlastung bei gescheiterten Investitionen; andererseits setzt sie eine detaillierte Erfassung und Dokumentation sämtlicher Transaktionen voraus, die bei hoher Handelsfrequenz oder DeFi-Nutzung kaum ohne spezialisierte Software oder Beratung zu bewältigen ist.

4.5.3 Alt- und Neubestände, DeFi-Modelle und internationale Schnittstellen

a) Altvermögen und Übergangsrecht: Die Unterscheidung zwischen „Altvermögen“ (vor 1. März 2021 erworben) und „Neuvermögen“ ist für private Nutzer:innen zentral. Für Altbestände sieht das Gesetz Übergangsbestimmungen vor, nach denen Veräußerungsgewinne unter definierten Voraussetzungen auch nach 2022 steuerfrei bleiben können. Für Neubestände gelten die Regelungen des § 27b EStG vollumfänglich.²⁴⁸

In der Beratungspraxis wird betont, dass die korrekte Zuordnung einzelner Bestände und die lückenlose Dokumentation der Anschaffungszeitpunkte entscheidend für die richtige steuerliche Behandlung ist.

b) DeFi, Staking, Lending und vergleichbare Modelle: Besondere Herausforderungen entstehen bei DeFi-Plattformen, Staking-Pools, Liquidity-Mining und ähnlichen Modellen. Das BMF ordnet laufende Erträge aus der Überlassung von Kryptowerten (z. B. Zinsen, Rewards, zusätzliche Token) grundsätzlich als Kapitalerträge ein; sie unterliegen daher ebenfalls dem Sondersteuersatz. Gleichzeitig, ist vielfach unklar, wie einzelne, technisch hochkomplexe Transaktionen (z. B. Protokollbelohnungen, Rebase-Token, Airdrops, Liquidity-Provider-Fee-Strukturen) einzuordnen sind.²⁴⁹

Für Verbraucher:innen führt dies zu einem Auslegungs- und Abgrenzungsrisiko, denn unterschiedliche Gestaltung kann zu unterschiedlichen steuerlichen Qualifikationen führen.

²⁴⁶ Vgl. §§ 27a, 27b und 95 EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022).

²⁴⁷ Ebd.

²⁴⁸ Vgl. § 27b EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022); vgl. ErtRV 1293 BlgNR 27. GP, 17.

²⁴⁹ Vgl. BMF, Information zur ertragsteuerlichen Behandlung von Kryptowährungen; vgl. §§ 27a und 27b EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022).

Fehler in der Einordnung können sowohl zu Überbesteuerung als auch zu Nachforderungen und Strafen führen, wenn die Verwaltung von einer abweichenden Rechtsauffassung ausgeht.²⁵⁰

c) Internationale Elemente: Kryptowerte weisen typischerweise einen starken grenzüberschreitenden Bezug auf. Dies zeigt sich insbesondere durch die Nutzung ausländischer Börsen, internationaler Plattformen sowie von Wallets ohne klaren Sitzbezug. Das österreichische Steuerrecht knüpft jedoch grundsätzlich an den Wohnsitz beziehungsweise den gewöhnlichen Aufenthalt der steuerpflichtigen Person an. Für Verbraucher:innen bedeutet dies, dass auch weltweite Gewinne aus Kryptogeschäften in Österreich steuerpflichtig sein können, unabhängig davon, in welchem Staat die verwendete Börse betrieben wird oder wo das jeweilige Kryptoprojekt ansässig ist. Die internationale Struktur des Kryptomarktes erhöht dadurch den Dokumentationsaufwand sowie die rechtliche und steuerliche Unsicherheit erheblich.²⁵¹

4.5.4 Steuerrecht und Konsumentenschutz: Informationsdefizite, Komplexität und faktische Risiken

Obwohl das Steuerrecht primär fiskalischen Zwecken dient, kann seine konkrete Ausgestaltung erhebliche verbraucherschutzrelevante Nebenwirkungen entfalten. Dies zeigt sich insbesondere bei der steuerlichen Anerkennung von Kryptowerten ohne eine gleichzeitig eindeutige zivilrechtliche Einordnung. Das Steuerrecht behandelt Kryptowerte als eigenständige steuerbare Vermögenspositionen, obwohl ihre zivilrechtliche Qualifikation – etwa als Sache, Forderung oder Recht sui generis – gesetzlich weiterhin nicht abschließend geklärt ist. Für Konsument:innen kann dadurch der Eindruck entstehen, dass es sich um ein umfassend rechtlich abgesichertes und eindeutig geregeltes Produkt handelt. Tatsächlich werden jedoch zentrale Fragen des Eigentums, der Besicherung, der Insolvenzbehandlung und des Erbrechts weiterhin überwiegend durch Literatur, Analogieüberlegungen und Rechtsprechung beantwortet. Dadurch entsteht ein Spannungsverhältnis zwischen steuerlicher Anerkennung und zivilrechtlicher Rechtsklarheit.²⁵²

Die Anwendung des § 27b EStG ist mit einer erheblichen Komplexität und Fehleranfälligkeit verbunden. Sie setzt eine lückenlose Erfassung sämtlicher Transaktionen, die Unterscheidung zwischen Alt- und Neubeständen, die korrekte Abbildung von Tauschvorgängen, die zutreffende Zuordnung laufender Erträge sowie eine ordnungsgemäße Verlustverrechnung voraus. Für Konsument:innen und insbesondere für Kleinanleger:innen, die häufig eine Vielzahl von

²⁵⁰ Vgl. BMF, Information zur ertragsteuerlichen Behandlung von Kryptowährungen, iVm §§ 27a und 27b EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022); vgl. §§ 201, 207 und 217 BAO.

²⁵¹ Vgl. § 1 Abs. 2 EStG 1988.

²⁵² Vgl. § 27b Abs. 1 EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022).

Transaktionen pro Jahr durchführen, stellt dies eine erhebliche Herausforderung dar. In der Praxis ist eine korrekte steuerliche Erfassung oftmals nur unter Einsatz spezialisierter Softwarelösungen oder mit fachkundiger Beratung möglich, wodurch zusätzlicher Aufwand und weitere Fehlerquellen entstehen können.²⁵³

Ein weiteres verbraucherschutzrelevantes Problem besteht im Risiko unerwarteter Steuerbelastungen. Informationsdefizite hinsichtlich der steuerlichen Behandlung von Kryptowerten können dazu führen, dass Verbraucher:innen Gewinne nicht oder fehlerhaft deklarieren, den Unterschied zwischen realisierten und nicht realisierten Gewinnen falsch einschätzen, Verluste nicht geltend machen oder steuerliche Fristen versäumen. Die daraus resultierenden Folgen können von Steuernachzahlungen und Säumniszuschlägen bis hin zu finanzstrafrechtlichen Konsequenzen reichen. Dadurch entsteht ein zusätzliches Risiko für Verbraucher:innen, dass nicht unmittelbar durch klassische verbraucherschutzrechtliche Instrumente wie die MiCA-Verordnung oder die PSD2 erfasst wird.²⁵⁴

Ein weiteres Problem besteht in der asymmetrischen Informationslage zwischen professionellen Marktteilnehmer:innen und Kleinanleger:innen. Professionelle Anbieter:innen und institutionelle Investor:innen verfügen regelmäßig über umfassende steuerliche Expertise und können ihre Geschäftsmodelle sowie Transaktionen gezielt so strukturieren, dass steuerliche Auswirkungen optimiert werden. Demgegenüber bewegen sich viele Kleinanleger:innen im Kryptobereich häufig in einem Spannungsfeld zwischen unzureichendem Wissen und der Komplexität der steuerlichen Regelungen. Dies kann dazu führen, dass steuerliche Risiken und Pflichten faktisch verstärkt auf die Endnutzer:innen verlagert werden. Insgesamt trägt das Steuerrecht dadurch – wenn auch nicht primär zu diesem Zweck – zu einer weiteren Erhöhung der Komplexität bei und schafft zusätzliche Risikodimensionen, die für durchschnittliche Verbraucher:innen häufig nur schwer überschaubar und kontrollierbar sind.

4.6 Datenschutzrechtliche Einordnung und Bedeutung der DSGVO für Verbraucher:innen

Die Nutzung von Kryptowerten und Kryptodienstleistungen erfolgt in einem digitalen Ökosystem, das von der Verarbeitung sensibler personenbezogener Daten geprägt ist. Transaktionsdaten, Identitätsinformationen, Wallet-Adressen, IP-Adressen, KYC-Daten, biometrische Verfahren, verhaltensbasierte Analyseparameter und – besonders relevant –

²⁵³ Vgl. § 27b EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022); vgl. §§ 119 und 131 BAO.

²⁵⁴ Vgl. §§ 27a, 27b und 95 EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022); vgl. §§ 119, 131, 201 und 217 BAO; vgl. Verordnung (EU) 2023/1114 (MiCA), Art. 2 Abs. 4; vgl. Richtlinie (EU) 2015/2366 (PSD2), Art. 2 und Art. 4 Nr. 3.

Blockchain-basierte Metadaten, die öffentlich und dauerhaft gespeichert werden. Für Verbraucher:innen ist entscheidend, dass die Datenschutz-Grundverordnung (DSGVO) als unionsrechtliches Querschnittsregelwerk in allen Phasen dieser Verarbeitung gilt und einen rechtsverbindlichen Rahmen zur Minimierung von Risiken, Transparenzdefiziten und Missbrauchsgefahren schafft.²⁵⁵

Gleichzeitig führt die besondere Struktur von Blockchains – Unveränderlichkeit, Dezentralität, globale Verteilung – zu einem strukturellen Spannungsverhältnis mit zentralen Datenschutzgrundsätzen wie Speicherbegrenzung, Zweckbindung und Löschpflichten.²⁵⁶ Die folgenden Ausführungen analysieren die datenschutzrechtliche Einordnung und zeigen die zentralen Risiken für Verbraucher:innen im österreichischen und unionsrechtlichen Kontext auf.

4.6.1 Grundanwendbarkeit der DSGVO auf Kryptowerte und Blockchain-Systeme

Die DSGVO gilt, sobald personenbezogene Daten verarbeitet werden. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (Art. 4 Z 1 DSGVO). Eine zentrale datenschutzrechtliche Frage im Zusammenhang mit Kryptowerten lautet, ob Blockchain-Daten als personenbezogene Daten im Sinne der DSGVO zu qualifizieren sind.

(1) Wallet-Adressen und Transaktionsdaten als personenbezogene Daten: Nach der überwiegenden Auffassung europäischer und nationaler Datenschutzbehörden werden Wallet-Adressen (Public Keys) trotz ihrer pseudonymen Ausgestaltung grundsätzlich als personenbezogene Daten angesehen. Begründet wird dies damit, dass eine Zuordnung zu einer natürlichen Person mit vertretbarem Aufwand möglich sein kann. Eine solche Identifizierung kann insbesondere über KYC-Daten von Kryptobörsen, On-Chain-Analyse-Tools, IP-Adressen oder durch die Auswertung von Verhaltens- und Transaktionsmustern erfolgen.²⁵⁷ Die Folge dieser Einordnung besteht darin, dass die Verarbeitung von Wallet-Adressen und damit zusammenhängenden Transaktionsdaten grundsätzlich den Anforderungen der Datenschutz-Grundverordnung (DSGVO) unterliegt.

(2) Unveränderlichkeit der Blockchain und das „Recht auf Vergessenwerden“: Die DSGVO sieht grundsätzlich vor, dass betroffene Personen unter bestimmten Voraussetzungen die Löschung personenbezogener Daten verlangen können (Art. 17 DSGVO). Blockchain-Systeme sind jedoch regelmäßig durch ihre Unveränderlichkeit (Immutability) gekennzeichnet, sodass einmal

²⁵⁵ Vgl. Art. 2, 3 und 4 Z 1, 5, 24 und 25 DSGVO; vgl. ErwGr 26 und 39 DSGVO.

²⁵⁶ Vgl. Art. 5 Abs. 1 lit. b und e sowie Art. 17 DSGVO.

²⁵⁷ Vgl. Art. 4 Z 1 sowie ErwGr 26 DSGVO; vgl. EDPB, Leitlinien zur Identifizierbarkeit und Pseudonymisierung; vgl. CNIL, Blockchain and the GDPR (2018).

gespeicherte Daten grundsätzlich nicht nachträglich gelöscht oder verändert werden können. Daraus ergibt sich ein grundlegendes Spannungsverhältnis zwischen den Anforderungen des Datenschutzrechts und den technischen Eigenschaften der Blockchain-Technologie. In der Literatur wird daher häufig auf einen strukturellen Konflikt zwischen dem Recht auf Löschung personenbezogener Daten und der dauerhaften Speicherung von Informationen in Blockchain-Systemen hingewiesen.²⁵⁸

(3) Verantwortliche:r („Controller“) in dezentralen Systemen: Bei vollständig dezentralisierten Netzwerken, etwa Bitcoin, stellt sich die Frage, wer als Verantwortliche:r im Sinne des Art. 4 Nr. 7 DSGVO anzusehen ist. Das Datenschutzrecht setzt grundsätzlich voraus, dass eine identifizierbare Stelle vorhanden ist, die über die Zwecke und Mittel der Datenverarbeitung entscheidet, die Ausübung von Betroffenenrechten ermöglicht und gegebenenfalls die Umsetzung datenschutzrechtlicher Verpflichtungen, einschließlich der Bearbeitung von Löschungsbegehren, sicherstellt. In dezentralen Blockchain-Netzwerken fehlt jedoch häufig ein solcher zentraler Verantwortlicher, wodurch erhebliche rechtliche und praktische Herausforderungen bei der Anwendung der DSGVO entstehen.²⁵⁹

Die europäische Datenschutzaufsicht stellt klar, dass die Qualifikation als Verantwortlicher oder Auftragsverarbeiter von der tatsächlichen Einflussnahme auf Zwecke und Mittel der Verarbeitung abhängt.²⁶⁰ Aus Sicht der Verbraucher:innen führt diese funktionsbezogene und vom jeweiligen Einzelfall abhängige Zuordnung jedoch zu einer erheblichen Intransparenz hinsichtlich der datenschutzrechtlichen Verantwortlichkeit. Für Betroffene ist häufig nur schwer erkennbar, welche Person oder Stelle für die Verarbeitung ihrer Daten verantwortlich ist, an wen datenschutzrechtliche Ansprüche zu richten sind und wer für die Einhaltung der Vorgaben der DSGVO einzustehen hat. Dies kann die Wahrnehmung und Durchsetzung von Betroffenenrechten erheblich erschweren.

4.6.2 Verarbeitungssituationen im Kryptobereich und ihre datenschutzrechtlichen Implikationen

(1) Börsen und Kryptoplattformen: Zentralisierte Kryptoplattformen (Centralized Exchanges – CEX) verarbeiten regelmäßig umfangreiche personenbezogene Daten. Dazu zählen insbesondere Identitätsdaten im Rahmen von KYC-Verfahren, verifizierte Adressdaten, Transaktionshistorien, verknüpfte Bankverbindungen, Risikobewertungen sowie Informationen, die im Zusammenhang mit geldwäscherechtlichen Meldepflichten an Behörden übermittelt

²⁵⁸ Vgl. Art. 17 iVm Art. 5 Abs. 1 lit. b und e DSGVO.

²⁵⁹ Vgl. Art. 4 Nr. 7 sowie Art. 12 und 17 DSGVO.

²⁶⁰ Vgl. Art. 4 Nr. 7 und 8 sowie Art. 26 DSGVO; vgl. EDPB, *Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO*, Version 2.0.

werden. Als Verantwortliche im Sinne der DSGVO sind diese Plattformen verpflichtet, die Betroffenenrechte, insbesondere Auskunfts-, Berichtigungs- und Löschungsrechte, zu gewährleisten. Darüber hinaus müssen sie geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten implementieren, die Anforderungen des Art. 32 DSGVO zur Datensicherheit einhalten und etwaige Datenschutzverletzungen gemäß Art. 33 DSGVO melden.²⁶¹ Aus Sicht der österreichischen Praxis bestehen jedoch erhebliche Vollzugsprobleme. Viele Kryptoplattformen haben ihren Sitz außerhalb Österreichs oder der Europäischen Union, wodurch die Durchsetzung datenschutzrechtlicher Ansprüche und behördlicher Maßnahmen in der Praxis oftmals erschwert wird. Dies kann die effektive Wahrnehmung der Datenschutzrechte von Verbraucher:innen zusätzlich beeinträchtigen.

(2) Wallet-Provider: Auch Anbieter:innen von Software- und Hardware-Wallets verarbeiten regelmäßig personenbezogene Daten. Dies betrifft insbesondere Backups, Informationen im Zusammenhang mit Seed-Phrases, IP-Adressen sowie verschiedene Log-in- und Nutzungsmetadaten. Aus Sicht vieler Verbraucher:innen besteht häufig die Annahme, dass die eigenständige Verwahrung von Kryptowerten (Self-Custody) datenschutzrechtlich neutral sei. Tatsächlich werden jedoch auch in diesem Bereich oftmals personenbezogene Daten verarbeitet, etwa durch Cloud-Backups, Browser-Erweiterungen, Synchronisationsdienste oder andere technische Komponenten.²⁶² Dadurch können datenschutzrechtliche Fragestellungen selbst dann entstehen, wenn keine zentrale Kryptobörse oder Verwahrstelle genutzt wird.

(3) DeFi-Plattformen: Bei DeFi-Protokollen gestaltet sich die datenschutzrechtliche Zuordnung besonders schwierig. Zwar verarbeiten Smart Contracts regelmäßig keine klassischen Off-Chain-Daten, jedoch werden die zugrunde liegenden On-Chain-Daten öffentlich, dauerhaft und für sämtliche Netzwerkteilnehmer:innen einsehbar gespeichert. Da auch pseudonyme Wallet-Adressen und Transaktionsdaten unter bestimmten Voraussetzungen als personenbezogene Daten qualifiziert werden können, entstehen erhebliche datenschutzrechtliche Herausforderungen. Insbesondere kann die Umsetzung datenschutzrechtlicher Ansprüche problematisch sein, da einmal in der Blockchain gespeicherte Daten aufgrund der technischen Struktur des Systems grundsätzlich nicht gelöscht oder verändert werden können. Dadurch entsteht ein Spannungsverhältnis zwischen den Anforderungen der DSGVO und den technischen Eigenschaften dezentraler Blockchain-Netzwerke.²⁶³ Für Verbraucher:innen bedeutet dies: Transaktionsfehler, Fehlüberweisungen oder die Verwendung kompromittierter Wallets sind dauerhaft sichtbar und nicht korrigierbar.

²⁶¹ Vgl. Art. 4 Z 1 und 7, Art. 12–22, Art. 32 und 33 DSGVO; vgl. §§ 2 Z 21, 6–11 und 16 ff. FM-GwG.

²⁶² Vgl. Art. 4 Z 1, 2 und 7 sowie ErwGr 26 DSGVO.

²⁶³ Vgl. Art. 4 Z 1, Art. 5 Abs. 1 lit. e sowie Art. 17 DSGVO; vgl. ErwGr 26 DSGVO.

Kapitel 5

Nationale Umsetzung und österreichischer Rechtsrahmen

5.1 Einbettung von Kryptowerten in das österreichische Rechtssystem

Die Einbettung von Kryptowerten in das österreichische Rechtssystem erfolgte über mehrere Jahre hinweg schrittweise und reagierte zunächst hauptsächlich auf geldwäscherechtliche Risiken sowie auf die zunehmende wirtschaftliche Bedeutung digitaler Vermögenswerte. Anstatt ein kohärentes Spezialgesetz für Kryptowerte zu schaffen, integrierte der Gesetzgeber relevante Elemente in unterschiedliche Materien-Gesetze. Dies führte zu einem fragmentierten Rechtsrahmen, dessen Einzelbestandteile aus unterschiedlichen Regulierungstraditionen stammen und daher für Konsument:innen nur schwer verständlich sind.²⁶⁴ Der Schutz der Nutzer:innen entsteht in dieser Struktur nicht durch ein einheitliches Verbraucherschutzinstrumentarium, sondern durch die Kombination verstreuter Einzelnormen, die in ihrer Summe keine lückenlose Sicherung gewährleisten.

Einen ersten systematischen Zugang eröffnete das Finanzmarkt-Geldwäschegesetz (FM-GwG), das Kryptowährungen in § 2 Z 21 FM-GwG als „digitale Darstellungen eines Wertes“ definiert, die weder gesetzliches Zahlungsmittel sind noch von einer Zentralbank ausgegeben werden, aber als Tausch- oder Wertaufbewahrungsmittel akzeptiert und elektronisch übertragen werden können.²⁶⁵ Diese Begriffsbestimmung leitet sich unmittelbar aus den unionsrechtlichen Vorgaben der Geldwäscherichtlinien ab und ordnet Kryptowerten eine funktionale Rolle im Rahmen der Prävention von Geldwäsche und Terrorismusfinanzierung zu.²⁶⁶ Sie trifft jedoch keine Aussage über die vermögensrechtliche Einordnung von Token, insbesondere nicht über ihre Stellung im Zivilrecht oder ihre Eigenschaft als eigentumsfähige Güter.²⁶⁷ Für Konsument:innen bedeutet dies, dass die zentrale Erstdefinition der Rechtsordnung den Charakter von Kryptowerten zwar umschreibt, aber keine Klarheit über deren rechtliche Behandlung bei Verlust, Insolvenz oder technischen Fehlfunktionen schafft.

Auch im Kapitalmarktrecht fehlte lange Zeit eine autonome gesetzliche Kategorie für Kryptowerte. Stattdessen wurden Token – sofern sie wirtschaftlich als Kapitalanlagen oder Beteiligungsinstrumente strukturiert waren – unter die bestehenden Regelungen des Kapitalmarktgesetzes 2019 (KMG 2019) subsumiert.²⁶⁸ Entscheidend war dabei nicht die

²⁶⁴ Vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 1–5, 10.

²⁶⁵ Vgl. § 2 Z 21 FM-GwG idF BGBl. I Nr. 37/2018.

²⁶⁶ Vgl. Art. 1 Z 2 lit. d sowie ErwGr 10 Richtlinie (EU) 2018/843 (AMLD5).

²⁶⁷ Vgl. Art. 1 Richtlinie (EU) 2018/843 (AMLD5); vgl. § 2 Z 21 FM-GwG; vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 4–5.

²⁶⁸ Vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 10; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), *Digital Law*, 2. Aufl. (2020), S. 61–62; vgl. § 1 KMG 2019.

technische Form des Tokens, sondern dessen ökonomische Funktion. Sobald eine Kapitalveranlagung, ein Rückzahlungsversprechen oder eine Gewinnbeteiligung vorlag, konnten Prospektpflichten ausgelöst werden. Für Konsument:innen führte diese Situation zu einem erheblichen Informations- und Sicherheitsdefizit, da Emittenten strukturelle Möglichkeiten hatten, Angebote so zu gestalten, dass sie formal nicht unter kapitalmarktrechtliche Vorschriften fielen, obwohl sie wirtschaftlich denselben Risiken wie klassische Anlageformen unterlagen.²⁶⁹

Parallel dazu existierte auf zivilrechtlicher Ebene weiterhin keine gesetzlich festgelegte Rechtsnatur von Kryptowerten. In der wissenschaftlichen Literatur wurde diskutiert, ob Token als unkörperliche Sachen, als Forderungsrechte, als sonstige Rechte eigener Art oder als technische Datensätze ohne dingliche Qualität zu qualifizieren sind.²⁷⁰ Diese dogmatische Uneinheitlichkeit hat unmittelbare Konsequenzen für Verbraucher:innen, da die zivilrechtliche Qualifikation die Grundlage dafür bildet, wie Eigentum, Verfügungsrechte, Schadenersatzansprüche oder insolvenzrechtliche Absonderungsrechte ausgestaltet sind. Die fehlende Kodifikation bedeutet daher, dass Nutzer:innen im Konfliktfall – etwa bei der Insolvenz eines Dienstleisters oder dem Verlust von Token infolge eines Hacks – nur eingeschränkt vorhersehen können, ob sie zivilrechtliche Ansprüche geltend machen können oder ob ihre Vermögenswerte der Insolvenzmasse zufallen.

Mit der Einführung der MiCA-Verordnung wurde erstmals ein unionsweit einheitlicher aufsichtsrechtlicher Rahmen geschaffen, der Kryptowerte ausdrücklich als Gegenstand des Finanzmarktaufsichtsrechts behandelt.²⁷¹ Österreich hat MiCA durch das MiCA-Verordnungsvollzugsgesetz (MiCA-VVG) umgesetzt, welches die Finanzmarktaufsicht (FMA) zur national zuständigen Behörde bestimmt und neue Verwaltungsstrafbestände verankert. Kryptowerte, die dem Anwendungsbereich der MiCA unterfallen, bewegen sich damit künftig in einem regulierten Marktsegment, in dem Dienstleister Zulassungs-, Organisations- und Informationspflichten einzuhalten haben.²⁷² Gleichzeitig verbleibt jedoch ein erheblicher Teil der Kryptomärkte – insbesondere dezentrale Protokolle (DeFi), algorithmische Stablecoins ohne vollständige Besicherung oder nicht-wirtschaftliche Utility-Token – außerhalb dieses regulierten Rahmens.²⁷³ Für Konsument:innen entsteht dadurch ein duales System: Im Gegensatz zu regulierten Anbietern, die ein Mindestmaß an Aufsicht und Transparenz gewährleisten müssen, bestehen

²⁶⁹ Vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), *Digital Law*, 2. Aufl. (2020), S. 62; vgl. § 1 KMG 2019.

²⁷⁰ Vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 10–11.

²⁷¹ Vgl. ErwGr 1 und 2 sowie Art. 1 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

²⁷² Vgl. Art. 1 Abs. 1, Art. 53 Abs. 1, Art. 59 Abs. 1 und Art. 66 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

²⁷³ Vgl. ErwGr 22, 26 und 45 sowie Art. 2 Abs. 4 Verordnung (EU) 2023/1114 (MiCA).

weiterhin unregulierte Bereiche, in denen klassische Schutzmechanismen nur eingeschränkt oder überhaupt nicht zur Anwendung kommen.

Die frühere österreichische Registrierungspflicht für „Dienstleister in Bezug auf virtuelle Währungen“ nach § 32a FM-GwG war primär geldwäscherechtlich motiviert und verpflichtete Anbieter zwar zu Identitätsfeststellungen, jedoch nicht zu organisatorischen, kapitalbezogenen oder kundenbezogenen Mindeststandards. Mit der Novelle BGBl I 151/2024 wurde ein unionsrechtskonformes Übergangsregime geschaffen. Bisher registrierte Dienstleister dürfen ihre Tätigkeit zeitlich befristet fortführen, sofern sie die Vorgaben der MiCA erfüllen oder auf dem Weg zur CASP-Zulassung nach MiCA sind.²⁷⁴ Erfüllen sie die Anforderungen nicht, kann die FMA die Registrierung widerrufen. Ein solcher Widerruf führt zugleich zum Verlust der Möglichkeit, sich auf die Übergangsbestimmungen des Art. 143 MiCA zu berufen. Für Konsument:innen bedeutet dies, dass sie während des Übergangs auf Anbieter treffen können, die zwar am Markt tätig sind, aber unterschiedlichen regulatorischen Standards unterliegen – ein Umstand, der Schutzlücken begünstigt und die Transparenz des Marktes beeinträchtigt.²⁷⁵

Neben diesen spezieller ausgestalteten Regelungsbereichen bestehen weitere Rechtsmaterien, die mittelbar Einfluss auf die Behandlung von Kryptowerten haben. Steuerrechtlich qualifiziert Österreich Einkünfte aus Kryptowerten grundsätzlich als Einkünfte aus Kapitalvermögen und unterwirft sie dem besonderen Steuersatz nach § 27a EStG.²⁷⁶ Aufsichtsrechtliche Normen wie das Wertpapieraufsichtsgesetz (WAG 2018), das Zahlungsdienstegesetz (ZaDiG 2018) oder das Alternative-Investmentfonds-Manager-Gesetz (AIFMG) können einschlägig werden, wenn Kryptowerte Teil komplexer Finanzprodukte sind oder Dienstleistungen in ihrer Struktur als Wertpapier- oder Zahlungsdienste qualifiziert werden.²⁷⁷ Diese verstreuten Anknüpfungspunkte verdeutlichen, dass ein umfassendes und in sich geschlossenes Kryptoverbraucherschutzregime in Österreich weiterhin fehlt.

Insgesamt zeigt die bisherige Entwicklung, dass Österreich zwar wesentliche Schritte zur Regulierung von Kryptowerten gesetzt hat, insbesondere durch die Implementierung von MiCA und die Anpassung des FM-GwG, jedoch kein System geschaffen wurde, das den besonderen Risiken und technischen Besonderheiten dieses Marktes gerecht wird.

²⁷⁴ Vgl. Art. 143 Abs. 3 Verordnung (EU) 2023/1114 (MiCA); vgl. § 43a FM-GwG idF BGBl. I Nr. 151/2024.

²⁷⁵ Vgl. Art. 143 Abs. 3 Verordnung (EU) 2023/1114 (MiCA).

²⁷⁶ Vgl. § 27b Abs. 1 sowie § 27a Abs. 1 EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022).

²⁷⁷ Vgl. § 1 Abs. 1 WAG 2018; vgl. § 1 Abs. 1 ZaDiG 2018; vgl. § 1 Abs. 1 AIFMG.

5.2 Zentrale Rechtsquellen: FM-GwG, MiCA-VVG, KMG und weitere Normen

Die regulatorische Behandlung von Kryptowerten in Österreich beruht auf einer Vielzahl von Einzelgesetzen, die jeweils unterschiedliche Aspekte des Kryptomarktes adressieren. Während diese Normen wichtige Teilfunktionen erfüllen, entsteht für Konsument:innen daraus kein kohärentes Regime, sondern ein komplexes, teilweise widersprüchliches Nebeneinander.²⁷⁸ Die folgenden Rechtsquellen bilden die tragenden Elemente des österreichischen Kryptorechts, sind jedoch in ihrer Zusammenschau nicht ausreichend, um die spezifischen Risiken des Kryptomarktes effektiv aufzufangen.

5.2.1 Finanzmarkt-Geldwäschegesetz (FM-GwG)

Das FM-GwG war die erste österreichische Norm, die ausdrücklich auf Kryptowährungen Bezug nahm. Mit der Einführung des „Dienstleisters in Bezug auf virtuelle Währungen“ in § 32a FM-GwG unterwarf der Gesetzgeber Anbieter wie Wallet-Dienstleister, Plattformbetreiber oder Tauschbörsen einer Registrierungspflicht und ordnete sie den geldwäscherechtlich Verpflichteten zu. Die Norm bezweckt in erster Linie die Verhinderung von Geldwäsche und Terrorismusfinanzierung, nicht aber den Schutz von Konsument:innen.²⁷⁹

Dienstleister mussten Identifizierungsmaßnahmen durchführen, interne Kontrollsysteme einrichten und bestimmte Meldepflichten erfüllen.²⁸⁰ Diese Anforderungen verbessern zwar die Marktintegrität, schaffen aber keine materielle Sicherung für Nutzer:innen, etwa im Fall eines Plattformzusammenbruchs, von Cyberangriffen oder betrügerischen Geschäftsmodellen. Das FM-GwG schützt somit eher das Finanzsystem als die einzelnen Konsument:innen, die weiterhin weitgehend ungeschützt bleiben.²⁸¹

Durch die Novelle BGBl I 151/2024 wurde § 32a FM-GwG an das Unionsrecht angepasst und in ein Übergangsregime eingebettet. Anbieter, die bereits nach altem Recht registriert waren, dürfen weiterhin tätig sein, sofern sie die Anforderungen des Unionsrechts erfüllen.²⁸² Kommt die FMA jedoch zum Schluss, dass diese Vorgaben nicht eingehalten werden, kann sie die Registrierung widerrufen, womit zugleich das unionsrechtliche Übergangsrecht entfällt.²⁸³ Für Konsument:innen entsteht damit eine Phase regulatorischer Unsicherheit, da sie mit Anbietern

²⁷⁸ Vgl. § 2 Z 21 FM-GwG; vgl. § 1 MiCA-VVG; vgl. § 1 KMG 2019; vgl. § 1 Abs. 1 WAG 2018; vgl. § 1 Abs. 1 ZaDiG 2018; vgl. § 1 Abs. 1 AIFMG.

²⁷⁹ Vgl. §§ 1 und 2 Z 21 und 22 FM-GwG; vgl. § 32a Abs. 1 FM-GwG.

²⁸⁰ Vgl. § 5 Abs. 1, § 6 Abs. 1 Z 1, § 16 Abs. 1 und § 22 Abs. 1 FM-GwG.

²⁸¹ Vgl. §§ 1, 16 Abs. 1 und 22 Abs. 1 FM-GwG.

²⁸² Vgl. § 32a Abs. 1 FM-GwG idF BGBl. I Nr. 98/2021; vgl. Art. 143 Abs. 3 Verordnung (EU) 2023/1114 (MiCA); vgl. BGBl. I Nr. 151/2024 (FM-GwG-Anpassungsgesetz).

²⁸³ Vgl. § 32a Abs. 4 FM-GwG idF BGBl. I Nr. 98/2021; vgl. Art. 143 Abs. 3 Verordnung (EU) 2023/1114 (MiCA).

interagieren, deren Schutzniveaus unterschiedlich ausgestaltet sind und sich in einem Wandel befinden.

5.2.2 MiCA-Verordnung-Vollzugsgesetz (MiCA-VVG)

Das MiCA-VVG wurde erlassen, um die EU-Verordnung „Markets in Crypto-Assets“ (MiCA) in das österreichische Recht zu integrieren. Es bestimmt die Finanzmarktaufsicht (FMA) zur zuständigen Behörde und regelt die Durchsetzung der MiCA, insbesondere durch neue Verwaltungsstrafbestände. MiCA schafft erstmals europaweite Vorgaben für Emittenten von Kryptowerten und für Crypto-Asset Service Provider (CASPs), darunter Zulassungspflichten, organisatorische Anforderungen und Transparenzmaßnahmen.

Obwohl MiCA einen bedeutenden Fortschritt darstellt, bleibt der Verbraucherschutz begrenzt. Marktmissbrauchstatbestände – wie Insiderhandel oder Marktmanipulation mit Kryptowerten – werden in Österreich ausschließlich verwaltungsstrafrechtlich sanktioniert.²⁸⁴ Dies unterscheidet sich von Kapitalmärkten traditioneller Finanzinstrumente, in denen schwerwiegende Verstöße auch strafrechtliche Konsequenzen nach sich ziehen können. Die geringere Sanktionsschärfe kann die Abschreckungswirkung mindern und lässt Konsument:innen im Falle von Marktmanipulation oftmals ohne ausreichenden Schutz zurück. Darüber hinaus bestehen strukturelle Lücken: MiCA erfasst keine vollständig dezentralen Systeme (DeFi), keine algorithmischen Stablecoins ohne echte Rücklagen und keine Utility-Token ohne wirtschaftlichen Gegenwert. Dies bedeutet, dass ein erheblicher Teil des Kryptomarktes weiterhin außerhalb der Aufsicht bleibt und Konsument:innen dort denselben Risiken wie zuvor ausgesetzt sind – ohne zusätzliche Schutzmechanismen.²⁸⁵

5.2.3 Kapitalmarktgesetz 2019 (KMG 2019) und Prospektrecht

Das KMG 2019 ist für Kryptowerte relevant, wenn Token Merkmale eines Wertpapiers oder einer „sonstigen Veranlagung“ aufweisen. In diesen Fällen kann ein Prospektpflicht bestehen, der Konsument:innen durch umfassende Informationen über Risiken, Emissionsbedingungen, wirtschaftliche Hintergründe und Verantwortlichkeiten schützen soll. Die FMA ist für die Prüfung und Billigung solcher Prospekte zuständig.²⁸⁶

Für Kryptowerte ist jedoch entscheidend, dass das Prospektrecht technologieneutral ist. Ob ein Token klassifiziert wird, hängt allein von seiner wirtschaftlichen Funktion ab. Dies eröffnet

²⁸⁴ Vgl. Art. 90 Abs. 1, Art. 91 Abs. 1, Art. 92 Abs. 1 sowie Art. 111 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); vgl. § 22 Abs. 1 MiCA-VVG.

²⁸⁵ Vgl. ErwGr 22, 26 und 45 sowie Art. 2 Abs. 4 Verordnung (EU) 2023/1114 (MiCA).

²⁸⁶ Vgl. §§ 1 und 3 Abs. 1 sowie § 8 Abs. 1 und 3 KMG 2019; vgl. Art. 6 Abs. 1 Verordnung (EU) 2017/1129 (ProspektVO).

Gestaltungsspielräume, die in der Praxis häufig dazu genutzt werden, Prospektpflichten zu vermeiden – etwa durch Airdrops, die Ausgabe reiner Utility-Token oder durch Konstruktionen, die bewusst keine Kapitalflussstrukturen abbilden.²⁸⁷ Die Folge ist, dass viele Kryptoangebote ohne regulierte Offenlegungspflichten am Markt erscheinen, was das Risiko intransparenter oder betrügerischer Emissionen für Konsument:innen erhöht.

Ein weiteres Problem besteht in der begrenzten Kontrollkapazität der FMA. Selbst wenn zahlreiche Projekte rechtlich prospektpflichtig wären, können sie aufgrund ihrer Vielzahl, Geschwindigkeit und internationalen Struktur oft nicht lückenlos geprüft oder sanktioniert werden. Für Konsument:innen bleibt damit ein strukturelles Informationsdefizit bestehen, das sich gerade in volatilen und technisch komplexen Märkten schwer ausgleichen lässt.

5.2.4 Weitere relevante Rechtsbereiche

Neben FM-GwG, MiCA-VVG und KMG berühren Kryptowerte weitere zentrale Rechtsmaterien. Steuerrecht: Österreich behandelt Einkünfte aus Kryptowerten grundsätzlich als Einkünfte aus Kapitalvermögen und unterwirft sie dem besonderen Steuersatz nach § 27a EStG.²⁸⁸ Zwar schafft dies steuerliche Klarheit, trägt jedoch nicht zum Verbraucherschutz bei, da steuerrechtliche Regelungen keine Sicherungsmechanismen für Verluste oder Betrugsfälle enthalten.

Zivilrecht: Mangels spezieller Kodifikation richten sich vertragliche Beziehungen zwischen Konsument:innen und Dienstleistern nach allgemeinen schuldrechtlichen Regeln.²⁸⁹ Es fehlen sektorspezifische Bestimmungen zu Risikoverteilung, Haftung oder Beweislast – ein signifikanter Nachteil angesichts der technischen Besonderheiten von Kryptotransaktionen. Aufsichtsrecht (WAG 2018, ZaDiG 2018, AIFMG): Diese Normen greifen nur ein, wenn Kryptowerte in regulierte Finanzinstrumente oder Zahlungsdienstleistungen eingebettet sind.²⁹⁰ Der Großteil der Kryptodienstleistungen fällt jedoch nicht in diese Bereiche, sodass deren Schutzmechanismen für Konsument:innen nicht zur Verfügung stehen.

²⁸⁷ Vgl. §§ 1 und 3 KMG 2019; vgl. Art. 6 Verordnung (EU) 2017/1129 (ProspektVO); vgl. ErwGr 45 Verordnung (EU) 2023/1114 (MiCA); vgl. BMF, *Information zur ertragsteuerlichen Behandlung von Kryptowährungen*, GZ 2021-0.586.907 idF GZ 2022-0.430.329.

²⁸⁸ Vgl. § 27b Abs. 1 und § 27a Abs. 1 EStG 1988 idF BGBl. I Nr. 10/2022 (Ökosoziales Steuerreformgesetz 2022); vgl. BMF, *Information zur ertragsteuerlichen Behandlung von Kryptowährungen*, GZ 2021-0.586.907 idF GZ 2022-0.430.329.

²⁸⁹ Vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 9.

²⁹⁰ Vgl. § 1 Abs. 1 WAG 2018; vgl. § 1 Abs. 1 ZaDiG 2018; vgl. § 1 Abs. 1 AIFMG.

5.3 Pflichten der Dienstleister und Aufsichtspraxis der FMA

Die österreichische Regulierung von Kryptodienstleistern befindet sich in einem grundlegenden Wandel. Ausgehend von einem reinen Registrierungsmodell, das im Wesentlichen geldwäscherechtlichen Zwecken diente, entwickelt sich ein vollwertiges aufsichtsrechtliches Zulassungsregime nach Maßgabe der MiCA-Verordnung.²⁹¹ Dieser Systemwechsel betrifft sowohl die materiellen Pflichten der Anbieter als auch die Eingriffsmöglichkeiten der Finanzmarktaufsicht (FMA). Für Konsument:innen bedeutet dies einerseits steigende Anforderungen an Transparenz und Organisationsqualität, andererseits aber eine Phase regulatorischer Unsicherheit sowie das Fortbestehen struktureller Lücken, die insbesondere in Krisensituationen ein erhebliches Risiko darstellen.

5.3.1 Vom VASP-Regime zum CASP-Regime

Bis zum Inkrafttreten der MiCA-Verordnung wurden Kryptodienstleister in Österreich nach § 32a FM-GwG lediglich als „Dienstleister in Bezug auf virtuelle Währungen“ registriert. Die Registrierung verlangte weder ein detailliertes Geschäftsmodell noch Governance-Strukturen, Kapitalanforderungen oder IT-Sicherheitskonzepte.²⁹² Das Regime konzentrierte sich auf die Prävention von Geldwäsche und Terrorismusfinanzierung und war für Konsument:innen nur indirekt vorteilhaft. Es schuf zwar eine gewisse Markttransparenz und ermöglichte behördliche Eingriffe bei Verstößen, bot jedoch keinerlei materiellen Schutzmechanismen – etwa im Fall von Plattforminsolvenzen, technischen Verlusten oder betrügerischen Geschäftsmodellen. Mit Inkrafttreten der MiCA und dem MiCA-Verordnung-Vollzugsgesetz (MiCA-VVG) wird dieses Registrierungsmodell schrittweise durch ein Zulassungsregime ersetzt. Dienstleister, die Kryptowerte verwahren, handeln, tauschen, vermitteln oder beraten, müssen künftig eine CASP-Bewilligung (Crypto-Asset Service Provider) erhalten.²⁹³ Die Anforderungen an diese Zulassung sind erheblich strenger als im bisherigen VASP-Regime (Virtual-Asset Service Provider) und umfassen unter anderem: Mindestkapital und angemessene Liquidität, robuste Geschäftsorganisation, wirksame Risikomanagementsysteme, IT-Sicherheitsstandards einschließlich Notfall- und Wiederanlaufplänen, Maßnahmen zum Schutz der Kundengelder und -kryptowerte und Transparenz über Geschäftsmodell, Risiken und Kosten.²⁹⁴

²⁹¹ Vgl. §§ 1 und 32a Abs. 1 FM-GwG idF BGBl. I Nr. 98/2021; vgl. Art. 63 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); vgl. § 1 MiCA-VVG.

²⁹² Vgl. § 2 Z 22 und § 32a Abs. 1 FM-GwG idF BGBl. I Nr. 98/2021; vgl. Art. 62 und Art. 63 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

²⁹³ Vgl. Art. 3 Abs. 1 Z 16 lit. a–h sowie Art. 63 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

²⁹⁴ Vgl. Art. 62 Abs. 1, Art. 62 Abs. 1 lit. j, Art. 66 Abs. 1, Art. 67 Abs. 1 und Art. 70 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

Für Konsument:innen stellt dieser Übergang einen wichtigen Fortschritt dar, da erstmals ein qualitativ geregelter Marktsektor entsteht. Gleichzeitig besteht jedoch eine Übergangsphase, in der sowohl frühere VASP-Dienstleister als auch neu zugelassene CASPs tätig sind – mit unterschiedlichen Anforderungen und Schutzstandards.²⁹⁵ Diese Koexistenz erzeugt Rechtsunsicherheit und erschwert es Nutzer:innen, das tatsächliche Risikoniveau eines Dienstleisters zu beurteilen.

5.3.2 Zulassungsvoraussetzungen und laufende Pflichten

Die FMA hat eine eigene „Roadmap für Crypto-Asset Service Provider“ veröffentlicht, die die Anforderungen an Zulassungsanträge konkretisiert.²⁹⁶ Diese Anforderungen gehen deutlich über die bisherigen geldwäscherechtlichen Verpflichtungen hinaus und sollen ein Mindestniveau an technischer, organisatorischer und finanzieller Stabilität gewährleisten.

Zu den zentralen materiellen Pflichten zählen:

- (1) Organisations- und Governance pflichten: CASPs müssen über eine klare Aufbau- und Ablauforganisation, angemessene Geschäftsleiter, Compliance-Funktionen, interne Kontrollsysteme und transparente Risikomanagementprozesse verfügen.²⁹⁷ Für Konsument:innen bedeutet dies, dass Anbieter künftig nicht mehr in intransparenten oder informellen Strukturen tätig sein dürfen.
- (2) Kapital- und Liquiditätsanforderungen: Die MiCA verlangt je nach Dienstleistungstyp Mindestkapitalanforderungen. Anbieter müssen jederzeit in der Lage sein, operationelle Risiken – etwa technische Störungen oder Marktvolatilität – finanziell abzufedern.²⁹⁸ Diese Anforderungen reduzieren zwar das Risiko eines ungeordneten Marktaustritts, ersetzen jedoch keinen echten Insolvenzschutz für Konsument:innen.
- (3) IT-Sicherheit und Kontinuitätsmanagement: Die FMA verlangt detaillierte IT-Sicherheitskonzepte, Notfallpläne und Systeme zur Sicherstellung der Wiederaufnahme des Betriebs.²⁹⁹ Dennoch bestehen weiterhin Risiken, da selbst streng regulierte Märkte nicht vor Cyberangriffen, technischen Defekten oder Angriffsflächen in Smart-Contracts geschützt sind. Für Konsument:innen bleibt unklar, inwiefern CASPs im Schadensfall haften.
- (4) Umgang mit Kundengeldern und Kryptobeständen: CASPs müssen Kundengelder und eigene Unternehmensmittel getrennt halten und Verfahren implementieren, die sicherstellen, dass die

²⁹⁵ Vgl. Art. 63 Abs. 1 und Art. 143 Abs. 3 Verordnung (EU) 2023/1114 (MiCA).

²⁹⁶ Vgl. Finanzmarktaufsicht (FMA), *Roadmap für Crypto-Asset Service Provider (CASP)*.

²⁹⁷ Vgl. Art. 62 Abs. 1, Art. 66 Abs. 1 und Art. 68 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

²⁹⁸ Vgl. Art. 67 Abs. 1 und 2 sowie ErwGr 73 Verordnung (EU) 2023/1114 (MiCA).

²⁹⁹ Vgl. Art. 62 Abs. 1 lit. j Verordnung (EU) 2023/1114 (MiCA); vgl. Art. 6 Abs. 1 und Art. 11 Abs. 1 Verordnung (EU) 2022/2554 (DORA); vgl. Finanzmarktaufsicht (FMA), *Roadmap für Crypto-Asset Service Provider (CASP)*.

Bestände der Kund:innen jederzeit nachvollziehbar und eindeutig zuordenbar sind.³⁰⁰ Diese Trennung soll verhindern, dass Vermögenswerte im Insolvenzfall automatisch in die Masse fallen, garantiert aber keine vollständige Herausgabesicherheit, da die zivilrechtliche Qualifikation von Token weiterhin nicht abschließend geklärt ist.

(5) Beschwerdemanagement und Transparenzpflichten: Dienstleister müssen leicht zugängliche Beschwerdeverfahren einrichten und Konsument:innen umfassend über Risiken, Kosten und Funktionsweisen der angebotenen Dienste informieren.³⁰¹ Die Wirksamkeit solcher Informationspflichten ist jedoch begrenzt, da viele Konsument:innen technische Risiken – insbesondere bei DeFi-Protokollen – nicht erfassen können.

5.3.3 Aufsichtsinstrumente und Eingriffsmöglichkeiten der FMA

Mit dem MiCA-VVG erhält die FMA zusätzliche Eingriffsbefugnisse, um den Kryptomarkt zu überwachen und Verstöße zu sanktionieren. Die wichtigsten Instrumente sind:

(1) Untersagung und Widerruf von Tätigkeiten: Die FMA kann Tätigkeiten untersagen, wenn sie ohne erforderliche Zulassung erfolgen, und CASP-Bewilligungen widerrufen, wenn schwerwiegende Verstöße vorliegen.³⁰²

(2) Verwaltungsstrafen und Marktmissbrauchsaufsicht: Österreich sanktioniert Marktmissbrauch – einschließlich Insiderhandel und Marktmanipulation – im Kryptobereich ausschließlich verwaltungsstrafrechtlich.³⁰³ Diese geringere Sanktionstiefe im Vergleich zu traditionellen Finanzmärkten wirft erhebliche Fragen der Abschreckungswirkung und Fairness auf.

(3) Warnmeldungen und Öffentlichkeitsarbeit: Die FMA veröffentlicht regelmäßig Warnungen zu unseriösen oder nicht registrierten Kryptoplattformen.³⁰⁴ Diese Meldungen erhöhen die Transparenz zwar erheblich, ersetzen aber kein materielles Schutzsystem: Konsument:innen, die auf betrügerische Angebote hereingefallen sind, erhalten dadurch weder Rückerstattung noch Rechtsansprüche.

(4) Eingriff bei geldwäscherechtlichen Verstößen: Bei Verstößen gegen das FM-GwG können die FMA-Registrierungen widerrufen oder Maßnahmen zur internen Kontrolle anordnen. Für

³⁰⁰ Vgl. Art. 70 Abs. 1 und 2 Verordnung (EU) 2023/1114 (MiCA).

³⁰¹ Vgl. Art. 66 Abs. 1 und 2 sowie Art. 71 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

³⁰² Vgl. § 3 Abs. 1 und § 4 Abs. 1 MiCA-VVG; vgl. Art. 63 Abs. 1, Art. 64 Abs. 1 lit. c sowie Art. 102 Abs. 1 lit. a Verordnung (EU) 2023/1114 (MiCA).

³⁰³ Vgl. Art. 86–88, Art. 102 Abs. 1 und Art. 111 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); vgl. § 22 Abs. 1 MiCA-VVG.

³⁰⁴ Vgl. Finanzmarktaufsicht (FMA), *Warnmeldungen zu nicht konzessionierten Anbietern*, abrufbar auf der Website der FMA.

Konsument:innen bedeutet dies jedoch nicht notwendigerweise ein Mehr an Schutz, da solche Eingriffe vor allem systembezogene Risiken adressieren.³⁰⁵

5.4 Nationale Schutzlücken im österreichischen Kryptorecht

Trotz der fortschreitenden Regulierung durch das FM-GwG, das MiCA-VVG und das kapitalmarktrechtliche Umfeld bestehen im österreichischen Recht weiterhin erhebliche Schutzdefizite für Konsument:innen. Diese Lücken ergeben sich nicht aus einzelnen Versäumnissen, sondern aus der strukturellen Fragmentierung des Rechtsrahmens, der technischen Besonderheit digitaler Vermögenswerte sowie der Tatsache, dass zentrale Risikofaktoren des Kryptomarktes bislang nicht oder nur unzureichend berücksichtigt werden.³⁰⁶ Die bestehenden Normen adressieren Teilaspekte des Marktes, doch kein Gesetz bietet ein in sich geschlossenes Verbraucherschutzsystem. Dadurch bleibt der Schutz der Konsument:innen abhängig von Einzelfallkonstellationen, Anbieterstrukturen und dem technischen Verständnis der Nutzer:innen.

5.4.1 Fehlende zivilrechtliche Kodifikation der Rechtsnatur von Kryptowerten

Eine der zentralen Lücken besteht in der fehlenden gesetzlichen Definition der Rechtsnatur von Kryptowerten im österreichischen Zivilrecht. Weder das Allgemeine Bürgerliche Gesetzbuch (ABGB) noch andere zentrale zivilrechtliche Kodifikationen enthalten Bestimmungen, die eindeutig festlegen, ob Token als Sachen, Forderungen, Rechte eigener Art oder bloße digitale Daten zu verstehen sind.³⁰⁷

Diese rechtliche Unbestimmtheit der Einordnung von Kryptowerten führt zu erheblichen praktischen Konsequenzen. So bleibt insbesondere im Bereich des Eigentumsschutzes offen, ob Verbraucher:innen an ihren Tokens ein zivilrechtlich geschütztes Eigentumsrecht innehaben und welche Rechtsfolgen daraus resultieren. Auch hinsichtlich möglicher Herausgabe- oder Ersatzansprüche bestehen Unsicherheiten, etwa bei technischen Verlusten, unbefugten Zugriffen oder der Schließung von Plattformen, da häufig unklar ist, auf welche rechtliche Grundlage solche Ansprüche gestützt werden können. Darüber hinaus ist auch die vertragsrechtliche Einordnung von Bedeutung, da sich je nach Ausgestaltung des jeweiligen Tokens unterschiedliche rechtliche Qualifikationen ergeben können und Tokenkaufverträge kaufrechtliche, werkvertragliche oder sonstige vertragliche Elemente aufweisen können. Für Konsument:innen bedeutet dies, dass ihre vermögensrechtliche Position im Konfliktfall unklar

³⁰⁵ Vgl. § 16 Abs. 1, § 22 Abs. 1 und § 32a Abs. 6 FM-GwG idF BGBl. I Nr. 98/2021.

³⁰⁶ Vgl. § 1 FM-GwG; vgl. § 1 MiCA-VVG; vgl. § 1 KMG 2019; vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 9.

³⁰⁷ Vgl. ABGB; vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 9.

bleibt und Ansprüche häufig über allgemeine Schuldrechtsnormen konstruiert werden müssen, die für digitale Vermögenswerte ursprünglich nicht entwickelt wurden. Dieser Zustand widerspricht dem Grundprinzip eines modernen Verbraucherschutzes, wonach Eigentums- und Haftungsfragen klar und vorhersehbar geregelt sein müssen.

5.4.2 Fehlende insolvenzrechtliche Absicherung

Ein weiteres gravierendes Defizit betrifft das Insolvenzrecht. Zwar verpflichtet die MiCA, Dienstleister dazu, Kundengelder und Unternehmensmittel getrennt zu verwahren, doch ersetzt diese organisatorische Trennung nicht die Frage, ob Kryptowerte im Insolvenzfall tatsächlich ausgesondert werden können.³⁰⁸

Da die zivilrechtliche Qualifikation von Kryptowerten vielfach nicht abschließend geklärt ist, bestehen auch im Insolvenzrecht erhebliche Unsicherheiten. Insbesondere bleibt offen, ob bestimmte Token als Sondervermögen zu behandeln sind, ob sie der Insolvenzmasse zuzurechnen sind und ob Verbraucher:innen im Insolvenzfall über Absonderungs- oder Aussonderungsrechte verfügen. Ebenso kann unklar sein, ob sie lediglich die Stellung einfacher Insolvenzgläubiger:innen einnehmen. Internationale Insolvenzfälle großer Kryptoplattformen haben gezeigt, dass das Fehlen klarer Regelungen zur Vermögenstrennung erhebliche Risiken für Nutzer:innen begründen kann. In solchen Konstellationen können selbst Verbraucher:innen, die davon ausgehen, ihre Kryptowerte seien rechtlich geschützt, erhebliche oder sogar vollständige Vermögensverluste erleiden.³⁰⁹ Aus systematischer Sicht ist dies für Konsument:innen besonders risikobehaftet, da Kryptodienstleister aufgrund der Volatilität der zugrunde liegenden Märkte, möglicher Liquiditätsengpässe sowie technischer Risiken strukturell ein erhöhtes Insolvenzrisiko aufweisen.

5.4.3 Kein Entschädigungssystem für Verluste

Im traditionellen Finanzmarkt existieren Mechanismen wie die Einlagensicherung (§ 93 ff BWG) oder Anlegerentschädigungssysteme nach dem Einlagensicherungs- und Anlegerentschädigungsgesetz (ESAEG). Für Kryptowerte existieren solche Systeme nicht.³¹⁰ Dies bedeutet, dass Verluste infolge von Hackerangriffen, technischen Fehlfunktionen oder organisatorischem Fehlmanagement eines Dienstleisters regelmäßig nicht durch Einlagensicherungs- oder vergleichbare Entschädigungssysteme abgesichert sind. Für Verbraucher:innen kann dies zur Folge haben, dass verbraucherschützende Ansprüche in der Praxis nur eingeschränkt wirksam werden, insbesondere wenn der Schaden nicht auf ein

³⁰⁸ Vgl. Art. 70 Abs. 2 Verordnung (EU) 2023/1114 (MiCA).

³⁰⁹ Vgl. KPMG, *The Collapse of FTX* (2022), S. 5–12; vgl. FDIC, *The FDIC's Investigation of Voyager Digital*.

³¹⁰ Vgl. § 93 Abs. 1 BWG; vgl. § 1 Abs. 1 und § 2 Z 2 ESAEG.

nachweisbares Fehlverhalten des Dienstleisters, sondern auf technische Ursachen oder systembedingte Risiken zurückzuführen ist. Selbst bei behördlich beaufsichtigten Dienstleister:innen besteht regelmäßig kein mit dem traditionellen Bankensektor vergleichbarer finanzieller Sicherungsmechanismus, der Vermögensverluste von Konsument:innen ausgleichen könnte.³¹¹ Dies stellt ein grundlegendes strukturelles Defizit des bestehenden Systems dar. Ein Markt, der durch eine hohe technische Komplexität, erhebliche Volatilität und vielfältige operationelle Risiken geprägt ist, würde grundsätzlich stabilisierende Schutzmechanismen erwarten lassen. In der rechts- und wirtschaftspolitischen Diskussion einzelner EU-Mitgliedstaaten werden, daher vereinzelt begrenzte Entschädigungs- oder Sicherungsmodelle für Verluste im Zusammenhang mit Kryptowerten erörtert.³¹²

5.4.4 Unzureichende Haftungsregeln bei technischen Risiken

Kryptowerte gehen mit besonderen technischen Risiken einher: Blockchain-Forks, Smart-Contract-Fehler, Seeds-Verlust, fehlerhafte Schlüsselverwaltung und Angriffe auf Plattformen können ohne menschliches Zutun Vermögenswerte vernichten.³¹³ Das österreichische Zivilrecht kennt jedoch keine spezialgesetzlichen Haftungsnormen, die diesen Besonderheiten Rechnung tragen. Dies führt zu einer Reihe praktischer und rechtlicher Probleme. So tragen Verbraucher:innen häufig die Beweislast dafür, dass ein technischer Fehler oder ein Sicherheitsmangel tatsächlich vom jeweiligen Dienstleister verursacht wurde, was aufgrund der technischen Komplexität der Systeme in der Praxis oftmals nur schwer nachweisbar ist. Hinzu kommt, dass Anbieter:innen in ihren Vertragsbedingungen regelmäßig weitreichende Haftungsbeschränkungen vorsehen. Weitere Unsicherheiten bestehen im Zusammenhang mit Smart Contracts, die rechtlich überwiegend als Softwareanwendungen behandelt werden. Fehler, Programmiermängel oder Sicherheitslücken führen dabei regelmäßig nur dann zu Haftungsansprüchen, wenn ein entsprechendes Verschulden nachgewiesen werden kann. Die Kombination aus komplexen technischen Risiken, schwierigen Nachweisanforderungen und teilweise unzureichenden zivilrechtlichen Haftungsregelungen kann dazu führen, dass Verbraucher:innen trotz bestehender Vertragsverhältnisse ihre Ansprüche nur eingeschränkt oder gar nicht durchsetzen können.³¹⁴

³¹¹ Vgl. § 93 Abs. 1 BWG; vgl. § 2 Z 2 ESAEG; vgl. Art. 70 Abs. 1 und 2 Verordnung (EU) 2023/1114 (MiCA).

³¹² Vgl. OECD, *Financial Consumer Protection Policy Approaches in the Digital Age* (2020).

³¹³ Vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 9; vgl. Schweizer Bundesrat, *DLT-Bericht* (2018), S. 21–23; vgl. OECD, *Financial Consumer Protection Policy Approaches in the Digital Age* (2020), S. 26–30; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), *Digital Law*, 2. Aufl. (2020), S. 90–97.

³¹⁴ Vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 9; vgl. Schweizer Bundesrat, *DLT-Bericht* (2018), S. 21–23; vgl. OECD, *Financial Consumer Protection Policy Approaches in the Digital Age* (2020), S. 26–30; vgl. Binder Grösswang Rechtsanwälte GmbH (Hrsg.), *Digital Law*, 2. Aufl. (2020), S. 90–97.

Kapitel 6

Internationaler Vergleich (USA, China, Japan)

6.1 Zielsetzung und Einordnung des internationalen Vergleichs

Die Regulierung von Kryptowerten entwickelt sich weltweit in sehr unterschiedlicher Geschwindigkeit und mit deutlich divergierenden inhaltlichen Schwerpunkten. Die internationalen Regulierungsansätze unterscheiden sich erheblich. Einige Staaten setzen auf weitreichende Eingriffsbefugnisse und unmittelbar durchsetzbare Aufsichtsmechanismen, während andere einen stärker innovationsorientierten Regulierungsansatz verfolgen oder – wie im Fall Chinas – auf umfassende Beschränkungen und Verbote zurückgreifen. Diese Vielfalt zeigt, dass es keine einheitliche regulatorische Logik gibt, sondern vielmehr unterschiedliche Antworten auf dieselben strukturellen Herausforderungen: hohe technische Komplexität, Informationsasymmetrien, Marktvolatilität, Anonymität und das Fehlen traditioneller Intermediäre. Vor diesem Hintergrund dient der internationale Vergleich nicht der deskriptiven Wiederholung ausländischer Rechtslagen, sondern der analytischen Verortung des unions- und österreichischen Rechtsrahmens. Er soll sichtbar machen, welche Schutzinstrumente andere Staaten entwickelt haben, wie diese ausgestaltet sind und ob sie zur Reduktion jener Verbraucherrisiken beitragen, die im europäischen Kontext – trotz MiCA – weiterhin bestehen. Der Vergleich bildet somit eine methodisch eigenständige Untersuchungsebene, die unmittelbar an die in Kapitel 5 entwickelte Diagnose der Schutzlücken anschließt, diese jedoch durch die Betrachtung alternativer internationaler Modelle ergänzt und vertieft. Die Auswahl der Vergleichsordnungen erfolgt nach drei Kriterien: erstens der internationalen Relevanz der jeweiligen Märkte, zweitens der grundsätzlichen Unterschiedlichkeit ihrer Regulierungsphilosophien und drittens der Bedeutung ihrer Regelungsmodelle für globale Entwicklungen. So stehen die Vereinigten Staaten für eine enforcement-dominierte Aufsichtspraxis, in der Rechtsklarheit häufig erst durch behördliche Maßnahmen und Gerichtsentscheidungen entsteht.³¹⁵ China repräsentiert einen weitgehend verbotsorientierten Ansatz, der große Teile kryptobasierter Aktivitäten strukturell aus dem Finanzsystem ausschließt.³¹⁶ Japan hingegen verfolgt ein stark lizenziertes und institutionell ausdifferenziertes

³¹⁵ Vgl. Middlebrook/Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, William Mitchell Law Review 40 (2014), S. 814 ff., 847; vgl. McDermott, *The Crypto Quandary: Is Bankruptcy Ready?*, Northwestern University Law Review 115 (2021), S. 1951 f.

³¹⁶ Vgl. People's Bank of China ua, *Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading*, 24. 9. 2021; vgl. Financial Stability Board, *Thematic Review on the Global Regulatory Framework for Crypto-asset Activities* (2023), S. 10.

Modell, das durch frühe gesetzliche Regelungen sowie ergänzende Selbstregulierung geprägt ist.³¹⁷

Dieser Dreiklang – Durchsetzungsmodell, Verbotsmodell und Lizenzmodell – dient als analytische Struktur für die folgenden Abschnitte von Kapitel 6. Er ermöglicht eine systematische Untersuchung der jeweiligen Schutzwirkungen, ohne nationale oder unionsrechtliche Rahmenbedingungen zu wiederholen. Zugleich bildet er die Grundlage für die spätere normative Bewertung, welche Elemente ausländischer Modelle geeignet wären, den unionsrechtlichen und österreichischen Verbraucherschutz im Kryptobereich weiterzuentwickeln.

6.2 Regulierungsprofile in komparativer Perspektive

Die globale Regulierung von Kryptowerten ist durch eine bemerkenswerte Divergenz an Ansätzen geprägt, die auf unterschiedliche wirtschaftliche Interessen, institutionelle Strukturen und verfassungsrechtliche Grundannahmen zurückzuführen ist. Für eine verbraucherschutzorientierte Analyse ist wesentlich, wie die Rechtsordnungen Risiken identifizieren, welche Instrumente sie zur Risikobeherrschung einsetzen und in welchem Verhältnis Marktöffnung, technische Innovation und staatliche Kontrolle zueinanderstehen. Der internationale Vergleich zwischen den Vereinigten Staaten, China und Japan zeigt drei ausgeprägt unterschiedliche Regulierungspfade: ein durchsetzungsorientiertes und institutionell fragmentiertes Modell (USA), ein restriktives, auf systemische Risikoblockade ausgerichtete Verbotssystem (China) und ein integrationsorientiertes, technisch-normatives Lizenzsystem (Japan). Diese Ansätze erlauben Rückschlüsse darauf, welche Strukturelemente für ein wirksames Verbraucherschutzsystem erforderlich sind und an welchen Stellen unions- und österreichisches Recht strukturell unterentwickelt bleibt.³¹⁸

³¹⁷ Vgl. Japan, *Payment Services Act* (Act No. 59 of 2009), engl. Übersetzung, S. 38; vgl. ASBJ Secretariat, *About the Practical Solution on the Accounting for Virtual Currencies under the Payment Services Act* (15. 3. 2018), S. 1; vgl. Japan Financial Services Agency, *Report of the Study Group on Virtual Currencies* (21. 12. 2018), S. 2.

³¹⁸ Vgl. Middlebrook/Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, William Mitchell Law Review 40 (2014), S. 813–814; vgl. People's Bank of China ua, *Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading*, 24. 9. 2021, Abs. 1; vgl. Japan Financial Services Agency, *Report of the Study Group on Virtual Currencies*, 21. 12. 2018, S. 2; vgl. Japan, *Payment Services Act* (Act No. 59 of 2009), engl. Übers., S. 38; vgl. Financial Stability Board, *Thematic Review on the Global Regulatory Framework for Crypto-asset Activities* (2023), S. 10; vgl. OECD, *2nd Global Cryptoasset Regulatory Landscape Study* (2024), S. 7.

6.2.1 Vereinigte Staaten: Fragmentierte Zuständigkeit und ex-post-orientiertes Regulierungsmuster

Die Vereinigten Staaten verfügen über keinen einheitlichen Bundesrechtsrahmen für Kryptowerte. Die Regulierung erfolgt vielmehr über ein komplexes Verbundsystem aus Bundesbehörden, einzelstaatlichen Lizenzregimen und gerichtlicher Auslegung vorhandener Finanzmarktgesetze.³¹⁹ Die Securities and Exchange Commission (SEC) qualifiziert Token regelmäßig als „investment contracts“ iSd Howey-Tests und unterwirft sie damit dem bundesrechtlichen Wertpapierrecht. Die Commodity Futures Trading Commission (CFTC) beansprucht Aufsicht über „digital commodities“, insbesondere über Derivate und bestimmte Spotmärkte. Parallel dazu übernehmen Financial Crimes Enforcement Network (FinCEN), Office of the Comptroller of the Currency (OCC), Federal Reserve, Federal Deposit Insurance Corporation (FDIC) und Consumer Financial Protection Bureau (CFPB), Aufgaben im Geldwäsche-, Banken- und Zahlungsverkehrsbereich. Die staatliche „BitLicense“ des Bundesstaates New York schafft darüber hinaus ein eigenständiges, streng formalisiertes Lizenzregime.

Diese institutionelle Pluralität führt zu einer regulatorischen Landschaft, die aus Verbrauchersicht erhebliche Rechtsunsicherheit erzeugt. Verbraucher müssen im Streitfall häufig erst klären, ob ein Produkt als „security“, „commodity“ oder Zahlungsdienst qualifiziert wird und welche Behörde zuständig ist. Die Literatur weist darauf hin, dass diese Unsicherheit gerade Kleinanleger benachteiligt, da sie die Rechtsqualität eines Angebots erst ex post erkennen können.³²⁰ Die Aufsichtspraxis der SEC bestätigt diese Diagnose, zahlreiche Klagen gegen Token-Emittenten wurden erst nach Schädigungen geführt, wodurch das System stark reaktiv und einzelfallbezogen bleibt.³²¹

³¹⁹ Vgl. Middlebrook/Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, William Mitchell Law Review 40 (2014), S. 814; vgl. Congressional Research Service, *Cryptocurrency: The Economics of Money and Selected Policy Issues* (2020), S. 21–23; vgl. 23 NYCRR § 200.3(a); vgl. McDermott, *The Crypto Quandary: Is Bankruptcy Ready?*, Northwestern University Law Review 115 (2021), S. 1952.

³²⁰ Vgl. Middlebrook/Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, William Mitchell Law Review 40 (2014), S. 814–815; vgl. Congressional Research Service, *Cryptocurrency: The Economics of Money and Selected Policy Issues* (2020), S. 21–22; vgl. Cambridge Centre for Alternative Finance, *Global Cryptoasset Regulatory Landscape Study* (2020), S. 14.

³²¹ Vgl. Oxford Law Blog, *The Unintended Consequences of SEC Crypto Enforcement Actions*, 15. 1. 2025; vgl. Georgetown Law Center on Business and Technology Law, *Beyond Enforcement: The SEC's Shifting Playbook on Crypto Regulation*, 9. 5. 2025; vgl. Chernin/Moran/Letson, *SEC Cryptocurrency Enforcement: 2024 Update*, Cornerstone Research (2025); vgl. O'Melveny & Myers LLP, *The SEC May Signal a New Crypto Enforcement Approach*, 4. 2. 2025.

Die jüngsten Gesetzesinitiativen – insbesondere der GENIUS Act 2025, der erstmals einen bundesweiten Rechtsrahmen für Zahlungs-Stablecoins schafft,³²² sowie die Digital Asset Market Structure-Vorhaben wie H.R.4763³²³ – markieren zwar eine Annäherung an kohärentere Strukturen, bleiben jedoch sektorbezogen und lösen die institutionelle Fragmentierung nicht auf. Verbraucher erhalten dadurch zwar punktuell stärkere Schutzmechanismen (z. B. strengere Reservestandards für Stablecoins), profitieren jedoch weiterhin nicht von einem vollständigen, kodifizierten Ex-ante-Schutzsystem, wie es unionsrechtlich mit MiCA intendiert ist. Aus verbraucherschutzrechtlicher Perspektive bildet der US-Ansatz daher ein Modell hoher Durchsetzungskraft, aber begrenzter präventiver Wirksamkeit.

6.2.2 China: Verbotsorientiertes Risikoblockademodell mit selektivem privatrechtlichen Eigentumsschutz

China verfolgt seit 2021 einen nahezu vollständigen Ausschluss privater Kryptotransaktionen. Durch ein gemeinsames Rundschreiben der People's Bank of China (PBoC) und weiterer Behörden wurden sowohl Mining-Tätigkeiten als auch der Handel mit Kryptowerten verboten; zugleich wurde klargestellt, dass auch Dienstleistungen ausländischer Börsen gegenüber inländischen Nutzern unzulässig sind. Dieser Ansatz beruht auf einer staatlichen Risikotheorie, die spekulative Blasen, Kapitalflucht und geldpolitische Destabilisierung als systemische Gefahren einstuft und durch umfassende Marktunterbindung einzudämmen versucht.³²⁴ Bemerkenswert ist, dass das chinesische Recht zwischen öffentlich-rechtlicher Marktregulierung und zivilrechtlicher Behandlung virtueller Vermögenswerte differenziert. Während Handel, Mining und Vermittlung von Kryptowerten öffentlich-rechtlich untersagt sind, bleiben zivilrechtliche Fragen im Einzelfall – etwa im Rahmen von Rückabwicklungs- oder Bereicherungsansprüchen – gerichtlich zu klären, ohne dass Kryptowährungen als sachenrechtliches Eigentum anerkannt würden.³²⁵ Aus verbraucherschutzrechtlicher Sicht führt dies zu einer paradoxen Konstellation. Der Staat verhindert Risiken durch vollständige

³²² Vgl. GENIUS Act of 2025, 118th Congress, Sec. 2 (Purposes).

³²³ Vgl. United States Congress, *H.R. 4763 – Financial Innovation and Technology for the 21st Century Act*, 118th Congress (2023), Long Title.

³²⁴ Vgl. People's Bank of China u. a., *Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading*, 24.09.2021, Abs. 1–2; vgl. National Development and Reform Commission u. a., *Notice on Regulating and Rectifying Virtual Currency "Mining" Activities*, 03.09.2021, Abs. 1; vgl. Financial Stability Board, *Thematic Review on the Global Regulatory Framework for Crypto-asset Activities*, 2023, S. 2; vgl. Supreme People's Court (PRC), *Minutes of the National Courts' Civil and Commercial Trial Work Conference*, 2021, Abs. 31.

³²⁵ Vgl. People's Bank of China u. a., *Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading*, 24.09.2021, Abs. 1; vgl. Art. 127 General Principles of the Civil Law of the People's Republic of China, 2017.

Marktunterbindung, schafft jedoch kein positives Schutzsystem für jene Nutzer, die weiterhin – oftmals inoffiziell – investieren.³²⁶ Anders als in den USA existieren daher keine aufsichtsrechtlichen Mechanismen, kein Haftungsrahmen und keine Informationspflichten. Der Schutz ist ausschließlich auf privatrechtliche Eigentumspositionen beschränkt. Dieses Modell zeigt, dass Restriktion zwar kurzfristig Risiken reduzieren kann, aber kein funktionierendes Verbraucherschutzsystem im materiellen Sinn ersetzt. Für unions- und österreichische Rechtsentwicklung ist dabei lehrreich, dass Marktunterbindung nicht automatisch Schutz ersetzt und dass ein Verbot ohne begleitende Mechanismen zu einem rechtsfreien Raum führt.

6.2.3 Japan: Integratives Lizenzmodell mit technischer Standardsetzung und Selbstregulierung

Japan gilt als eine der ersten Rechtsordnungen, die ein kohärentes, technikaffines und präventiv orientiertes Regelsystem für Kryptowerte entwickelt hat. Ausgangspunkt waren die Ereignisse rund um den Zusammenbruch der Börse Mt. Gox 2014, die zu erheblichen Verbraucherverlusten führten und grundlegende gesetzgeberische Maßnahmen auslösten.³²⁷ Bereits 2016 wurden durch Änderungen des Payment Services Act (PSA) ein einheitlicher Registrierungszwang für Kryptodienstleister, Mindestkapitalanforderungen, AML/CFT-Standards, IT-Sicherheitsvorgaben und Trennungsgebote für Kundengelder eingeführt.³²⁸ Eine Besonderheit des japanischen Modells ist die institutionalisierte Selbstregulierung. Die Japan Virtual and Crypto Assets Exchange Association (JVCEA) wurde durch die Financial Services Agency (FSA) als Selbstregulierungsorganisation anerkannt und erlässt technische und organisatorische Detailregelungen, etwa zu Hebelbegrenzungen, Token-Listungsanforderungen und IT-Standards.³²⁹ Diese Regeln wirken als verbindliche branchenspezifische Mindeststandards, die von der staatlichen Aufsicht überwacht werden. Die japanische Literatur

³²⁶ Vgl. People's Bank of China u. a., Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading, 24.09.2021, Abs. 1; vgl. Art. 127 General Principles of the Civil Law of the People's Republic of China, 2017; vgl. Financial Stability Board, Thematic Review on the Global Regulatory Framework for Crypto-asset Activities, 2023, S. 2.

³²⁷ Vgl. Japan Financial Services Agency, Examination of the Regulatory Systems Related to Cryptoassets, 10.04.2025, S. 2; vgl. Nomura Research Institute, Virtual Currencies: Issues Remain, 2016, S. 2; vgl. Art. 63-2 Payment Services Act (Japan, engl. Übers.); vgl. Legal Landscapes Governing Digital Tokens in Japan, 2022, S. 11.

³²⁸ Vgl. Art. 63-2, 63-5, 63-10 und 63-11 Payment Services Act (Japan, Gesetzesnovelle 2016); vgl. Act on Prevention of Transfer of Criminal Proceeds (Japan).

³²⁹ Vgl. Art. 63-2 ff., Art. 87 Payment Services Act (Japan); vgl. Financial Services Agency of Japan, Certification of a Self-Regulatory Organization for Crypto-asset Exchange Services, 24.10.2018; vgl. Japan Virtual and Crypto Assets Exchange Association, Self-Regulatory Rules; vgl. Financial Stability Board, Crypto-asset Activities: Regulatory Approaches, 2019.

betont, dass dadurch technische Expertise und staatliche Kontrollstrukturen systematisch miteinander verknüpft werden.³³⁰

Darüber hinaus integriert Japan Kryptowerte zunehmend in das allgemeine Finanzmarktrecht, indem bestimmte Token-Derivate und Anlageprodukte ausdrücklich unter den Financial Instruments and Exchange Act (FIEA) fallen und somit Marktmissbrauchs- und Insiderhandelsregeln anwendbar werden.³³¹ Diese gesetzestechnische Einbettung gewährleistet eine starke präventive Schutzwirkung, insbesondere in Bezug auf Vermögenszuordnung, Insolvenzbehandlung und Informationsstandards. Zivilrechtliche Strukturentscheidungen wie die klare Zuordnung von Eigentumsrechten und die Trennung von Kunden- und Eigenvermögen bilden eine wesentliche Grundlage für den Schutz von Nutzer:innen im Kryptomarkt. Fehlen solche Strukturen, entstehen insbesondere im Insolvenz- und Durchsetzungskontext erhebliche Risiken für Verbraucher:innen.

Im Ergebnis bildet das japanische Modell ein konsistentes Zusammenspiel aus technischer Standardsetzung, institutioneller Aufsicht und zivilrechtlicher Integration. Damit stellt es das wohl präventivste und strukturell geschlossenste Verbraucherschutzregime unter den hier betrachteten Rechtsordnungen dar.

6.3 Strukturelle Vergleichsanalyse der untersuchten Regulierungsmodelle

Die Gegenüberstellung der Regulierungsordnungen der USA, Chinas und Japans zeigt drei grundlegend verschiedene Ansätze, die jeweils unterschiedliche Annahmen über staatliche Steuerungsfähigkeit, marktwirtschaftliche Dynamik und Schutzbedarfe der Verbraucher:innen widerspiegeln. Eine systematische Analyse dieser Modelle erlaubt es, zentrale Strukturprinzipien zu identifizieren, die für den unions- und österreichischen Rechtsrahmen von besonderer Relevanz sind. Die Untersuchung ergibt, dass keines der drei Systeme ein vollständig kohärentes oder umfassendes Verbraucherschutzregime bereitstellt; jedoch eröffnet jedes Modell spezifische Einsichten, die zur Schließung der im europäischen Kontext festgestellten Schutzlücken beitragen können.

³³⁰ Vgl. Art. 63-2 ff., Art. 87 Payment Services Act (Japan); vgl. Financial Services Agency of Japan, *Certification of a Self-Regulatory Organization for Crypto-asset Exchange Services*, 24.10.2018; vgl. Financial Stability Board, *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements*, 2020.

³³¹ Vgl. Art. 2 para. 8, Art. 28 para. 1, Art. 157, Art. 166 para. 1 Financial Instruments and Exchange Act (Japan); vgl. Art. 1-3 Cabinet Office Ordinance on Financial Instruments Business (Japan).

6.3.1 Regulierungsphilosophie: Ex-post-Durchsetzung, Risikoblockade und präventive Lizenzierung

Die drei untersuchten Modelle lassen sich regulierungstheoretisch entlang einer Achse einordnen, die von nachgelagerter Durchsetzung (USA) über systemische Verdrängung (China) bis hin zu technikgestützter Ex-ante-Prävention (Japan) reicht.³³²

Im US-amerikanischen System dominiert ein enforcement-basiertes Paradigma, das davon ausgeht, dass Innovation gefördert und Marktversagen primär durch behördliche oder gerichtliche Maßnahmen im Nachhinein korrigiert werden sollen. Dieses Modell bietet hohe Flexibilität, führt aber zu einer erheblichen Rechtsunsicherheit für Verbraucher:innen, da Risikotransparenz erst nach Schädigungen entsteht.³³³

Das chinesische System beruht dagegen auf einer makropolitischen Risikoblockadelogik, die spekulative Blasen und finanzielle Instabilität als staatsgefährdend einstuft und durch vollständige Marktunterbindung neutralisiert.³³⁴ Verbraucherschutz wird hier als Funktion der Marktverhinderung verstanden; ein materielles Schutzsystem wird jedoch nicht aufgebaut, weshalb verbleibende Nutzer:innen faktisch ohne institutionellen Schutz agieren.³³⁵

Das japanische System schließlich folgt einer präventiven Lizenzierungslogik, in der staatliche Aufsicht, technische Standards und Selbstregulierung eng miteinander verflochten sind.³³⁶

Dieser Ansatz erkennt die Unvermeidbarkeit technologischer Risiken an, versucht diese jedoch ex ante zu begrenzen, statt ex post zu sanktionieren oder pauschal zu verbieten.

Aus Verbrauchersicht zeigt die Analyse, dass Präventionsmechanismen – insbesondere solche, die auf technische Mindeststandards und klare Vermögenszuordnungen beruhen – eine höhere Schutzqualität aufweisen als nachgelagerte Durchsetzung oder Marktunterdrückung.³³⁷

³³² Activities, 2019, S. 5.

Vgl. Middlebrook/Hughes, William Mitchell Law Review 40, 2014, S. 814; vgl. PBoC u. a., Notice on Virtual Currency Trading, 24.09.2021, Abs. 1; vgl. Art. 63-2 Abs. 1 Payment Services Act (Japan); vgl. FSA Japan, Crypto-asset Exchange Services Regulation, 2019, S. 2; vgl. FSB, Crypto-asset Activities, 2019, S. 5.

³³³ Vgl. Congressional Research Service, Cryptocurrency: Selected Policy Issues, R47425, Washington D.C. 2023, S. 2; vgl. Middlebrook/Hughes, Regulating Cryptocurrencies in the United States: Current Issues and Future Directions, William Mitchell Law Review 40, 2014, S. 842; vgl. U.S. House of Representatives, The Future of Digital Assets: Identifying the Regulatory Gaps in the Digital Asset Market Structure, Hearing vom 27.04.2023, S. 34.

³³⁴ Vgl. People's Bank of China u. a., Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading, 24.09.2021, Abs. 1–3; vgl. State Council of the PRC, China's Financial Stability Report 2022, S. 1.

³³⁵ Vgl. People's Bank of China u. a., Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading, 24.09.2021; vgl. State Council of the PRC, China's Financial Consumer Protection Report 2021, S. 4; vgl. State Council of the PRC, China's Financial Stability Report 2022, S. 1.

³³⁶ Vgl. Art. 63-2 Abs. 1, Art. 63-11 Abs. 1 Payment Services Act (Japan); vgl. Financial Services Agency of Japan, Certification of a Self-Regulatory Organization for Crypto-asset Exchange Services, 24.10.2018.

³³⁷ Vgl. Art. 63-11 Abs. 1, Art. 63-11-2 Abs. 1 Payment Services Act (Japan); vgl. Congressional Research Service, Cryptocurrency: Selected Policy Issues, R47425, Washington D.C. 2023, S. 20; vgl. People's Bank

6.3.2 Institutionelle Architektur: Fragmentierung, Zentralisierung und funktionale Koordination

Die institutionellen Strukturen der untersuchten Staaten unterscheiden sich erheblich und erklären maßgeblich die jeweilige Schutzwirkung.

In den USA führt die fragmentierte Behördenlandschaft zu einem Nebeneinander unterschiedlicher Qualifikationen und Aufsichtsregime.³³⁸ Diese institutionelle Vielfalt ermöglicht zwar eine flexible Anpassung an neue Produkte, erschwert jedoch die Konsistenz der Rechtsanwendung und führt zu erheblichen Informationsnachteilen für Verbraucher:innen.

China besitzt dagegen ein hochgradig zentralisiertes System, in dem politische Organe, Zentralbank und Cyberspace Administration ein kohärentes Verbots- und Kontrollregime durchsetzen.³³⁹ Institutionelle Fragmentierung spielt keine Rolle und vielmehr wird Regulierung durch administrative Einheitlichkeit ersetzt. Diese Struktur stärkt zwar die Durchsetzungskraft, erzeugt jedoch kein funktionales Verbraucherschutzsystem im materiellen Sinn.³⁴⁰

Japan kombiniert wiederum staatliche Aufsicht mit delegierter Selbstregulierung. Die JVCEA verfügt über technische Expertise und erstellt bindende Standards, während die FSA-Aufsicht, Konsolidierung und Sanktion übernimmt.³⁴¹ Diese funktionale Koordination führt zu einer stabilen und innovationskompatiblen Architektur, die sich als effektiver erweist als rein staatliche oder rein administrative Modelle.

6.3.3 Vermögenszuordnung, Eigentumsstruktur und Insolvenzschutz

Eine der zentralen Erkenntnisse der vergleichenden Analyse betrifft die Frage, wie Regime die Vermögenszuordnung und den Insolvenzschutz ausgestalten – ein Bereich, der im unions- und österreichischen Recht bislang unzureichend geregelt ist. In den USA existiert bislang kein umfassender eigenständiger Rechtsrahmen für digitale Vermögenswerte und ihre rechtliche Behandlung erfolgt daher im Ausgangspunkt unter Rückgriff auf bestehende echtskategorien.³⁴²

of China u. a., Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading, 24.09.2021, Abs. 1.

³³⁸ Vgl. Congressional Research Service, Cryptocurrency: Selected Policy Issues, R47425, Washington D.C. 2023, S. 20.

³³⁹ Vgl. People's Bank of China u. a., Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading, 24.09.2021, Einleitung, Abs. 1; vgl. Cyberspace Administration of China, Notice on Further Preventing the Risks of Virtual Currency Trading, 2021, Art. 3, 4.

³⁴⁰ Vgl. People's Bank of China u. a., Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading, 24.09.2021, Einleitung, Abs. 1; vgl. State Council of the PRC, China's Financial Consumer Protection Report 2021, S. 4.

³⁴¹ Vgl. Financial Services Agency of Japan, Certification of a Self-Regulatory Organization for Crypto-asset Exchange Services, 24.10.2018; vgl. Art. 63-17 Abs. 1 Payment Services Act (Japan).

³⁴² Vgl. Congressional Research Service, Cryptocurrency: Selected Policy Issues, R47425, Washington D.C. 2023.

Ein ausdrücklicher Token-Eigentumsbegriff fehlt, der Insolvenzschutz ist weitgehend vertraglich zu lösen und daher für Verbraucher:innen unsicher.³⁴³

Obwohl der Handel mit Kryptowerten und die Erbringung kryptobezogener Dienstleistungen in China weitgehend untersagt sind, bleibt die zivilrechtliche Behandlung bereits bestehender Token-Bestände uneinheitlich und in wesentlichen Punkten rechtlich ungeklärt.³⁴⁴

Japan stellt als einzige der drei Rechtsordnungen explizite zivilrechtliche Strukturen bereit, einschließlich Trennung von Kunden- und Unternehmensvermögen,

Sicherstellungsmechanismen im Insolvenzfall und expliziter Regeln zur

Vermögensverwahrung.³⁴⁵ Solche zivilrechtlichen Festlegungen für ein funktionierendes Verbraucherschutzregime zentral sind, da ohne klare Zuordnung die Durchsetzung von Herausgabe- oder Schadensersatzansprüchen im Insolvenzfall unklar bleibt.

6.4 Normative Schlussfolgerungen für das unions- und österreichische Verbraucherschutzrecht

Der internationale Vergleich verdeutlicht, dass die untersuchten Rechtsordnungen zwar keine abschließenden oder vollständig konsistenten Verbraucherschutzsysteme geschaffen haben, jedoch jeweils Strukturprinzipien enthalten, die zur Weiterentwicklung des unions- und österreichischen Rechtsrahmens beitragen können. Die MiCA bildet zwar einen bedeutenden Schritt hin zu einem einheitlichen Ordnungsrahmen, doch bleibt sie in zentralen Bereichen – insbesondere der zivilrechtlichen Vermögenszuordnung, der technischen Risikoprävention und des Insolvenzschutzes – unvollständig.³⁴⁶ Vor diesem Hintergrund lassen sich aus den Modellen der USA, Chinas und Japans drei zentrale normative Handlungslinien ableiten, die für eine kohärente Weiterentwicklung des Verbraucherschutzes im Kryptobereich maßgeblich sind.

6.4.1 Erfordernis eines erweiterten, kohärenten Ex-ante-Schutzsystems

Der unionsrechtliche Ansatz konzentriert sich primär auf Marktorganisation, Transparenzpflichten und Aufsichtsmechanismen.³⁴⁷ Demgegenüber zeigt besonders das japanische Modell, dass ein wirksamer Verbraucherschutz im Kryptobereich nicht allein durch organisatorische Mindeststandards erreicht wird, sondern technische, zivilrechtliche und insolvenzrechtliche Mechanismen voraussetzt, die auf präventive Risikoabwehr ausgerichtet

³⁴³ Vgl. Congressional Research Service, *Cryptocurrency: Selected Policy Issues*, R47425, Washington D.C. 2023; vgl. McDermott, Megan, *The Crypto Quandary: Is Bankruptcy Ready?*, Northwestern University Law Review 115, 2021, S. 1932.

³⁴⁴ Vgl. People's Bank of China u. a., *Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading*, 24.09.2021.

³⁴⁵ Vgl. Art. 63-11 Abs. 1, Art. 63-11-2 Abs. 1, Art. 63-17 Abs. 1 Payment Services Act (Japan).

³⁴⁶ Vgl. Art. 1 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); ErwGr 6, 8, 9 und 10 MiCA.

³⁴⁷ Vgl. Art. 1 Abs. 1, Art. 4 Abs. 1, Art. 53 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); ErwGr 9 MiCA.

sind. Die JVCEA-Regeln demonstrieren, wie verbindliche Mindeststandards zu Cyber-Sicherheit, Token-Listungsprüfung und Verwahrprozessen einen direkten Schutz für Verbraucher:innen erzeugen.³⁴⁸

Ein unionsreicher Ansatz müsste daher über MiCA hinaus verpflichtende technische Sicherheitsstandards definieren, die nicht nur organisatorisch, sondern technologisch verankert werden. Dies gilt insbesondere für Verwahrsysteme, Smart-Contract-Infrastruktur, Schlüsselverwaltung und Liquidationsmechanismen. Die Rechtswissenschaft hat mehrfach betont, dass technische Risikoprävention ein unverzichtbarer Bestandteil digitaler Vermögensregime ist.³⁴⁹

6.4.2 Kodifikation eines unionsweit einheitlichen Token-Eigentums- und Insolvenzschutzregimes

Der internationale Vergleich zeigt weiterhin, dass der unions- und österreichische Rechtsrahmen bei der zentralen Frage der Vermögenszuordnung unterentwickelt ist. Während die USA tokenbezogene Rechte faktisch über Vertragsrecht und Wertpapierqualifikation lösen und China zumindest die zivilrechtliche Eigentumsfähigkeit von Token anerkennt, verfügt Japan über ein formalisiertes System der Vermögenstrennung und Insolvenzabsicherung.³⁵⁰

Ein funktionsfähiger Verbraucherschutz ein klares, normativ festgeschriebenes Konzept zur Vermögenszuordnung erfordert, da ansonsten die Durchsetzung von Herausgabe- oder Ersatzansprüchen unterbleibt oder auf allgemeine Schuldrechtsgrundsätze zurückfällt. Der unionsrechtliche Gesetzgeber sollte daher einheitliche Mindeststandards schaffen, die klar festlegen, wie Kryptowerte zivilrechtlich einzuordnen sind, insbesondere ob sie als sachenrechtlich geschützte Vermögenswerte, schuldrechtliche Ansprüche oder eigenständige Rechtspositionen (*sui generis*) zu qualifizieren sind. Ebenso sollte eindeutig geregelt werden, unter welchen Voraussetzungen Kryptowerte im Insolvenzfall aussonderungs- oder absonderungsfähig sind und wie Kundengelder sowie Kryptowerte in Insolvenzverfahren zu behandeln sind. Dadurch könnten bestehende Rechtsunsicherheiten reduziert und der Schutz von Verbraucher:innen innerhalb der Europäischen Union gestärkt werden.

³⁴⁸ Vgl. Art. 63-11 Abs. 1, Art. 63-11-2 Abs. 1 Payment Services Act (Japan); vgl. Financial Services Agency of Japan, Certification of a Self-Regulatory Organization for Crypto-asset Exchange Services, 24.10.2018.

³⁴⁹ Vgl. ErwGr 6, 8 und 9 Verordnung (EU) 2023/1114 (MiCA); vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, Paris 2020, S. 19; vgl. Financial Stability Board, Regulation, Supervision and Oversight of Global Stablecoin Arrangements, Basel 2020, S. 4.

³⁵⁰ Vgl. ErwGr 6, 8 und 9, Art. 1 Abs. 1, Art. 4 Abs. 1, Art. 53 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); vgl. Art. 63-11 Abs. 1, Art. 63-11-2 Abs. 1 Payment Services Act (Japan).

6.4.3 Stärkung der institutionellen Koordinationsmechanismen nach dem Vorbild funktionaler Modelle

Die Vergleichsanalyse zeigt, dass institutionelle Fragmentierung – wie in den USA – die Transparenz und Rechtssicherheit erheblich beeinträchtigt.³⁵¹ Gleichzeitig zeigt China, dass vollständige Zentralisierung ohne funktionale Differenzierung kein materielles Schutzsystem ersetzt. Japan liefert mit seiner Verzahnung von FSA und JVCEA ein Modell funktionaler Koordination, wobei staatliche und selbstregulative Elemente komplementär wirken.³⁵² Für die Europäische Union bedeutet dies, dass die Zuständigkeiten von ESMA, EBA und den nationalen Aufsichtsbehörden stärker harmonisiert und präzisiert werden sollten. Dies betrifft insbesondere die Entwicklung konsistenter Durchsetzungsstrategien, die Schaffung abgestimmter technischer Mindeststandards, den Ausbau europäischer Aufsichts- und Überwachungstechnologien sowie eine klare Kompetenzabgrenzung bei Marktmissbrauchstatbeständen. Eine derart koordinierte Aufsichtsarchitektur könnte die Gefahr unterschiedlicher oder widersprüchlicher Auslegungen innerhalb der Europäischen Union erheblich reduzieren und zugleich zu einer effektiveren Durchsetzung der regulatorischen Vorgaben sowie zu einem höheren Schutzniveau für Verbraucher:innen beitragen.

6.4.4 Integration eines technologiebezogenen Risikorahmens in das europäische Aufsichtsmodell

Der Vergleich zeigt, dass die Risikoqualität digitaler Vermögenswerte sich grundlegend von klassischen Finanzinstrumenten unterscheidet. USA und EU adressieren diese Risiken primär über Markttransparenz und Enforcement, während Japan konkrete technologische Anforderungen stellt.³⁵³ Die Rechtsentwicklung im Kryptobereich erfordert daher eine explizite Einbettung technischer Risikoanalyse in die Aufsicht, einschließlich:

Bewertung von Protokollrisiken (z. B. Fork-Risiken),³⁵⁴

Analyse von Smart-Contract-Schwachstellen,

Überwachung dezentraler Liquidationsmechanismen,

³⁵¹ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 41; vgl. The FDIC's Investigation of Voyager Digital, Crypto-Fintech FDIC Misrepresentations, North Carolina Banking Institute Journal 27, 2023, S. 200–201.

³⁵² Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 41; vgl. Schweizer Bundesrat, DLT-Bericht, 2018, S. 141.

³⁵³ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 41; vgl. Art. 59–61 und Art. 63 Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final, S. 94–99; vgl. McDermott, Megan, The Crypto Quandary: Is Bankruptcy Ready?, Northwestern University Law Review 115, 2021, S. 1952.

³⁵⁴ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 41 und 43.

Anforderungen an Schlüsselmanagement und Wiederherstellungsprozesse,³⁵⁵

Mindestanforderungen für Verwahrtechnologien.

Der unionsrechtliche Gesetzgeber könnte hierfür ein System technischer Mindestanforderungen analog zu IT-Handbüchern des Bankensektors oder Sicherheitsstandards der Netz- und Informationssystemsisicherheit entwickeln.³⁵⁶

6.4.5 Erforderlichkeit einer unionsweiten Reform des kollektiven Rechtsschutzes

Ein weiterer struktureller Schwachpunkt des unionsrechtlichen Systems betrifft die fehlenden Mechanismen kollektiven Rechtsschutzes bei systemischen Verlusten. Während in den USA Sammelklagen und class actions ein wesentliches Durchsetzungsinstrument gegen betrügerische oder fehlerhafte Anbieter bilden,³⁵⁷ existiert im europäischen Kryptobereich kein äquivalentes Instrument, das Opfern von Plattforminsolvenzen oder technischen Fehlern eine realistische Form der kollektiven Rechtsdurchsetzung bietet.

Eine unionsweite Ergänzung der MiCA-Verordnung um kollektive Anspruchsmechanismen, Ombudssysteme, verbraucherschutzorientierte Schlichtungsstellen sowie standardisierte Beschwerdemechanismen könnte bestehende Schutzlücken schließen und die Rechtsdurchsetzung für Verbraucher:innen erheblich erleichtern. Dadurch würde ein zusätzliches Schutzniveau geschaffen, das im Bereich der Kryptowerte derzeit nur eingeschränkt oder gar nicht vorhanden ist.

³⁵⁵ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 16.

³⁵⁶ Vgl. Art. 14 Abs. 1 Richtlinie (EU) 2016/1148 (NIS-Richtlinie); vgl. Art. 74 Abs. 1 Richtlinie 2013/36/EU (CRD IV); vgl. EBA, Guidelines on ICT and Security Risk Management, 2019, S. 14.

³⁵⁷ Vgl. The FDIC's Investigation of Voyager Digital, North Carolina Banking Institute Journal 27, 2023, S. 199; vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 41.

Kapitel 7

Bewertung der Effektivität bestehender Schutzmechanismen

7.1 Systematische Ausgangslage des unionsrechtlichen Verbraucherschutzes im Bereich kryptobasierter Dienstleistungen

Der unionsrechtliche Verbraucherschutz bildet ein komplex aufgebautes und sektorenübergreifend harmonisiertes Schutzsystem, das auf die Sicherung der wirtschaftlichen Entscheidungsfreiheit, der Transparenz vertraglicher Beziehungen und der strukturellen Gleichstellung von Verbraucher:innen gegenüber gewerblichen Anbietern ausgerichtet ist. Dieses System wurde jedoch wesentlich vor dem Aufkommen kryptobasierter Produkte und Dienstleistungen geschaffen. Da Kryptowerte und kryptobezogene Dienstleistungen in ihrer wirtschaftlichen Funktion, technischen Struktur und ihrem Risikoprofil teilweise erheblich von traditionellen Vertrags- und Finanzdienstleistungsformen abweichen, stellt sich die Frage, in welchem Umfang die klassischen unionsrechtlichen Verbraucherschutzvorschriften auf diese Rechtsverhältnisse anwendbar sind. Zu untersuchen ist insbesondere, ob und inwieweit bestehende Verbraucherschutznormen geeignet sind, die besonderen Eigenschaften und Risiken kryptobezogener Geschäftsmodelle zu erfassen und einen angemessenen Schutz für Verbraucher:innen zu gewährleisten.³⁵⁸

Die unionsrechtliche Konzeption des Verbraucherschutzes beruht auf dem Grundsatz der Technologieneutralität, wonach Schutzmechanismen unabhängig von der eingesetzten Technologie gelten sollen, sofern die gesetzlichen Tatbestände erfüllt werden.³⁵⁹ Dieser Grundsatz führt jedoch im Kryptobereich zu einer grundlegenden rechtswissenschaftlichen Herausforderung. Die wirtschaftliche Struktur eines Kryptoprodukts lässt sich häufig nicht bruchlos in die unionsrechtlichen Kategorien „Dienstleistung“, „digitale Dienstleistung“, „Finanzdienstleistung“ oder „Verbrauchervertrag“ einordnen, da Token nicht notwendig eine eindeutige vertragliche oder funktionale Zuordnung besitzen.³⁶⁰ Die Folge ist, dass das unionsrechtliche Verbraucherschutzsystem im Kryptobereich zwar prinzipiell Anwendung finden kann, seine Reichweite und Schutzintensität jedoch erheblich davon abhängen, wie die jeweiligen Vertragsbeziehungen rechtlich qualifiziert werden.

³⁵⁸ Vgl. Art. 169 Abs. 1 AEUV; vgl. EuGH 14.06.2012, Rs. C-618/10 (Banco Español de Crédito), Rn. 39; vgl. Art. 1 Richtlinie 2011/83/EU; vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 8 f., 11, 40 f.

³⁵⁹ Vgl. Europäische Kommission, A Digital Single Market Strategy for Europe, COM(2015) 192 final, S. 5; vgl. Art. 2 und Art. 3 Richtlinie 2011/83/EU; vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 8.

³⁶⁰ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 17, 28, 35 und 40; vgl. Art. 3 Abs. 1 Richtlinie 2011/83/EU; vgl. Art. 3 Abs. 1 Richtlinie (EU) 2019/770; vgl. Rn. 116 Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final.

Eine besondere strukturelle Komplexität ergibt sich daraus, dass die MiCA-Verordnung ein eigenes sektorales Regime für Kryptowerte schafft, das jedoch nur den aufsichtsrechtlichen Bereich harmonisiert und keine umfassenden verbraucherrechtlichen oder zivilrechtlichen Regelungen enthält. Dadurch entsteht ein zweistufiges System: Einerseits gelten für Kryptowerte die besonderen aufsichtsrechtlichen Anforderungen der MiCA und andererseits bleibt für Verbraucherschutzrechtliche Fragen die Anwendbarkeit der horizontalen Verbraucherschutznormen entscheidend.³⁶¹ Diese Normen – insbesondere die Verbraucherrechte-Richtlinie, die Richtlinie über unlautere Geschäftspraktiken, die Richtlinie zum Fernabsatz von Finanzdienstleistungen, die Modernisierungsrichtlinie sowie die Verbandsklagerichtlinie – bilden somit den maßgeblichen Rahmen, innerhalb dessen verbraucherrechtliche Ansprüche und Durchsetzungsmechanismen im Kryptobereich zu verorten sind.

Diese doppelte Rechtsstruktur führt zu einer Regelungslücke, die nicht aus dem Fehlen normativer Vorgaben resultiert, sondern aus der mangelnden Passgenauigkeit zwischen den unionsrechtlichen Verbraucherschutzinstrumenten und der spezifischen Vertragsarchitektur kryptobasierter Dienste. Im Gegensatz zu traditionellen digitalen Dienstleistungen, die durch klare vertragliche Leistungsgegenstände geprägt sind, beruhen kryptobasierte Produkte häufig auf programmatischen Mechanismen, dezentralen Strukturen und multilateralen Interaktionen, die sich klassischen Begriffen nur eingeschränkt zuordnen lassen.³⁶²

7.2 Struktur und systematische Funktion der unionsrechtlichen Verbraucherschutznormen im Bereich kryptobasierter Dienstleistungen

Das unionsrechtliche Verbraucherschutzsystem besteht aus einer Reihe horizontaler Richtlinien, die sektorenübergreifend grundlegende Schutzmechanismen für Verbraucher:innen bereitstellen. Diese Normen wurden historisch unabhängig von kryptobasierten Vertragsmodellen entwickelt, sind jedoch technologieneutral ausgestaltet und knüpfen ausschließlich an die Struktur eines Verbrauchervertrags an.³⁶³ Im Kryptobereich entsteht dadurch eine erhebliche rechtliche und systematische Herausforderung. Die unionsrechtlichen Kategorien, auf denen die bestehenden Richtlinien aufbauen, erfassen vielfach nicht jene

³⁶¹ Vgl. Art. 1 Abs. 1 sowie Art. 2 Abs. 2 und Abs. 3 Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final; vgl. Art. 3 Abs. 1 Richtlinie 2011/83/EU.

³⁶² Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 4, 7 f., 13 f.; vgl. Art. 3 Abs. 1 Richtlinie 2011/83/EU; vgl. Art. 3 Abs. 1 Richtlinie (EU) 2019/770; vgl. Art. 2 Abs. 3 Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final.

³⁶³ Vgl. Art. 169 Abs. 1 AEUV; vgl. Art. 1 und Art. 3 Abs. 1 Richtlinie 2011/83/EU; vgl. Art. 3 Abs. 1 Richtlinie (EU) 2019/770; vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 40.

Leistungsformen, die durch Tokenisierung, automatisierte Ausführungsmechanismen oder dezentrale Systeme geschaffen werden. Dadurch können Abgrenzungs- und Anwendungsfragen entstehen, da neuartige kryptobezogene Geschäftsmodelle nicht immer eindeutig den traditionellen Regelungskategorien des Verbraucherrechts zugeordnet werden können.³⁶⁴ Ziel der unionsrechtlichen Verbraucherschutznormen ist der Ausgleich struktureller Informationsasymmetrien.³⁶⁵ Diese Zielsetzung ist auch für kryptobasierte Dienstleistungen relevant, da Verbraucher:innen häufig mit Leistungsmechanismen konfrontiert sind, deren Funktionsweise sie nicht nachvollziehen können. Die unionsrechtliche Systematik verlangt jedoch eine funktionale Einordnung der jeweiligen Leistung, unabhängig davon, ob diese auf programmtechnischer, digitaler oder traditioneller Weise erbracht wird. Maßgeblich ist somit nicht die technische Ausgestaltung der Leistung, sondern ihre tatsächliche wirtschaftliche und rechtliche Funktion. Dadurch ist stets im Einzelfall zu prüfen, ob ein kryptobasierter Vertrag als Dienstleistung, digitale Dienstleistung oder Finanzdienstleistung qualifiziert werden kann. Die MiCA-Verordnung schafft ein spezielles aufsichtsrechtliches Rahmenwerk, enthält jedoch keine verbraucherrechtliche Harmonisierung des Vertragsverhältnisses zwischen Anbieter und Verbraucher:in.³⁶⁶ Daher bleiben Informationspflichten, Widerrufsrechte, Transparenzvorgaben, Geschäftspraktiken und kollektive Rechtsdurchsetzung vollständig in den allgemeinen Verbraucherschutzrichtlinien verankert. Dieses Nebeneinander zweier Ebenen – aufsichtsrechtlich (MiCA) und verbraucherrechtlich (CRD, UCPD etc.) – führt im Kryptobereich zu einer strukturellen Schutzlücke, weil die unionsrechtlichen Richtlinien nicht auf irreversible oder protokollbasierte Leistungsabläufe zugeschnitten sind.³⁶⁷

7.2.1 Verbraucherrechte-Richtlinie (CRD) im Kontext kryptobasierter Dienstleistungen

Die Verbraucherrechte-Richtlinie 2011/83/EU harmonisiert zentrale Informationspflichten und Widerrufsrechte. Ihr Anwendungsbereich ist technologieneutral und knüpft allein an das Vorliegen eines Verbrauchervertrags an.³⁶⁸ Damit kann die Consumer Rights Directive (CRD) auf

³⁶⁴ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 40 sowie S. 56 (Notes).

³⁶⁵ Vgl. Art. 169 Abs. 1 AEUV; vgl. EuGH 14.06.2012, Rs. C-618/10 (Banco Español de Crédito), Rn. 39; vgl. Art. 1 Richtlinie 2011/83/EU.

³⁶⁶ Vgl. Art. 1 Abs. 1 sowie Art. 2 Abs. 2 und Abs. 3 Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final.

³⁶⁷ Vgl. Art. 2 Abs. 2 und Abs. 3 Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final; vgl. Art. 1 und Art. 9 Abs. 1 Richtlinie 2011/83/EU; vgl. Art. 1 Richtlinie 2005/29/EG; vgl. Art. 1 Abs. 1 Richtlinie (EU) 2020/1828; vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 40 f.

³⁶⁸ Vgl. Art. 1, Art. 3 Abs. 1, Art. 6 Abs. 1 und Art. 9 Abs. 1 Richtlinie 2011/83/EU.

kryptobasierte Dienstleistungen Anwendung finden, sofern eine entgeltliche Leistung eines Unternehmers gegenüber einem Verbraucher:in vorliegt.

Die rechtliche Herausforderung ergibt sich aus der Zuordnung kryptobasierter Leistungen zu den Begriffen der „Dienstleistung“ beziehungsweise „digitalen Dienstleistung“. Da Token häufig automatisiert über Smart Contracts bereitgestellt und ausgeführt werden, fehlt oftmals ein klassischer, eindeutig abgrenzbarer Leistungsinhalt, wie er traditionellen Vertragsverhältnissen zugrunde liegt. Die funktionale Ausrichtung der CRD ermöglicht jedoch grundsätzlich eine Einordnung solcher Leistungen, sofern ihre wirtschaftliche Funktion einem Verbrauchervertrag entspricht. Maßgeblich ist dabei nicht die technische Ausgestaltung der Leistung, sondern deren tatsächlicher wirtschaftlicher Zweck und ihre Bedeutung für die Vertragsbeziehung mit Verbraucher:innen.³⁶⁹

Die Widerrufsrechte der CRD können bei irreversiblen Token-Transaktionen nur eingeschränkt verwirklicht werden. Die Richtlinie geht von reversiblen digitalen Leistungen aus. Kryptografisch ausgeführte Transaktionen sind jedoch technisch nicht rückabwickelbar.³⁷⁰ Dadurch entsteht ein strukturelles Schutzdefizit, da die bestehenden Regelungsmechanismen der CRD die besonderen Merkmale und Risiken kryptobasierter Geschäftsmodelle nur eingeschränkt abbilden können.

Die Informationspflichten der CRD – insbesondere zu Vertragsinhalt, Risiken und unternehmerischer Identität – sind jedoch anwendbar.³⁷¹ Die Herausforderung besteht darin, dass Anbieter häufig keine vollständigen Risikoinformationen bereitstellen können, weil unionsrechtliche technische Mindeststandards fehlen.

7.2.2 Richtlinie über unlautere Geschäftspraktiken (UCPD)

Die UCPD schützt Verbraucher:innen vor irreführenden oder aggressiven geschäftlichen Handlungen. Das unionsrechtliche Irreführungsverbot ist uneingeschränkt auf kryptobasierte Werbung und Vertriebsmodelle anwendbar, sofern ein Geschäftsverhalten gegenüber Verbraucher:innen vorliegt. Im Kryptobereich ist die UCPD besonders relevant, weil Werbeaussagen häufig spekulative Elemente enthalten und technische Informationen schwer verständlich sind. Irreführungen können etwa vorliegen bei Angaben zur Wertentwicklung, Liquidität, Stabilität eines Tokens oder zu angeblich garantierten Leistungen.³⁷²

³⁶⁹ Vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 11, 40 und 56 (Notes); vgl. Art. 1 und Art. 3 Abs. 1 Richtlinie 2011/83/EU.

³⁷⁰ Vgl. Art. 9 Abs. 1 und Art. 16 lit. m Richtlinie 2011/83/EU.

³⁷¹ Vgl. Art. 6 Abs. 1 lit. a, b, e und h Richtlinie 2011/83/EU.

³⁷² Vgl. Art. 1, Art. 6 Abs. 1 lit. b und c, Art. 7 Abs. 1 sowie Anhang I Nr. 17 Richtlinie 2005/29/EG.

Problematisch ist, dass die UCPD keine spezifischen Vorgaben für algorithmische oder automatisierte Geschäftsmodelle enthält. Dadurch entstehen Schutzlücken bei personalisierten Werbeinhalten oder bei der automatisierten Gestaltung von Benutzeroberflächen, die Verbraucher:innen manipulierend beeinflussen können.

7.3 Verhältnis zwischen MiCA und dem allgemeinen unionsrechtlichen Verbraucherschutzrecht

Das Verhältnis zwischen der MiCA-Verordnung und den horizontalen unionsrechtlichen Verbraucherschutznormen ist von einer doppelten Systematik geprägt: MiCA schafft ein sektorales Aufsichtsregime für kryptobasierte Dienstleistungen, ohne jedoch das vertragliche Innenverhältnis zwischen Anbieter und Verbraucher:in zu harmonisieren. Daraus entsteht eine parallele Struktur, in der die MiCA einerseits organisatorische und aufsichtsrechtliche Mindestanforderungen festlegt, während die materiell-vertragliche Verbraucherschutzdimension weiterhin ausschließlich von allgemeinen Richtlinien getragen wird.³⁷³ Dieses Nebeneinander führt zu einer systemischen Besonderheit, die im europäischen Verbraucherschutzrecht bislang ohne Vorbild ist.

MiCA regelt primär die Zulassungsvoraussetzungen, organisatorischen Mindeststandards, Informationspflichten gegenüber der Aufsicht sowie Marktdisziplinierung durch Aufsichtsbehörden.³⁷⁴ Diese Regelungsziele unterscheiden sich grundlegend von jenen der horizontalen Verbraucherschutzrichtlinien, die auf Transparenz, Entscheidungsfreiheit und vertragliche Schutzpositionen der Verbraucher:innen abzielen. Die beiden Regelungsebenen sind deshalb **nicht konkurrierend**, sondern **komplementär**, jedoch ohne kohärente Verzahnung. Diese fehlende Verzahnung führt zu systematischen Abgrenzungsproblemen, die insbesondere im Kryptobereich sichtbar werden, da Token weder klassisch-finanzielle noch klassische digitale Dienstleistungen darstellen.³⁷⁵

Eine zentrale Problematik ergibt sich aus der unterschiedlichen Begriffssystematik: MiCA verwendet Begriffe wie „Krypto-Asset“, „Krypto-Asset-Dienstleistung“ und „Krypto-Asset-Dienstleister“, die unionsrechtlich eigenständig und sektorspezifisch geprägt sind. Diese Begriffe decken sich nicht mit den Kategorien der CRD („Dienstleistung“, „digitale

³⁷³ Vgl. Art. 1 Abs. 1 sowie Art. 2 Abs. 2 und Abs. 3 Vorschlag für eine Verordnung über Märkte für Krypto-Assets (MiCA), COM(2020) 593 final; vgl. Art. 1 und Art. 3 Abs. 1 Richtlinie 2011/83/EU.

³⁷⁴ Vgl. Art. 1 Abs. 1, Art. 52 Abs. 1, Art. 60 Abs. 1, Art. 61 Abs. 1 und Art. 90 Abs. 1 Verordnung (EU) 2023/1114 (MiCA, konsolidierte Fassung vom 09.01.2024).

³⁷⁵ Vgl. Art. 1 Abs. 1 sowie Art. 2 Abs. 2 und Abs. 3 Verordnung (EU) 2023/1114 (MiCA); vgl. Art. 1 Richtlinie 2011/83/EU; vgl. Art. 1 Richtlinie 2005/29/EG; vgl. OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, 2020, S. 11 und 40.

Dienstleistung“), der UCPD („geschäftliche Handlung“), der Fernabsatzrichtlinie („Finanzdienstleistung“) oder der Modernisierungsrichtlinie („digitaler Inhalt“).³⁷⁶ Die Folge ist, dass das gleiche kryptobasierte Produkt in unterschiedlichen Regelungskontexten unterschiedlich eingeordnet werden kann.

Diese begriffliche Divergenz führt dazu, dass MiCA zwar ein einheitliches Marktregime schafft, jedoch nicht die funktionale Grundlage dafür legt, kryptobasierte Vertragsverhältnisse in das bestehende unionsrechtliche Verbraucherschutzsystem einzugliedern. Die Verbraucher:innen sind damit formal durch zwei Ebenen geschützt, in der praktischen Rechtsanwendung jedoch häufig unklar, welche Normebene im konkreten Fall Vorrang hat oder ob bestimmte Schutzmechanismen tatsächlich greifen.³⁷⁷

Hinzu kommt, dass MiCA – anders als klassische Finanzmarktregime – keine zivilrechtlichen Rechtsfolgen normiert. Sie enthält weder ausdrückliche Haftungsregelungen noch vertragliche Rückabwicklungsmechanismen noch Bestimmungen zur Ausgestaltung von Widerrufsrechten, zur Informationsklarheit in Verbraucherverträgen oder zum Umgang mit automatisierten Leistungsabläufen.³⁷⁸ Die horizontale Verbraucherschutzarchitektur muss daher Schutzlücken schließen, für die sie systematisch nicht entwickelt wurde.

Besonders herausfordernd ist das Verhältnis zwischen MiCA und der UCPD. Während MiCA Informationspflichten gegenüber der Aufsicht und gegenüber Nutzer:innen im Rahmen von Whitepapers vorsieht, legt die UCPD den Schwerpunkt auf die materielle Richtigkeit, Vollständigkeit und Nicht-Irreführung geschäftlicher Handlungen.³⁷⁹ Ein MiCA-konformes Whitepaper garantiert daher nicht zwingend, dass die Marketing- oder Vertriebspraxis eines Dienstleisters unionsrechtlich zulässig ist.³⁸⁰ Die beiden Normkomplexe verfolgen unterschiedliche Zielrichtungen und greifen nur unmittelbar, wenn ein Sachverhalt gleichzeitig die tatbestandlichen Voraussetzungen beider Regime erfüllt.

Auch die Beziehung zwischen MiCA und der Verbraucherrechte-Richtlinie (CRD) ist dogmatisch ungeklärt. Die CRD setzt einen einheitlichen, reversibel ausgestalteten Leistungsmechanismus

³⁷⁶ Vgl. Art. 3 Abs. 1 Nr. 5, Nr. 15 und Nr. 16 Verordnung (EU) 2023/1114 (MiCA); vgl. Art. 3 Abs. 1 Richtlinie 2011/83/EU; vgl. Art. 2 lit. d Richtlinie 2005/29/EG; vgl. Art. 2 lit. b Richtlinie 2002/65/EG; vgl. Art. 3 Abs. 1 Richtlinie (EU) 2019/770.

³⁷⁷ Vgl. Art. 1 Abs. 1, Art. 2 Abs. 1–4, Art. 3 Abs. 1 Nr. 5, Nr. 15 und Nr. 16 Verordnung (EU) 2023/1114 (MiCA, konsolidierte Fassung vom 09.01.2024).

³⁷⁸ Vgl. Art. 1 Abs. 1 und Art. 2 Abs. 1 Verordnung (EU) 2023/1114 (MiCA, konsolidierte Fassung vom 09.01.2024); vgl. Art. 6 Abs. 1 und Art. 9 Abs. 1 Richtlinie 2011/83/EU.

³⁷⁹ Vgl. Art. 8 Abs. 1–4, Art. 9 Abs. 1–2, Art. 14 Abs. 1 lit. d, Art. 15 Abs. 1 und Abs. 6 Verordnung (EU) 2023/1114 (MiCA, konsolidierte Fassung vom 09.01.2024); vgl. Art. 6 Abs. 1 Richtlinie 2005/29/EG (UCPD, idF 28.05.2022).

³⁸⁰ Vgl. Art. 8 Abs. 1 und Abs. 3, Art. 9 Abs. 1 sowie Art. 15 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); vgl. Art. 6 Abs. 1 und Art. 7 Abs. 1 Richtlinie 2005/29/EG (UCPD).

voraus, der bei kryptobasierten Ausführungen regelmäßig nicht gegeben ist. MiCA harmonisiert lediglich die Transparenz gegenüber der Aufsicht und den Mindestinhalt von Whitepapers, nicht jedoch die zivilrechtliche Beziehung zwischen Anbieter und Verbraucher:innen.³⁸¹ Dadurch entsteht ein strukturelles Spannungsfeld. Ein Unternehmen kann aufsichtsrechtlich vollständig compliant sein und dennoch verbraucherschutzrechtliche Pflichten verletzen, weil die beiden Normkomplexe unterschiedliche Schutzbereiche und unterschiedliche Risikoprofile adressieren. Dieses Nebeneinander zweier unkoordiniert wirkender Schutzsysteme führt in der unionsrechtlichen Literatur zu der Einschätzung, dass MiCA zwar Transparenz und Marktstabilität erhöhen kann, jedoch keine Antworten auf grundlegende zivilrechtliche Schutzfragen gibt. Die unionsrechtlichen Verbraucherschutznormen bleiben daher strukturell überfordert, da sie nicht für irreversible, automatisch ausgeführte und technisch vermittelte Leistungen entwickelt wurden. Zusammenfassend lässt sich feststellen, dass das Verhältnis zwischen MiCA und dem allgemeinen Verbraucherschutzrecht nicht durch eine Hierarchie, sondern durch ein strukturell unvollständiges Nebeneinander geprägt ist. MiCA adressiert Marktstrukturen und Aufsicht, während das Verbraucherschutzrecht die individuellen Rechtspositionen der Verbraucher:innen schützen soll – allerdings ohne definitorische Klarheit, wie kryptobasierte Leistungen in diese Schutzmechanismen einzuordnen sind. Diese fehlende Abstimmung führt zu materiellen Schutzdefiziten und macht eine vertiefte Analyse der zivilrechtlichen Folgen in den folgenden Abschnitten erforderlich.

7.4 Unionsrechtliche Schutzdefizite im Lichte technischer und organisatorischer Risiken kryptobasierter Dienstleistungen

Die unionsrechtlichen Verbraucherschutznormen sind funktional ausgestaltet und verfolgen das Ziel, Verbraucher:innen vor intransparenten Vertragsbedingungen, unlauteren Geschäftspraktiken und fehlenden Informationen zu schützen. Sie setzen jedoch voraus, dass die Leistung, die den Gegenstand eines Verbrauchervertrags bildet, nach unionsrechtlichen Kategorien bestimmbar, nachvollziehbar und rechtlich fassbar ist.³⁸² Zentral ist, dass die Verbraucherschutzrichtlinien auf kontrollierbare Leistungsabläufe zugeschnitten sind. Sie setzen voraus, dass Unternehmer:innen die Vertragsleistung gestalten, beeinflussen und gegebenenfalls korrigieren können.³⁸³ Bei kryptobasierten Leistungen, deren Ausführung

³⁸¹ Vgl. Art. 3 Abs. 1, Art. 9 Abs. 1 und Art. 16 lit. m Richtlinie 2011/83/EU (CRD); vgl. Art. 1 Abs. 1, Art. 5 Abs. 1, Art. 8 Abs. 1 und Art. 15 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

³⁸² Vgl. Art. 1, Art. 3 Abs. 1 und Art. 6 Abs. 1 Richtlinie 2011/83/EU; vgl. Art. 1 und Art. 7 Abs. 1 Richtlinie 2005/29/EG.

³⁸³ Vgl. Art. 3 Abs. 1, Art. 6 Abs. 1, Art. 9 Abs. 1 und Art. 16 lit. m Richtlinie 2011/83/EU; vgl. Art. 6 Abs. 1 Richtlinie 2005/29/EG.

automatisch durch Protokolle oder programmatische Mechanismen erfolgt, fehlt häufig die Möglichkeit einer nachträglichen Einflussnahme. In der unionsrechtlichen Literatur wird darauf hingewiesen, dass der Verbraucherschutz in solchen Fällen seine Steuerungsfunktion nur eingeschränkt entfalten kann, weil der Anbieter nicht dieselbe Kontrolle über den Leistungsprozess besitzt wie bei traditionellen digitalen Diensten.

Hinzu kommt, dass viele kryptobasierte Dienstleistungen auf dezentralen oder nur teilweise kontrollierbaren Infrastrukturen beruhen, deren technische Stabilität, Verfügbarkeit oder Fehlertoleranz nicht unionsrechtlich normiert ist. Die allgemeinen Verbraucherschutzrichtlinien enthalten jedoch keine Vorgaben zu technischen Mindeststandards, Sicherheitsarchitekturen oder Stabilitätsanforderungen digitaler Dienste, sodass sie Risiken strukturell nicht abbilden.³⁸⁴

Die fehlende Verbindung zwischen technischer Risikosteuerung und verbraucherrechtlicher Schutznorm führt zu einer Schutzlücke. Verbraucher:innen tragen Risiken, die aus der Funktionsweise der Infrastruktur resultieren, ohne dass das Unionsrecht Mechanismen bereitstellt, um diese abzubilden oder vertraglich einzuhegen.

Besonders problematisch ist, dass die Verbraucherschutznormen von einem zeitlich klar abgrenzbaren Leistungsbeginn und Leistungsende ausgehen.³⁸⁵ Kryptobasierte

Dienstleistungen können jedoch einen offenen, andauernden oder autonom fortlaufenden Charakter haben, ohne dass ein klarer Leistungszeitpunkt identifizierbar ist. Für viele Richtlinien – insbesondere CRD und Fernabsatz-Finanzdienstleistungsrichtlinie – ist der Zeitpunkt der Leistungserbringung jedoch zentral für Widerrufsrechte, Transparenzanforderungen und Haftungsfragen. Wenn der Leistungszeitpunkt technisch nicht eindeutig bestimmbar ist, verlieren klassische unionsrechtliche Schutzmechanismen ihre praktische Wirksamkeit.³⁸⁶

Weiterhin bestehen unionsrechtliche Schutzdefizite in Bezug auf die Informationsvorgaben, da die Richtlinien Transparenz zwar verlangen, jedoch nicht definieren, welche Informationen für kryptobasierte Leistungen spezifisch erforderlich sind.³⁸⁷ Anbieter müssen zwar über wesentliche Merkmale der Dienstleistung informieren, doch bleibt unklar, ob hierzu auch Informationen über algorithmische Ausführungslogiken, Risiken von technischer Fehlfunktionen, Liquiditätsmechanismen oder mögliche Wertverluste aufgrund systemischer Faktoren gehören. Das Unionsrecht enthält keine Kriterien dafür, wann ein technisches Risiko

³⁸⁴ Vgl. Art. 1 und Art. 3 Abs. 1 Richtlinie 2011/83/EU; vgl. Art. 1 und Art. 6 Abs. 1 Richtlinie 2005/29/EG; vgl. Art. 14 Abs. 1 lit. d Verordnung (EU) 2023/1114 (MiCA).

³⁸⁵ Vgl. Art. 3 Abs. 1, Art. 6 Abs. 1 lit. g, Art. 9 Abs. 1 und Art. 16 lit. m Richtlinie 2011/83/EU.

³⁸⁶ Vgl. Art. 6 Abs. 1 lit. g, Art. 9 Abs. 1 und Art. 16 lit. m Richtlinie 2011/83/EU (CRD); vgl. Art. 6 Abs. 1 und Art. 7 Abs. 1 Richtlinie 2002/65/EG.

³⁸⁷ Vgl. Art. 1 und Art. 6 Abs. 1 Richtlinie 2011/83/EU; vgl. Art. 7 Abs. 1 Richtlinie 2005/29/EG; vgl. Art. 5 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

„wesentlich“ im Sinne der Informationspflicht ist. Dies führt dazu, dass Verbraucher:innen formell informiert werden, ohne dass die materiellen Risiken der Dienstleistung tatsächlich erfasst werden.³⁸⁸ Ein weiteres Schutzdefizit ergibt sich aus der Haftungsverteilung. Die horizontalen Verbraucherschutznormen setzen voraus, dass der Unternehmer die Verantwortung für die Erfüllung des Vertrags trägt und bei Pflichtverletzungen haftet.³⁸⁹ Bei kryptobasierten Dienstleistungen ist jedoch häufig unklar, wer als haftungsrechtlich relevanter Akteur anzusehen ist, wenn technische oder organisatorische Störungen auftreten. Weder MiCA noch die allgemeinen Verbraucherschutznormen legen fest, wie Verantwortung verteilt wird, wenn Fehler in der Protokollausführung auftreten oder wenn Drittanbieter wesentliche Funktionen übernehmen. In der Literatur wird hervorgehoben, dass diese Zersplitterung der Verantwortung zu einer faktischen Aushöhlung verbraucherrechtlicher Ansprüche führen kann.³⁹⁰ Schließlich ergibt sich ein erhebliches unionsrechtliches Schutzdefizit aus dem Fehlen einer Regelung zur Behandlung von Leistungsstörungen im digitalen Kontext, die nicht von einem klassischen Vertragspartner verursacht werden. Im Gegensatz zu traditionellen Vertragsverhältnissen, bei denen Unternehmer:innen regelmäßig die Möglichkeit haben, Leistungsstörungen zu beheben oder Ersatz zu leisten, bestehen bei kryptobasierten Dienstleistungen häufig nur eingeschränkte Möglichkeiten einer nachträglichen Korrektur. Aufgrund der technischen Ausgestaltung vieler Blockchain-Systeme können einmal ausgeführte Transaktionen oder automatisierte Prozesse oftmals nicht oder nur schwer rückgängig gemacht werden.³⁹¹ Besteht diese Möglichkeit technisch nicht, greifen zentrale verbraucherrechtliche Schutzmechanismen ins Leere.

Insgesamt zeigt sich, dass die unionsrechtlichen Verbraucherschutznormen im Bereich kryptobasierter Dienstleistungen an strukturelle Grenzen stoßen. Dies beruht nicht auf einem Mangel an bestehenden Regelungen, sondern darauf, dass die zugrunde liegenden Regelungskonzepte nur eingeschränkt auf die programmatisch gesteuerten, häufig nicht reversiblen und teilweise dezentral organisierten Leistungsstrukturen kryptobasierter Dienste abgestimmt sind. Dadurch entstehen Schutzlücken und Anwendungsprobleme, die mit den bestehenden Instrumenten des Verbraucherrechts nur teilweise erfasst werden können.

³⁸⁸ Vgl. Art. 7 Abs. 1 und Abs. 4 Richtlinie 2005/29/EG (UCPD); vgl. Art. 1 und Art. 6 Abs. 1 Richtlinie 2011/83/EU (CRD); vgl. Art. 5 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

³⁸⁹ Vgl. Art. 2 Nr. 2, Art. 3 Abs. 1, Art. 13 Abs. 1 und Art. 14 Abs. 4 Richtlinie 2011/83/EU (CRD); vgl. Art. 5 Abs. 1 und Abs. 2 Richtlinie 2005/29/EG (UCPD).

³⁹⁰ Vgl. Art. 1 Abs. 1 und Art. 15 Abs. 1 Verordnung (EU) 2023/1114 (MiCA); vgl. Art. 3 Abs. 1 Richtlinie 2011/83/EU (CRD); vgl. Art. 5 Abs. 2 Richtlinie 2005/29/EG (UCPD).

³⁹¹ Vgl. Art. 3 Abs. 1, Art. 13 Abs. 1, Art. 14 Abs. 3 und Art. 16 lit. m Richtlinie 2011/83/EU (CRD); vgl. Art. 1 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

Kapitel 8

Reformvorschläge und normative Handlungsempfehlungen

8.1 Normativer Ausgangsrahmen und zentrale Erkenntnislinien

Die Entwicklung eines zukunftsfähigen Verbraucherschutzes im Bereich kryptobasierter Dienstleistungen setzt voraus, dass die normativen Grundlagen, Leitprinzipien und strukturellen Ausgangsbedingungen des österreichischen und unionsrechtlichen Systems klar bestimmt werden. Der Verbraucherschutz ist im europäischen Rechtsraum nicht nur ein politisches Ziel, sondern ein rechtlich verbindliches Prinzip, das in Art. 38 GRC ausdrücklich verankert ist und dem Gesetzgeber wie der Rechtsanwendung einen hohen Schutzniveauftrag auferlegt.³⁹² Dieses Leitbild bildet die normative Ausgangsebene für die Beurteilung, ob bestehende rechtliche Instrumente im Umgang mit Kryptovermögen geeignet sind, Verbraucher:innen wirksam zu schützen.

Zugleich ist die materielle Rechtswirklichkeit im digitalen und kryptobasierten Kontext von besonderen Unsicherheiten geprägt. Kryptowertbezogene Dienstleistungen zeichnen sich durch neuartige Leistungsstrukturen, automatisierte Abläufe und erhöhte Informationsasymmetrien aus, die in der traditionellen Verbraucherrechtsdogmatik nicht vorgesehen sind.³⁹³ Daraus ergibt sich ein Spannungsfeld zwischen normativem Anspruch und rechtspraktischer Durchsetzbarkeit. Die bestehenden Verbraucherschutznormen beanspruchen einen hohen Schutzstandard, erreichen ihn aber nur, wenn die ihnen zugrunde liegenden Konzepte – insbesondere Vertragsgegenstand, Leistungsbeschreibung und Rechtsnatur digitaler Vermögenspositionen – eindeutig bestimmbar sind.³⁹⁴

Die Analyse der bisherigen Kapitel hat gezeigt, dass die unionsrechtliche Regulierung kryptobasierter Dienstleistungen zwar eine zunehmende Strukturierung erfahren hat, wesentliche zivilrechtliche und insolvenzrechtliche Grundfragen jedoch weiterhin offenbleiben. Kapitel 8 knüpft an diese Erkenntnisse an, erweitert sie um die nationale Perspektive und untersucht, welchen Beitrag das österreichische Recht zur Schließung dieser Schutzlücken leisten kann. Der normative Ausgangspunkt ist dabei dreifach strukturiert:

³⁹² Vgl. Art. 38 Charta der Grundrechte der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 391): „Die Politik der Union stellt ein hohes Verbraucherschutzniveau sicher.“

³⁹³ Vgl. ErwGr 1 Vorschlag für eine Verordnung über Märkte für Krypto-Assets, COM(2020) 593 final („Crypto-assets are a new form of digital assets which are not currently regulated at Union level.“); vgl. OECD, Financial Consumer Protection Policy Approaches in the Digital Age, 2020.

³⁹⁴ Vgl. Art. 38 Charta der Grundrechte der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 391); vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 41.

Erstens erfordert ein moderner Verbraucherschutz im Kryptobereich eine systematische Einordnung digitaler Vermögensformen in die bestehende Struktur des Zivilrechts. Das Allgemeine Bürgerliche Gesetzbuch (ABGB) baut traditionell auf klar definierten Vermögenskategorien auf, anhand derer Rechte, Pflichten und Rechtsfolgen zugeordnet werden. Die rechtliche Behandlung von Kryptowerten wirft jedoch neue Einordnungsfragen auf, da diese Vermögensformen nicht ohne Weiteres in die klassischen Kategorien des Zivilrechts eingeordnet werden können.³⁹⁵ Kryptowerte entziehen sich jedoch diesen Strukturen, sodass der österreichische Gesetzgeber, die Rechtsprechung und die Privatrechtslehre herausfinden müssen, wie Token in die Kategorien der Sachen, Forderungen oder unkörperlichen Rechte eingeordnet werden können.

Zweitens basiert ein wirksamer Verbraucherschutz auf Transparenz und Informiertheit. Die österreichischen Umsetzungsakte – insbesondere FAGG, KSchG und UWG – verlangen, dass Unternehmer:innen klare, verständliche und vollständige Informationen bereitstellen.³⁹⁶ Im Kryptobereich besteht jedoch ein strukturelles Informationsgefälle. Anleger:innen verstehen häufig weder die Funktionsmechanismen der Token noch die technischen Risiken der zugrunde liegenden Systeme. Der normative Anspruch umfassender Transparenz stößt somit an die Grenzen praktischer Verständlichkeit.

Drittens erfordert ein zukunftsfähiger Verbraucherschutz effektive Rechtsdurchsetzung. Österreich verfügt mit Verbandsklagen, UWG-Instrumenten und Schadenersatzrecht über mächtige Werkzeuge, deren Effektivität jedoch voraussetzt, dass der zugrunde liegende Rechtsverstoß klar einem geregelten Pflichtenkanon zugeordnet werden kann.³⁹⁷ Solange die Rechtsnatur von Kryptovermögen offenbleibt und die vertraglichen Strukturen nicht eindeutig kategorisiert werden können, ist die gerichtliche Durchsetzung von Ansprüchen erschwert oder faktisch unmöglich.

Aus diesen drei normativen Leitlinien ergibt sich die zentrale Erkenntnis dieses Kapitels: Der österreichische Verbraucherschutz verfügt zwar über ausgeprägte formelle Schutzmechanismen, deren tatsächliche Wirksamkeit jedoch maßgeblich von der rechtlichen Einordnung kryptobasierter Vermögenspositionen abhängt. Solange zentrale Fragen der Qualifikation und Zuordnung von Kryptowerten nicht abschließend geklärt sind, können auch bestehende Schutzinstrumente ihre Wirkung nur eingeschränkt entfalten. Solange grundlegende Kategorien – insbesondere Eigentum, Vertragsgegenstand, Leistungsstörung,

³⁹⁵ Vgl. § 285 ABGB; vgl. § 292 ABGB.

³⁹⁶ Vgl. § 4 Abs. 1 FAGG; vgl. § 6 Abs. 3 KSchG; vgl. § 2 Abs. 1 UWG.

³⁹⁷ Vgl. Richtlinie (EU) 2020/1828 (ABl. L 409 vom 04.12.2020, S. 1); vgl. § 1 Abs. 1 UWG, BGBl. Nr. 448/1984; vgl. § 1295 Abs. 1 ABGB.

Aus- und Absonderung, Anspruchskategorien und Beweislast – nicht abschließend geklärt sind, bleiben selbst hohe regulatorische Standards nur begrenzt wirksam.

8.2 Zivilrechtliche Einordnung von Kryptovermögen im österreichischen Recht

Das ABGB definiert eine Sache als einen körperlichen Gegenstand (§ 285 ABGB). Kryptowerte sind jedoch rein digitale Manifestationen, die technisch als verteilte Datensätze existieren. Eine Einordnung als körperliche Sache ist daher ausgeschlossen. Auch die Subsumtion unter den Begriff der unkörperlichen Sache – wie bei Forderungen oder Immaterialgüterrechten – ist problematisch, weil Token regelmäßig keine selbstständige rechtliche Position verkörpern, sondern lediglich den Zugriff auf ein technisches System oder ein wirtschaftliches Versprechen symbolisieren.³⁹⁸

Die österreichische Literatur betont daher, dass Token nicht als Rechtsobjekte ex lege existieren, sondern nur dann eine rechtliche Wirkung entfalten können, wenn ihnen eine zivilrechtliche Position zugrunde liegt, wie etwa eine schuldrechtliche Forderung oder ein Anteil.³⁹⁹ Dies führt zu einer kategorialen Unsicherheit, da viele Token weder eindeutig einer Forderung noch einem Beteiligungs- oder Nutzungsrecht zugeordnet werden können.

Eine verbreitete Ansicht sieht Kryptowerte als rein schuldrechtliche Positionen. Der Token repräsentiere lediglich einen Anspruch gegen einen Emittenten oder Dienstleister.⁴⁰⁰ Dies ist insbesondere bei zentral ausgegebenem Token oder bei Plattformdiensten relevant, bei denen das „Guthaben“ der Nutzer:innen nicht auf einer eigenständigen Vermögensposition beruht, sondern lediglich eine interne Verrechnung darstellt.

Für den Verbraucherschutz bedeutet diese Einordnung, dass Kund:innen keine dinglich gesicherte Rechtsposition besitzen, sondern lediglich einen Anspruch gegenüber dem Dienstleister. Im Insolvenzfall werden sie zu einfachen Insolvenzgläubiger:innen, ohne Aussonderungsrecht. Die österreichische Insolvenzordnung sieht ein Aussonderungsrecht (§ 44 IO) nur für eindeutig fremde Vermögensgegenstände vor.⁴⁰¹ Bei bloßen schuldrechtlichen Ansprüchen greift dieses Instrument nicht.

Eine zweite hervorgehobene Sichtweise versteht Token nicht als Rechtsobjekte, sondern als „faktische Machtposition“, die durch technische Kontrolle entsteht.⁴⁰² Die Verfügungsbefugnis folge aus dem Besitz des privaten Schlüssels, nicht aus einem rechtlichen Eigentumstitel.

³⁹⁸ Vgl. Richtlinie (EU) 2020/1828 (ABl. L 409 vom 04.12.2020, S. 1); vgl. § 1 Abs. 1 UWG, BGBl. Nr. 448/1984; vgl. § 1295 Abs. 1 ABGB.

³⁹⁹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 213 f.

⁴⁰⁰ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 671-673.

⁴⁰¹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 651-658.

⁴⁰² Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 789, 652.

Diese Auffassung trägt zwar den technischen Gegebenheiten von Blockchain-Systemen Rechnung, führt jedoch zu erheblichen rechtlichen Unsicherheiten. Die Verfügungsmacht über einen Kryptowert beruht dabei im Wesentlichen auf der Kontrolle des privaten Schlüssels und damit auf einer technischen Zugriffsmöglichkeit, ohne dass hieraus automatisch ein eindeutiger Rechtstitel folgt. Gleichzeitig entsteht kein klassischer sachenrechtlicher Schutz, da das ABGB grundsätzlich nicht bloße faktische Machtpositionen, sondern nur rechtlich anerkannte Rechtspositionen schützt. Dadurch können Unsicherheiten hinsichtlich des Umfangs und der Durchsetzbarkeit der Rechte von Verbraucher:innen entstehen. Im Streitfall fehlt eine klare Anspruchsgrundlage, da der Verlust des privaten Schlüssels nicht als Eigentumsverletzung im Sinne des § 366 ABGB verstanden werden kann. Dies führt dazu, dass Verbraucher:innen im Konfliktfall lediglich deliktische oder vertragliche Ansprüche geltend machen können, deren Erfolg von der Nachweisbarkeit einer Pflichtverletzung abhängt – ein erhebliches Hindernis angesichts komplexer technischer Abläufe.

Die Literatur diskutiert, ob Token als „sonstige Rechte“ einzuordnen sind.⁴⁰³ Darunter fallen Vermögenswerte Positionen, die keine Sachen oder Forderungen sind, aber dennoch ein subjektives Recht begründen. Klassische Beispiele sind Immaterialgüterrechte oder gesellschaftsrechtliche Beteiligungsrechte.

Die Einordnung von Token als sonstige Rechte könnte theoretisch eine Brücke zwischen technischer Struktur und rechtlicher Dogmatik schlagen. Praktisch scheitert diese Lösung jedoch häufig daran, dass Token mangels rechtlicher Normierung kein eigenes Rechtsinstitut darstellen. Ein „Recht an einem Token“ lässt sich nur begründen, wenn der Token selbst ein vom Recht anerkanntes Rechtsobjekt darstellt. Dies ist bislang nicht der Fall.⁴⁰⁴

Damit bleibt die Kategorie der „sonstigen Rechte“ ein theoretischer Ansatz ohne tragfähige Grundlage im geltenden Recht.

8.2.1 Konsequenzen für den Eigentumsschutz

Da Kryptowerte in keiner bestehenden Kategorie des Sachenrechts eindeutig verankert sind, können Verbraucher:innen kein Eigentum im Sinne des ABGB erwerben. Eigentum setzt ein Rechtsobjekt voraus.⁴⁰⁵ Daraus ergeben sich weitreichende Konsequenzen: Es besteht kein Herausgabeanspruch nach § 366 ABGB, kein Eigentumsfreiheitsanspruch nach § 354 ABGB, keine dingliche Abwehrposition gegenüber Eingriffen Dritter, kein gutgläubiger Erwerb sowie

⁴⁰³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 213.

⁴⁰⁴ Ebd

⁴⁰⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 76; vgl. § 285, § 292 und § 353 ABGB.

keine sachenrechtliche Vindikation. Die fehlende Einordnung als Rechtsobjekt kann somit den Umfang des zivilrechtlichen Schutzes erheblich einschränken.⁴⁰⁶

Die Folgen für den Verbraucherschutz sind gravierend. Selbst wenn Verbraucher:innen nach ihrem subjektiven Verständnis „Eigentümer“ eines Tokens sind, besitzen sie rechtlich nur eine faktische Verfügungsposition, nicht aber eine sachenrechtlich abgesicherte Rechtsposition.

8.2.2 Konsequenzen für das Insolvenzrecht

Im Insolvenzfall eines Dienstleisters hängt die Zuordnung von Kryptowerten maßgeblich davon ab, ob diese als fremdes Eigentum qualifiziert, werden können. Nur wenn eine solche Zuordnung möglich ist, kommen Aussonderungsrechte in Betracht. Fehlt hingegen eine eigentumsrechtlich geschützte Rechtsposition, besteht regelmäßig auch kein Aussonderungsanspruch, sodass die betroffenen Vermögenswerte der Insolvenzmasse zugeordnet werden können. Vereinfacht gilt daher: Ohne Eigentum kein Aussonderungsrecht.⁴⁰⁷ Für die insolvenzrechtliche Behandlung von Kryptowerten ist die rechtliche Einordnung von entscheidender Bedeutung. Werden Token lediglich als schuldrechtliche Positionen qualifiziert, besteht regelmäßig kein Aussonderungsrecht. Gleiches gilt, wenn Token lediglich als faktische Positionen beziehungsweise technische Zugriffsmöglichkeiten verstanden werden. Selbst wenn Kryptowerte als sonstige Rechte eingeordnet werden, kommt eine Aussonderung grundsätzlich nur dann in Betracht, wenn eine eindeutige individuelle Zuordnung der betreffenden Vermögenswerte möglich ist. Gerade bei der Verwahrung in Sammelwallets (Omnibus Wallets) ist eine solche eindeutige Zuordenbarkeit jedoch häufig nur eingeschränkt oder gar nicht gegeben.⁴⁰⁸

8.3 Vertragsrechtliche Behandlung kryptobasierter Dienstleistungen im österreichischen Recht

Die vertragliche Einordnung kryptobasierter Dienstleistungen bildet die zentrale Schnittstelle zwischen der zivilrechtlichen Struktur des ABGB und den speziellen Schutzmechanismen des Verbraucherschutzrechts. Auch wenn die Erstellung und Übertragung von Kryptowerten technisch auf automatisierten Protokollprozessen beruht, richtet sich ihre rechtliche Behandlung maßgeblich nach den vertraglichen Rechtsverhältnissen zwischen Unternehmer:in und Verbraucher:in. Die technischen Abläufe der Blockchain bestimmen zwar die praktische Durchführung von Transaktionen, die daraus resultierenden Rechte und Pflichten werden jedoch grundsätzlich durch die jeweiligen vertraglichen Vereinbarungen und die anwendbaren

⁴⁰⁶ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 76; vgl. §§ 354, 366 und 367 ABGB.

⁴⁰⁷ Vgl. § 44 Abs. 1 IO; vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 653, 658.

⁴⁰⁸ Ebd

Rechtsvorschriften bestimmt.⁴⁰⁹ Die Frage, welche Vertragstypen dabei einschlägig sind und welche Pflichten daraus resultieren, ist für den Verbraucherschutz von grundlegender Bedeutung, da die vertragliche Struktur den Anwendungsbereich des FAGG, des KSchG und der AGB-Kontrolle determiniert und zugleich die Ausgangsebene für Haftungs- und Leistungsstörungenfolgen bildet.⁴¹⁰

8.3.1 Vertragstypologie und hybride Leistungsmodelle

Kryptodienstleistungen lassen sich nicht ohne Weiteres in die klassischen Vertragskategorien des ABGB einordnen. Die Praxis zeigt eine Vielzahl hybrider Modelle, die Elemente des Kaufvertrags, der Werkleistung, der Geschäftsbesorgung und der Verwahrung kombinieren.⁴¹¹ Typische Erscheinungsformen sind:

Token-Erwerbsverträge (z. B. Kauf oder Tausch digitaler Einheiten),
Plattformnutzungsverträge (Zugang zu Handels- oder Verwahrungsumgebungen),
Verwahrverträge (Custody Services),
Dienstleistungsverträge (z. B. Staking, Brokerleistungen),
Austauschverträge mit integrierter Risikopartizipation (z. B. Pools, automatisierte Liquiditätsmechanismen).

Das österreichische Vertragsrecht verlangt für jede vertragliche Beziehung eine eindeutige Bestimmung von Leistung und Gegenleistung. Diese Bestimmbarkeit ist bei kryptobasierten Leistungen jedoch systemisch erschwert, da der Vertragsgegenstand häufig nicht in einer materiellen oder rechtlich eindeutig definierten Position besteht. Nach österreichischem Vertragsrecht setzt das wirksame Zustandekommen eines Vertrages voraus, dass der Vertragsgegenstand ausreichend bestimmt oder zumindest bestimmbar ist.⁴¹² Bei Token und digitalen Wallet-Strukturen ist diese Bestimmtheit jedoch nicht selbstverständlich.

Problematisch sind insbesondere jene Konstellationen, in denen ein Token zwar eine bestimmte wirtschaftliche Funktion erfüllt, rechtlich jedoch keiner klaren Kategorie zugeordnet werden kann. Weitere Unsicherheiten entstehen, wenn die interne Kontenführung eines Dienstleisters nicht erkennen lässt, ob Verbraucher:innen einen originären Rechtsanspruch oder lediglich eine faktische Zuordnung erwerben, wenn der betreffende Token nicht eindeutig identifizierbar ist, etwa im Fall von Sammelverwahrung oder fungiblen Einheiten, oder wenn nicht offengelegt

⁴⁰⁹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 214, 641; vgl. § 861 ABGB; vgl. § 1 Abs. 1, § 6 Abs. 1 KSchG.

⁴¹⁰ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 640–643; vgl. § 1 Abs. 1 FAGG; vgl. § 1 Abs. 1, § 6 Abs. 1 KSchG; vgl. § 1295 Abs. 1, § 918 Abs. 1 ABGB.

⁴¹¹ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 641–643.

⁴¹² Vgl. § 861 und § 878 ABGB; vgl. OGH 7 Ob 253/01k, RIS-Justiz RS0013955.

wird, ob die Plattform den ausgewiesenen Token tatsächlich hält oder lediglich interne Verrechnungen vornimmt. Eine solche fehlende oder eingeschränkte Bestimmbarkeit des Vertragsgegenstands kann zu Unklarheiten hinsichtlich des Leistungsinhalts führen, die rechtliche Beurteilung von Leistungsstörungen erschweren und die Durchsetzung von Ansprüchen durch Verbraucher:innen beeinträchtigen.⁴¹³

8.3.2 Leistungsstörungen und Risikoverteilung

Das österreichische Vertragsrecht unterscheidet zwischen Unmöglichkeit, Verzug, Gewährleistung und Wandlung.⁴¹⁴ Kryptobasierte Vertragsmodelle führen jedoch zu Auslegungsschwierigkeiten, da nicht eindeutig bestimmt werden kann, welche Pflicht als „Hauptleistungspflicht“ des Unternehmers gilt und welche Rechtsfolgen bei Pflichtverletzung eintreten.

Beispiele: Bei Token-Erwerb ist unklar, ob die Leistungspflicht in der Übertragung eines spezifischen Tokens oder in der Ermöglichung einer Verfügungsmacht besteht.

Bei Wallet-Diensten stellt sich die Frage, ob der Anbieter lediglich technische Infrastruktur zur Verfügung stellt oder ob er für die Sicherung und Erhaltung der Tokenbestände haftet.

Bei Staking- oder Protokolldiensten ist strittig, ob der Anbieter für Verluste durch Protokollrisiken eintreten muss oder ob diese dem Verbraucher zugeordnet werden.

Die Beurteilung hängt maßgeblich von der rechtlichen Qualifikation des jeweiligen Vertragsmodells ab.⁴¹⁵

8.3.3 Intransparente Leistungsbeschreibungen

Ein strukturelles Problem kryptobasierter Dienstleistungsverträge ist die fehlende Transparenz.

Das KSchG fordert zwar klare und verständliche Vertragsinformationen (§ 5a KSchG), doch die Beschreibung kryptobasierter Leistungen ist aufgrund ihrer technischen und ökonomischen Komplexität oftmals selbst für sachkundige Verbraucher:innen schwer zu erfassen.⁴¹⁶

Intransparenz entsteht insbesondere durch:

unpräzise Begriffe (z. B. „Token“, „Guthaben“, „Erträge“),

fehlende Offenlegung der Rechtsnatur der übertragenen Position,

⁴¹³ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 213 f., 650–658; vgl. OGH 7 Ob 253/01k, RIS-Justiz RS0013955.

⁴¹⁴ Vgl. § 878, § 918 Abs. 1, § 922 Abs. 1 und § 932 Abs. 4 ABGB.

⁴¹⁵ Vgl. Miernicki, Kryptowerte im Privatrecht, MANZ (2023), S. 214, 641, 652 und 658; vgl. § 918 Abs. 1 ABGB.

⁴¹⁶ Vgl. § 5a Abs. 1, § 6 Abs. 3 KSchG; vgl. OECD, Financial Consumer Protection Policy Approaches in the Digital Age, 2020, S. 20 f.

Vermischung technischer und rechtlicher Kategorien in AGB, unklare Risikozuschreibungen (z. B. Hacks, Protokollfehler, Liquiditätsverluste), unvollständige Angaben über Verwahrstrukturen.

Die Rechtsprechung fordert, dass Klauseln so formuliert werden müssen, dass ein durchschnittlicher Verbraucher die Rechte und Pflichten ohne rechtliche Vorbildung nachvollziehen kann.⁴¹⁷ Bei vielen Kryptodienstleistungen ist dies praktisch nicht realisierbar. Die AGB-Kontrolle nach § 879 ABGB und § 6 KSchG kommt im Kryptobereich besondere Bedeutung zu. Kryptodienstleister verwenden regelmäßig Vertragsklauseln, die ihre Haftung für technische Ausfälle oder Systemstörungen einschränken oder ausschließen, Risiken weitgehend auf Verbraucher:innen verlagern, einseitige Änderungen von Leistungen oder Vertragsbedingungen ermöglichen oder auf unklaren und schwer verständlichen Formulierungen beruhen. Teilweise enthalten die Vertragsbedingungen zudem Regelungen, die die Geltendmachung von Ansprüchen durch Verbraucher:innen erschweren oder beschränken können. Vor diesem Hintergrund stellt die AGB-Kontrolle ein wesentliches Instrument dar, um die Transparenz und Fairness kryptobezogener Vertragsverhältnisse zu überprüfen und Verbraucher:innen vor unangemessenen Vertragsklauseln zu schützen. Nach österreichischem Recht sind Klauseln unzulässig, wenn sie den Verbraucher gröblich benachteiligen oder wesentliche Rechte aushöhlen.⁴¹⁸ Viele kryptospezifische Klauseln würden diesem Maßstab nicht standhalten, insbesondere weil sie die Rechtsnatur der übertragenen Position verschleiern oder das Risiko unabhängig von der Verantwortlichkeit dem Verbraucher zuordnen.

8.4 Haftung und Risikoallokation bei kryptobasierten Dienstleistungen

Die Haftungsordnung des österreichischen Rechts basiert auf der Annahme klar definierter Pflichtinhalte, eindeutig bestimmbarer Leistungsgegenstände und einer Zuordnung von Verantwortungsbereichen.⁴¹⁹ Kryptobasierte Dienstleistungen hingegen zeichnen sich durch komplexe technische Abläufe, verteilte Verantwortlichkeiten und schwer kontrollierbare Risikoquellen aus, die innerhalb der traditionellen Haftungssystematik nicht vorgesehen sind. Die Frage, wer für Verluste, Fehlfunktionen oder Systemrisiken einzustehen hat, ist daher für den Verbraucherschutz von zentraler Bedeutung.

⁴¹⁷ Vgl. § 6 Abs. 3 KSchG; vgl. OGH 25.02.2016, 2 Ob 20/15b; vgl. OGH, RIS-Justiz RS0016590 („Unklarheiten in Allgemeinen Geschäftsbedingungen gehen zu Lasten des Verwenders.“).

⁴¹⁸ Vgl. § 6 Abs. 1 KSchG; vgl. § 879 Abs. 3 ABGB.

⁴¹⁹ Vgl. § 1293, § 1295 Abs. 1, § 918 Abs. 1 und § 922 Abs. 1 ABGB; vgl. § 6 Abs. 3 KSchG.

8.4.1 Ausgangspunkt: Haftungssystematik im österreichischen Recht

Das österreichische Zivilrecht unterscheidet grundsätzlich zwischen verschiedenen Haftungsformen. Dazu zählen insbesondere die vertragliche Haftung, die an Pflichtverletzungen aus bestehenden Schuldverhältnissen anknüpft, die deliktische Haftung gemäß § 1295 ABGB für rechtswidrige und schuldhafte Schädigungen, die Gefährdungshaftung, die in bestimmten Sondergesetzen unabhängig von einem Verschulden vorgesehen ist, sowie die Haftung für Gehilfen nach § 1313a ABGB, bei der sich eine Person das Verhalten ihrer Erfüllungsgehilfen zurechnen lassen muss.⁴²⁰

Für die Beurteilung kryptobasierter Dienstleistungen ist vor allem die vertragliche Haftung relevant, da die Leistungserbringung auf vertraglichen Beziehungen zwischen Dienstleister und Verbraucher:in beruht. Haftung setzt jedoch voraus, dass eine Pflicht verletzt wurde – und genau dies ist im Kryptobereich oft unklar, weil die wesentlichen Pflichten aufgrund der unbestimmten Rechtsnatur des Vertragsgegenstands nicht eindeutig definiert sind.⁴²¹

8.4.2 Haftung für technische Systemrisiken

Kryptosysteme sind mit technischen Risiken verbunden, die teilweise außerhalb des unmittelbaren Einflussbereichs eines Dienstleisters liegen können. Dazu zählen etwa Netzwerkangriffe, Protokollfehler oder Störungen des Konsensmechanismus. Daraus ergibt sich die zentrale rechtliche Frage, ob ein eingetretener Schaden dem Verantwortungsbereich des Dienstleisters oder jenem der Verbraucher:innen zuzurechnen ist. Das österreichische Vertragsrecht verfolgt hierbei eine differenzierte Betrachtungsweise. Stellt ein Dienstleister die technische Infrastruktur zur Verfügung, ist er grundsätzlich für deren ordnungsgemäße Funktionsfähigkeit verantwortlich und hat für Mängel oder Störungen innerhalb seines Einflussbereichs einzustehen. Die Abgrenzung wird jedoch schwieriger, wenn die Ursache des Schadens in dezentralen Netzwerkstrukturen oder außerhalb der vom Dienstleister kontrollierten technischen Systeme liegt.⁴²² Wenn er lediglich eine Schnittstelle zu einem Drittsystem anbietet, hängt die Haftung vom konkret vereinbarten Leistungsumfang ab.⁴²³ Die meisten Kryptodienstleister versuchen, die Verantwortung durch AGB-Klauseln auszuschließen, indem sie z. B. erklären, dass „alle technischen Risiken beim Nutzer liegen“.

⁴²⁰ Vgl. § 1295 Abs. 1 und 2 sowie § 1313a ABGB.

⁴²¹ Vgl. § 1295 Abs. 1, § 918 Abs. 1 und § 922 Abs. 1 ABGB; vgl. § 6 Abs. 3 KSchG; vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 655.

⁴²² Vgl. § 1295 Abs. 1, § 918 Abs. 1, § 922 Abs. 1 und § 1313a ABGB.

⁴²³ Vgl. §§ 914, 915, § 1295 Abs. 1 und § 918 Abs. 1 ABGB.

Solche Klauseln sind im Verbrauchergeschäft jedoch nach § 6 KSchG regelmäßig unwirksam, weil sie wesentliche Rechte des Verbrauchers aushöhlen.⁴²⁴

8.4.3 Haftung für Verlust von Token (z. B. durch Hacks oder Fehltransaktionen)

Ein besonders praxisrelevanter Konfliktfall ist der Verlust von Kryptowerten infolge fehlerhafter Transaktionen, Hackerangriffe, Sicherheitslücken in Wallet-Systemen, Fehlbedienungen durch Verbraucher:innen oder Systemausfällen des Dienstleisters. Eine gefestigte österreichische Rechtsprechung zu diesen Fallkonstellationen hat sich bislang noch nicht herausgebildet. Die allgemeinen zivilrechtlichen Grundsätze bieten jedoch einen rechtlichen Orientierungsrahmen. So gehört bei Verwahr- und Plattformdienstleistungen regelmäßig die sichere Verwahrung der Kryptowerte zu den vertraglichen Hauptleistungspflichten, soweit eine entsprechende Verwahrung vereinbart wurde. Wird dieses vertraglich geschuldete Sicherheitsniveau nicht eingehalten, kann dies eine Verletzung vertraglicher Pflichten darstellen und entsprechende Haftungsfolgen auslösen.⁴²⁵

Im Haftungsfall tragen Verbraucher:innen grundsätzlich die Beweislast für den eingetretenen Schaden sowie für das Vorliegen einer Pflichtverletzung. Demgegenüber hat der Dienstleister darzulegen, dass er die erforderlichen und zumutbaren Sicherheitsmaßnahmen getroffen hat, um Schäden zu verhindern. In der Praxis gestaltet sich diese Beweisführung jedoch häufig schwierig, da die zugrunde liegenden technischen Abläufe, Sicherheitsmechanismen und Ursachen eines Schadens für Verbraucher:innen oftmals nur schwer nachvollziehbar sind. Die hohe technische Komplexität kryptobasierter Systeme kann daher die Durchsetzung von Ansprüchen erheblich erschweren.⁴²⁶

Haftungsausschlüsse: Vertragsklauseln, die die Haftung für Hackerangriffe oder für eine pauschal definierte „höhere Gewalt digitaler Systeme“ ausschließen, können rechtlich problematisch sein. Soweit solche Klauseln zu einer unangemessenen Verlagerung von Risiken auf Verbraucher:innen führen oder wesentliche vertragliche Pflichten aushöhlen, können sie insbesondere im Rahmen der AGB-Kontrolle nach dem ABGB und dem KSchG als unzulässig angesehen werden. Dadurch soll verhindert werden, dass Dienstleister:innen zentrale Risiken ihres Geschäftsmodells einseitig auf Verbraucher:innen übertragen.⁴²⁷

⁴²⁴ Vgl. § 6 Abs. 1 und 3 sowie § 9 KSchG.

⁴²⁵ Vgl. § 1295 Abs. 1, § 918 Abs. 1, § 922 Abs. 1 und § 914 ABGB.

⁴²⁶ Vgl. § 1293, § 1295 Abs. 1 und § 1298 ABGB.

⁴²⁷ Vgl. § 6 Abs. 1 und 3, § 9 KSchG; vgl. § 1298 ABGB.

In der Praxis führt dies jedoch nicht automatisch zu effektiven Ansprüchen, da Verbraucher:innen die technische Beweisführung kaum leisten können — ein strukturelles Durchsetzungsdefizit.

8.4.4 Haftung bei Staking-, Lending- und Protokollinteraktionen

Besondere rechtliche Fragen stellen sich bei Plattformen, die Dienstleistungen im Zusammenhang mit Staking, DeFi-Lending oder Liquiditätspools anbieten. In diesen Fällen ist zunächst zu klären, welche konkrete Leistung der Dienstleister gegenüber Verbraucher:innen übernimmt. Dabei stellt sich insbesondere die Frage, ob der Anbieter einen bestimmten Ertrag oder eine Rendite schuldet, lediglich eine technische Vermittlungsleistung erbringt oder darüber hinaus ein eigenes wirtschaftliches Risiko übernimmt. Die Haftung richtet sich maßgeblich nach der jeweiligen Vertragsgestaltung und dem Inhalt der übernommenen Verpflichtungen. Wird Verbraucher:innen ein bestimmter Ertrag oder Erfolg zugesagt, kann dies dazu führen, dass der Dienstleister für das Erreichen dieses Erfolgs einzustehen hat. In solchen Fällen kann sich die Haftung nicht allein auf die Bereitstellung einer technischen Infrastruktur beschränken.⁴²⁸ Wird nur die Teilnahme am Protokoll ermöglicht, haftet der Dienstleister für sorgfaltswidrige Auswahl, Fehlkonfigurationen oder unzureichende Sicherheitsmaßnahmen.⁴²⁹ Werden Risiken auf den Verbraucher überwältzt, sind diese Klauseln regelmäßig intransparent.⁴³⁰ Österreichische Verbraucherschutznormen setzen voraus, dass ein Verbraucher die wirtschaftlichen Folgen eines Risikos einschätzen kann. Bei Staking- oder Protokolldiensten ist dies systemisch kaum möglich.

8.4.5 Haftung bei Fehlberatung und Informationspflichtverletzungen

Verletzungen von Informationspflichten können nach § 1300 ABGB sowie nach den einschlägigen Bestimmungen des KSchG Schadenersatzansprüche begründen. Eine Haftung kommt insbesondere dann in Betracht, wenn Verbraucher:innen über wesentliche Umstände des Geschäfts nicht ordnungsgemäß informiert werden. Dies kann etwa der Fall sein, wenn erhebliche Risiken nicht offengelegt, unzutreffende Angaben zu Eigentums- oder Rechtsverhältnissen gemacht, technische Sicherheitsmerkmale falsch dargestellt oder irreführende Aussagen über mögliche Renditen und Ertragschancen getroffen werden. In solchen Konstellationen kann die fehlerhafte oder unvollständige Information für die Anlage- oder Vertragsentscheidung der Verbraucher:innen ursächlich sein und entsprechende

⁴²⁸ Vgl. § 914, § 918 Abs. 1, § 922 Abs. 1 und § 1295 Abs. 1 ABGB.

⁴²⁹ Vgl. § 914, § 1295 Abs. 1, § 1298 und § 1313a ABGB.

⁴³⁰ Vgl. § 879 Abs. 3 ABGB; vgl. § 6 Abs. 3 KSchG.

Schadenersatzansprüche auslösen.⁴³¹ Die Schwierigkeit besteht aber darin, den Kausalzusammenhang zwischen unzureichender Information und Vermögensschaden zu beweisen. Aufgrund der Volatilität von Kryptomärkten ist dieser Nachweis mit erheblichen Unsicherheiten verbunden.

8.5 Reformbedarf und normative Handlungsoptionen für einen zukunftsfähigen Verbraucherschutz

Die bisherige Analyse hat gezeigt, dass das österreichische Zivilrecht, das Insolvenzrecht und die kollektivrechtlichen Durchsetzungsinstrumente den besonderen Herausforderungen kryptobasierter Dienstleistungen nicht vollständig gewachsen sind. Die zentralen Defizite – fehlende Eigentumstitel, intransparente Vertragsmodelle, mangelnde Insolvenzfestigkeit und eingeschränkte Rechtsdurchsetzung – sind struktureller Natur und lassen sich innerhalb des bestehenden Rahmens nur begrenzt lösen.⁴³²

Art. 38 GRC verpflichtet die Union, ein hohes Verbraucherschutzniveau sicherzustellen. Vor diesem Hintergrund stellt sich die Frage, inwieweit das bestehende nationale Rechtsgefüge den spezifischen Herausforderungen kryptobasierter Dienstleistungen gerecht wird.⁴³³

8.5.1 Einführung eines gesetzlichen Sondervermögensregimes für Kryptowerte

Ein zentrales Problem der österreichischen Rechtsordnung liegt darin, dass Kryptowerte mangels dinglicher Einordnung nicht als fremdes Eigentum qualifiziert werden können.

Um Verbraucher:innen zu schützen, wäre die Einführung eines Sondervermögensregimes notwendig, das Kryptowerte funktional, wie Wertpapier- oder Sondervermögen behandelt.⁴³⁴

Ein solches Regime könnte auf mehreren zentralen Schutzmechanismen beruhen. Dazu zählen insbesondere eine gesetzlich vorgeschriebene Trennung von Kundenvermögen und Unternehmensvermögen, die Verpflichtung zur individuellen oder zumindest indexbasierten Zuordenbarkeit der verwahrten Kryptowerte, ein Aussonderungsrecht im Insolvenzfall unabhängig von ihrer zivilrechtlichen Qualifikation sowie umfassende Aufzeichnungs- und Dokumentationspflichten, die eine eindeutige Zuordnung der Vermögenswerte zu den jeweiligen Kund:innen sicherstellen. Ein vergleichbarer Schutzgedanke findet sich bereits im Bereich der Wertpapierverwahrung. Das Depotgesetz sieht insbesondere die gesonderte Verwahrung anvertrauter Wertpapiere, die Führung individueller Depot- beziehungsweise

⁴³¹ Vgl. § 1300, § 1295 Abs. 1 ABGB; vgl. § 2 Abs. 1 UWG; vgl. § 4 Abs. 1 FAGG; vgl. § 6 Abs. 3 KSchG.

⁴³² Vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 6, 820; vgl. § 354 ABGB; vgl. § 44 IO; vgl. § 28 Abs. 1 KSchG; vgl. § 624 Abs. 1 ZPO idF BGBl. I 2024/85.

⁴³³ Vgl. Art. 38 GRC.

⁴³⁴ Vgl. § 285 und § 354 ABGB; vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 821.

Kontostrukturen sowie entsprechende Buchführungs- und Dokumentationspflichten vor. Darüber hinaus stehen die in einem Sammeldepot verwahrten Wertpapiere grundsätzlich im Miteigentum der Hinterleger:innen, wodurch deren Rechtsposition im Insolvenzfall besonders geschützt wird. Diese Grundsätze können als Orientierung für die Ausgestaltung eines vergleichbaren Schutzsystems im Bereich der Kryptoverwahrung dienen.⁴³⁵

8.5.2 Klarstellung der Rechtsnatur von Token durch eine gesetzliche Definition

Die Anwendbarkeit der klassischen privatrechtlichen Kategorien der Sache, der Forderung oder sonstiger absoluter Rechte auf Kryptowerte ist eigenständig zu prüfen. Daraus kann sich im Einzelfall ein Klärungsbedarf hinsichtlich ihrer zivilrechtlichen Qualifikation ergeben. Eine gesetzliche Klarstellung könnte dazu beitragen, den Status von Token systematisch zu bestimmen und sie – sofern geboten – als eigenständige vermögensrechtliche Position normativ zu erfassen.⁴³⁶ Eine solche Definition sollte einen klar abgegrenzten Anwendungsbereich aufweisen und die rechtliche Stellung von Kryptowerten eindeutig festlegen. Darüber hinaus sollte sie Eigentums- oder sonstige Zuweisungsstrukturen normieren, die Voraussetzungen und Wirkungen von Verfügungen über Kryptowerte, einschließlich möglicher Regelungen zum gutgläubigen Erwerb, festlegen sowie die rechtliche Behandlung von Verlusten, Hackerangriffen und Fehltransaktionen ausdrücklich regeln. Schließlich sollte ein solcher Rechtsrahmen auch sicherstellen, dass die Rechtsposition von Verbraucher:innen im Insolvenzfall wirksam geschützt wird und eine ausreichende Insolvenzfestigkeit der zugeordneten Vermögenswerte gewährleistet ist.⁴³⁷ Das ABGB unterscheidet zwischen Sachen im Sinne des § 285 ABGB und Vermögenswerten Rechten wie Forderungen (§ 1392 ABGB). Die Anwendbarkeit dieser Kategorien auf Kryptowerte ist eigenständig zu prüfen. In der Literatur werden gesetzgeberische Klarstellungen zur systematischen Einordnung diskutiert.⁴³⁸

8.5.3 Mindeststandards für Verwahr-, Plattform- und Stakingdienste

Die Verordnung (EU) 2023/1114 erfasst unter anderem die Verwahrung und Verwaltung von Kryptowerten für Kunden. Unabhängig davon gelten allgemeine zivilrechtliche Sorgfaltspflichten. Spezifische kryptobezogene Mindeststandards sind jedoch unionsrechtlich nur für regulierte Dienstleistungen ausdrücklich normiert.⁴³⁹

Ein modernes Verbraucherschutzregime für Kryptowerte sollte daher spezifische

⁴³⁵ Vgl. § 2 Abs. 1, § 4 Abs. 1, § 5 und § 11 DepotG; vgl. § 44 IO.

⁴³⁶ Vgl. § 285, § 354 und § 1392 ABGB; vgl. Miernicki, *Kryptowerte im Privatrecht*, MANZ (2023), S. 821.

⁴³⁷ Vgl. § 354 und § 367 ABGB; vgl. § 44 IO; vgl. Art. 2 Verordnung (EU) 2023/1114 (MiCA).

⁴³⁸ Vgl. § 285 und § 1392 ABGB.

⁴³⁹ Vgl. Art. 3 Abs. 1 Z 16 und Art. 6 Verordnung (EU) 2023/1114 (MiCA); vgl. § 1299 ABGB; vgl. § 2a Abs. 1 UWG.

Mindeststandards vorsehen. Dazu gehören insbesondere Pflichten zur sicheren Verwahrung und Risikominderung, die teilweise bereits durch bestehende unionsrechtliche Regelungen abgedeckt werden. Ergänzend sollten technische Mindestanforderungen, etwa der Einsatz von Multi-Signature-Lösungen oder segmentierten Wallet-Strukturen, festgelegt werden. Ebenso erforderlich sind Transparenzpflichten hinsichtlich der Verwahrstruktur und Wallet-Architektur, regelmäßige externe Sicherheitsprüfungen sowie eine klare Offenlegung der Risikoverteilung bei Staking-, Lending- und vergleichbaren Modellen. Darüber hinaus dürfen Allgemeine Geschäftsbedingungen Verbraucher:innen nicht gröblich benachteiligen und sind unwirksam, wenn sie unklar oder intransparent formuliert sind. Vor diesem Hintergrund kann eine gesetzliche Konkretisierung der Pflichten und Verantwortlichkeiten dazu beitragen, eine unangemessene Verlagerung technischer, wirtschaftlicher oder rechtlicher Risiken auf Verbraucher:innen zu verhindern und das Schutzniveau im Kryptobereich nachhaltig zu stärken.⁴⁴⁰

8.5.4 Anpassung des FAGG und des KSchG an digitale, technisch irreversible Dienstleistungen

Das Fern- und Auswärtsgeschäfte-Gesetz gewährt dem Verbraucher grundsätzlich ein 14-tägiges Rücktrittsrecht bei Fernabsatzverträgen.⁴⁴¹ Dieses Rücktrittsrecht kann jedoch unter bestimmten Voraussetzungen vorzeitig erlöschen, insbesondere wenn der Unternehmer – auf Grundlage eines ausdrücklichen Verlangens des Verbrauchers – vor Ablauf der Rücktrittsfrist mit der Ausführung der Dienstleistung beginnt und der Verbraucher seine Kenntnis vom Verlust des Rücktrittsrechts bestätigt.⁴⁴² Gleiches gilt für die Lieferung digitaler Inhalte, wenn der Verbraucher ausdrücklich zustimmt und den Verlust des Rücktrittsrechts zur Kenntnis nimmt.⁴⁴³ Diese gesetzliche Systematik ist auf einen Leistungsaustausch zugeschnitten, bei dem der Zeitpunkt der vollständigen Leistungserbringung rechtlich eindeutig bestimmbar ist. Bei kryptobasierten Transaktionen stellt sich jedoch die Frage, wie diese Voraussetzungen bei technisch automatisierten oder blockchainbasierten Abläufen zu beurteilen sind. Zwar enthält das FAGG klare Informationspflichten, wonach dem Verbraucher rechtzeitig vor Abgabe seiner Vertragserklärung bestimmte Informationen klar und verständlich zur Verfügung zu stellen sind,⁴⁴⁴ doch regelt das Gesetz nicht ausdrücklich, wie irreversible digitale Transaktionen im Einzelnen zu behandeln sind.

⁴⁴⁰ Vgl. § 879 Abs. 3 ABGB; vgl. § 6 Abs. 3 KSchG; vgl. § 2a Abs. 1 UWG.

⁴⁴¹ Vgl. § 11 Abs. 1 FAGG.

⁴⁴² Vgl. § 18 Abs. 1 Z 1 FAGG.

⁴⁴³ Vgl. § 18 Abs. 1 Z 11 FAGG.

⁴⁴⁴ Vgl. § 4 Abs. 1 FAGG.

Vor diesem Hintergrund könnten – unter Wahrung der bestehenden Systematik – folgende Aspekte einer näheren gesetzlichen Präzisierung bedürfen:

Klarstellung des Beginns der vollständigen Leistungserbringung bei blockchainbasierten Dienstleistungen, insbesondere bei automatisierten Smart-Contract-Abläufen.

Konkretisierung der Zustimmungserfordernisse im Sinne des § 18 FAGG, etwa hinsichtlich Form, Deutlichkeit und technischer Gestaltung der Zustimmungserklärung.

Transparenzanforderungen in unmittelbarem Zusammenhang mit dem Widerrufsverlust, um sicherzustellen, dass die Kenntnisbestätigung nicht bloß formelhaft erfolgt.

Abgrenzung zwischen digitalen Inhalten und digitalen Dienstleistungen im Kontext von Token-Übertragungen oder Staking-Modellen.

Kohärente Verzahnung mit dem KSchG, insbesondere hinsichtlich der Unzulässigkeit gröblich benachteiligender Klauseln (§ 879 Abs 3 ABGB) und unklarer Vertragsbestimmungen (§ 6 Abs 3 KSchG).

Eine solche Präzisierung würde nicht die Grundstruktur des FAGG verändern, sondern die bestehenden Informations- und Zustimmungserfordernisse an die Besonderheiten technisch determinierter Transaktionen anpassen.

8.5.5 Stärkung der kollektiven Rechtsdurchsetzung im Kryptobereich

Die kollektive Rechtsdurchsetzung stellt eine zentrale Säule des österreichischen Verbraucherschutzsystems dar. Nach § 28 Abs 1 KSchG können qualifizierte Einrichtungen gegen gesetzwidrige Vertragsklauseln auf Unterlassung klagen.⁴⁴⁵ Auch nach § 1 Abs 1 UWG besteht die Möglichkeit, unlautere Geschäftspraktiken gerichtlich zu untersagen.⁴⁴⁶ Diese Instrumente sind strukturell auf präventiven Rechtsschutz ausgerichtet und bezwecken primär die Unterbindung rechtswidriger Verhaltensweisen. Mit der Umsetzung der Verbandsklagen-Richtlinie wurde zudem in der ZPO eine „Verbandsklage auf Abhilfe“ eingeführt, wonach qualifizierte Einrichtungen im Namen von zumindest 50 Verbrauchern Klage erheben können.⁴⁴⁷ Damit wurde das kollektive Rechtsschutzinstrumentarium erweitert. Gleichwohl bleibt festzuhalten, dass die bestehenden Modelle in ihrer Ausgestaltung spezifische Herausforderungen kryptobasierter Geschäftsmodelle nur begrenzt adressieren. Zum einen folgt die zivilprozessuale Beweislast grundsätzlich dem allgemeinen Grundsatz, wonach derjenige, der sich auf ein Recht beruft, dessen Voraussetzungen zu beweisen hat.⁴⁴⁸ In

⁴⁴⁵ Vgl. § 28 Abs. 1 KSchG.

⁴⁴⁶ Vgl. § 1 Abs. 1 UWG.

⁴⁴⁷ Vgl. § 624 Abs. 1 ZPO idF BGBl. I 2024/85.

⁴⁴⁸ Vgl. § 1298 ABGB.

technisch komplexen Sachverhalten – etwa bei Verwahrstrukturen, algorithmischen Abläufen oder internen Wallet-Zuordnungen – kann diese Beweisführung faktisch erschwert sein, da wesentliche Informationen ausschließlich im Einflussbereich des Dienstleisters liegen. Das geltende Recht enthält hierfür keine allgemeine kryptospezifische Beweiserleichterung. Zum anderen sind die bestehenden Verbandsinstrumente überwiegend auf Unterlassung oder – im Fall der Abhilfeklage – auf eine Bündelung gleichgerichteter Ansprüche ausgerichtet. Sie ersetzen jedoch keine umfassende Sammelklage im Sinne eines automatisch für alle Betroffenen wirkenden kollektiven Schadenersatzverfahrens.⁴⁴⁹

Vor diesem Hintergrund könnten Reformüberlegungen an mehreren Punkten ansetzen, ohne die Systematik des bestehenden Rechts grundlegend zu verändern:

Präzisierung der Beweisregeln bei technisch komplexen Sachverhalten, insbesondere durch verstärkte Dokumentations- oder Offenlegungspflichten von Plattformbetreibern;

Erweiterung bestehender Auskunftsrechte, soweit diese zur Durchsetzung zivilrechtlicher Ansprüche erforderlich sind;

Stärkung der Verbandslegitimation in besonders komplexen Marktsegmenten;

Verzahnung mit aufsichtsrechtlichen Informationsstrukturen, insbesondere im Rahmen der Zuständigkeiten nach Art 93 VO (EU) 2023/1114.⁴⁵⁰

Solche Maßnahmen würden nicht neue materielle Rechte schaffen, sondern die effektive Durchsetzung bestehender Ansprüche unterstützen und damit das unionsrechtlich vorgegebene Ziel eines hohen Verbraucherschutzniveaus strukturell absichern.⁴⁵¹

8.5.6 Institutionelle Weiterentwicklung des Kryptoverbraucherschutzes

Die unionsrechtliche Regulierung sieht vor, dass die Mitgliedstaaten eine oder mehrere zuständige Behörden benennen, welche die Einhaltung der Vorschriften über Kryptowerte-Dienstleistungen überwachen.⁴⁵² In Österreich nimmt diese Funktion die Finanzmarktaufsichtsbehörde wahr.⁴⁵³ Damit besteht ein sektorales Aufsichtssystem für jene Kryptowerte-Dienstleistungen, die in den Anwendungsbereich der Verordnung (EU) 2023/1114 fallen. Gleichwohl ist der unionsrechtliche Regelungsbereich sachlich determiniert. Die Verordnung gilt nur für die in ihrem Anwendungsbereich erfassten Kryptowerte und Dienstleistungen.⁴⁵⁴ Daraus ergibt sich, dass die aufsichtsrechtliche Zuständigkeit ebenfalls an

⁴⁴⁹ Vgl. § 624 Abs 1 ZPO.

⁴⁵⁰ Vgl. Art. 93 Abs. 1 Verordnung (EU) 2023/1114 (MiCA).

⁴⁵¹ Vgl. Art 38 GRC.

⁴⁵² Vgl. Art 93 Abs 1 VERORDNUNG (EU) 2023/1114 (MICA).

⁴⁵³ Vgl. § 1 Abs 1 MiCA-VVG.

⁴⁵⁴ Vgl. Art 2 VERORDNUNG (EU) 2023/1114 (MICA).

diesen Anwendungsbereich gebunden ist. Die privatrechtliche Durchsetzung von Verbraucheransprüchen – etwa aus Vertrags-, Delikts- oder Bereicherungsrecht – bleibt davon unberührt und erfolgt weiterhin im Wege zivilgerichtlicher Geltendmachung.⁴⁵⁵

Vor diesem Hintergrund stellt sich die systematische Frage, ob die bestehende institutionelle Architektur sämtliche verbraucherschutzrechtlich relevanten Konstellationen kryptobasierter Geschäftsmodelle in ausreichender Weise abbildet. Während die Finanzmarktaufsicht auf die Einhaltung regulatorischer Vorgaben ausgerichtet ist, verfolgt das Zivilrecht primär individualrechtliche Ausgleichsmechanismen. Eine funktionale Verzahnung beider Ebenen ist gesetzlich nicht umfassend normiert. Reformüberlegungen könnten daher – ohne die bestehende Kompetenzordnung grundlegend zu verändern – an einer institutionellen Spezialisierung oder Koordinierung ansetzen. Denkbar wären etwa eine vertiefte Marktbeobachtung digitaler Vermögenswerte im Rahmen der bestehenden Aufsichtszuständigkeiten, der Aufbau strukturierter Informationskanäle zwischen Aufsichtsbehörden und qualifizierten Einrichtungen im Sinne des § 29 KSchG, die systematische Veröffentlichung verbraucherrelevanter Risiko- und Warnhinweise sowie koordinierte Analysen besonders komplexer Marktpraktiken und Geschäftsmodelle. Solche Maßnahmen könnten dazu beitragen, Transparenz zu erhöhen, Risiken frühzeitig zu identifizieren und Verbraucher:innen besser über die Besonderheiten und Gefahren kryptobasierter Dienstleistungen zu informieren.

Solche Maßnahmen würden keine neue materiellrechtliche Anspruchsgrundlage schaffen, sondern könnten die Effektivität der Durchsetzung bestehender Rechte stärken. Dabei ist zu berücksichtigen, dass das unionsrechtliche Leitbild ein hohes Verbraucherschutzniveau verlangt.⁴⁵⁶ Eine institutionelle Weiterentwicklung müsste sich daher an diesem Ziel orientieren und zugleich die Kompetenzverteilung zwischen Aufsicht und Gerichten wahren.

8.5.7 Gesamtsynthese

Die Untersuchung hat gezeigt, dass kryptobezogene Dienstleistungen nicht an einzelnen Regelungsdefiziten leiden, sondern strukturelle Spannungen zwischen bestehenden Rechtsbereichen offenlegen. Die Herausforderungen ergeben sich weniger aus einem völligen Fehlen normativer Instrumente als aus deren fehlender Kohärenz im digitalen Kontext. Eigentumszuordnung, insolvenzrechtliche Behandlung, vertragliche Ausgestaltung, Informationsregime und kollektive Rechtsdurchsetzung sind jeweils eigenständig geregelt, greifen jedoch bei digital vermittelten Vermögenspositionen nicht durchgehend ineinander.

⁴⁵⁵ Vgl. § 28 Abs. 1 KSchG; vgl. § 1295 Abs. 1 ABGB.

⁴⁵⁶ Vgl. Art. 38 GRC.

Die Analyse verdeutlicht, dass der formale Anwendungsbereich bestehender Normen nicht automatisch deren materielle Schutzwirkung garantiert. Gerade bei technisch determinierten und grenzüberschreitenden Geschäftsmodellen entstehen Situationen, in denen Verbraucher:innen zwar rechtlich adressiert sind, ihre Position jedoch faktisch geschwächt bleibt. Die Schutzinstrumente wirken fragmentiert, während die ökonomische und technische Struktur der Dienstleistungen systematisch integriert ist. Dadurch entsteht ein strukturelles Ungleichgewicht zwischen normativer Ordnung und tatsächlicher Marktpraxis.

Dieses Ungleichgewicht manifestiert sich insbesondere in drei Dimensionen: in der Unklarheit über die rechtliche Zuordnung digitaler Vermögenspositionen, in der praktischen Durchsetzbarkeit individueller Ansprüche sowie in der begrenzten institutionellen Verzahnung zwischen privatrechtlicher und aufsichtsrechtlicher Ebene. Diese Aspekte verstärken einander und führen dazu, dass bestehende Schutzmechanismen nicht in vollem Umfang ihre intendierte Wirkung entfalten.

Die zentrale Leitthese der Arbeit bestätigt sich damit: Konsument:innen sind im Umgang mit kryptobasierten Dienstleistungen strukturell, rechtlich und faktisch nur eingeschränkt geschützt. Strukturell, weil die Systemarchitektur digitaler Vermögensmodelle nicht vollständig mit den traditionellen rechtlichen Einordnungs- und Regelungskonzepten übereinstimmt. Rechtlich, weil zentrale Qualifikations- und Zuweisungsfragen nicht ausdrücklich normiert sind. Faktisch, weil Informationsasymmetrien und technische Komplexität die effektive Rechtsdurchsetzung erschweren.

Ein zukunftsfähiger Verbraucherschutz im Kryptobereich erfordert daher keine Abkehr von den Grundprinzipien der österreichischen Rechtsordnung, sondern deren konsistente Fortentwicklung unter Wahrung systematischer Kohärenz. Maßgeblich ist, dass rechtliche Zuweisungen eindeutig bestimmbar bleiben, Durchsetzungsmechanismen praktisch zugänglich sind und Transparenzpflichten die tatsächliche Entscheidungsfreiheit der Verbraucher:innen stärken. Nur unter diesen Voraussetzungen kann das unionsrechtliche Leitbild eines hohen Verbraucherschutzniveaus auch im Bereich digitaler Vermögenswerte wirksam verwirklicht werden.

Literaturverzeichnis

1. **Andrade, Joao / Sharman, Stephen / Xiao, Lydia Y. / Newall, Philip W. S. (2022):** *Safer Gambling and Consumer Protection Failings Among 40 Frequently Used Crypto-Gambling Services*. Journal of Gambling Studies. Verfügbar unter : [Safer gambling and consumer protection failings among 40 frequently visited cryptocurrency-based online gambling operators - PubMed](#) am 10.06.2026
2. **ASBJ Secretariat (2018):** *About the Practical Solution on the Accounting for Virtual Currencies under the Payment Services Act*. Tokio: Accounting Standards Board of Japan. Verfügbar unter: https://www.asb-j.jp/en/wp-content/uploads/sites/5/20180315-02_e.pdf am 10.06.2026
3. **Badev, Anton / Watsky, Michael (2023):** *Interconnected DeFi: Ripple Effects from the Terra Collapse*. Washington D.C.: Federal Reserve Board. Verfügbar unter: <https://www.federalreserve.gov/econres/feds/files/2023044pap.pdf> am 10.06.2026
4. **Bank for International Settlements (2023):** *The Crypto Ecosystem: Key Elements and Risks*. Basel: Bank for International Settlements. Verfügbar unter: <https://www.bis.org/publ/othp72.pdf> am 10.06.2026
5. **Binder Grösswang Rechtsanwälte GmbH (Hrsg.) (2020):** *Digital Law. 2. Auflage*. Wien: LexisNexis.
6. **Cambridge Centre for Alternative Finance (2024):** *2nd Global Cryptoasset Regulatory Landscape Study*. Cambridge: University of Cambridge. Verfügbar unter: <https://www.jbs.cam.ac.uk/wp-content/uploads/2024/10/2024-2nd-global-cryptoasset-regulatory-landscape-study.pdf> am 10.06.2026
7. **Chainalysis (2022):** *Crypto Crime Report 2022*. New York: Chainalysis. Verfügbar unter: <https://blog.blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf> am 10.06.2026
8. **Chamber of Digital Commerce – Token Alliance (2022):** *Legal Landscapes Governing Digital Tokens in Japan*. Verfügbar unter: <https://innovationlaw.jp/wp-content/uploads/2022/09/Japan-Legal-Landscapes.pdf>
9. **Coinbase, User Agreement, Governing Law (USA):** Verfügbar unter: https://www.coinbase.com/legal/user_agreement/united_states am 13.06.2026
10. **CNIL (2018):** *Blockchain and the GDPR*. Paris: Commission Nationale de l'Informatique et des Libertés. Verfügbar unter: <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> am 10.06.2026
11. **Congressional Research Service (2020):** *Cryptocurrency: The Economics of Money and Selected Policy Issues*. Washington D.C.: Congressional Research Service. Verfügbar unter: https://www.congress.gov/crs_external_products/R/PDF/R45427/R45427.3.pdf am 10.06.2026
12. **Congressional Research Service (2023):** *Cryptocurrency: Selected Policy Issues (R47425)*. Washington D.C.: Congressional Research Service. Verfügbar unter: <https://www.congress.gov/crs-product/R47425> am 10.06.2026
13. **Chernin, Abe / Moran, Nicole M. / Letson, Robert (2025):** *SEC Cryptocurrency Enforcement: 2024 Update*. Menlo Park: Cornerstone Research. Verfügbar unter: <https://www.cornerstone.com/insights/research/sec-cryptocurrency-enforcement-2025-update/> am 10.06.2026
14. **EBA – European Banking Authority (2019):** *Guidelines on ICT and Security Risk Management*. Paris: European Banking Authority. Verfügbar unter: <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-ict-and-security-risk-management?version=2019#activity-versions> am 10.06.2026

15. **EBA – European Banking Authority (2024):** *Draft Regulatory Technical Standards under MiCAR*. Paris: European Banking Authority. Verfügbar unter:
<https://www.eba.europa.eu/sites/default/files/2024-06/4998fc26-cc88-4ada-835c-292f831a4ccd/Final%20report%20on%20draft%20RTS%20on%20governance%20arrangements%20for%20remuneration%20under%20%20MICAR.pdf> am 10.06.2026
16. **ECB – Europäische Zentralbank (2022):** *Bitcoin's Last Stand*. Frankfurt am Main: Europäische Zentralbank. Verfügbar unter:
<https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog221130~5301eecd19.en.html> am 10.06.2026
17. **EDPB – European Data Protection Board:** *Guidelines on Identifiability and Pseudonymisation*. Brüssel: European Data Protection Board.
 Verfügbar unter: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf am 10.06.2026
18. **EDPB – European Data Protection Board:** *Guidelines on Controllers and Joint Controllers*. Brüssel: European Data Protection Board. Verfügbar unter:
https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf am 10.06.2026
19. **ESMA – European Securities and Markets Authority (2022):** *Advice on Crypto-Assets*. Paris: ESMA. Verfügbar unter:
https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets_de.pdf am 10.06.2026
20. **ESMA – European Securities and Markets Authority (2023):** *Decentralised Finance Report*. Paris: ESMA. Verfügbar unter: https://www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf am 10.06.2026
21. **Ethereum Foundation (2022):** *The Merge – Proof-of-Stake Documentation*. Zug: Ethereum Foundation. Verfügbar unter:
<https://ethereum.org/roadmap/merge/> am 10.06.2026
22. **Europäische Kommission (2015):** *A Digital Single Market Strategy for Europe (COM(2015) 192 final)*. Brüssel: Europäische Kommission. Verfügbar unter:
https://ec.europa.eu/commission/presscorner/api/files/attachment/8210/DSM_communication.pdf am 10.06.2026
23. **Europäische Kommission (2020):** *Proposal for a Regulation on Markets in Crypto-assets (MiCA) (COM(2020) 593 final)*. Brüssel: Europäische Kommission.
 Verfügbar unter: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0022.02/DOC_1&format=PDF am 10.06.2026
24. **Europäische Zentralbank, Bitcoin's last stand**, ECB Blog vom 30.11.2022. Verfügbar unter:
<https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog221130~5301eecd19.en.html> am 13.06.2026
25. **FATF – Financial Action Task Force (2021):** *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF.
 Verfügbar unter: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html> am 10.06.2026
26. **FDIC – Federal Deposit Insurance Corporation (2023):** *The FDIC's Investigation of Voyager Digital: Crypto-Fintech FDIC Misrepresentations*. North Carolina Banking Institute Journal, Band 27. Verfügbar unter: <https://scholarship.law.unc.edu/ncbi/vol27/iss1/> am 13.06.2026
27. **Financial Stability Board (2019):** *Crypto-Asset Work underway, regulatory approaches and potential gaps*. Basel: Financial Stability Board. Verfügbar unter:
<https://www.fsb.org/uploads/P310519.pdf> am 10.06.2026

28. **Financial Stability Board (2020):** *Regulation, Supervision and Oversight of Global Stablecoin Arrangements*. Basel: Financial Stability Board. Verfügbar unter: <https://www.fsb.org/uploads/P131020-3.pdf> am 10.06.2026
29. **Financial Stability Board (2023):** *Thematic Review on the Global Regulatory Framework for Crypto-Asset Activities*. Basel: Financial Stability Board. Verfügbar unter: <https://www.fsb.org/uploads/P161025-1.pdf> am 10.06.2026
30. **Georgetown Law Center on Business and Technology Law – Ralhi, Akshay S. (2025):** *Beyond Enforcement: The SEC’s Shifting Playbook on Crypto Regulation*. Washington D.C.: Georgetown University Law Center. Verfügbar unter: <https://www.law.georgetown.edu/ctbl/blog/beyond-enforcement-the-secs-shifting-playbook-on-crypto-regulation/> am 10.06.2026
31. **Innes, Alfred Mitchell (1913):** *What Is Money?* In: *The Banking Law Journal*, Band 30. Verfügbar unter: https://cooperative-individualism.org/innes-a-mitchell_what-is-money-1913-may.pdf am 10.06.2026
32. **International Monetary Fund (2021):** *Global Financial Stability Report – Crypto Ecosystem and Financial Stability*. Washington D.C.: International Monetary Fund. Verfügbar unter: <https://www.imf.org/-/media/files/publications/gfsr/2021/october/english/ch2.pdf> am 10.06.2026
33. **Japan Financial Services Agency (2018):** *Certification of a Self-Regulatory Organization for Crypto-Asset Exchange Services*. Tokio: Financial Services Agency. Verfügbar unter: <https://www.iosco.org/library/ico-statements/Japan%20-%20FSA%20-%2020181221%20-%20Report%20of%20the%20Study%20Group%20on%20Virtual%20Currencies.pdf> am 10.06.2026
34. **Japan Financial Services Agency (2025):** *Examination of the Regulatory Systems Related to Cryptoassets*. Tokio: Financial Services Agency. Verfügbar unter: https://www.fsa.go.jp/en/news/2025/20250410_2/01.pdf am 10.06.2026
35. **Japan Virtual and Crypto Assets Exchange Association (JVCEA):** *Self-Regulatory Rules*. Tokio: Japan Virtual and Crypto Assets Exchange Association. Verfügbar unter: https://www.fsa.go.jp/news/30/virtual_currency/20181024-1.html am 11.06.2026
36. **Kirchmayr-Schliesselberger, Sabine / Klas, Wolfgang / Miernicki, Martin / Rinderle-Ma, Stefanie / Weilingner, Arthur (Hrsg.) (2019):** *Kryptowährungen*. Wien: Facultas.
37. **KPMG (2022):** *The Collapse of FTX*. London: KPMG. Verfügbar unter: <https://assets.kpmg.com/content/dam/kpmgsites/tr/pdf/2026/04/the-collapse-of-ftx.pdf> am 11.06.2026
38. **Kraemer, Klaus / Brugger, Florian (Hrsg.) (2021):** *Schlüsselwerke der Wirtschaftssoziologie*. 2. Auflage. Wiesbaden: Springer VS.
39. **Lawson, Tony (2016):** *Social Positioning and the Nature of Money*. *Cambridge Journal of Economics*, Band 40.
40. **McDermott, Megan (2020):** *The Crypto Quandary: Is Bankruptcy Ready?* In: *Northwestern University Law Review*, Band 115. Verfügbar unter: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1290&context=nulr_online am 11.06.2026
41. **Middlebrook, Stephen T. / Hughes, Sarah Jane (2014):** *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*. In: *William Mitchell Law Review*, Band 40. Verfügbar unter: <https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1567&context=wmlr> am 11.06.2026
42. **Miernicki, Martin (2023):** *Kryptowerte im Privatrecht*. Wien: MANZ.

43. **Model Framework for Consumer Protection and Crypto-Exchanges Regulation (2023):** *Model Framework for Consumer Protection and Crypto-Exchanges Regulation*. In: *Journal of Risk and Financial Management*, Band 16, Heft 7. Verfügbar unter:
(<https://www.mdpi.com/1911-8074/16/7/305>)
44. **Nakamoto, Satoshi (2008):** *Bitcoin: A Peer-to-Peer Electronic Cash System*. Verfügbar unter: <https://bitcoin.org/bitcoin.pdf> am 11.06.1983
45. **National Development and Reform Commission et al. (2021):** *Notice on Regulating and Rectifying Virtual Currency Mining Activities*. Peking: National Development and Reform Commission. Verfügbar unter: <https://zfxgk.ndrc.gov.cn/web/iteminfo.jsp?id=18271> am 11.06.2026
46. **Nomura Research Institute (2016):** *Virtual Currencies: Issues Remain*. Tokio: Nomura Research Institute. Verfügbar unter: <https://www.nri.com/content/900013443.pdf> am 11.06.2026
47. **OBLIN Rechtsanwälte (2020):** *Österreich: Regulierung virtueller Währungen im Jahr 2020 – Licht auf Österreichs Blockchain-Landschaft werfen*. Wien: OBLIN Rechtsanwälte. Verfügbar unter: (<https://oblin.at/de/wissen/veroeffentlichungen/oesterreich-regulierung-virtueller-waehrungen-im-jahr-2020-licht-auf-oesterreichs-blockchain-landschaft-werfen/>)
48. **OECD (2020):** *Consumer Data Rights and Competition - Background note*. by Anna Barker. Verfügbar unter:
https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/04/consumer-data-rights-and-competition_dadf5c13/10264d71-en.pdf am 11.06.2026
49. **OECD (2020):** *Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data and privacy*. Verfügbar unter:
https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/12/financial-consumer-protection-policy-approaches-in-the-digital-age_dc8c14b2/3f205e60-en.pdf am 11.06.2026
50. **OECD (2020):** *The Tokenisation of Assets and Potential Implications for Financial Markets*. Paris: Organisation for Economic Co-operation and Development. Verfügbar unter: https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/03/the-tokenisation-of-assets-and-potential-implications-for-financial-markets_370f9853/83493d34-en.pdf am 11.06.2026
51. **O'Melveny & Myers LLP (2025):** *The SEC May Signal a New Crypto Enforcement Approach*. Los Angeles: O'Melveny & Myers LLP. Verfügbar unter:
(<https://www.omm.com/insights/alerts-publications/the-sec-may-signal-new-crypto-enforcement-approach-in-upcoming-court-filing/>)
52. **Oxford Law Blog – Saggu, Aman / Ante, Lennart / Kopiec, Kaja (2025):** *The Unintended Consequences of SEC Crypto Enforcement Actions*. Oxford: University of Oxford. Verfügbar unter:
(<https://blogs.law.ox.ac.uk/oblb/blog-post/2025/01/unintended-consequences-sec-crypto-enforcement-actions/>)
53. **People's Bank of China et al. (2021):** *Notice on Further Preventing and Disposing of the Risks in Virtual Currency Trading*. Peking: People's Bank of China. Verfügbar unter:
https://www.spp.gov.cn/spp/zd gz/202109/t20210924_530777.shtml am 13.10.2026
54. **PwC (2025):** *Global Crypto Regulation Report 2025*. London: PricewaterhouseCoopers. Verfügbar unter: <https://legal.pwc.de/content/services/global-crypto-regulation-report/pwc-global-crypto-regulation-report-2025.pdf> am 13.06.2026
55. **Reuters (2021):** *China's Top Regulators Ban Crypto Trading and Mining*. Reuters, 24.09.2021. Verfügbar unter:
(<https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/>)

- 56. Schweizer Bundesrat (2018):** *Bericht des Bundesrates zu virtuellen Währungen*. Bern: Schweizer Bundesrat. Verfügbar unter : <https://www.newsd.admin.ch/newsd/message/attachments/35361.pdf> am 13.06.2026
- 57. Schweizer Bundesrat (2018):** *Rechtliche Grundlagen der Distributed-Ledger-Technologie und Blockchain in der Schweiz*. Bern: Schweizer Bundesrat. Verfügbar unter: <https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf> am 13.06.2026
- 58. Smit, Dirk / Buekens, Filip / du Plessis, Stan (2011):** *What Is Money? An Alternative to Searle's Institutional Facts*. Stellenbosch: University of Stellenbosch. Verfügbar unter: <https://philpapers.org/archive/SMIWIM-3.pdf> am 13.06.2026
- 59. Stanford Encyclopedia of Philosophy (2024):** *Philosophy of Money and Finance*. Stanford: Stanford University. Verfügbar unter: <https://plato.stanford.edu/entries/money-finance/> am 13.06.2026
- 60. Sumsb (2024):** *Global Cryptocurrency Regulations 2024*. London: Sumsb. Verfügbar unter: <https://sumsub.com/blog/aml-cryptocurrency-regulations-around-the-world/> am 13.06.2026
- 61. United States Congress (2023):** *Financial Innovation and Technology for the 21st Century Act (FIT21), H.R. 463, 118th Congress*. Washington D.C.: United States Congress. Verfügbar unter: <https://www.congress.gov/118/bills/hr4763/BILLS-118hr4763ih.pdf> am 13.06.2026
- 62. United States Congress (2025):** *Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act)*. Washington D.C.: United States Congress. Verfügbar unter: <https://www.congress.gov/119/bills/s394/BILLS-119s394is.pdf> am 13.06.2026