



**FRIEDRICH NAUMANN
STIFTUNG** Für die Freiheit.



Frankfurt School
Blockchain Center



intas.tech

KRYPTO REGELN

**Welche Regulierung brauchen digitale Währungen?
Ein Rahmenwerk zur Bewertung**

Philipp Sandner, Eduard Grigorjan und Benjamin Schaub

Impressum

Herausgeberin

Friedrich-Naumann-Stiftung für die Freiheit
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

 /freiheit.org

 /FriedrichNaumannStiftungFreiheit

 /FNFreiheit

 /stiftungfuerdiefreiheit

Autoren

Prof. Dr. Philipp Sander, Leiter des Frankfurt School Blockchain Centers
Eduard Grigorjan, Senior Consultant, intas.tech
Benjamin Schaub, Chief Digital Officer, intas.tech

Redaktion

World Order and Globalization Hub, Washington D.C.
Abteilung Globale Themen, Berlin

Kontakt

Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Stand

Oktober 2022

Hinweis zur Nutzung dieser Publikation

Diese Publikation ist ein Informationsangebot der Friedrich-Naumann-Stiftung für die Freiheit. Die Publikation ist kostenlos erhältlich und nicht zum Verkauf bestimmt. Sie darf nicht von Parteien oder von Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden (Bundestags-, Landtags- und Kommunalwahlen sowie Wahlen zum Europäischen Parlament).

Lizenz

Creative Commons (CC BY-NC-ND 4.0)



**FRIEDRICH NAUMANN
STIFTUNG** Für die Freiheit.



Frankfurt School
Blockchain Center



intas.tech

Eine gemeinsame Studie der Friedrich-Naumann-Stiftung für die Freiheit,
des Frankfurt School Blockchain Center und intas.tech

Inhalt

EXECUTIVE SUMMARY	4
1. EINLEITUNG	5
2. KRYPTOWERTE	6
2.1. Definition.....	6
2.2. Technische Grundlagen	6
2.3. Anwendungsszenarien.....	7
3. RISIKEN IM KONTEXT VON KRYPTOWERTEN	9
3.1. Compliance-Risiken.....	9
3.2. Operationelle Risiken	10
3.3. Konsumenten-Risiken	11
4. RAHMENBEDINGUNGEN EINER GEEIGNETEN REGULIERUNG FÜR KRYPTOWERTE	12
5. HANDLUNGSEMPFEHLUNG	14
6. AUSBLICK UND FAZIT	15
LITERATURVERZEICHNIS	16

In dieser Studie wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Die ausschließliche Verwendung der männlichen Form ist geschlechtsunabhängig zu verstehen.

Executive Summary

Der aktuelle Markt rund um Kryptowerte ist gekennzeichnet von einem weiterhin starken Wachstum verschiedenster Anwendungsfälle. Getrieben durch das Interesse von Privatpersonen, Investoren und Unternehmen aus vielen Industrien zieht die Branche trotz extremer Preisschwankungen ungebrochen eine hohe Nachfrage an. Die internationale Regulierungslandschaft ist dabei fragmentiert: So reichen nationale Gesetzgebungen von keiner Regulation, über explizite Verbote bis hin zu umfassender Integration in die Finanzwirtschaft. Auch internationale Abstimmungen zeichnen sich ab. So wird künftig etwa in der Europäischen Union mit der Markets in Crypto-Assets Regulation (MiCAR) die Harmonisierung von 27 Jurisdiktionen erfolgen. Insgesamt ist so in verschiedenen Bereichen des Krypto-Marktes eine schrittweise Professionalisierung zu beobachten.

Diese Studie schafft ein systematisches Rahmenwerk, um eine sachliche und standardisierte Bewertung unterschiedlicher Jurisdiktionen zu ermöglichen. Dafür wird auf Basis der Definition von Kryptowerten des deutschen Kreditwesengesetzes der Anwendungsbereich von Kryptowerten konkretisiert und eine Unterteilung in verschiedene Anwendungsfälle und Anwendergruppen für eine adressatengerechte Behandlung getroffen. Die Erläuterung von relevanten technischen Merkmalen dient zum Verständnis der zwei wesentlichen Faktoren von Kryptowerten: Dezentralität und Pseudonymität.

Diese Studie konzentriert sich in der Einordnung von Regulatorik vor allem auf die Risiken im Umgang mit Kryptowerten. Sie bilden die Grundlage für die zu adressierenden Elemente im Rahmen der Regulierung von Kryptowerten. Dafür werden allen voran Compliance-Themen wie die Bekämpfung von Geldwäsche und Terrorismusfinanzierung, Risiken rund um den Verbraucher- und Anlegerschutz sowie operationelle Risiken berücksichtigt.

Auf dieser Basis wird ein gesamtheitliches Rahmenwerk entwickelt, das aus zwei Kategorien und zwölf zu bewertenden Faktoren besteht. Die Bewertung der Faktoren erfolgt gemäß einer Skala, die den jeweiligen Erfüllungsgrad in einer Jurisdiktion darstellt.

Abschließend werden Handlungsempfehlungen im Hinblick auf eine ausgewogene und adäquate Regulierung für Kryptowerte ausgesprochen. Ein Ausblick auf potenzielle Neuentwicklungen innerhalb der Kryptowerte integriert das Modell in die disruptive Evolution eines noch jungen Marktes.

1. Einleitung

Kryptowerte sind stark im Trend: Durch sie ermöglichte, innovative Dienstleistungen und Geschäftsmodelle erzeugen immer mehr Nachfrage. Und das trotz herber Rückschläge wie starken Preisschwankungen oder Insolvenzen wie im Falle vom US-amerikanischen Kryptowerte-Verleiher Celsius¹ oder der deutschen Nuri Bank.² Das Interesse von Privatpersonen, institutionellen Investoren und Finanzinstituten an Krypto-Dienstleistungen ist ungebrochen. So halten im Euro-Raum etwa zehn Prozent der Bevölkerung Kryptowerte; der Großteil in einem Wert von bis zu 5000 EUR.³ Mit 40 Millionen Personen in den USA, die in Kryptowerte investieren, diese handeln und nutzen, ist die Marktdurchdringung auf einem ähnlichen Niveau wie im Euro-Raum.⁴

Durch die voranschreitende Professionalisierung im Krypto-Markt, begünstigt durch mehr regulatorische Klarheit, ergeben sich immer mehr Möglichkeiten, am Markt der Kryptowerte zu partizipieren – ohne dafür ein zu hohes Risiko einzugehen. Dabei bemühen sich Gesetzgeber, ein angemessenes Vorgehen bei der Regulierung von Kryptowerten zu definieren. Diese Bemühungen sind bislang meist auf nationaler und regionaler Ebene zu beobachten. Dadurch ist eine global stark fragmentierte Regulierungslandschaft entstanden, in der Teilnehmer teils sehr unterschiedliche Ansätze verfolgen. So gibt es Länder auf der Welt, die Kryptowerte explizit verbieten, wohingegen in anderen Staaten noch gar keine Gesetze zu ihnen erlassen wurden.

Die Europäische Union (EU) hat 2020 mit der Verordnung *Markets in Crypto Assets (MiCAR)*⁵ einen ersten Schritt gemacht, um ein einheitliches Regelwerk für ihre 27 Mitgliedstaaten zu entwerfen. Die MiCAR wird weite Teile des Krypto-Marktes regulieren und erhebliche Auswirkungen auf den Wirtschaftsraum EU mit einer Bevölkerung von über 400 Millionen haben. Es ist zu erwarten, dass auf Basis von MiCAR ähnliche Regulierungen in anderen Jurisdiktionen folgen werden und eine langsame, aber stetige Harmonisierung mancher globalen Regulierungsregime anlaufen wird.

Deswegen versuchen immer mehr Regulatoren, sich tiefgehend mit Kryptowerten auseinanderzusetzen und eine adäquate Regulierung zu finden, die die Risiken der Branche minimiert und gleichermaßen die Innovationskraft nicht bedeutend einschränkt.

Das Ziel dieser Studie ist es, ein Verständnis über die vorherrschenden Risiken im Umgang mit Kryptowerten zu erläutern und ein Rahmenwerk zu entwickeln, mit dem die weltweit bestehenden, länderspezifischen Regulierungen übergreifend verglichen und bewertet werden können. Als Leitplanken hierfür werden sowohl Aspekte der Kryptowerte-Regulierung in Deutschland als auch der MiCAR herangezogen, da in diesen Fällen bereits ein umfassendes Regelwerk erarbeitet wurde.

¹ Vgl. manager magazin, 2022.

² Vgl. Schwarz et al., 2022.

³ Vgl. European Central Bank (ECB), 2022.

⁴ Vgl. White House (WH), 2022.

⁵ Vgl. Europäische Union (EU), 2020.

2. Kryptowerte

Um Kryptowerte zu verstehen, ist es wichtig, einige Definitionen und inhaltliche Abgrenzung festzulegen. Hierzu werden insbesondere bestehende Gesetzestexte aus dem europäischen Raum als Grundlage betrachtet.

2.1. Definition

Lange Zeit gab es keine uniforme Definition des Begriffes *Kryptowährung*. Der Begriff wurde synonym für verschiedene Aspekte des Blockchain-Ökosystems verwendet. Durch die europäische MiCAR-Verordnung sowie das deutsche Kreditwesengesetz (KWG) haben sich nun zwei Definitionen im europäischen Raum etabliert. Dabei führen beide Definitionen den neuen Begriff *Kryptowert* – anstatt *Kryptowährung* – ein. Die vorläufige MiCAR-Definition für Kryptowerte⁶ ist dabei weit gefasst und beinhaltet verschiedene Subkategorien.

Das KWG zeigt, etwa bei der digitalen Abbildung und Übertragbarkeit, Parallelen zu MiCAR, verfolgt aber einen anderen Ansatz: Das KWG benennt in seiner Definition die Dezentralität und entsprechende Governance von digitalen Werten und grenzt Kryptowerte somit klar von bestehenden Geldmitteln ab. So lautet die Definition gemäß § 1 Abs. 11 Satz 4 des KWG: "Kryptowerte im Sinne dieses Gesetzes sind digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann."⁷ Kryptowerte sind damit eine Kategorie dezentraler Vermögensgegenstände, wie z.B. Bitcoin und Ethereum (siehe Kapitel 2.2).

Diese Studie greift auf die Definition des KWG zurück. Denn hier werden Kryptowerte enger gefasst; das KWG deckt u.a. die größten dezentralen Netzwerke wie Bitcoin und Ethereum ab. Aufbauend auf der KWG-Definition werden Kryptowerte somit wie folgt definiert:

- Ein Kryptowert ist ein digitaler Vermögenswert, der mit einer Distributed-Ledger-Technologie (DLT) aufgezeichnet und kryptografisch gesichert wird
- Kryptowerte haben keine bestehende zentrale Instanz, etwa in Form einer staatlichen Behörde oder juristischen Person/Entität

- Kryptowerte haben keinen intrinsischer Wert und keine Absicherung durch Vermögenswerte mit intrinsischem Wert

2.2. Technische Grundlagen

Die Blockchain-Technologie bildet die Basis der meisten Kryptowerte und ist von besonderer Relevanz für deren Funktionalität, Sicherheit und Skalierbarkeit. Um zu verstehen, weshalb die Blockchain-Technologie so viele Vorteile bietet, ist es sinnvoll, einige ihrer Charakteristika zu verstehen. Nur so kann auch eine adäquate Regulierung getroffen werden.

Große öffentliche Blockchains wie Bitcoin und Ethereum sind dezentral: Sie haben keinen einzelnen Entscheider, der Transaktionen zensieren oder Guthaben doppelt ausgeben kann. Diese Dezentralität liegt an der IT-Architektur der Blockchains: Mit Hilfe des Konsensmechanismus, betrieben durch ein global verteiltes Netzwerk von Rechnern, werden Transaktionen nur validiert, wenn die Mehrheit des Netzwerks jene Transaktion bestätigt. Dabei kann jeder Mensch mit einem handelsüblichen Computer an diesem Prozess teilnehmen⁸ – die Entscheidungsfindung erfolgt damit dezentralisiert über die gesamte Welt. Die Transaktionen werden dann in Blöcken gespeichert und diese kryptographisch miteinander verbunden. Dadurch ist eine nachträgliche Änderung der Daten nicht mehr möglich.

Durch die dezentrale Aufzeichnung der Transaktionen in einer öffentlichen Blockchain sind bestimmte Transaktionsdaten für alle Teilnehmer und auch für Außenstehende transparent. Teilnehmer des Netzwerks können ohne Intermediär jederzeit digitale Werte untereinander transferieren. Weil die Blockchain fälschungssicher ist, können Teilnehmer einander vertrauen, ohne sich gegenseitig zu kennen (Peer-to-Peer-Charakter). Es entsteht ein sich selbsterhaltendes System, welches zentrale Akteure und Administratoren obsolet macht.

Der Grad der Dezentralität verschiedener Blockchain-Systeme kann variieren. Faktoren wie etwa Governance-Regeln oder Barrieren bei der Partizipation am Konsensmechanismus bestimmen, wie dezentral eine Blockchain tatsächlich ist. Je dezentraler die Blockchain ist, desto schwieriger gestalten sich die Regulierungsmöglichkeiten, da bereits eine Internetverbindung genügt, um ein solches Netzwerk zu nutzen.

⁶ Im MiCAR-Wortlaut: "[Ein] Kryptowert [ist] eine digitale Darstellung von Werten oder Rechten, die unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden können", vgl. Europäische Union, 2020.

⁷ Vgl. Bundesministerium der Justiz, 2022.

⁸ Zwar kann jeder Computer an dem Konsensmechanismus teilnehmen, jedoch lohnt sich das sogenannte *Mining* wirtschaftlich meist erst mit spezialisierten Computern auf einer großen Skala an globalen Standorten mit günstiger Energie.

Das dezentrale globale Netzwerk, der Peer-to-Peer-Charakter sowie die Integrität ohne zentrale Kontrollinstanz sind die grundlegenden Vorteile von Kryptowerten. Gleichzeitig entsteht im Kontext der Regulierung zusätzliche Komplexität. Ein global einvernehmliches Regulierungsregime sollte entwickelt werden, um potentiellen regulatorischen Arbitragemöglichkeiten entgegenzuwirken und illegale Aktivitäten zu minimieren.

Eine weitere Facette der Blockchain ist die Pseudonymität. Diese ist verknüpft mit der Notwendigkeit des Besitzes einer Wallet.⁹ Sie ist das Eintrittstor zur Partizipation am Blockchain-Ökosystem. Wallets ermöglichen das Halten, Senden und Empfangen von Kryptowerten. Technisch funktioniert das folgendermaßen: Um Zugang zu den eigenen Kryptowerten zu bekommen, wird ein privater Schlüssel, vergleichbar mit einem Passwort, verwendet. Dieser Schlüssel ist ein zufällig generierter, alpha-numerischer Code. Damit Transaktionen empfangen werden können, ist ein öffentlicher Schlüssel, vergleichbar mit einer IBAN, notwendig. Im Aufbau ähnelt er dem privaten Schlüssel. Der öffentliche Schlüssel ist für alle Beteiligten transparent, während der private Schlüssel nur dem Eigentümer bekannt sein sollte. Obwohl der öffentliche Schlüssel theoretisch mit einem privaten Account in Verbindung gebracht werden kann, ist die eindeutige Zuordnung zu einer Identität komplex, mit hohem Energieeinsatz verbunden und in manchen Fällen trotzdem nicht möglich. Deshalb wird im Zusammenhang mit Blockchains häufig über Pseudonymisierung von Akteuren gesprochen, die insbesondere Themen wie Identitätsprüfungen und die Bekämpfung von Geldwäsche und Terrorismusfinanzierung erschweren können.

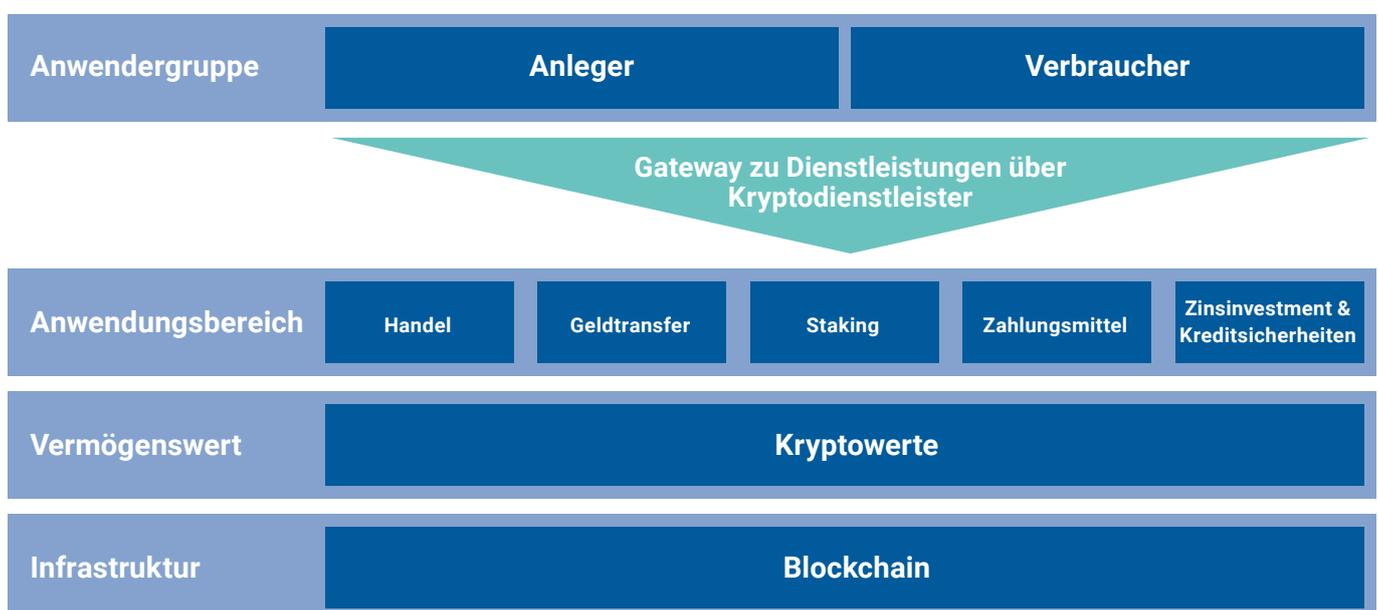
⁹ Krypto-Wallets sind der Ausgangspunkt für die Interaktion mit einer Blockchain. Transaktionen jeglicher Form können nur mit einer Wallet ausgeführt werden. Bei der Einrichtung einer Wallet wird ein privater und öffentlicher Schlüssel erstellt. Derjenige, der den privaten Schlüssel einer Wallet kennt, kann Transaktionen mit ihr tätigen. Eine Wallet ist somit ein Speichermedium, auf dem Transaktionsdaten gespeichert werden (Vgl. Suratkar et al., 2020).

Im Kontext von privaten Schlüsseln ist auch das Thema Verwahrung von hoher Relevanz. Es gibt zwei Arten der Verwahrung von privaten Schlüsseln: Custodial und Non-custodial Wallets. Im Falle einer Custodial Wallet wird die Verantwortung über das Verwahren des privaten Schlüssels (und somit auch den Zugang zu den Kryptowerten) an einen externen Dienstleister übertragen; hiermit wird auch die Gefahr des Verlustes des privaten Schlüssels verlagert. Bei Non-custodial Wallets liegt die Verwahrung des privaten Schlüssels in der eigenen Verantwortung. Dafür gibt es verschiedene Methoden. Der Verlust des privaten Schlüssel hat dann, unabhängig ob in Form eines Stück Papiers oder eines USB-Stick, den endgültigen und unwiderrufbaren Verlust des Zugangs zu den eigenen Kryptowerten zur Folge.

2.3. Anwendungsszenarien

Vor allem in der Finanzindustrie werden zunehmend Kryptowerte verwendet, wenngleich auf einem bislang niedrigen Niveau. Daher bedarf die Regulation von Kryptowerten einer Auseinandersetzung mit den verschiedenen Anwendungsfällen unter Einbezug relevanter Marktteilnehmer und Nutzergruppen. Denn die Nutzung von Kryptowerten ist in der Finanzindustrie mittlerweile weit fortgeschritten: Einzelpersonen halten vermehrt Kryptowerte, investieren regelmäßig in sie oder nutzen sie für Transaktionen. Und auch die Nachfrage von professionellen Investoren und Finanzinstituten ist steigend. Mittlerweile haben sich Anbieter für Dienstleistungen rund um Kryptowerte am Markt etabliert, die Services wie Verwahrung, Verwaltung und Handel anbieten. Mit den Anwendergruppen bilden die Anwendungsbereiche sinnvolle Leitplanken, anhand dessen eine zielgerichtete regulatorische Betrachtung vorgenommen werden kann (siehe Abbildung 1).

Abb. 1 | Analyseeinheiten der Anwendergruppen und -bereiche von Kryptowerten



8 2. KRYPTOWERTE

Im Bereich der Kryptowerte gibt es vor allem folgende finanzrelevante Anwendungen¹⁰:

- **Handel:** Kauf und Verkauf von Kryptowerten auf zentralen oder dezentralen Krypto-Handelsplätzen für spekulative oder Anlage-Zwecke (dabei übernehmen manche Krypto-Handelsplätze auch die Verwahrung und Verwaltung der Kryptowerte)
- **Peer-to-Peer Geldtransfer:** Grenzübergreifende, fälschungssichere und direkte Transaktionen zwischen Nutzern eines Kryptowerts ohne Intermediäre
- **Staking:** Bereitstellung von eigenen Kryptowerten für den jeweiligen Konsensmechanismus einer Blockchain und dadurch Partizipation an Ausschüttungen
- **Zahlungsmittel:** Nutzung von Kryptowerten (z.B. Stablecoins¹¹) zur Bezahlung von Dienstleistungen, Produkten oder anderen digitalen Vermögenswerte
- **Zinsinvestments und Kreditsicherheiten:** Verleihung von Kryptowerten zur Generierung von Zinszahlungen bzw. Hinterlegung von Kryptowerten als Kreditsicherheit für die Kreditaufnahme

¹⁰ Vgl. Coinbase, 2022.

¹¹ Stablecoins sind Kryptowerte, die sich auf Stabilisierungsinstrumente (u.a. Algorithmen) stützen, um einen stabilen Wert im Verhältnis zu einer oder mehreren offiziellen Währungen oder anderen Vermögenswerten (einschließlich Kryptowerten) zu erhalten. Um die Bedeutung einer vertrauenswürdigen zentralen Instanz in ihrem Betrieb zu verringern, verwenden Stablecoins auf Basis der Blockchain sogenannte Smart Contracts (Vgl. European Central Bank (ECB), 2021).

3. Risiken im Kontext von Kryptowerten

Das Wachstum des Krypto-Marktes ist weiterhin hoch; trotz der traditionell extremen Preisschwankungen lässt sich auch aktuell kein Abflachen dieses Trends beobachten. Immer wieder setzen sich neue, innovative Entwicklungen im jungen Markt durch. Kryptowerte gewinnen für immer mehr Jurisdiktionen an Bedeutung. Im Zuge dessen versuchen Regulatoren überall auf der Welt mit den Entwicklungen Schritt zu halten, indem sie relevante Informationen sammeln und sich sukzessive das erforderliche Wissen aneignen. Dabei stoßen sie auf zwei inhärente Eigenschaften von Kryptowerten, die sich immer wieder als Herausforderung herausstellen:

- Die dezentrale Struktur erschwert es, eine zuständige Instanz zu identifizieren, die die Verantwortung für jegliche aufkommende Frage- bzw. Problemstellungen trägt
- Die Pseudonymität, also die eingeschränkte Nachverfolgbarkeit von Transaktionen und Identitäten von Sender und Empfänger, verschärft diesen Umstand im Falle von illegalen Aktivitäten noch weiter

Die Nutzung von Kryptowerten ist in vielen Ländern ohne oder mit wenigen Einschränkungen möglich. Bei besonders dezentralen, global operierenden Blockchains sind sogar Einschränkungen seitens staatlicher Kontrollinstanzen kaum durchzusetzen. Dies hat Risiken zur Folge, mit denen verschiedene Herausforderungen einhergehen. Diese werden im Folgenden genauer analysiert.

3.1. Compliance-Risiken

Ein wesentliches Risiko, welches traditionell einen grenzübergreifenden Charakter hat und einen hohen Grad an internationaler Kooperation bedarf, sind Compliance-Anforderungen im Zusammenhang mit:

- Geldwäschebekämpfung (Anti-Money Laundering, AML)
- Terrorismusbekämpfung (Countering the Financing of Terrorism, CFT)
- Identitätsprüfungen (Know Your Customer, KYC)

Die dezentrale Struktur von Kryptowerten ermöglicht Nutzern, Transaktionen in Form von direkten Geldtransfers ohne jegliche regulierte Intermediäre zu tätigen und damit (ansonsten etablierten) Kontrollen zu umgehen. Für den Umtausch von Kryptowerten in offizielle Währungen sind Intermediäre wie z.B. Krypto-Handelsplattformen erforderlich. Grundsätzlich erschwert der Peer-to-Peer-Charakter von Kryptowerten den zuständigen Behörden, ihre aufsichtsrechtlichen Pflichten zu erfüllen und verdächtige Aktivitäten nachzuverfolgen.¹²

Auch wenn in manchen Ländern Kryptowerte bereits reguliert sind, unterscheiden sich die in Kraft befindlichen Gesetze meist stark voneinander. Diese heterogene Regulierungslandschaft erschwert die internationale Zusammenarbeit bei Geldwäsche, Terrorismusfinanzierung und bei der Durchsetzung von Sanktionen oder Embargos.¹³ Auch die Erkennung von Verschleierungen der Mittelherkunft, um Steuerzahlungen zu vermeiden, ist erschwert.¹⁴

Schon heute gibt es globale Richtlinien für den Umgang mit Kryptowerten im Kontext von AML und CTF. Diese werden insbesondere durch die Empfehlungen der Financial Action Task Force (FATF) getrieben, welche ein Staaten-unabhängiges Gremium ist, das internationale Standards zur Verhinderung von potenziell illegalen Aktivitäten festlegt.¹⁵ Seit der Erweiterung globaler Standards zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung auf Anbieter von Krypto-Dienstleistungen im Jahr 2019 erstellt die FATF einen jährlichen Report, mit dem der Fortschritt der beteiligten Ländern bei der Umsetzung der Empfehlungen nachverfolgt wird. Im Jahr 2021 haben bereits 27 der 38 FATF-Mitglieder erforderliche Rechtsvorschriften für die AML/CTF-Regelung für Anbieter von Krypto-Dienstleistungen implementiert bzw. arbeiten aktuell daran, entsprechende Vorschriften zu implementieren (sieben Mitglieder).¹⁶

Die Maßnahmen scheinen zu wirken: Im Jahr 2021 wurde nach Studien zwar absolut gesehen 30 Prozent mehr Geld durch die Nutzung von Kryptowerten gewaschen als in 2020 (siehe [Abbildung 2](#)).¹⁷ Doch dieser zunächst hohe Anstieg sollte in Relation zu dem Gesamttransaktionsvolumen gesehen werden, das gegenüber 2020 um ganze 567 Prozent wuchs. Insgesamt machte die Geldwäsche im Jahr 2021 damit nur noch 0,05 Prozent des gesamten Transaktionsvolumens von Kryptowerten aus – der niedrigste Wert in den vergangenen fünf Jahren.¹⁸

¹³ Vgl. World Economic Forum (WEF), 2021.

¹⁴ Ebd.

¹⁵ Vgl. Bundesministerium der Finanzen (BMF), 2020.

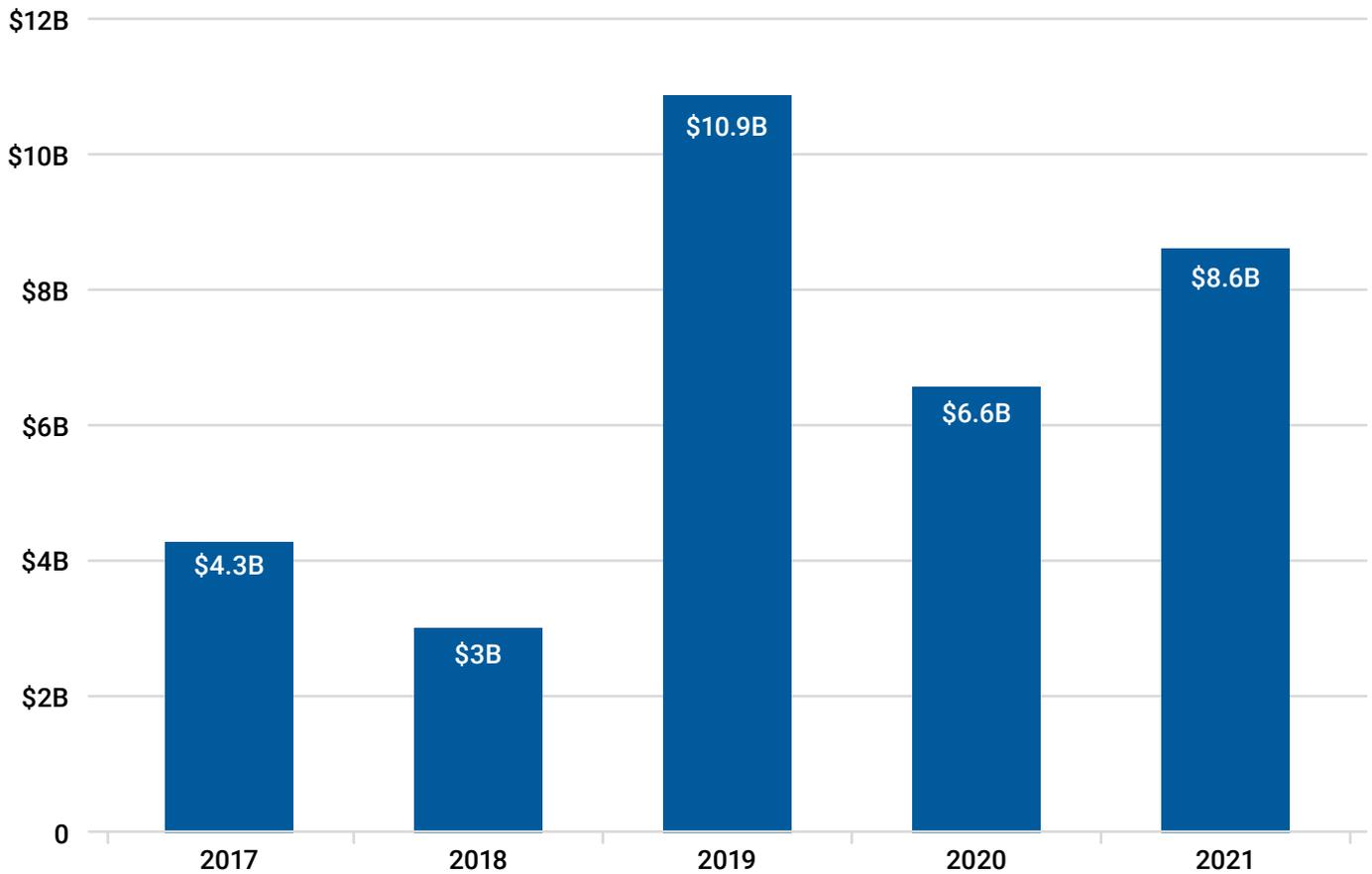
¹⁶ Vgl. Financial Action Task Force (FATF), 2021.

¹⁷ Vgl. Chainalysis, 2022a.

¹⁸ Ebd.

¹² Vgl. International Monetary Fund (IMF), 2020.

Abb. 2 | Gesamtwert des mit Kryptowerten gewaschenen Geldes (in Milliarden US-Dollar)



Quelle: Chainalysis, 2022a

Dass es überhaupt solche Statistiken gibt, zeigt, dass Transaktionen auf der Blockchain aufgrund ihrer Transparenz einerseits zwar gut nachverfolgt werden. Andererseits bedeutet das aber nicht, dass es einfach ist, die Identität der beteiligten Parteien zu erkennen. Denn durch die Pseudonymität können Geldströme nicht immer eindeutig zugeordnet werden, um im Falle von illegalen Aktivitäten die verantwortlichen Personen oder Organisationen zur Rechenschaft zu ziehen. Aber auch hier sind Fortschritte zu verzeichnen: Unternehmen wie Chainalysis¹⁹ spezialisieren sich auf die Transaktionsüberwachung, um illegale Aktivitäten zu entdecken und vorzubeugen. Hierbei wird vermehrt über Know Your Transaction (KYT) und weniger über KYC gesprochen, da kontinuierlich und in Echtzeit Transaktionsverläufe beobachtet werden, um Muster illegaler Absichten festzustellen und aufzudecken.

3.2. Operationelle Risiken

Ein weiterer Aspekt, welcher aus Risikogesichtspunkten relevant ist, ist das operationelle Risiko im Umgang mit Kryptowerten und der damit einhergehenden Nutzung von Blockchain-Infrastrukturen. Im traditionellen Zahlungsverkehr kann im Falle eines Fehlers dieser an die zentrale Verwaltungsstelle (bei einer IBAN-Überweisung z.B. an die eigene Bank) ge-

meldet werden und je nach Regelung kann die Transaktion umgekehrt bzw. storniert werden. Diese Art von Reversibilität ist bei Blockchain-basierten Transaktionen in der Regel nicht möglich, da Transaktionen endgültig sind und es keine zentrale Verwaltungsstelle gibt, bei der Fehler gemeldet und behoben werden können. Verbraucher haben somit in der Regel keinen Anspruch auf die Umkehrbarkeit einer Transaktion. Bei Fehlern sind entsprechende Gelder somit verloren, sofern kein regulierter Intermediär in Form eines Krypto-Dienstleisters genutzt wird.²⁰

Darüber hinaus können Verbraucher und Anleger bei der Nutzung von Kryptowerten Teile bzw. ihr gesamtes Vermögen verlieren, wenn sie ihren privaten Schlüssel verlieren oder dieser gestohlen wird. Diese Gefahr besteht sowohl bei Custodial als auch bei Non-custodial Wallets. Bei Custodial Wallets trägt die Verantwortung für die sichere Verwahrung der privaten Schlüssel der Drittanbieter. Solch ein Unternehmen kann dann beispielsweise durch Hackerangriffe auf eine ungenügend gesicherte IT-Umgebung attackiert werden. Durch solchen illegalen Zugriff können Anleger ihre Kryptowerte ganz oder teilweise verlieren. Die vergangenen Jahre haben gezeigt, dass derartige Sicherheitslücken im Krypto-Markt vorkommen und das Risiko von Hackerangriffen weiterhin

¹⁹ Vgl. Chainalysis, 2022b.

²⁰ Vgl. World Economic Forum (WEF), 2021.

präsent ist.²¹ Wenn der Anbieter des Custodial Wallets den privaten Schlüssel seiner Kunden verliert, können diese Entschädigungsansprüche potenziell geltend machen.

Diese Sicherheit gibt es bei Non-custodial Wallets nicht. Hier obliegt die Verantwortung für den Schutz des privaten Schlüssels dem Anleger selbst. Die Nutzung von Non-custodial Wallets birgt damit eine höhere Verantwortung für Verbraucher und Anleger: Wenn sie ihren privaten Schlüssel verlieren, sind auch alle Guthaben auf der Wallet unwiederbringlich verloren.

3.3. Konsumenten-Risiken

Verbraucher- und Anlegerschutz sind zwei der wichtigsten Prioritäten des Gesetzgebers. Mit dem Aufkommen von innovativen und wenig regulierten Geschäftsmodellen steigt auch das Risiko für Verbraucher, Opfer von unlauteren und betrügerischen Handlungen zu werden. Das ist auch im Krypto-Markt zu beobachten. Verbraucher und Anleger verlieren immer wieder ihr Vermögen aufgrund von Betrugsprojekten, Marktmanipulationen, Hackerangriffen oder fehlender Einlagensicherung bei Krypto-Dienstleistern.²²

Hierbei sind insbesondere zwei Faktoren von großer Relevanz: Zum einen ist es ein mangelndes Wissen über den Krypto-Markt seitens Verbrauchern und nicht-professionellen Anlegern. Viele von ihnen sind sich nicht bewusst, dass sie in einem noch nicht regulierten Umfeld handeln. Fälschlicherweise wird der Krypto-Markt mit traditionellen Finanzdienstleistungen verglichen. Das führt in vielen Fällen zu fehlerhaften Risikoeinschätzungen.

Zum anderen ergeben sich für Verbraucher und Anleger indirekte Risiken im Umgang mit regulierten Krypto-Dienstleistern. Zwar liegen hier die Verantwortung und das Risiko für Verluste bei den Anbietern der Krypto-Dienstleistungen. Dennoch können beispielsweise unzureichende Kapitalanforderungen an Krypto-Dienstleister im Falle einer Insolvenz oder ähnlicher finanzieller Krisen für Anleger zu einem Teil- oder Totalverlust ihrer Vermögenswerte führen (Liquiditätsrisiko). In diesem Kontext kann auch die fehlende Einlagensicherung in Form von der Trennung des verwalteten und des verwahrten Vermögens zu ähnlichen Konsequenzen führen (Kredit- und Ausfallrisiko).²³

Darüber hinaus ist der Schutz der Kundendaten relevant. In vielen Jurisdiktionen gibt es nämlich bereits bestehende Datenschutz-Regelungen. Aufgrund der transparenten Natur von Blockchains stellt sich dann die Frage, inwiefern bestehende Regelungen bei der Blockchain-basierten und pseudonymisierten Datentransparenz berücksichtigt werden sollen. Dabei können insbesondere die fehlende Verantwortlichkeit und Rechenschaftspflicht von Kryptowerten eine Herausforderung darstellen.²⁴

²¹ Ebd.

²² Vgl. Charoenwong & Bernardi, 2021.

²³ Vgl. World Economic Forum (WEF), 2021.

²⁴ Vgl. European Parliament (EP), 2019.

4. Rahmenbedingungen einer geeigneten Regulierung für Kryptowerte

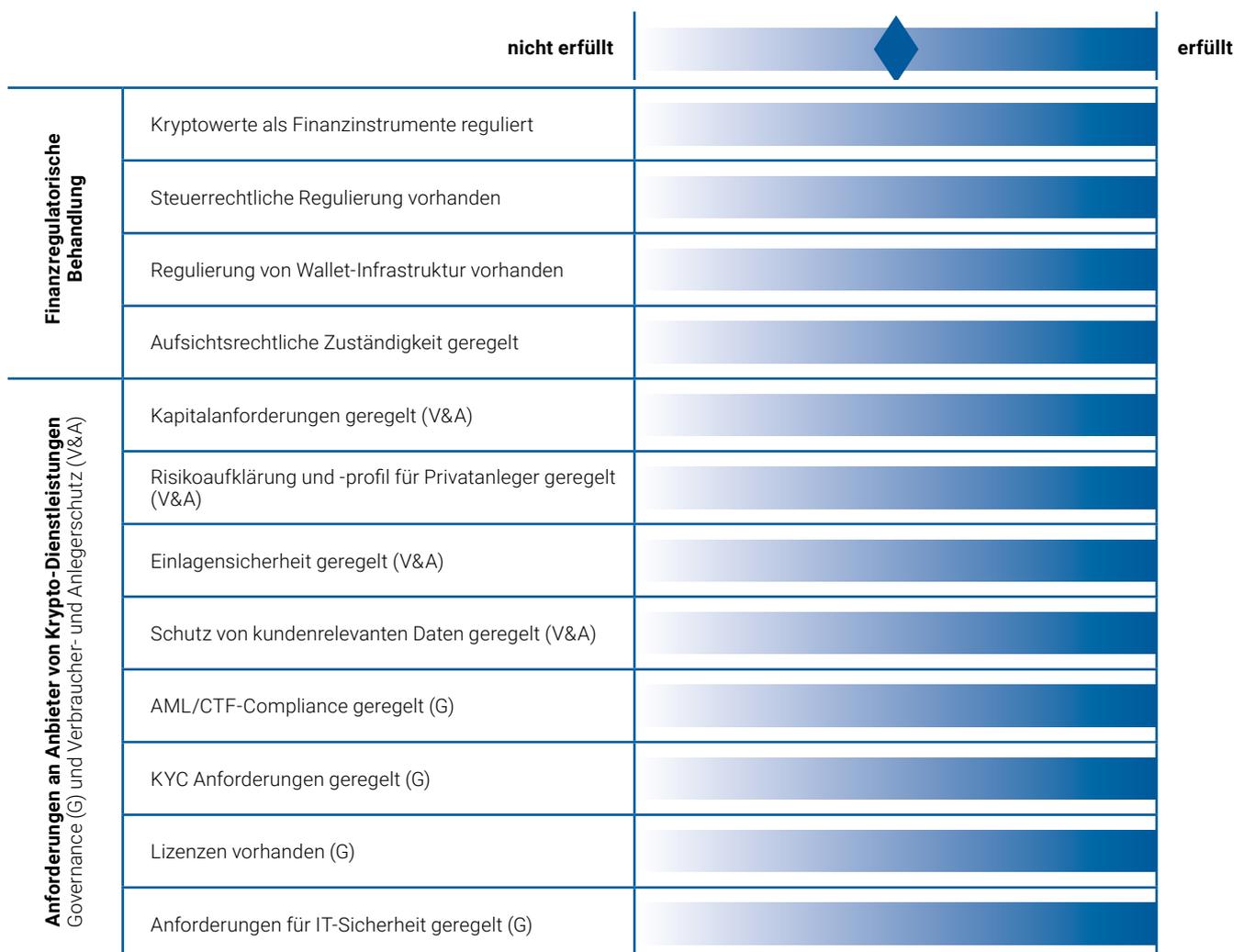
Die aktuell fragmentierte Regulierungslandschaft ist ein Hemmnis für die internationale Regulatorik. Um effiziente und ganzheitliche Regelungen für den Umgang mit Kryptowerten zu implementieren, braucht es grenzübergreifende Initiativen. Doch bisher verfolgen die einzelnen Jurisdiktionen eigene Ansätze bei der Regulierung von Kryptowerten, die sich folglich auch in ihrem Entwicklungsgrad unterscheiden.

Um den Fortschritt der verschiedenen Gesetzgebungen übergreifend zu analysieren, wurde auf Basis der analysierten Risiken in Kapitel 3 ein standardisiertes Rahmenwerk entwickelt. Es zeigt einen ganzheitlichen Stand der Regulierung einer jeweiligen Jurisdiktion und ermöglicht damit Vergleiche und Bewertungen. Das Rahmenwerk dient als Instrument, um die im Kontext von Kryptowerten relevanten regulatorischen Frage-

stellungen dahingehend zu bewerten, inwiefern existierende Regelungen einer Jurisdiktion die Nutzung von Kryptowerten erlauben.

Bevor eine bestimmte Jurisdiktion anhand des Rahmenwerks bewertet wird, ist vorab zu prüfen, inwiefern in der jeweiligen Jurisdiktion ein explizites bzw. implizites Verbot von Kryptowerten besteht. Ein implizites Verbot wäre dabei z.B. dass es Unternehmen verboten ist, Krypto-Dienstleistungen anzubieten. In diesen Fällen ist die Anwendung des Rahmenwerks nicht zielführend. Das Rahmenwerk besteht aus zwei übergreifenden Kategorien, aufgeteilt auf zwölf Bewertungskriterien. Diese können anhand einer Bewertungsskala evaluiert werden (siehe Abbildung 3).

Abb. 3 | Rahmenwerk zur Bewertung von Regulierungsregimen



Quelle: Eigene Darstellung

In der ersten Kategorie wird die finanzregulatorische Behandlung von Kryptowerten in der jeweiligen Jurisdiktion anhand der folgenden Faktoren bewertet:

- **Kryptowerte als Finanzinstrumente reguliert:** Einstufung von Kryptowerten als aufsichtsrechtlich anerkannte Finanzinstrumente.
- **Steuerrechtliche Regulierung vorhanden:** Bestehende Steuerregelungen für den Umgang mit Kryptowerten sowohl für Privatpersonen als auch für Unternehmen.
- **Regulierung von Wallet-Infrastrukturen vorhanden:** Bestehende Regelungen zu Custodial und Non-custodial Wallets im Kontext von privaten Schlüsseln und Verwahrung von Kryptowerten.
- **Aufsichtsrechtliche Zuständigkeit geregelt:** Eindeutige Mandatierung und Abgrenzung der Zuständigkeiten von Behörden hinsichtlich der Aufsichtspflichten im Umgang mit Kryptowerten.

Da Anbieter von Krypto-Dienstleistungen eine wichtige Rolle im Krypto-Ökosystem einnehmen (siehe [Abbildung 1 in Kapitel 2.3](#)), werden in der zweiten Kategorie die regulatorischen Anforderungen an Anbieter von Krypto-Dienstleistungen unter den Aspekten Governance sowie Verbraucher- und Anlegerschutz anhand der folgenden Faktoren bewertet:

Verbraucher- und Anlegerschutz:

- **Kapitalanforderungen geregelt:** Pflichten zur Haltung von Eigenkapital zur Mitigation von Kredit- und Ausfallrisiken.
- **Risikoaufklärung und -profil für Privatanleger geregelt:** Aufklärungspflichten gegenüber Kunden über Risiken im Umgang mit Kryptowerten sowie Kategorisierung von Kunden gemäß Risikoklassen.
- **Einlagensicherheit geregelt:** Regelungen zum Schutz von Kundeneinlagen, z.B. durch Trennung der Vermögenswerte der Kunden von den eigens gehaltenen Vermögenswerten.
- **Schutz kundenrelevanter Daten geregelt:** Datenschutz-Regelungen für Kryptowerte bzw. Anwendungsmöglichkeit bestehender Regelungen auf Kryptowerte.

Governance:

- **AML/CTF Compliance geregelt:** Anforderung zur Einhaltung von nationalen und/oder internationalen Regelungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung.
- **KYC Anforderungen geregelt:** Regelungen zur Identifikation und Prüfung von (angehenden) Kunden auf Basis der persönlichen Daten.
- **Lizenzen vorhanden:** Bestehende Lizenzen zur Erbringung von Krypto-Dienstleistungen bzw. Zulassungen als Anbieter von Krypto-Dienstleistungen.
- **Anforderungen für IT-Sicherheit geregelt:** Anforderungen zum Schutz von IT-Systemen inkl. entsprechender Sicherheitsvorkehrungen.

Die Bewertung der einzelnen Faktoren erfolgt über eine Skala, die den Erfüllungsgrad des jeweiligen Faktors darstellt. Bei der Bewertung ist zu beachten, dass diese nicht dichotom aus "erfüllt" bzw. "nicht erfüllt" besteht, sondern vielmehr unterschiedliche Ausprägungen annehmen kann. Der Erfüllungsgrad kann also auch als ein Prozess verstanden werden. Neue Entwicklungen im Markt können damit Modifizierungen an den regulatorischen Faktoren zur Folge haben. Zudem sollte der Erfüllungsgrad nicht normativ verstanden werden: Ein hoher Erfüllungsgrad ist nicht per se "gut", ein niedriger nicht per se "schlecht". Vielmehr ist das Ziel, eine objektive Bewertung vorzunehmen, die die Charakteristika einer einzelnen Jurisdiktion trennscharf gemäß der qualitativen Merkmale wiedergibt.

Insbesondere kann, je nach Betrachtungsperspektive, eine bestimmte Ausprägung mal positiv und mal negativ interpretiert werden. Beispielsweise ist aus Sicht des Anlegers eine vollumfängliche Regulierung von Kryptowerten positiv zu bewerten. Aus Innovations-Sicht hingegen kann Regulation durchaus negativ bewertet werden, weil sie neue Geschäftsideen im Krypto-Bereich erschwert, verhindert oder gestandene Unternehmen begünstigt.

Das Bewertungsmodell ist daher immer auch im Kontext der individuellen Betrachtung des Themas Kryptowerte zu sehen.

5. Handlungsempfehlung

Um eine angemessene Regulierung der Kryptowerte zu schaffen, sollten die Interessen und Vorstellungen aller Marktteilnehmer und Beteiligten verstanden und eingebracht werden. Im Falle von Interessenskollisionen (z.B. zwischen Anlegerschutz und Innovation) muss eine Balance gefunden werden. Dabei divergieren die Interessen im Krypto-Markt teils stark.

Es ist ein Balanceakt: Zum einen muss der Gesetzgeber sicherstellen, dass Verbraucher und Anleger ausreichend vor illegalen Aktivitäten sowie inhärenten Risiken geschützt sind. Zum anderen sollte einem so jungen und sich entwickelnden Markt Freiraum gegeben werden, damit sich Innovationen entfalten können. Nur durch einen ausgewogenen Ansatz kann eine Massentauglichkeit von Kryptowerten erreicht werden. Die folgenden Anregungen können dabei als Leitplanken dienen.²⁵

Zuerst bedarf es einer konkreten Abgrenzung zwischen den Anwendergruppen, um eine adressatengerechte regulatorische Behandlung sicherzustellen. Ähnlich relevant ist die eindeutige Prüfung der Anwendungsbereiche von Kryptowerten, die aktuell und zukünftig genutzt werden. Denn der Risikograd der Anwendergruppen und -bereiche variiert stark. Entsprechende Risiken können dann seitens des Gesetzgebers besser adressiert werden, wenn möglichst viele Ausprägungen von Risiken berücksichtigt werden. Beispielsweise kann der Gesetzgeber mit der Travel Rule der FATF²⁶ einen derartigen risikobasierten und adressatengerechten Ansatz (hier: Anleger) verfolgen. Gleichzeitig führt diese Travel Rule aber auch zu erheblichen Anforderungen und Aufwänden bei Krypto-Dienstleistern. Diese Konsequenzen sollten diskutiert und gegeneinander abgewogen werden. Ein elementarer Bestandteil und grundlegender Anwendungsbereich von Kryptowerten ist deren Verwahrung. Sie stellt den Ausgangspunkt für andere Anwendungen dar und steigert für Nutzer die Sicherheit im Umgang mit Kryptowerten. In Deutschland wurde bereits 2020 durch die Kryptoverwahrlicenz, verankert im KWG, für Rechtssicherheit gesorgt.

Des Weiteren sind für einen professionalisierten Markt, insbesondere aus der Perspektive von Verbrauchern und Anlegern, vertrauensvolle Marktteilnehmer und Dienstleister erforderlich. Hierfür ist allen voran die Institutionalisierung und aufsichtsrechtliche Kontrolle von Krypto-Dienstleistern sinnvoll, da diese zumeist die ersten Berührungspunkte von Nutzern mit Kryptowerten gestalten. Auf EU-Ebene werden Krypto-Dienstleister und ihre unterschiedlichen Rollen im Rahmen von MiCAR gewürdigt und umfassend reguliert

Im dynamischen und komplexen Krypto-Markt ist daher eine fortlaufende Zusammenarbeit zwischen Anbietern und Gesetzgeber dringend zu empfehlen. Gesetzgeber sollten sich permanent Erkenntnisse aus der Krypto-Branche einholen, um eine gute Durchdringung und ein aktuelles Verständnis des Marktes zu erlangen. Im Rahmen dieses Prozesses sollten Regulierungsansätze auf Basis neuer Entwicklungen immer hinterfragt und ggf. modifiziert werden.²⁷

Abschließend ist aufgrund des grenzüberschreitenden Charakters von Kryptowerten eine internationale Kooperation unter Einbezug globaler Gremien wie der FATF, der Bank für Internationalen Zahlungsausgleich (BIZ) oder des Financial Stability Boards (FSB) sowie nationaler Organisationen wie Zentralbanken und Aufsichtsbehörden unausweichlich.²⁸ Neben der Standardisierung von Prozessen und optimierter Koordination zwischen unterschiedlichen Jurisdiktionen kann so die regulatorische Arbitrage niedrig gehalten werden. Studien haben bisher gezeigt, dass zunehmende Regulierung die gesamte Marktaktivität der Kryptowerte nicht abschwächt. Es ist insbesondere keine signifikante Migration von Geschäftsaktivitäten von vermeintlich stärker regulierten Jurisdiktionen hin zu weniger stark regulierten Jurisdiktionen zu beobachten.²⁹

²⁵ Vgl. Ferreira & Sandner, 2021.

²⁶ Die Travel Rule der FATF sieht u.a. vor, dass Krypto-Dienstleister ab einer Grenze von 1000 Euro verpflichtet sind, Informationen über Sender und Empfänger von Transaktionen an eine staatliche Institution zu melden (Vgl. Financial Action Task Force (FATF), 2021).

²⁷ Vgl. International Monetary Fund (IMF), 2020.

²⁸ Vgl. Ferreira et al., 2021.

²⁹ Vgl. Feinstein & Werbach, 2021.

6. Ausblick und Fazit

In dieser Studie wird ein standardisiertes Rahmenwerk entwickelt, um den Fortschritt der Regulierung von Kryptowerten einer Jurisdiktion zu bewerten und zu vergleichen. Das Rahmenwerk dient als Instrument, um die im Kontext von Kryptowerten relevanten regulatorischen Fragestellungen dahingehend zu bewerten, inwiefern existierende Regelungen einer Jurisdiktion die Nutzung von Kryptowerten erlauben. Dabei wurde zwischen verschiedenen Analyseeinheiten unterschieden: Den Anwendergruppen und -bereichen. Die Analyse wurde in ein standardisiertes Rahmenwerk gegossen. Mit ihm können die unterschiedlichen globalen Regularien von Kryptowerten übergreifend verglichen und bewertet werden. So können Risiken mit den voraussichtlich höchsten Auswirkungen auf den Verbraucher- und Anlegerschutz sowie Compliance und operationelle Aspekte identifiziert werden. Das präsentierte Rahmenwerk deckt dabei die aktuell relevantesten Faktoren ab. Die in Deutschland bereits verabschiedeten Verordnungen greifen viele Aspekte der in Kapitel 5 genannten Handlungsempfehlungen auf und bieten gleichzeitig eine solide Basis für die bevorstehende MiCAR auf EU-Ebene, deren Eckpunkte die Grundlage für das Rahmenwerk darstellen.

Im jungen und innovativen Krypto-Markt können sich die Eigenheiten jedoch schnell verändern, daher sollten die Marktentwicklungen kontinuierlich überwacht, neu bewertet und ggf. in das Rahmenwerk integriert werden. So wird zum Beispiel das Thema ESG (Environment, Social, Governance) zunehmend in vielen Bereichen der Wirtschaft immer relevanter. Im Hinblick auf den Energieverbrauch von verschiedenen Blockchains werden insbesondere die Umwelt-Aspekte von Kryptowerten mitunter kritisch betrachtet. So verpflichtet die MiCAR in ihrer aktuellen Fassung Krypto-Dienstleister, Informationen über Klima- und Umweltauswirkungen von verwendeten Kryptowerten zu veröffentlichen. Ähnliche Anforderungen sind künftig auch außerhalb der EU zu erwarten und könnten den Erfolg von Kryptowerten maßgeblich beeinflussen. Es ist zu erwarten, dass Dienstleistungen im Zusammenhang mit dem Bitcoin auch ESG-Kriterien genügen müssen.

Ähnlich wichtig ist die teils mangelnde Transparenz der Besitzverhältnisse von Kryptowerten. Zwar müssen in manchen Jurisdiktionen die Identitäten von Sender und Empfänger einer Krypto-Transaktion offengelegt werden, sofern gewisse Bedingungen greifen. Aber bislang sind konkrete Anforderungen in Form von Offenlegungspflichten über gehaltene Vermögen kaum zu beobachten, was aktuell Markt- und Kursmanipulationen immer noch ermöglicht. Durch marktorientierte Offenlegungspflichten könnte die Konzentration von Krypto-Vermögen sowie entsprechende Marktbewegungen besser nachvollzogen und Manipulationen vorgebeugt werden.

Neben den zu berücksichtigenden Faktoren und Risiken ist das Vorgehen von Regulatoren wie gezeigt entscheidend für die Förderung oder Beeinträchtigung der Entwicklung von Kryptowerten. Wünschenswert ist dabei ein Vorgehen, das die in Kapitel 5 beschriebenen Vorgehensweisen bündelt. Ein solcher Regulatorik-Ansatz vereint die risikobasierte und anwendergerechte Abgrenzung von Anwendungsfällen, die Institutionalisierung von Krypto-Dienstleistern und die öffentlich-private Zusammenarbeit sowie internationale Kooperation. Eine solche Regulatorik bietet stabile Leitplanken auf dem Weg zu einer innovationsfreundlichen und gleichzeitig verbraucher- und anlegerschützenden Zukunft der Kryptowerte.

Literaturverzeichnis

Bank for International Settlements (BIS). (2019, Dezember). Designing a prudential treatment for cryptoassets. <https://www.bis.org/bcbs/publ/d490.pdf>

Bundesministerium der Finanzen. (2020, Juni). Deutschlandprüfung 2020/2021 der Financial Action Task Force – Bundesfinanzministerium - BMF-Monatsbericht Juni 2020. Abgerufen am 23. August 2022, von <https://www.bundesfinanzministerium.de/Monatsberichte/2020/06/Inhalte/Kapitel-3-Analysen/3-2-deutschlandpruefung-der-fatc.html>

Bundesministerium der Justiz. (2022, 20. Juli). § 1 KWG - Einzelnorm. Gesetze im Internet. Abgerufen am 23. August 2022, von https://www.gesetze-im-internet.de/kredwg/_1.html

Chainalysis. (2022a, Februar). The 2022 Crypto Crime Report. <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>

Chainalysis. (2022b, August 23). Cryptocurrency Compliance Software. Abgerufen am 23. August 2022, von <https://www.chainalysis.com/chainalysis-kyt/>

Charoenwong, B. and Bernardi, M. (2021). A Decade of Cryptocurrency 'Hacks': 2011 – 2021. <http://dx.doi.org/10.2139/ssrn.3944435>

Coinbase. (2022, Mai). Coinbase Crypto Report – Europe 2022 H1. <https://intas.tech/wp-content/uploads/2022/05/Coinbase-Crypto-Report-Europe-2022-H1-DE.pdf>

European Central Bank (ECB). (2022, Mai). Financial Stability Review. <https://www.ecb.europa.eu/pub/pdf/fsr/ecb.fsr202205~f207f46ea0.en.pdf>

European Central Bank (ECB). (2021, November). Financial Stability Review. <https://www.ecb.europa.eu/pub/pdf/fsr/ecb.fsr202111~8b0aebc817.en.pdf>

Europäische Union. (2020, 24. September). Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937. EUR-Lex. Abgerufen am 23. August 2022, von <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020PC0593>

European Parliament (EP). (2019, Juli). Blockchain and the General Data Protection Regulation. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/6344445/EPRS_STU\(2019\)6344445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/6344445/EPRS_STU(2019)6344445_EN.pdf)

Federal Reserve Economic Data (FRED). (2021, 15. April). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets | St. Louis Fed. Federal Reserve Bank of St. Louis. Abgerufen am 23. August 2022, von <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets>

Feinstein, B. D. & Werbach, K. (2021). The Impact of Cryptocurrency Regulation on Trading Markets. *Journal of Financial Regulation*, 7(1), 48–99. <https://doi.org/10.1093/jfr/fjab003>

Ferreira, A. & Sandner, P., (2021). Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law & Security Review*, Volume 43, November 2021, 105632. <https://doi.org/10.1016/j.clsr.2021.105632>

Ferreira, A., Sandner, P., Dünser, T. (2021). Cryptocurrencies, DLT and Crypto Assets – the Road to Regulatory Recognition in Europe. *Handbook on Blockchain*. <http://dx.doi.org/10.2139/ssrn.3891401>

Financial Action Task Force (FATF). (2021). SECOND 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf>

International Monetary Fund (IMF). (2020, 10. Januar). Regulation of Crypto Assets. Abgerufen am 23. August 2022, von <https://www.imf.org/en/Publications/fintech-notes/Issues/2020/01/09/Regulation-of-Crypto-Assets-48810>

manager magazin. (2022, 14. Juli). Krypto-Verleiher Celsius Network meldet Insolvenz an. Abgerufen am 23. August 2022, von <https://www.manager-magazin.de/finanzen/geldanlage/celsius-network-krypto-firma-meldet-insolvenz-an-a-23216a68-8e35-45bb-9a78-45fabeeef5e04>

Schwarz, D., Kröner, A. & Schütze, A. (2022, 12. August). Fintech: Berliner Kryptobank Nuri ist insolvent. *Handelsblatt*. Abgerufen am 23. August 2022, von <https://www.handelsblatt.com/finanzen/fintech-berliner-kryptobank-nuri-ist-insolvent-500-000-kunden-mit-500-millionen-euro-vermoe-gen-betroffen/28586210.html>

Suratkar, S., Shirole, M. & Bhirud, S. (2020). Cryptocurrency Wallet: A Review. 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP). <https://doi.org/10.1109/icccsp49186.2020.9315193>

White House (WH). (2022, März). FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets. Abgerufen am 05. September 2022, von <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/>

World Economic Forum (WEF). (2021, September). Navigating Cryptocurrency Regulation: An Industry Perspective on the Insights and Tools Needed to Shape Balanced Crypto Regulation. https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

