



LEITFADEN ZU KRYPTO-ASSETS



WIRTSCHAFTSKAMMER ÖSTERREICH
Die Finanzdienstleister

Fachverband Finanzdienstleister
Bundessparte Information und Consulting
Wirtschaftskammer Österreich
Wiedner Hauptstraße 63 | 1045 Wien
T 05 90 900-4818 | F 05 90 900-4817
E finanzdienstleister@wko.at
W <http://wko.at/finanzdienstleister>

STADLER VÖLKEL

RECHTSANWÄLTE · ATTORNEYS AT LAW

10. Oktober 2022

Leitfaden zu Krypto Assets I Index

1.	Begriffe in der Krypto-Welt	5
1.1.	Krypto-Asset, Kryptowährung, virtuelle Währung, NFT	5
1.2.	Bitcoin, Wallet	7
1.3.	Blockchain, Nodes, Miner, Validatoren	7
1.4.	(Alt-)Coin und Token	8
1.5.	Initial Coin Offering / Initial Token Offering und Initial Exchange Offering.....	10
2.	Smart Contract	11
3.	Exkurs: Bitcoins	11
4.	Exkurs: Mining, Minting, Staking, MEV	12
5.	Hinweis: Zur steuerrechtlichen Beurteilung von Mining verweisen wir auf unseren Leitfaden „Besteuerung von Kapitalvermögen im Privatvermögen“ (Punkt 4.8). Charakteristika von Krypto-Assets.....	13
6.	Einstufung von Krypto-Assets	14
6.1.	...als übertragbares Wertpapier	14
6.2.	...als E-Geld, Zahlungsinstrument oder Zahlungsmittel.....	15
6.3.	...als Packaged Retail and Insurance based Investment Product (PRIIP)	15
6.4.	... als Alternativer Investmentfonds Manager	15
7.	Tokenisierung	15
7.1.	Schritte zur Tokenisierung.....	16
7.2.	Modelle zur Tokenisierung.....	16
7.3.	Beispiele für Tokenisierung.....	18
7.3.1.	Tokenisierte Substanzgenussrechte	18
7.3.2.	Tokenisierte Umsatzgenussrechte	19
7.3.3.	Tokenisierte Nachrangdarlehen	19
7.3.4.	Tokenisierte Verwendungszusagen	19
7.3.5.	Tokenisierung bei der Gesellschaft mit beschränkter Haftung	20
7.3.6.	Tokenisierung bei der Aktiengesellschaft.....	21
7.3.7.	Tokenisierung von Realgütern wie etwa Edelmetallen oder Zinshausanteilen	21
7.3.8.	Tokenisierung von Gutscheinanprüchen	21
7.4.	Rechtliche, steuerliche und bilanzielle Strukturierung	21
7.5.	Öffentliches Angebot von Werttoken	22
8.	Zugang: Konzession oder Gewerbe?.....	23
8.1.	Beratung und Vertrieb von Krypto-Assets	23
8.2.	Mining.....	24
8.3.	Handel mit Krypto-Assets	24
8.4.	Betreiben einer Online-Börse für Krypto-Assets („Krypto-Börse“)......	25
8.5.	Betreiben eines Krypto-Asset-Geldautomaten („Elektronische Wechselstube“)......	25
9.	Vorteile und Risiken von Krypto-Assets bzw Blockchain-Technologie	25

10. Geldwäscheprävention und Registrierungspflicht von Dienstleister virtueller Währungen	26
11. EU-Rechtsrahmen über Märkte in Kryptowerte („MiCA“)	30
12. Anhang: Auszug - Was ist die Blockchain?	33
13. Anhang 2: Eine alternative Erklärung der Blockchain	34



Sie wollen mehr Informationen?
Dann schauen Sie auch in unsere

Wissensdatenbank!

www.wko.at/wissensdatenbank oder www.wko.at/wdb

Wichtiger Hinweis

Die **Rechtslage** in Bezug auf Krypto-Assets unterliegt einem **stetigen Wandel**. Derzeit gibt es zu Tätigkeiten in Zusammenhang mit Krypto-Assets (wie zB dem Mining oder Handel) wenige bzw strittige Aussagen. Für gewisse Geschäftsmodelle ist eine Gewerbeberechtigung, Registrierung bei, oder Konzession der Finanzmarktaufsichtsbehörde (FMA) notwendig (siehe Informationen dazu auf www.fma.gv.at - Stichwort „Virtuelle Währungen“).

Ihre Anfragen richten Sie daher direkt an:

- **FMA**, wenn eine Registrierung oder Konzession für Ihr Geschäftsmodell notwendig ist, www.fma.gv.at oder direkt über den FinTech Navigator der FMA: <https://www.fma.gv.at/kontaktstelle-fintech-sandbox/fintechnavigator/>
- **Fachgruppe Finanzdienstleister** (Ihres Bundeslandes), wenn eine Beratung/Vermittlung von Krypto-Assets in Betracht gezogen wird (Gewerbe: Gewerbliche Vermögensberatung)
- **Fachgruppe Werbung und Marktkommunikation** (Ihres Bundeslandes), wenn es um das Anwerben von Kunden für Zurverfügungstellung deren Rechnerleistung (Mining) geht (Gewerbe: Ankündigungsunternehmen)
- **Fachgruppe für Unternehmensberatung, Buchhaltung und Informationstechnologie** (Ihres Bundeslandes, www.ubit.at), sofern Softwareanwendungen für Dritte programmiert oder Rechenzentrumsdienstleistungen angeboten werden, die Dritten in Bezug auf Blockchain-Anwendungen dienen. Dies kann im Rahmen des IT-Berufsbild für das freie Gewerbe „Dienstleistungen der automatischen Datenverarbeitung und Informationstechnik (IT Gewerbe)“ erfolgen.
- **Fachgruppe Gewerbliche Dienstleister** (Ihres Bundeslandes): Gewerbe „Vermittlung von Werk- und Dienstleistungsverträgen an Befugte“, wenn reine Vermittlungstätigkeiten stattfinden, wenn zB die Vermittlung von Rechenleistungen von Kunden zu Miningfirmen stattfinden und ein Entgelt für die Vermittlung ausbezahlt wird.

Für eine Beratung zu konkreten Geschäftsmodellen empfehlen wir, sich an einen **Rechtsexperten Ihrer Wahl** (zB Rechtsanwalt) zu wenden.

1. Begriffe in der Krypto-Welt

Fragen:

1. Was ist ein Krypto-Asset?
2. Was ist eine Kryptowährung?
3. Was sind virtuelle Währungen?
4. Was sind NFTs?
5. Was sind Bitcoins?
6. Was ist eine Wallet?
7. Was ist eine Blockchain?
8. Was sind Nodes?
9. Was ist ein Miner/Staker?
10. Was ist der Unterschied zwischen „(Alt-)Coin“ und „Token“?
11. Welche Arten von Token gibt es?
12. Was ist das Initial Coin Offering bzw. Initial Token Offering?
13. Was ist ein Smart Contract?

1.1. Krypto-Asset, Kryptowährung, virtuelle Währung, NFT

Anfänglich wurde im Bereich der Krypto-Welt nicht von „Krypto-Assets“, sondern von Kryptowährungen gesprochen. Eine Kryptowährung wird im Unterschied zu gesetzlich anerkannten Währungen nicht von der Zentralbank, sondern durch Private ausgegeben oder erzeugt.¹ Sinn und Zweck ist es beispielsweise Waren, Dienstleistungen, IT-Anwendungen oder Freizeitangebote erwerben zu können.

Hinweis: Da es sich bei Kryptowährungen aber eben NICHT um gesetzlich anerkannte Zahlungsmittel handelt, hat sich der Überbegriff „Krypto-Asset“ etabliert, um eine stärkere Abgrenzung zur gesetzlich anerkannten „Währung“ zu schaffen.

§ 2 Z 21 FM-GwG verwendet - in Umsetzung der 5. Geldwäsche-Richtlinie ([Richtlinie \(EU\) 2018/843](#)) - wiederum den Begriff der „virtuellen Währung“, der wie folgt definiert ist:

*Eine „virtuelle Währung“ ist „eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist und die nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann“.*²

Achtung: Gerade weil virtuelle Währungen nicht von einer zentralen Stelle bzw von Zentralbanken ausgegeben werden, bestehen hier besondere Risiken, da es keine Aufsichts- und Kontroll- oder Regulierungsmöglichkeiten gibt.

Die Begriffe Kryptowährung und virtuelle Währung werden in der Praxis synonym verwendet.

Da die derzeitigen Geldwäschebestimmungen nur Regelungen für bestimmte Kategorien von Krypto-Anbietern enthalten, soll eine neue unmittelbar anwendbare Verordnung³ als einheitliches EU-Regelbuch (Single Rulebook) die auf der 5. Geldwäsche-Richtlinie beruhenden

¹ Die ursprüngliche Ausgabestelle ist dabei meist nicht mehr nachvollziehbar. Stand Juni 2022 gibt es über 10.000 verschiedene Kryptowährungen. [Zur Auflistung aller aktuellen Kryptowährungen.](#)

² Das FM-GwG hat zudem den Begriff „Dienstleister in Bezug auf virtuelle Währungen“ eingeführt. Mehr dazu siehe unten.

³ Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, COM/2021/420 final.

nationalen Geldwäschebestimmungen innerhalb der Union harmonisieren. Diese in Kurzform als "MiCA" betitelte Verordnung wird mit dem Begriff des Krypto-Assets (bzw. Kryptowert in der deutschen Fassung) eine einheitliche Definition innerhalb der EU einführen.

Die Definition in § 2 Z 21 FM-GwG soll daher in Umsetzung des EU-Pakets zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung aufgegeben werden, indem auf den Begriff des Crypto-Asset in der MiCA verwiesen wird. Siehe dazu genauer unter Punkt 11.

In der Literatur werden Krypto-Assets üblicherweise in Coins und Token⁴ bzw in Krypto-Assets im engeren Sinn und Krypto-Assets im weiteren Sinn unterteilt. Unter Krypto-Assets im engeren Sinn werden Coins wie Bitcoin, Ether oder Litecoin verstanden, die auf einer eigenständigen Blockchain basieren.⁵ Unter Krypto-Assets im weiteren Sinn werden hingegen Token verstanden, die auf bereits bestehenden Plattformen, wie etwa Ethereum, aufbauen.⁶ Siehe dazu genauer unter Punkt 1.4.

Abgesehen von der geldwäscherechtlichen Regulierung gibt es derzeit weder auf nationaler noch auf europäischer Ebene eine gesetzliche oder einheitliche Definition von Krypto-Assets. Auch Rechtsprechung im Bereich von Krypto-Assets ist bisher nur sehr vereinzelt vorhanden.⁷ Klarheit wird daher erst der europäische Gesetzgeber durch den Erlass der MiCA schaffen.⁸ Für Krypto-Assets gibt es derzeit in Österreich - anders als in anderen Ländern wie bspw Liechtenstein - keine gesetzlichen Sonderregelungen. Das österreichische Recht ist allerdings technik-neutral, sodass sämtliche Regelungen - inklusive der zivilrechtlichen Bestimmungen des Allgemein Bürgerlichen Gesetzbuches (Besitz, Eigentum, Pfandrecht etc.) - auch auf Krypto-Assets anwendbar sind.⁹

Die FMA versteht unter Krypto-Assets *"eine Art finanzieller Vermögenswert, der auf Kryptographie und "distributed ledger" ("verteiltes Hauptbuch") oder ähnlicher Technologie beruht. Krypto-Assets können als Übergruppe verstanden werden."*¹⁰

Ein relativ neues Phänomen sind sogenannte **"Non-Fungible Token"** (= nicht austauschbare, einzigartige Wertmarke, kurz NFTs). Dabei handelt es sich um spezielle Krypto-Assets, die sich von anderen Krypto-Assets dadurch unterscheiden, dass sie einzigartig und nicht standardisiert ausgestaltet sind. Ein bestimmter NFT ist daher nicht 1:1 gegen andere NFTs austauschbar (= non-fungible).

Nicht austauschbar bedeutet, dass es keine identische Kopie des jeweiligen NFT gibt. In technischer Hinsicht handelt es sich um Datensätze, die auf einer Blockchain gespeichert sind und auf Metadaten verweisen.¹¹ Daher ermöglichen NFTs mit entsprechender vertraglicher Ausgestaltung die Übertragung digitaler und analoger Werke, indem sie als Echtheitszertifikat

⁴ Vgl. Tuder in Kirchmayr-Schliesselberger u. a., Kryptowährungen, 278 ff; Marek in Piska/Völkel, Blockchain rules (2019), Rz 9.4 ff; Pekler/Rirsch in Kirchmayr-Schliesselberger u. a., Kryptowährungen, 338 f; Veronesi in Anderl, #Blockchain in der Rechtspraxis, 16 f; Völkel in Piska/Völkel, Blockchain rules (2019), Rz 1.22 ff; Tuder/Ahari in Artmann/Biedber/Mayrhofer/Schmidt/Tumpel (Hrsg), Crypto Assets, 126.

⁵ Vgl. Schneider in Artmann et al., Crypto Assets (2022), 127; Tuder/Ahari in Hanzl/Pelzmann/Schragl, 45; Pekler/Rirsch/Tuder in Kirchmayr-Schliesselberger u. a., Kryptowährungen - Krypto Assets, ICOs und Blockchain - Recht - Technik - Wirtschaft (2019), 278, 339.

⁶ Vgl. Schneider in Artmann et al., Crypto Assets (2022), 127; Tuder/Ahari in Hanzl/Pelzmann/Schragl, 46; Tuder in Kirchmayr-Schliesselberger u. a., Kryptowährungen, 279; Schmidt, Kryptowährungen und Blockchains - Technologie, Praxis, Recht, Steuern¹ (2019), 67.

⁷ Vgl. EuGH 22.10.2015, Rs C-264/14, Hedqvist.

⁸ [Pressemitteilung](#) des Rates der EU zur MiCA. Siehe dazu genauer unter Punkt 10.

⁹ Vgl. Paulmayr in Kirchmayr-Schliesselberger u. a., Kryptowährungen (2019), S 318.

¹⁰ <https://www.fma.gv.at/glossar/krypto-assets/>

¹¹ Kresbach/Zhang, Urheberrechtliche Aspekte von Non-Fungible Token, MMR 2021, S 195.

und Herkunftsnachweis fungieren. Besonders bekannt und für die Erstellung und Herausgabe von NFTs weltweit wohl am meisten genutzt wird die Ethereum Blockchain.¹²

Derzeit unterliegen NFTs nach herrschender Ansicht nicht dem Regime des Kapitalmarktrechts. Weiterhin unklar ist, ob NFTs in den Anwendungsbereich der MiCA fallen. Im jüngsten Verordnungsentwurf wird festgehalten, dass die Ausgabe von NFTs in einer größeren Serie oder Sammlung als Zeichen für deren Austauschbarkeit dienen soll. Dies würde unter Umständen bei der Ausgabe bestimmter NFTs zu der Anwendbarkeit der MiCA führen.

1.2. Bitcoin, Wallet

Bitcoin ist im weitesten Sinne das allererste verwendete Krypto-Asset mit Zahlungscharakter und kann in entsprechenden Akzeptanzstellen in Fiat-Währung bzw Fiat-Geld umgetauscht werden. Weitere Beispiele für Krypto-Assets sind zB Ether oder Ripple.

Zugang zu Bitcoins erlangt man über eine sogenannte „**Wallet**“, das den bzw die privaten Schlüssel (private key) des Users zu seinen Krypto-Assets verwaltet. Geht dieser verloren, kann niemand auf das Krypto-Asset zugreifen. Unterschieden werden „Hosted“ und "Unhosted“ Wallets.

Eine sogenannte „Unhosted-Wallet“ oder „Non-Custodial-Wallet“ ist eine Wallet-Adresse, die nicht von einem Krypto-Dienstleister gehalten oder verwaltet wird. Es handelt sich dabei um eine vom Inhaber der Krypto-Assets selbst verwaltete Wallet-Adresse. Die privaten Schlüssel hat ausschließlich der Inhaber der Wallet. Im Unterschied dazu wird eine „Hosted-Wallet“ durch einen registrierten Dienstleister in Bezug auf virtuelle Währungen zur Verfügung gestellt, der die privaten Schlüssel für den Nutzer verwaltet.

1.3. Blockchain, Nodes, Miner, Validatoren

Unter **Blockchain** versteht man eine Technologie, welche Transaktionen erfasst und als digitales Kontobuch zu verstehen ist. Es handelt sich um ein dezentrales Peer-to-Peer-Netzwerk, dh die Transaktionen gehen direkt von Nutzer zu Nutzer bzw Node zu Node und es existiert keine zentrale Stelle. Die Transaktionsdaten werden in Blöcken erfasst, dezentral gespeichert und auf sämtlichen Nodes der Mitglieder abgelegt. Dadurch werden die Netzwerkmitglieder sozusagen „Zeugen der Transaktion“, welche auch die Transaktion bestätigen (Validierung der Transaktion).

Als Erfinder der Bitcoin-Blockchain gilt *Satoshi Nakamoto*¹³, der am 1. November 2008 in seinem White Paper „*Bitcoin: A Peer-to-Peer Electronic Cash System*“¹⁴, die theoretischen Grundlagen von Bitcoin vorstellte.¹⁵ Mittlerweile haben sich verschiedene Blockchain-Systeme etabliert.

Unterschieden wird zwischen permissionless und permissioned Blockchain-Systemen. Bei letzteren können nur zugelassene Nutzer am Konsensalgorithmus teilnehmen und bestimmte Funktionen ausführen. Bei öffentlichen bzw permissionless Systemen hingegen steht der Zugang zum Netzwerk jeder beliebigen Person offen und es gibt keine Beschränkungen. Bitcoin und Ethereum laufen etwa auf öffentlichen Blockchains so wie die meisten Payment-Token.

¹² Die genauen Rahmenbedingungen für NFTs finden sich im Standard ECR-721

(<https://eips.ethereum.org/EIPS/eip-721>) und im neueren ERC-1155 (<https://eips.ethereum.org/EIPS/eip-1155>).

¹³ Der Name ist ein Pseudonym, wobei bis heute unbekannt ist, welche Person oder Personengruppe sich dahinter verbirgt.

¹⁴ Abrufbar unter <<https://bitcoin.org/bitcoin.pdf>>.

¹⁵ Vgl. *Schmidt* in *Schmidt*, Kryptowährungen und Blockchains, 3; *Aigner*, Das Pfandrecht und die Blockchain, ÖBA 2019, 816.

Hinweis: Eine Erklärung, wie die Blockchain-Technologie (auch **Distributed Ledger-Technologie** genannt) genau funktioniert, befindet sich im Anhang bzw auf der Seite der WKO zu „[Blockchain - Grundlagen](#)“.

Alle Mitglieder des Systems werden als **Nodes** bezeichnet.

Ein **Miner** ist jener Node, der das Mining betreibt. Es können auch sehr viele „Rechner“ unter einem Node verbunden sein. Als Mining wird das Bestätigen von eingereichten Transaktionswünschen bezeichnet. Nach Bestätigung einer Transaktion werden Miner entschädigt. Zum einen sind neu erzeugte Einheiten einer virtuellen Währung als Belohnung vorgesehen. Zum anderen können Minern auch Belohnungen in Form von Transaktionsgebühren gewährt werden. Die Belohnung steht jenem Miner zu, der einen Transaktionswunsch am schnellsten auf seine Vereinbarkeit mit der bisherigen Transaktionshistorie einer Blockchain überprüft hat (Proof-of-Work). Dies gleicht dem Lösen eines hochkomplexen mathematischen Problems. Je mehr Rechenleistung vom Miner eingesetzt wird, desto wahrscheinlicher kann das Problem gelöst werden und desto eher erhält der Miner seine Belohnung.¹⁶

Ein **Validator** ist jener Node, der das Staking betreibt. Er ist ebenfalls für die Überprüfung und Genehmigung von Transaktionswünschen zuständig. Das Recht, Transaktionen zu validieren hängt dabei aber nicht von der Rechenleistung, sondern von der Anzahl der hinterlegten Einheiten einer virtuellen Währung ab (Proof-of-Stake). Wichtig ist, dass jede Blockchain unterschiedliche Voraussetzungen für die Zulassung von Validatoren in ihren Protokollen vorsieht. Die Ethereum-Blockchain sieht bspw als Voraussetzung den Einsatz von mindestens 32 Ether für die Zulassung von Validatoren vor.

Die Regeln der Zuteilung von Transaktionswünschen hängen von dem Konsensmechanismus einer Blockchain ab. Siehe dazu genauer unter Punkt 3.

Die **Blockchain-Technologie** kann und wird auch in anderen und unterschiedlichen Bereichen eingesetzt zB im Derivatehandel (Nasdaq-Initiative) oder Energiebereich (Direktvermarktung bei Solarenergie). Auch im behördlichen Bereich sind Varianten denkbar (Datennachweise, Ersatz behördlicher Register, Vereinfachung von Behördenverfahren).¹⁷

1.4. (Alt-)Coin und Token

Eine weitere wichtige Unterscheidung in der Krypto-Welt sind die Begriffe „**Coin**“ und „**Token**“. Diese Begriffe werden nicht immer richtig abgegrenzt und in der Praxis häufig sogar als Synonym verwendet.¹⁸

Während der Coin auf einer neuen, eigenen Blockchain basiert, werden Token auf einer bereits bestehenden Blockchain erzeugt. Coins sind also der jeweiligen Blockchain immanent, während Token erst später durch die Nutzer der Blockchain hinzugefügt werden, da sie nicht von Beginn an im Protokoll vorgesehen sind.¹⁹

In diesem Zusammenhang fällt oft auch der Begriff „**Altcoin**“. Altcoin ist die Abkürzung für „**alternative Coins**“ und bezieht sich auf alle Krypto-Assets, die nach dem Bitcoin entstanden sind. Bitcoin gilt demnach als die erste Kryptowährung. Alle danach entstandenen Alternativen bzw Varianten zu Bitcoin werden daher als Altcoins bezeichnet und können verschiedene Unterschiede zu Bitcoin aufweisen.

¹⁶ Völkel in Piska/Völkel (Hrsg), Blockchain rules, 2019, Rz 1.51 ff.

¹⁷ Raschauer, N./Silbernagl, R.: Grundsatzfragen des liechtensteinischen „Blockchain-Gesetzes“ - TVTG, in ZFR 1/2020, S 11.

¹⁸ Siehe auch Steiner, Ch.: Krypto-Assets und das Aufsichtsrecht, Wien, 2019, S 9.

¹⁹ Völkel in Piska/Völkel (Hrsg), Blockchain rules, 2019, Rz 1.22 ff.

Derzeit besteht weder in Österreich noch auf europäischer oder internationaler Ebene eine rechtlich anerkannte Klassifizierung von Token. Erst mit Inkrafttreten der MiCA wird eine gesetzliche Definition verschiedener Arten von Token eingeführt werden.

Eine inhaltliche Annäherung an den Begriff kann derzeit über die wirtschaftliche Funktion der Token erfolgen. In der Literatur werden Token nach ihrer wirtschaftlichen Funktion in Security Token, Utility Token und Payment Token unterteilt. Auch die österreichische Finanzmarktaufsichtsbehörde (FMA) verwendet diese Unterscheidung.

- **Investment-, Asset- oder Security Token** haben einen finanzinstrumenteähnlichen Charakter²⁰ und es bestehen zB Ansprüche auf einen Cashflow (Dividenden, Zinsen) oder Bezugsrechte auf ein Wertpapier. Die Literatur vertritt die Ansicht, dass Security Token idR das Recht auf Zahlung von Zinsen oder auf Beteiligung an Gewinnen des Token-Emittenten begründen und wertpapierähnliche Rechte gewähren.²¹ Die FMA vertritt ebenso die Auffassung, dass Security Token Ansprüche auf Auszahlungen gegenüber dem Emittenten verkörpern, welche gesellschaftsrechtlich oder schuldrechtlich ausgestaltet sein können. Mit Security Token können demnach gesellschaftsrechtliche Ansprüche, etwa Stimmrechte bei einer Hauptversammlung verbunden sein. Diese Token verkörpern somit idR Ansprüche auf Zahlung von Kapital, sei es in Form von Beteiligungen am Unternehmensgewinn oder in Form von Verzinsung und Rückzahlung. Dabei ist es grundsätzlich nicht zwingend erforderlich, dass diese Ansprüche in gesetzlicher Währung bestehen. Die Ausgestaltung solcher Security Token ähnelt somit jener von "klassischen Wertpapieren", insbesondere Anleihen oder Aktien. Security Token werden somit häufig als Wertpapiere im Sinne der VO (EU) 2017/1129 sowie des Wertpapieraufsichtsgesetzes 2018 (WAG 2018) anzusehen sein.²²
- **Payment Token (Currency- oder Exchange-Token)** haben eine Zahlungs- und Wertaufbewahrungsfunktion wie zB Bitcoin, dh sie werden von Dritten als Tauschmittel akzeptiert. Vor diesem Hintergrund werden Payment Token zum Teil auch Coins genannt. Die Ausgabe von Payment Token verfolgt daher regelmäßig das Ziel, eine neue Kryptowährung zu etablieren.²³ Payment Token fallen daher grundsätzlich unter den Begriff der virtuellen Währung im Sinne der 5. Geldwäscherichtlinie²⁴ bzw. unter den Begriff der virtuellen Währungen im Sinne des § 2 Z 21 FM-GwG. Die FMA vertritt die Ansicht, dass es sich bei Payment Token um einen Token handelt, dessen primärer Zweck in einer Bezahlungsfunktion liegt. Payment Token verkörpern daher einen bestimmten Wert, mit denen Waren oder Dienstleistungen auch bei vom Emittenten verschiedenen Personen erworben werden können. Eine sonstige Verwendung sehen Payment Token grundsätzlich nicht vor. Payment Token, die nicht nur in einem begrenzten Netz eingesetzt werden sollen, können somit je nach Ausgestaltung eine Konzessionspflicht des Emittenten nach Bankwesengesetz (BWG), Zahlungsdienstegesetz 2018 (ZaDiG 2018) oder E-Geldgesetz 2010 (E-GeldG 2010) auslösen.
- **Utility Token** gewähren dem Inhaber Zugang zu einem (digitalen) Produkt oder einer Dienstleistung des Token-Emittenten und dienen in erster Linie dazu, dem Inhaber einen Nutzen in Hinblick auf ein bestimmtes (digitales) Produkt oder eine Dienstleistung zu verschaffen.²⁵

²⁰ § 1 Z 7 WAG 2018: Finanzinstrumente.

²¹ Heckenthaler/Rakar in Binder Grösswang (Hrsg), Digital Law² (2020) Finance - Initial Coin Offerings.

²² FMA, FinTech Navigator - ICO - Aufsichtsrechtliche Einordnung von Coins und Tokens, abrufbar unter: <https://www.fma.gv.at/kontaktstelle-fintech-sandbox/fintechnavigator/initial-coin-offering/>.

²³ Heckenthaler/Rakar in Binder Grösswang (Hrsg), Digital Law² (2020) Finance - Initial Coin Offerings.

²⁴ Richtlinie 2018/843.

²⁵ Heckenthaler/Rakar in Binder Grösswang (Hrsg), Digital Law² (2020) Finance - Initial Coin Offerings.

Die FMA vertritt ebenso die Auffassung, dass Utility Token in erster Linie dazu dienen, dem Token-Inhaber einen Nutzen in Hinblick auf ein bestimmtes Produkt oder eine Dienstleistung zu verschaffen. Häufig gewähren sie Zugang zu einer digitalen Plattform des Emittenten, die durch den Inhaber des Utility Token in bestimmter Weise genutzt werden kann. Hierbei betont die FMA, dass Utility Token in zahlreichen unterschiedlichen Formen auftreten und oft auch die Funktion von Payment Token oder Security Token (hybride Ausgestaltung) erfüllen, sodass die Definition komplex und die aufsichtsrechtliche Einordnung schwierig ist. Insbesondere kann mit Utility Token das Recht verbunden sein, ein Produkt oder eine Dienstleistung mitzugestalten, ein Produkt oder eine Dienstleistung zu nutzen oder den Token gegen ein Produkt oder eine Dienstleistung einzulösen. Häufig sind Utility Token etwa mit einer immanenten Bezahlungsfunktion gegenüber dem Emittenten oder anderen Nutzern der Plattform des Emittenten verbunden.

Ist der Token nur für die Gestaltung eines Produkts oder einer Dienstleistung einsetzbar und sonst mit keinerlei Ansprüchen verbunden oder gewährt der Token lediglich Zugang zu einem Produkt oder einer Dienstleistung, ohne dabei zugleich der Bezahlung zu dienen, liegt nach Ansicht der FMA kein aufsichtsrechtlicher Anknüpfungspunkt vor.

Kann der Token hingegen beim Emittenten oder bei anderen Nutzern der Plattform für die Nutzung eines Produkts oder einer Dienstleistung eingelöst werden, erfüllt er eine Bezahlungsfunktion und ist insofern mit einem Payment Token vergleichbar. Für die aufsichtsrechtliche Einordnung sind daher in diesem Fall dieselben Kriterien und Ausnahmen relevant, wie für Payment Token. Oft wird aber die Ausnahme des "begrenzten Netzes" zur Anwendung gelangen²⁶.

•

Achtung: Eine klare pauschale Kategorisierung ist nicht möglich. Eine Klassifizierung von Krypto-Assets, zB als Finanzinstrument, ist daher immer im Einzelfall zu beurteilen.

Eine eigene Kategorie stellen sogenannte „Stablecoins“ dar. Es handelt sich dabei um Krypto-Assets, die darauf abzielen, Preisstabilität zu gewährleisten. Ziel dieser Krypto-Assets ist es, der hohen Volatilität entgegenzuwirken, die Krypto-Assets für gewöhnlich aufweisen. Kursschwankungen sollen vermieden werden, indem der Wert jeder ausgegebenen Einheit an eine gesetzliche Währung geknüpft ist. Dies wird dadurch sichergestellt, dass etwa für einen an US-Dollar geknüpften Stablecoin pro ausgegebener Einheit ein US-Dollar hinterlegt wird. Gleichzeitig verspricht der Emittent, dass diese Einheit jederzeit gegen einen US-Dollar umgetauscht werden kann. Das wahrscheinlich bekannteste Beispiel eines Stablecoins ist der von Facebook im Jahr 2019 angekündigte Libra bzw Diem Stablecoin.

1.5. Initial Coin Offering / Initial Token Offering und Initial Exchange Offering

Das **Initial Coin Offering (ICO)** oder auch **Initial Token Offering (ITO)** ist eine Form der Unternehmens- und Projektfinanzierung, die auf der Blockchain-Technologie basiert. Es bezeichnet das initiale Angebot eines neuen Krypto-Assets bzw die Kapitalaufnahme über ein bestehendes Krypto-Asset. Diese Abkürzung wurde abgeleitet von „Initial Public Offering“ (IPO), welcher für einen Börsengang steht.

Im Rahmen eines ICO werden zur Realisierung einer Geschäftsidee durch ein Unternehmen finanzielle Mittel eingeworben. Für diese finanziellen Mittel erhalten Anleger sodann „Token“ oder „Coins“. Bei ICOs werden regelmäßig sogenannte White Paper bereitgestellt, welche

²⁶ FMA, FinTech Navigator - ICO - Aufsichtsrechtliche Einordnung von Coins und Tokens, abrufbar unter: <https://www.fma.gv.at/kontaktstelle-fintech-sandbox/fintechnavigator/initial-coin-offering/>.

beispielsweise Informationen zum geplanten Geschäftszweck, zu den handelnden Personen und der technischen Ausgestaltung der Token beinhalten können. Diese White-Paper sind jedoch bis zum Inkrafttreten der MiCA nicht reguliert und in ihrer Form und ihrem Inhalt beliebig gestaltbar.²⁷ Nach Inkrafttreten der MiCA wird für die Ausgabe von Krypto-Assets regelmäßig verpflichtend ein White-Paper zu erstellen sein.

Eine einheitliche Darstellung von ICO oder ITO ist auf Grund der Vielzahl der Ausgestaltungsoptionen nicht möglich.²⁸

Sollten beim ICO Token ausgeben, welche als Wertpapiere oder Veranlagungen qualifiziert werden, besteht für diesen ICO auch eine Prospektspflicht nach § 2 KMG 2019 bzw nach der Prospekt-VO. Von zentraler Bedeutung für die rechtliche Einstufung sind die Rechte, die durch den Token verliehen werden. Deswegen ist vor Durchführung eines ICO oder ITO eine umfassende rechtliche Beurteilung der Coins bzw Token durchzuführen, um das Projekt mit den aufsichtsrechtlichen Anforderungen abzustimmen.

Seit Beginn 2019 gibt es auch das sogenannte Initial Exchange Offering (IEO). So wird ein ICO bezeichnet, bei dem eine Krypto-Handelsplattform die Abwicklung durchführt oder begleitet. Auch hier gibt es zahlreiche Ausgestaltungsmöglichkeiten.²⁹

2. Smart Contract

Unter dem Begriff Smart Contract versteht man ein Computerprogramm, dessen Code auf einer Blockchain gespeichert ist, und das allgemeine Berechnungen und Wenn-Dann-Bedingungen selbständig ausführen kann, um das Ergebnis der Berechnung auf der Blockchain festzuhalten. Smart Contracts führen basierend auf ihrer Programmierung bestimmte Aufgaben aus. Sowohl die Programmierung als auch alle Änderungen, die durch einen Smart Contract an der Blockchain vorgenommen werden, werden dauerhaft auf der Blockchain gespeichert.

Der Begriff des Smart Contracts wurde von dem US-amerikanischen Informatiker, Rechtswissenschaftler und Kryptographen *Nick Szabo* geprägt.³⁰ Er definierte einen Smart Contract ursprünglich als ein "*computerized transaction protocol that executes the terms of a contract*".³¹

Ein Smart Contract ist nach österreichischem Recht kein zivilrechtlicher Vertrag.³²

3. Exkurs: Bitcoins

Fragen:

14. Was sind Bitcoins? Worum handelt es sich bei Bitcoins?
15. Wie werden Bitcoins in der Praxis verwendet?

Unter allen verfügbaren Krypto-Assets hat sich **Bitcoin** am stärksten etabliert. **Bitcoin** ist eine Form des Krypto-Assets, welche es ermöglicht, Beträge direkt von Teilnehmer zu Teilnehmer

²⁷ Der im September 2020 veröffentlichte EK Vorschlag der Verordnung über Märkte für Kryptowerte („MiCA“) (COM(2020) 593 final) sieht Vorschriften zu White Paper vor.

²⁸ Ausführliches zu ICO/ITO siehe Literaturverzeichnis im Anhang.

²⁹ *Steiner, Ch*: Krypto-Assets und das Aufsichtsrecht, S 19.

³⁰ Vgl. *Schnell/Schwaab*, Vertragsgestaltung beim Einsatz von Smart Contracts zur Automatisierung von Lieferbeziehungen, BB 2021, 1091; *Hanzl/Rubey*, Smart Contracts - die intelligente Art Verträge zu schließen?, Zak 2018, 238; *Smets/Kapeller*, Smart Contracts: Vertragsabschluss und Haftung, ÖJZ 2018, 293.

³¹ Vgl. *Schnell/Schwaab*, BB 2021, 1091.

³² *Buchleitner/Rabl*, Blockchain und Smart Contracts - Revolution oder alter Wein im digitalen Schlauch, *ecolex* 2017, 6; *Welten/Ozsvar* in *Binder Grösswang*, Digital Law² (2020) Zivilrecht, 15f; *Rauer/Bibi*, Non-fungible Tokens - Was können sie wirklich?, ZUM 2022, 22; ebenso *Hoeren/Sieber/Holznaegel/Guggenberger*, Handbuch Multimediarecht, 55. EL Mai 2021, Teil 13.7 Rz 4; *Heine/Stang*, Weiterverkauf digitaler Werke mittels Non-Fungible-Token aus urheberrechtlicher Sicht MMR 2021, 756, 759.

(Peer-to-Peer-Netzwerk) zu übertragen. Im engeren Sinn handelt es sich um ein Protokoll zur sicheren Überweisung eines Wertes zwischen zwei Parteien.³³

In der **Praxis** werden Bitcoins für Zahlungen (über sogenannte Wallets) oder auch als Wertspeicher im Anlageportfolio verwendet. Jedoch ist Bitcoin als Speicher für die gesamten persönlichen Ersparnisse nicht zu empfehlen, da sich der Preis ausschließlich durch Angebot und Nachfrage bestimmt. Der Tauschkurs unterliegt daher hohen Schwankungen. Dies ist sowohl ein Vorteil (Gewinnrisiko) als auch ein Nachteil (Verlustrisiko).

Bitcoin basiert auf dem Proof-of-Work Konsensmechanismus. Daher wird von **Minern** viel Rechenleistung aufgewendet, um Transaktionen zu validieren und Belohnungen zu erhalten. Mittlerweile hat das gesamte Bitcoin-Netzwerk einen enormen Energieverbrauch. Aus diesem Grund wird Proof-of-Stake als Konsensmechanismus mittlerweile als eine klimafreundlichere Alternative zum etablierten Proof-of-Work Konsensmechanismus angesehen.

Krypto-Assets wie etwa Bitcoin unterliegen mangels Emittenten derzeit nicht der Aufsicht der FMA.³⁴ Zu beachten ist jedoch, dass Handelsplattformen für virtuelle Währungen (inklusive Bitcoin) sich in Österreich als Dienstleister in Bezug auf virtuelle Währungen registrieren müssen und daher der Aufsicht der FMA unterliegen. Auch die OeNB sieht Bitcoins in Österreich aktuell als ein Nischenphänomen. Bitcoins sind keine Währung, sondern ein Spekulationsobjekt und unterliegen nicht der Aufsicht der OeNB.³⁵

Bitcoin kann unter den Begriff des Krypto-Assets nach MiCA subsumiert werden, da dieser eine digitale Darstellung eines Wertes ist, welcher unter Verwendung der DLT elektronisch übertragen und gespeichert werden kann. Bitcoin ist mangels Emittenten von der Anwendung der MiCA ausgenommen.

4. Exkurs: Mining, Minting, Staking, MEV

Fragen:

16. Was ist Mining?
17. Welche Arten von Mining gibt es?
18. Unterliegt das Mining einer Gewerbeberechtigung?
19. Wie erfolgt die steuerliche Beurteilung von Mining?
20. Was ist Minting?
21. Was ist Staking?
22. Was bedeutet MEV?

Das „**Mining**“ stellt die „Schöpfung von Krypto-Assets“ im Rahmen der Blockchain-Technologie dar. Dabei werden neue Blöcke erzeugt, die der Blockchain hinzugefügt werden. Dieser Vorgang bedarf einer bestimmten Rechenleistung (bei Proof-of-Work ist diese sehr hoch), weshalb quasi eine Belohnung erteilt wird, wenn man seinen eigenen Rechner zur Verfügung stellt. Die Belohnung besteht aus zwei Teilen: einerseits aus Einheiten einer virtuellen Währung und andererseits aus Transaktionsgebühren (von jenen Personen, die für die Transaktion eine Gebühr „ausgelobt“ haben).³⁶ Nach Ansicht der FMA ist das reine Minen von Bitcoin im eigenen Namen und auf eigene Rechnung durch eine natürliche Person nicht konzessionspflichtig.³⁷

³⁴ <https://www.fma.gv.at/kontaktstelle-fintech-sandbox/fintechnavigator/bitcoin-co/>

³⁵ <<https://www.oenb.at/FAQ/krypto-assets.html>>

³⁶ Je höher die Transaktionsgebühr ist, desto schneller erfolgt die Bestätigung einer Transaktion. Daher spielen Transaktionsgebühren eine große Rolle.

³⁷ <https://www.fma.gv.at/kontaktstelle-fintech-sandbox/fintechnavigator/bitcoin-co/>

Man unterscheidet drei Arten von Mining:

- Solo-Mining
- Pool-Mining
- Cloud-Mining

In der Vergangenheit hat die FMA Geschäftsmodelle iZm mit Pool-Mining als Alternativen Investmentfonds (AIF) qualifiziert.³⁸ Betreiber eines Mining-Pools hätten daher unter Umständen eine Konzession nach dem AIFMG zu erlangen. Es ist daher jedes Geschäftsmodell dahingehend zu untersuchen, ob die Voraussetzungen eines Alternativen Investmentfonds erfüllt sind und das AIFMG³⁹ anwendbar ist. Siehe dazu genauer unter Punkt 8.2.

Steuerliche Beurteilung von Mining: Nach hM handelt es sich beim Mining um einen Herstellungsvorgang, bei dem durch den Einsatz von Ressourcen wie Strom, Rechenleistung usw ein Wirtschaftsgut entsteht. Daher liegt beim Mining im privaten Bereich eine gewerbliche Tätigkeit vor, deren Erträge als Einkünfte aus Gewerbebetrieb zu qualifizieren sind.⁴⁰

"**Staking**" ist der Prozess, bei dem ein fester Betrag an virtueller Währung eingesetzt wird, um an der Blockerstellung und -prüfung teilzunehmen. In Proof-of-Stake-Systemen erhalten Validatoren eine Belohnung, wenn sie die native virtuelle Währung des jeweiligen Netzwerks einsetzen und korrekt am Netzwerk teilnehmen. Bei allen Proof-of-Stake-Systemen sind die gesperrten Mittel (*Stake*) proportional zur Wahrscheinlichkeit, für die Validierung eines Blocks ausgewählt zu werden.⁴¹ Auf der Ethereum-Blockchain müssen Validatoren mindestens 32 Ether (ETH) einsetzen, um teilnehmen zu können. Proof-of-Stake benötigt erheblich weniger Rechenleistung für die Verifizierung von Blöcken und Transaktionen als Proof-of-Work.

"**Minting**" (auf Deutsch "Prägen") ist der Prozess, mit dem neue Token für eine Blockchain geschaffen werden.

Maximal (Miner) Extractable Value (MEV) ist der Prozess der Extraktion von Wert aus einem Blockchain-Netzwerk durch Hinzufügen, Entfernen oder Ändern der Reihenfolge der in einem Block enthaltenen Transaktionen. Miner analysieren die Auswirkungen von Transaktionswünschen und platzieren anstelle des Transaktionswunsches des Absenders eine eigene gleichlautende Transaktion, um etwa Arbitragemöglichkeiten auszunutzen.

5. Hinweis: Zur steuerrechtlichen Beurteilung von Mining verweisen wir auf unseren Leitfaden „[Besteuerung von Kapitalvermögen im Privatvermögen](#)“ (Punkt 4.8). Charakteristika von Krypto-Assets

Fragen:

23. Was sind die Charakteristika von Krypto-Assets?

Zusammenfassend lassen sich Krypto-Assets wie folgt charakterisieren:

- Sämtliche Prozesse werden in der Blockchain gespeichert.
- Sie werden digital über eine elektronische Geldbörse („Wallet“) verwaltet.
- Geht der private Schlüssel zur Wallet verloren, kann auch auf die Krypto-Assets in keiner Weise zugegriffen werden.

³⁸ FMA: FAQ zur Anwendung des Alternativen Investmentfonds Manager-Gesetz (AIFMG), 2020.

³⁹ Alternative Investmentfonds Manager-Gesetz (AIFMG), BGBl I 135/2013 idF I 9/2020.

⁴⁰ Petritz/Wimmer/Deichsel, Kryptosteuerhandb. 2021 (2021), S. 48.

⁴¹ Fdhila, Walid in Kirchmayr-Schliesselberger/Klas Miernicki/Rinderle-Ma/Weilinger: Kryptowährungen (2019), S. 51.

6. Einstufung von Krypto-Assets

Fragen:

24. Wann gilt ein Krypto-Asset als Wertpapier?
25. Sind Krypto-Assets E-Geld, Zahlungsinstrumente, Zahlungsmittel oder Alternativer Investmentfonds?
26. Fallen Krypto-Assets in den Anwendungsbereich der PRIIP-VO?

Krypto-Assets können je nach ihrer Ausgestaltung unterschiedlich eingeordnet werden. Die Komplexität der Krypto-Assets macht pauschale aufsichtsrechtliche Zuordnungen unmöglich. Deshalb empfiehlt es sich - noch vor der Verwirklichung eines Geschäftsmodells - die [FinTech](#) Kontaktstelle der FMA zu konsultieren.

Sowohl die FMA als auch andere europäische Aufsichtsbehörden wie die deutsche Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und die Eidgenössische Finanzmarktaufsicht (FINMA) klassifizieren Token in folgende Kategorien:

- Security/Investment Token, die "Ansprüche auf Auszahlungen" gegenüber dem Emittenten begründen;
- Payment/Currency Token, dessen primärer Zweck in dessen Bezahlungsfunktion liegt;
- Utility Token, die dem Inhaber einen Nutzen im Hinblick auf ein bestimmtes Produkt oder eine Dienstleistung verschaffen; sowie
- Mischformen (hybride Token).

In der Folge werden einige mögliche Zuordnungen zu bestehenden Rechtskonzepten aufgezählt. Ein Krypto-Asset kann uU auch gleichzeitig mehreren Rechtskonzepten zugeordnet werden. Die aufsichtsrechtliche Einstufung von Krypto-Assets ist immer einzelfallbezogen. Entscheidend ist stets, welche Rechte oder Rechtspositionen mit dem Krypto-Asset verbunden sind. Nach dem Prinzip *falsa demonstratio non nocet* ist es für die rechtliche Einordnung nicht maßgeblich, wie bspw der Emittent ein Krypto-Asset bezeichnet oder einstuft - ausschlaggebend ist stattdessen die tatsächliche technische und wirtschaftliche Ausgestaltung der Krypto-Assets.⁴²

6.1...als übertragbares Wertpapier

Bei der Einstufung eines Krypto-Assets als übertragbares Wertpapier im Sinn der MiFID II kommt es auf die Kategorisierung des Tokens an, idR kommen sogenannte Security-Token als übertragbare Wertpapiere in Betracht. Dabei ist unerheblich, ob diese Krypto-Assets den österreichischen Wertpapierbegriff erfüllen.

Folgende Tatbestandsmerkmale werden dabei in der Literatur als maßgebend betrachtet:

- Verkörperung eines Rechts
- Fungibilität und Standardisierung
- Übertragbarkeit
- Handelbarkeit am Kapitalmarkt
- Fehlen einer Ausnahme vom Wertpapierbegriff als Zahlungsmittel
- Vergleichbarkeit mit anderen am Kapitalmarkt handelbaren Gattungen von Wertpapieren.

Sind die mit dem Token verknüpften Rechte vergleichbar mit jenen Rechten, die man üblicherweise mit Wertpapieren, etwa Aktien oder Anleihen verbindet, handelt es sich um ein übertragbares Wertpapier iSd MiFID II. Eine Anwendung der MiCA ist in diesem Fall

⁴² Vgl. Tuder/Ahari in Artmann/Bieber/Mayrhofer/Schmidt/Tumpel (Hrsg), *Crypto Assets*, S 129 f; Pekler/Rirsch in Kirchmayr-Schliesselberger u. a., *Kryptowährungen* (2019), S 339.

ausgeschlossen, da die MiCA explizit nur auf jene Krypto-Assets anwendbar ist, die nicht der MiFID II unterliegen.⁴³

Eine abschließende Einstufung kann nur im Einzelfall erfolgen.

6.2....als E-Geld, Zahlungsinstrument oder Zahlungsmittel

Bei der Einstufung als E-Geld, Zahlungsinstrument oder Zahlungsmittel steht der Einsatz als Zahlungsmittel im Rahmen eines Systems im Vordergrund, bei dem eine oder mehrere Stellen sich dazu verpflichten, die ausgegebenen Token gegen einen bestimmten und festen Kurs anzukaufen. Da es immer einen Abnehmer zu diesem festen Kurs gibt, kann der Token - nach der Idee - wie früher etwa ein Wechsel oder Scheck, als ein Zahlungsmittel verwendet werden. Eine abschließende Einstufung kann nur im Einzelfall erfolgen.

6.3....als Packaged Retail and Insurance based Investment Product (PRIIP)

Welche Veranlagungen im Allgemeinen oder Krypto-Assets unter die PRIIP-VO fallen, ist stets am konkreten Produkt zu beurteilen. Für den Anwendungsbereich sei es nämlich unerheblich, dass und ob das Krypto-Asset als Finanzinstrument nach MiFID II bzw WAG 2018 einzustufen ist oder nicht. Jedenfalls müssten im Falle der Anwendung ein Mindeststandard für vorvertragliche Kundeninformation eingehalten werden (Bereitstellung des Kundeninformationsdokuments - KID).⁴⁴

6.4.... als Alternativer Investmentfonds Manager

Unter einem Alternativen Investmentfonds (AIF) versteht man einen Organismus für gemeinsame Anlagen, der von einer Vielzahl von Anlegern Kapital einsammelt, um es gemäß einer festgelegten Anlagestrategie zum Nutzen der Anleger zu investieren.

Ein Alternativer Investmentfonds Manager liegt nur dann vor, wenn das eingesammelte Kapital nicht unmittelbar einer operativen Tätigkeit dient. Wenn den Token-Inhabern laufende Kontroll- und Ermessensbefugnisse hinsichtlich des Vermögens eingeräumt werden, ist der Anwendungsbereich des AIFMG nicht eröffnet.

Die Emission von Krypto-Assets im Rahmen eines ICO bzw ITO kann unter den Anwendungsbereich des Alternative Investmentfonds Manager-Gesetz (AIFMG) fallen.⁴⁵ Eine abschließende Einstufung kann nur im Einzelfall erfolgen.

7. Tokenisierung

Fragen:

27. Was ist Tokenisierung?

28. Welche Vorteile hat Tokenisierung?

Allgemein versteht man unter Tokenisierung den Vorgang, für bestimmte reale Vermögenswerte ein digitales Abbild auf der Blockchain zu schaffen. Durch den Einsatz Blockchain-basierter Token ist eine digitale Abbildung nahezu aller Vermögenswerte zumindest in den Bereich des Möglichen gerückt. Häufig sind dies Wertpapiere, Zahlungsmittel, Unternehmens- oder Projektbeteiligungen, Darlehen, Edelmetalle oder auch Anteile an Immobilien. Die Tokenisierung erfüllt dabei in der Regel zwei verschiedene Funktionen:

1. Entfall der Notwendigkeit für bestimmte Intermediäre zur Einsparung von Kosten.

⁴³ Siehe dazu genauer unten zu Punkt 10.

⁴⁴ Ausführlich dazu *Rirsch, R./ Dämon, R./ Tomanek, S.*: PRIIP-VO - Der vergessene Anwendungsbereich, in ÖBA 1/20, S 37-45.

⁴⁵ <https://www.fma.gv.at/kontaktstelle-fintech-sandbox/fintechnavigator/initial-coin-offering/>

2. Illiquide Vermögenswerte können einfach handelbar gemacht werden.

Die erste Funktion der Tokenisierung betrifft die Reduzierung notwendiger Intermediäre. Dies ist vor allem bei der Ausgabe von tokenisierten Wertpapieren ein wesentlicher Aspekt. Anders als bei klassischen Emissionen am Kapitalmarkt sind weder eine Zahlstellenbank, noch eine Hinterlegungsstelle oder sonstige Intermediäre erforderlich. Das geldsuchende Unternehmen emittiert die tokenisierten Wertpapiere (oder auch "Werttoken") direkt an den kapitalgebenden Investor. Dieser hält Werttoken selbst in seiner eigenen Wallet.

Die zweite Funktion der Tokenisierung betrifft die Möglichkeit, illiquide Vermögenswerte liquid zu machen, folglich für den einfachen und raschen Handel vorzubereiten. Diese Funktion wird besonders evident bei schwierig zu handelnden Vermögensgütern, wie beispielsweise Edelmetalle (physischer Goldbarren) oder Anteile an einem Zinshaus.

Die Grenzen der Tokenisierung werden im Wesentlichen von wirtschaftlichen, steuerlichen und bilanziellen Überlegungen vorgegeben. Daher ist bei einem Tokenisierungsprojekt die Einbindung qualifizierter Berater dringend empfohlen, um nachteilige Auswirkungen zu vermeiden und eine rechtskonforme, vorteilhafte Struktur zu finden.

7.1. Schritte zur Tokenisierung

Fragen:

29. Wie funktioniert Tokenisierung?

30. Wie verknüpfe ich einen realen Vermögenswert mit einem Token?

Die Tokenisierung erfolgt in der Regel in zwei Schritten: Erzeugen des technischen Abbilds auf der Blockchain und Verknüpfung des realen Vermögenswerts mit dem digitalen Abbild.

In einem ersten Schritt wird in technischer Hinsicht das digitale Abbild des Vermögenswerts erzeugt: Auf einer beliebigen Blockchain wird ein Smart Contract⁴⁶ veröffentlicht, der die gewünschte Anzahl an Token herstellt und verwaltet. In der Praxis kommt dafür am häufigsten die Ethereum-Blockchain zum Einsatz. Die auf diese Weise selbstgeschaffenen Token sollen später den gewünschten Vermögenswert digital repräsentieren. Aus technischer Sicht entstehen Token auf zwei Arten: Entweder durch Mining oder durch Minting.

In einem zweiten Schritt ist diese digitale Abbildung mit dem realen Vermögenswert zu verknüpfen. Im Ergebnis soll der Inhaber eines Tokens so gestellt werden, dass er einen in der realen Welt durchsetzbaren Anspruch auf den tokenisierten Vermögenswert hat. Der rechtliche Schutz des Tokeninhabers muss bei der Strukturierung des Vorhabens oberste Priorität haben, möchte man aus dem gegenwärtigen Trend zur Tokenisierung auch einer langfristigen und nachhaltigen Entwicklung den Weg ebnen.

Die rechtlich abgesicherte Verknüpfung von Token und realem Vermögenswert ist der Kern der Tokenisierung. Die Umsetzung hängt vom Vermögenswert ab und nach welcher Rechtsordnung tokenisiert wird.

7.2. Modelle zur Tokenisierung

Fragen:

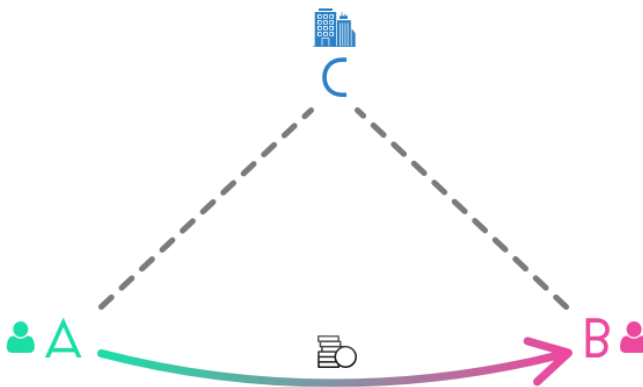
31. Welche Instrumente und Rechtskonzepte können für Tokenisierung eingesetzt werden?

⁴⁶ Smart Contracts sind Quellcodes, in denen Bedingungen für die Ausführung bestimmter Aktivitäten nach einfachem Logikmuster festgelegt werden (Wenn A erfüllt ist, soll B erfüllt werden). Die Ausführung eines Vertrags erfolgt durch den Einsatz von Smart Contracts automatisiert und machen zwischengeschaltete, zentrale Vertrauenspersonen obsolet.

Für die Tokenisierung können mehrere Modelle verwendet werden.

Unmittelbare Verknüpfung von Recht und Token

Handelt es sich um ein Forderungsrecht, wie dies etwa bei Wertpapieren, Zahlungsmitteln oder Darlehen der Fall ist, so kann in der Regel das Forderungsrecht mit dem Token unmittelbar verknüpft werden. Für die Ausübung des Rechts ist sodann die Inhaberschaft des Tokens notwendig. Zur Übertragung des Forderungsrechts wird der Token auf der Blockchain an eine andere Person übertragen. Wer den Token besitzt, der ist Gläubiger der Wertpapier-, Zahlungs-, oder Darlehensforderung. Erreicht wird dies durch entsprechende Klauseln in der vertraglichen Vereinbarung zwischen den Parteien.

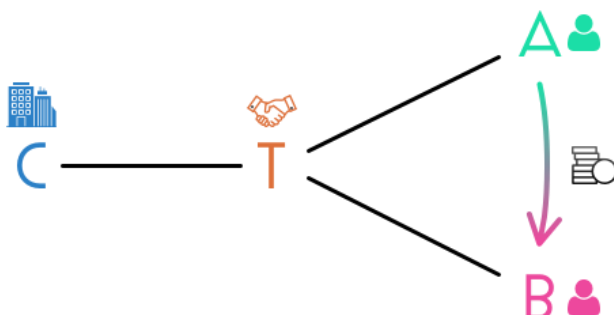


Modell 1: Direkte Übertragung eines Forderungsrechts durch Übertragung eines Tokens auf der Blockchain, der das Recht repräsentiert (C: Unternehmen, A: Bisheriger Gläubiger des Unternehmens, B: Neuer Gläubiger nach Besitzanweisung oder Forderungszession durch Übertragung des Tokens).

Zwischenschaltung eines Treuhänders

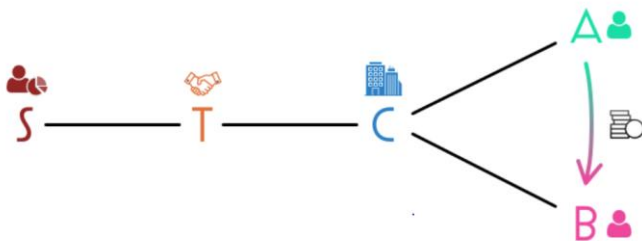
Sollen nicht nur einfache Forderungsrechte tokenisiert werden, sondern eine Eigentümerposition, oder ist für die Übertragung des Rechts eine bestimmte Form vorgeschrieben (zB schriftlicher Vertrag), kann Tokenisierung durch Zwischenschaltung eines Treuhänders erfolgen. Zu denken ist an die Tokenisierung greifbarer Gegenstände wie etwa Warenbestände, Edelmetalle, Anteile an Immobilien oder auch Beteiligungen an Unternehmen.

Je nach Erfordernis gibt es auch hier zwei unterschiedliche Varianten. In der ersten Variante (Modell 2.A) vermittelt ein Treuhänder (T) direkt die Eigentümerposition. Der Treuhänder besitzt zB physische Goldbarren für die Tokeninhaber (A und B). Im Zusammenhang mit einem Beispiel zur Tokenisierung von Realgütern wie Edelmetallen oder Zinshausanteilen gehen wir weiter unten näher auf diese Konstruktion ein.



Modell 2.A: Treuhandkonstruktion, bei der das tokenisierte Eigentumsrecht von einem Treuhänder für die Tokeninhaber ausgeübt wird (C: Unternehmen, T: Treuhänder, A: Bisheriger Eigentümer, B: Neuer Eigentümer nach Besitzanweisung durch Übertragung des Tokens).

In der zweiten Variante (Modell 2.B) stellt der Treuhänder (T) lediglich indirekt sicher, dass das Unternehmen (U) ein bestimmtes Versprechen auch tatsächlich einhalten kann. Diese Variante ist gerade bei der Tokenisierung von Verwendungszusagen relevant (mehr dazu weiter unten). In der Regel ist für die Einhaltung dieses Versprechens nämlich die Mitwirkung der Eigentümer (S) notwendig. In solchen Fällen wird der Treuhänder zum Gesellschafter des Unternehmens bestellt. Dies ist vor allem bei Gesellschaftsformen interessant, die kein genehmigtes Kapital kennen.



Modell 2.B: Treuhandkonstruktion, bei der ein Treuhand-Gesellschafter (T) sicherstellt, dass das Unternehmen (C) Versprechen in Bezug auf eigene Anteile erfüllen kann, die eigentlich von den Eigentümern (S) zu erfüllen wären. Durch Übertragung des Tokens von A an B werden diese sogenannten Verwendungszusagen übertragen.

Achtung: Nicht jede Rechtsordnung ist gleich. Während etwa das österreichische Recht gut für die vorgestellten Arten der Tokenisierung gerüstet ist, und in Liechtenstein sogar ein eigenes Gesetz zur Tokenisierung von Vermögenswerten geschaffen wurde, weicht die Rechtslage in anderen Ländern möglicherweise davon ab. In vielen Fällen kann jedoch mit einer Rechtswahlklausel österreichisches oder auch liechtensteinisches Recht zur Anwendung gebracht werden, um diese günstigen Rechtsordnungen für sich zu nutzen, auch wenn das Unternehmen nicht in Österreich oder Liechtenstein ansässig ist.

7.3. Beispiele für Tokenisierung

Fragen:

32. Welche Arten von Vermögenswerten und Rechten können tokenisiert werden?
33. Wie sieht Tokenisierung bei einer GmbH aus?
34. Wie sieht Tokenisierung bei einer AG aus?
35. Kann ich Immobilien Tokenisieren?

7.3.1. Tokenisierte Substanzgenussrechte

Substanzgenussrechte dienen der Unternehmensfinanzierung. Ein Unternehmen nimmt Kapital von Anlegern auf und verspricht dafür im Gegenzug eine Beteiligung am Gewinn und Verlust des Unternehmens sowie auch am Unternehmenswert. Ein Substanzgenussrecht kann rückzahlbar oder auch nicht-rückzahlbar ausgestaltet werden. Personen, die Substanzgenussrechte zeichnen, haben damit - ausgenommen Mitspracherechte - eine Stellung ähnlich den Gesellschaftern des Unternehmens. Ihre Position ist jenen von Kommanditisten bei einer Kommanditgesellschaft ähnlich. Die Auszahlung der Gewinnbeteiligung kann in Euro oder etwa auch in einer virtuellen Währung erfolgen, wie zB Ether. In einem solchen Fall erfolgt die Zahlung an jene Adressen auf der Ethereum-Blockchain, die sich in Besitz der Token befinden. Durch die Tokenisierung wird das Substanzgenussrecht zum übertragbaren Wertpapier im Sinne der EU-Gesetzgebung.

Aufgrund seiner Flexibilität ist das Substanzgenussrecht sehr beliebt. Es lassen sich damit sehr unterschiedliche Zwecke erreichen. Die aufgenommenen Mittel können in der Bilanz des Unternehmens, je nach Ausgestaltung, entweder im Eigenkapital oder im Fremdkapital ausgewiesen werden. Entscheidet sich das Unternehmen für die Eigenkapital-Variante, kann dies das Auftreten gegenüber anderen potentiellen Fremdkapitalgebern stärken.

7.3.2. Tokenisierte Umsatzgenussrechte

Umsatzgenussrechte sind den Substanzgenussrechten insofern ähnlich, als es sich in beiden Fällen um das Versprechen des Unternehmens auf Zahlungen handelt, die von einer bestimmten Messgröße abhängig sind. Während diese Messgröße beim Substanzgenussrecht der Gewinn oder Verlust des Unternehmens ist, bildet beim Umsatzgenussrecht eben der Umsatz den Bezugspunkt. Gewinn und Verlust können bis zu einem gewissen Grad vom Unternehmen beeinflusst werden, etwa durch das Vorziehen von Investitionen. Beim Umsatz ist das nicht der Fall, was gegenüber potentiellen Investoren hervorgehoben werden kann.

Auch das Umsatzgenussrecht kann recht flexibel ausgestaltet werden. Es kann rückzahlbar, oder nicht-rückzahlbar sein. Es können bestimmte Mindest- und Höchstschwellen der Beteiligung festgelegt werden, oder die Umsatzbeteiligung kann von anderen Faktoren abhängig gemacht werden. Durch die Tokenisierung wird das Umsatzgenussrecht zum übertragbaren Wertpapier im Sinne der EU-Gesetzgebung.

7.3.3. Tokenisierte Nachrangdarlehen

Das qualifizierte Nachrangdarlehen ist jenes Instrument, das sich im Bereich des Crowdfunding derzeit der größten Beliebtheit erfreut. Bei einem Nachrangdarlehen nimmt das Unternehmen Gelder auf, verspricht gewöhnlich eine dem Risiko angemessene Verzinsung und eine Rückzahlung am Ende einer festgelegten Laufzeit. Die qualifizierte Nachrangigkeit führt dazu, dass die Geldgeber erst nach allen anderen nicht nachrangigen Gläubigern eine Zahlung fordern dürfen. Können versprochene Zins- oder auch die Rückzahlung nicht geleistet werden, so muss wegen der qualifizierten Nachrangigkeit auch kein Insolvenzverfahren eröffnet werden. Auch das Nachrangdarlehen wird durch den Vorgang der Tokenisierung zum übertragbaren Wertpapier im Sinne der EU-Gesetzgebung.

7.3.4. Tokenisierte Verwendungszusagen

Bei der Tokenisierung von Verwendungszusagen handelt es sich um die jüngste Entwicklung tokenisierter Instrumente. Verwendungszusagen sind Versprechen eines Unternehmens, bei einem Dritten eine Leistung zu erwirken. Das Unternehmen ‚verwendet‘ sich dazu, dass ein Dritter leistet. Verwendungszusagen kommen meist dann zum Einsatz, wenn das Unternehmen ein Versprechen abgibt, das nur von einer anderen Person erfüllt werden kann. Im Zusammenhang mit der Unternehmensfinanzierung können Verwendungszusagen verschieden ausgestaltet werden. Beispiele aus der Praxis sind etwa:

- **Zusagen über eigene Geschäftsanteile:** Sofern ein Unternehmen nicht über genehmigtes Kapital verfügt, können nur die Eigentümer des Unternehmens wirksame Versprechen hinsichtlich ihrer Anteile am Unternehmen machen. Das Unternehmen selbst kann aber beispielsweise die Verwendungszusage abgeben, dass bei Eintritt bestimmter Bedingungen eine Beteiligung des Tokeninhabers am Unternehmen erfolgen wird, etwa im Wege einer Anteilsübertragung oder Kapitalerhöhung.
- **Zusagen über die Gewinnverwendung:** Ebenso wie nur den Eigentümern des Unternehmens die Anteile am Unternehmen zustehen, steht auch nur ihnen der Gewinn

zu. Das Unternehmen kann aber im Wege der Verwendungszusage das Versprechen machen, für eine bestimmte Verwendung des ausgeschütteten Gewinns durch seine Eigentümer einzustehen. Auf diese Weise kann etwa das Versprechen gegeben werden, dass Gewinne an Tokeninhaber weitergeleitet werden.

- **Gesellschaftsrechtliche Vereinbarungen:** Im Wege der Verwendungszusage kann eine Vielzahl von Vereinbarungen nachgebildet werden, die andernfalls nur zwischen Gesellschaftern des Unternehmens vereinbart werden könnten. Zu denken ist hier an Mitverkaufsrechte, Vorkaufsrechte oder Mitbestimmungsrechte. Diese Verwendungszusagen können auch mit den anderen oben vorgestellten Instrumenten kombiniert zum Einsatz kommen. So kann etwa ein tokenisiertes Substanzgenussrecht auch die Verwendungszusage enthalten, unter bestimmten Bedingungen Gesellschaftsanteile am Unternehmen zu erwerben.

Versprechen zulasten Dritter können diese Dritten selbstverständlich nicht wirksam verpflichten. Dafür ist stets auch die Zustimmung der verpflichteten Person erforderlich. Um dem Versprechen des Unternehmens Gewicht zu geben, muss es also dafür sorgen, dass der Dritte auch wirklich das Versprochene leistet, und zwar auch dann, wenn dieser Dritte das vielleicht nicht möchte. In den oben dargestellten Beispielen muss also die Verpflichtung des Unternehmens auf dessen Eigentümer überbunden werden.

In der Praxis geschieht dies auf zwei verschiedene Arten. Entweder die Satzung des Unternehmens wird um entsprechende Klauseln angepasst, die sicherstellen, dass die Eigentümer des Unternehmens diese vom Unternehmen gemachten Versprechen erfüllen müssen. Oder ein Treuhänder übernimmt die Gesellschaftsanteile und stellt auf diese Weise sicher, dass nach entsprechender Aufforderung durch das Unternehmen die gegebenen Versprechen erfüllt werden (siehe dazu oben das Modell 2.B bei der Tokenisierung).

7.3.5. Tokenisierung bei der Gesellschaft mit beschränkter Haftung

Geschäftsanteile an Gesellschaften mit beschränkter Haftung wurden (zumindest in Österreich und Deutschland) mit Absicht „immobilisiert“. Um Anteile an einer GmbH zu übertragen, muss ein Abtretungsvertrag in Form eines Notariatsakts abgeschlossen werden. Auch das bloße Angebot auf Übertragung muss bereits in Form eines Notariatsakts erfolgen, um wirksam zu sein. Wird diese Formvorschrift nicht eingehalten, so ist das Angebot oder die Übertragung absolut nichtig.

Wegen dieser Formvorschriften kann der Geschäftsanteil an einer GmbH nicht unmittelbar tokenisiert werden. Allerdings kann das oben vorgestellte Instrument der Verwendungszusage herangezogen werden. Eine Übertragungszusage, gemeinsam mit der Zusage der Gewinnverwendung und allenfalls Zusage von Mitspracherechten kann wirksam tokenisiert werden. Diese Versprechen können formfrei übertragen werden. Die Einhaltung der Zusagen kann mit dem Treuhandmodell B durch das Unternehmen selbst sichergestellt werden. Auf diese Weise kann das Unternehmen Versprechen hinsichtlich seiner eigenen Anteile wirksam abgeben, und zwar auch dann, wenn es nicht über bereits genehmigtes Kapital verfügt (wie dies etwa bei Aktiengesellschaften der Fall sein kann).

Diese Formvorschriften bestehen nicht für die Begründung der Übertragungspflicht des Treuhänders an den Treugeber aus einer Treuhandschaft. Die Treuhandvereinbarung kann daher nach hM nur schriftlich abgeschlossen werden.

7.3.6. Tokenisierung bei der Aktiengesellschaft

In Österreich ist bei nicht börsennotierten Aktiengesellschaften nur noch die Ausgabe von Namensaktien zulässig. Die Namen der Aktionäre sind im sogenannten Aktienbuch einzutragen. Durch die Tokenisierung wird das Aktienbuch auf die Blockchain gebracht. Übertragungen von Aktien erfolgen durch die Verständigung der Gesellschaft, die die Übertragung im Aktienbuch auf der Blockchain verzeichnet.

Bei börsennotierten Aktiengesellschaften kann auch die Ausgabe von Inhaberaktien erfolgen. In diesem Fall ist aber eine Verbriefung der Aktien ausschließlich in Form einer oder mehrerer Sammelurkunde(n) zulässig. Diese Sammelurkunde muss bei einer Wertpapiersammelbank bzw. einem Zentralverwahrer hinterlegt werden. Um die Tokenisierung von Inhaberaktien zu ermöglichen ist also (zumindest in Österreich) noch der Gesetzgeber am Zug. Allerdings könnte auch eine Aktiengesellschaft tokenisierte Verwendungszusagen im Hinblick auf eigenes genehmigtes Kapital begeben. Dies wäre vergleichbar mit dem oben vorgestellten Modell der Tokenisierung von Verwendungszusagen in Bezug auf GmbH-Anteile, allerdings könnte in diesem Fall (sofern genehmigtes Kapital vorhanden ist) auf die Bestellung eines Treuhänders verzichtet werden.

7.3.7. Tokenisierung von Realgütern wie etwa Edelmetallen oder Zinshausanteilen

Nicht nur Versprechen (Forderungen) oder Gesamtsachen wie Unternehmen können der Tokenisierung zugänglich sein. Insbesondere das Interesse an der Tokenisierung von Realgütern wie beispielsweise Edelmetallen, Edelsteinen oder auch Anteilen an Zinshäusern wächst in jüngster Zeit zunehmend. Nicht der Finanzierungsgedanke steht dabei im Vordergrund, sondern der Wunsch, diese relativ illiquiden Mittel zu leicht handelbaren Gütern zu verwandeln.

Die Verknüpfung der realen Welt mit dem tokenisierten Abbild gelingt in der Regel mit der Treuhandvariante A. Ein Treuhänder wird dazu bestellt, die tokenisierten Realgüter in Verwahrung zu nehmen. Der Treuhänder steht zunächst dafür ein, dass die tokenisierten Güter tatsächlich existieren. Das weitere Verhältnis zwischen Treuhänder und Tokeninhaber kann unterschiedlich ausgestaltet werden. So kann der Treuhänder als Besitzmittler echte (Mit-)Eigentumspositionen für den jeweiligen Tokeninhaber vermitteln, wie dies am klassischen Kapitalmarkt, etwa bei Wertpapierdepots, der Fall ist. Es kann aber auch gegenüber dem Treuhänder lediglich ein schuldrechtlicher Ausfolgeanspruch eingeräumt werden. Welcher Variante der Vorzug gegeben wird, hängt von den Umständen des Einzelfalls ab.

7.3.8. Tokenisierung von Gutscheinanprüchen

Nicht unerwähnt bleiben soll das sogenannte Gutscheinmodell. Dieses hat sich im Zuge der ICO-Welle 2017 erstmals als taugliches Instrument etabliert. Und obwohl der ICO-Boom längst vorüber ist, hat das Gutscheinmodell in bestimmten Bereichen weiterhin seine Berechtigung. Bei diesem Instrument verspricht das Unternehmen, einen Token in der Zukunft gegen eine bestimmte Leistung einzutauschen. Die eingenommenen Mittel dienen der Unternehmensfinanzierung. Je nachdem wie der Gutschein ausgestaltet ist, können damit bilanzielle und steuerliche Folgen gesteuert werden. Die Gutschein-Eigenschaft kann mit den anderen oben vorgestellten Instrumenten verknüpft werden, sodass ein Token gleichzeitig Aspekte etwa eines Substanzgenussrechts, einer Verwendungszusage und eines Gutscheins aufweisen kann.

7.4. Rechtliche, steuerliche und bilanzielle Strukturierung

Die oben vorgestellten Arten der Tokenisierung können je nach konkreter Ausgestaltung sehr unterschiedliche steuerliche Auswirkungen und auch Auswirkungen auf die bilanzielle Situation des Unternehmens haben. Diese Auswirkungen können gezielt für das Unternehmen genutzt werden. Sollen etwa Verlustvorträge verwerten, kann ein Instrument gewählt werden, das zu einem Ertrag im Unternehmen führt. Soll die Eigenkapitalausstattung ohne ertragsteuerliche

Belastung gestärkt werden, kann dies etwa mit tokenisierten Substanzgenussrechten realisiert werden. Die mögliche Steuerbelastung mit Umsatz- und Körperschaftsteuern muss gerade bei nicht rückzahlbaren Instrumenten stets genau im Auge behalten werden. Um nicht unerwartet eine Steuerpflicht auszulösen, empfehlen wir daher frühzeitig einen Steuerberater oder Wirtschaftsprüfer in die Strukturierung einzubinden.

Abhängig von den vorgenannten steuerlichen und bilanziellen Überlegungen wird das tokenisierte Instrument strukturiert. Hierzu werden entweder die entsprechenden Werttokenbedingungen erarbeitet oder es werden andere notwendig Verträge aufgesetzt. Ist es erforderlich, kommt es zu Anpassungen der Satzung der Gesellschaft. Nötigenfalls wird eine Treuhandenschaft eingerichtet.

7.5. Öffentliches Angebot von Werttoken

Die Erarbeitung der notwendigen Verträge und allenfalls die Anpassung der Satzung sind in der Regel allerdings bloß der erste Schritt. Der zweite Schritt ist in vielen Fällen der Verkauf der tokenisierten Vermögenswerte in einem öffentlichen Angebot. Dabei bietet das geldsuchende Unternehmen die tokenisierten Wertpapiere oder Veranlagungen der breiten Öffentlichkeit zur Zeichnung an.

Zu diesem Zweck legt das Unternehmen in der Regel eine eigene Landingpage für die Abwicklung der Emission auf seiner Website an. Die Landingpage soll zunächst sicherstellen, dass nur Personen Einsicht in das Angebot erhalten, an die es sich richtet. Interessierte Investoren bestätigen dabei zum Beispiel, dass sie aus der EU stammen. Darüber hinaus dient die Landingpage vor allem der Information der Investoren. Sie enthält jene Dokumente und Unterlagen, die von Gesetzes wegen interessierten Investoren zu geben sind. Zuletzt kann die Landingpage dazu dienen, den Zeichnungsprozess abzubilden: Interessierte Investoren zeichnen in diesem Fall die Werttoken direkt beim Emittenten.

Welche Dokumente und Informationen auf der Landingpage aufzunehmen sind, hängt im Wesentlichen von der Mindestzeichnungssumme pro Anleger und von der Gesamtmenge der Mittel ab, die das Unternehmen aufnehmen möchte. Liegt die Mindestzeichnungssumme pro Anleger bei zumindest EUR 100.000, so sind in der Regel neben den Werttokenbedingungen und einem Zeichnungsschein keine weiteren Informationen notwendig.

Liegt die Mindestzeichnungssumme pro Anleger hingegen bei unter EUR 100.000, soll also beispielsweise eine Zeichnung schon um wenige hundert Euro möglich sein, so sind in der Regel mehr Informationen auf der Landingpage zu geben. Was genau erforderlich ist, richtet sich dabei nach dem Gesamtvolumen:

Volumen < EUR 250.000	Volumen < EUR 5 Millionen	Volumen >= EUR 5 Millionen
Bei Kleinstplatzierungen ist eine allgemeine Risikoaufklärung mit den Eckpunkten des Instruments ausreichend	Bei kleineren Platzierungen kann mit einem Informationsblatt das Auslangen gefunden werden.	Bei größeren Platzierungen ist ein Kapitalmarktprospekt nach der EU-Prospekt Verordnung zu erstellen und von einem Regulator innerhalb des EWR (FMA, BaFin, CSSF, etc) zu billigen.

Hinweis: Die Erstellung eines Kapitalmarktprospekts ist aufwändig. Unternehmen sollten eine Vorlaufzeit von zumindest drei Monaten einplanen. Der Vorteil liegt darin, ein Angebot in mehreren Ländern des EWR vorzunehmen, ohne sich um das nationale Recht kümmern zu müssen. Wird hingegen kein Kapitalmarktprospekt erstellt und soll das Angebot in mehreren Ländern erfolgen, sind die jeweiligen nationalstaatlichen Vorschriften zu beachten.

8. Zugang: Konzession oder Gewerbe?

8.1. Beratung und Vertrieb von Krypto-Assets

Die „Beratung“ sowie die „Annahme und Übermittlung“ (Vermittlung) von Krypto-Assets kann - abhängig von der Ausgestaltung des Vermögenswerts - eine Registrierung oder Konzession bei der FMA oder eine Gewerbeberechtigung notwendig machen. Das ist im Einzelfall von der zuständigen Aufsichtsbehörde (FMA bzw. Gewerbebehörde) zu beurteilen. Aufgrund der vielen neuen Produkte auf Basis dieser Technologie und der mangelnden Regulierung sind pauschale Aussagen nicht möglich.

Hinweis: Die FMA hat die Kontaktstelle [FinTech](#) eingerichtet, wo Sie Antworten auf Ihre Fragen zu Konzessionspflicht, Prospektpflicht, Compliance oder Geldwäschevorschriften, Ablauf von FMA-Verfahren und Kosten erhalten.

Beim [FinTech-Navigator](#) finden Sie weiterführende Informationen, wie zB auch zu virtuellen Währungen.

Die Gewerbeberechtigung Gewerbliche Vermögensberatung erlaubt die „Beratung“ und die „Annahme und Übermittlung“ von Investitionen und Veranlagungen. Bei Beratungs- und Vermittlungsdienstleistungen im Zusammenhang mit Krypto-Assets ist jedoch besondere Vorsicht geboten. Unterliegt der Vermögenswert beispielsweise einer Konzessionspflicht, ist sie nicht vom Gewerbeumfang - und damit auch nicht von der Vermögensschadenhaftpflichtversicherung - gedeckt.

Achtung: Ein Gewerblicher Vermögensberater hat entsprechende Sorgfaltsmaßnahmen zu beachten, wenn er über Investitionen/Veranlagungen berät und diese vermittelt, auch wenn er diese über Krypto-Assets durchführt.

Aufgrund der vorhandenen Fachkompetenz werden Gewerbliche Vermögensberater von Gerichten voraussichtlich als **Sachverständige** eingestuft und im Schadensfall vermutlich allein vor Gericht zur Rechenschaft gezogen. Bei einem vertraglich gebundenen Vermittler oder Wertpapiervermittler ist die Vermittlung von Krypto-Assets grundsätzlich nicht dem Haftungsdach zuzurechnen. Im Ergebnis besteht daher direkte Klagemöglichkeit gegenüber dem Vermittler.

Wichtig: Es wird ausdrücklich darauf hingewiesen, dass es sich um eine neue Tätigkeitsform handelt und die Vermögensschadenhaftpflichtversicherung eventuell ohne Zutun nicht automatisch das neue Geschäftsfeld deckt. Es wird daher empfohlen, sich bei der Vermögensschadenhaftpflichtversicherung zu erkundigen, ob die Anpassung des Vertrages notwendig ist, wenn die Beratung oder Vermittlung von Krypto-Assets angeboten wird.

Für den Fall, dass der Tatbestand der gewerblichen Vermögensberatung betreffend das Krypto Asset zutrifft, ist auch bei Vertriebskonzepten besondere Vorsicht geboten. Beim Einsatz von Direktberatern sollte daher das Vorliegen einer entsprechenden Gewerbeberechtigung überprüft werden. Für den Fall, dass beim Vertrieb von Krypto-Assets Personen ohne die entsprechende Gewerbeberechtigung eingesetzt werden, besteht die Gefahr der Verwirklichung des Straftatbestandes der organisierten Schwarzarbeit (§ 153e StGB). Zusätzlich droht eine Verwaltungsstrafe nach der Gewerbeordnung.

Weiters ist Vorsicht bei mehrstufigen Multi-Level-Marketing Vertriebskonzepten betreffend Krypto Assets geboten. Mehrstufige Multi-Level-Marketing Systeme sind nicht per se verboten. Dennoch bestehen in der Judikatur Ansätze, die bei einer Weiterempfehlung von mehr als einem Kunden eine unlautere Geschäftspraktik bei bestimmten Umständen bejahen. Es besteht das Risiko gegen das Gesetz zur Verhinderung des Unlauteren Wettbewerbs (UWG) zu verstoßen.

Weiter besteht die Gefahr eventuell je nach den konkreten Umständen den Straftatbestand der Ketten- oder Pyramidenspiele oder eines Schneeballsystems zu verwirklichen.

Wichtig: Es wird ausdrücklich darauf hingewiesen, dass mehrstufige Multi-Level-Marketing Vertriebskonzepte problematisch sein können. Vor Umsetzung eines derartigen Systems sollte dieses dringend auf rechtskonforme Umsetzungsmöglichkeit geprüft werden.

8.2. Mining

Ob das Mining allein einer **Gewerbeberechtigung** unterliegt, ist **strittig**. Werden aber Softwareanwendungen für Dritte programmiert oder Rechenzentrumsdienstleistungen angeboten, die Dritten in Bezug auf Blockchainanwendungen dienen, kann dies jedenfalls im Rahmen des Berufsbilds für das freie Gewerbe „Dienstleistungen der automatischen Datenverarbeitung und Informationstechnik (IT Gewerbe)“ angeboten werden.

Für die Beurteilung einer etwaigen **Konzessionspflicht** kann Folgendes ausgeführt werden: Grundsätzlich ist das reine Minen von Bitcoin im eigenen Namen und auf eigene Rechnung durch eine natürliche Person nicht konzessionspflichtig.

Die FMA macht jedoch darauf aufmerksam, dass Geschäftsmodelle, die eine Beteiligung am Mining von Krypto-Assets wie Bitcoin vorsehen, abhängig von der konkreten Ausgestaltung im Einzelfall, eine konzessionspflichtige Tätigkeit darstellen können. Insbesondere können Geschäftsmodelle im Zusammenhang mit Mining von Kryptowährungen, sofern sie im Übrigen alle Kriterien eines AIF erfüllen, vom Anwendungsbereich des AIFMG erfasst sein (FAQ 2022 zur Anwendung des AIFMG).⁴⁷

Zur steuerlichen Beurteilung verweisen wir auf unseren Artikel zur [Besteuerung von Kapitalvermögen im Privatvermögen](#).

8.3. Handel mit Krypto-Assets

Der Handel mit Krypto-Assets kann der GewO unterliegen, wenn diese nicht als Zahlungsmittel iSd BWG bzw. Zahlungsinstrumente iSd ZaDiG 2018 oder Finanzinstrumente iSd WAG 2018 ausgestaltet sind.⁴⁸ Es kommt auf die Funktion bzw den Token an, wie die folgende Übersicht aufzeigt:

Tokenart	Funktion	GewO	Finanzinstrument iSd WAG 2018	Zahlungsmittel bzw. -instrument iSd BWG/ ZaDiG
Investment-, Asset- oder Security Token	Investmentfunktion	eher nein	eher ja	nein
Payment Token	Zahlungs- und Wertaufbewahrungsfunktion	möglich	nein	eher ja
Utility Token	verschiedene Funktionen	möglich	beides möglich	beides möglich
hybride Token	verschiedene Komponenten	eher nein	eher ja	eher ja

⁴⁷ <https://www.fma.gv.at/querschnittsthemen/fintechnavigator/bitcoin-co/>

⁴⁸ Siehe auch Ansicht von *Bernsteiner, Ch.:* Kryptowährungen und Gewerbeberecht.

Aktuell gilt daher: Konzession oder Gewerbe möglich.

8.4. Betreiben einer Online-Börse für Krypto-Assets („Krypto-Börse“)

Für die Frage, ob eine Konzession oder eine Gewerbeberechtigung notwendig ist, hängt es davon ab, welche Krypto-Assets auf der Online-Börse gehandelt werden. Unabhängig davon besteht jedenfalls eine Registrierpflicht gemäß FM-GwG (siehe unten).

Aktuell daher: Registrierpflicht gemäß FM-GwG. Zusätzlich Konzession oder Gewerbe möglich.

8.5. Betreiben eines Krypto-Asset-Geldautomaten („Elektronische Wechselstube“)

Es besteht eine Registrierpflicht gemäß FM-GwG für den Betrieb von Krypto-Asset Geldautomaten (siehe unten).

Nach steuerrechtlicher Ansicht des BMF, ist *„das Betreiben eines Krypto-Asset-Geldautomaten, bei dem man mit Bargeld Krypto-Assets beziehen kann, grundsätzlich als eine gewerbliche Tätigkeit anzusehen, die entsprechende steuerliche Konsequenzen nach sich zieht“*.

Aktuell daher: Registrierpflicht gemäß FM-GwG.

9. Vorteile und Risiken von Krypto-Assets bzw Blockchain-Technologie

Fragen:

36. Welche Vorteile bietet mir eine Investition in Krypto-Assets?

37. Mit welchen Risiken ist bei Investition in Krypto-Assets zu rechnen?

Die Vorteile:

- **Kein Double-Spending** möglich: Der Vorteil zB bei Bitcoin ist, dass das sogenannte Double-Spending-Problem nicht besteht. Dabei handelt es sich um die Frage, wie verhindert werden kann, dass ein und dasselbe Geld zweimal ausgegeben wird. Dies ist bei Überweisungen von Bitcoins technisch nicht möglich. Eine Überweisung kann nur an einen Empfänger ergehen und dies auch nur dann, wenn die Verfügbarkeit besteht.
- **Kein Kredit bzw keine Verschuldungsmöglichkeit:** Da nur so viel überwiesen werden kann, wie auch tatsächlich in der Kryptowährung verfügbar ist, kommt es zu keiner Verschuldung oder Möglichkeit eines sogenannten Überziehungsrahmens.
- **Transparenz, da Pseudonymität:** Jede Transaktion wird in der Blockchain pseudonymisiert. Das bedeutet, dass die entsprechende IP-Adresse des Nutzers mit einem Pseudonym verschleiert wird, welches aus alphanummerischen Zeichen besteht. Bei Bitcoin bedeutet dies, dass jede Zahlung auf eine Bitcoin-Adresse rückführbar und auch von jedem Nutzer einsehbar ist.
- **Unveränderlichkeit, Unstoppbarkeit und Unwiderruflichkeit:** Das Ziel der Abwicklung einer Transaktion über eine Blockchain-Technologie ist an sich die Unveränderlichkeit, Unstoppbarkeit und Unwiderruflichkeit, sodass keine Auseinandersetzungen gegeben sind.

Die Nachteile:

- **Keine Umkehrbarkeit der Zahlung:** Wenn jemand irrtümlich eine Transaktion erhalten hat, dann kann ein Rücküberweisung nur freiwillig erfolgen. Problem dahinter ist jedoch, dass wenn nur die Bitcoin-Adresse bekannt ist, eine Kontaktaufnahme schwierig ist.
- **Weitere zB bei Bitcoins:** hohe Rechenleistung erforderlich, hoher Stromverbrauch.

Risiken, welche im Zusammenhang mit Kryptowährungen gegeben sind:

- **Verlustrisiko:** Auch Kryptowährungen können wie Bargeld „gestohlen“ oder verloren gehen, indem zB die privaten Schlüssel oder notwendigen (Computer-)Adressen entwendet werden.
- **Kostenrisiko:** Kosten für Transaktionen können steigen.
- **Wertschwankungsrisiko:** Der Wert ergibt sich aus Angebot und Nachfrage, sodass es zu Kursschwankungen und Blasen kommen kann.
- **Technische Risiken:** Hackerangriffe, Manipulationen.
- **Geldwäscherisiko:** Auf Grund von Pseudonymitäten („Teilanonymität“) kann es zu illegalen Handlungen und Missbrauch kommen.

10. Geldwäscheprävention und Registrierungspflicht von Dienstleister virtueller Währungen

Fragen:

38. Wo wird die „virtuelle Währung“ definiert?
39. Wer zählt zu den „Dienstleistern in Bezug auf virtuelle Währungen“?
40. Wen trifft die FMA-Registrierungspflicht und wie hat eine solche zu erfolgen?

Mit Umsetzung der 5. Geldwäsche-Richtlinie im Finanzmarkt-Geldwäschegesetz (FM-GwG) wird erstmalig eine Definition der „virtuellen Währung“ erfasst.

„Virtuelle Währung: eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist und die nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann.“

Zudem werden Dienstleister in Bezug auf virtuelle Währungen definiert⁴⁹, dazu gehören im Wesentlichen:

- „Wallet-Provider“ (oder Verwahrungsdienstleister oder Anbieter von elektronischen Geldbörsen): Dienste zur Sicherung privater kryptografischer Schlüssel, um virtuelle Währungen im Namen eines Kunden zu halten, zu speichern und zu übertragen
- „Umtausch-Plattformen“ (elektronische Wechselstuben): den Tausch von virtuellen Währungen in Bargeld (Fiatgeld) und umgekehrt;
- „Handelsplattformen“: Tausch einer oder mehrerer virtueller Währungen untereinander;
- die Übertragung von virtuellen Währungen;
- die Zurverfügungstellung von Finanzdienstleistungen für die Ausgabe und den Verkauf von virtuellen Währungen.

⁴⁹ § 2 Z 22 FM-GwG: Dienstleister in Bezug auf virtuelle Währungen.

Dienstleister in Bezug auf virtuelle Währungen unterliegen seit 10.1.2020 einer gebührenpflichtigen Registrierungspflicht.⁵⁰ Wenn ein Dienstleister in Bezug auf virtuelle Währungen beabsichtigt, im Inland seine Tätigkeit zu erbringen oder vom Inland aus seine Tätigkeiten anzubieten, hat er zuvor bei der FMA eine Registrierung zu beantragen. Dem Antrag sind folgende Angaben und Unterlagen anzuschließen:

- der Name oder die Firma des Dienstleisters und sofern vorhanden der oder die Geschäftsleiter;
- der Sitz des Unternehmens und die für Zustellungen maßgebliche Geschäftsanschrift;
- eine Beschreibung des Geschäftsmodells, aus dem insbesondere die Art der beabsichtigten Dienstleistungen hervorgeht;
- eine Beschreibung des internen Kontrollsystems, das der Antragsteller einzuführen beabsichtigt, sowie eine Beschreibung der geplanten Strategien und Verfahren, um die Anforderungen dieses Bundesgesetzes und der VO (EU) 2015/847 zu erfüllen und
- bei juristischen Personen zusätzlich die Identität und die Höhe des Beteiligungsbetrages der Eigentümer, die direkt oder indirekt eine qualifizierte Beteiligung gemäß Art 4 Abs 1 Z 36 der VO (EU) 575/2013 am Antragsteller halten.

Der Registrierungsantrag ist in elektronischer Form an die FMA zu richten (reg.virtuellewaehrungen@fma.gv.at). Der Eintrag wird auf der Homepage der FMA in der Unternehmensdatenbank veröffentlicht.

Sofern die FMA zweifelt, dass aufgrund der Angaben und Unterlagen die Anforderungen des FM-GwG nicht erfüllt werden können oder die FMA Zweifel hat, an der persönlichen Zuverlässigkeit des oder der Geschäftsleiter, der natürlichen Person, die eine qualifizierte Beteiligung hält oder der natürlichen Person, die beabsichtigt als solcher Dienstleister tätig zu werden, darf keine Registrierung vorgenommen werden.

Tipp: Die konkreten bekanntzugebenden Informationen und Unterlagen können Sie der [Homepage der FMA](#) entnehmen, unter www.fma.gv.at, Stichwort: Registrierung von Dienstleistern in Bezug auf virtuelle Währungen.

Damit zählen diese Dienstleister auch zu den „Verpflichteten“ nach dem FM-GwG, welche Sorgfalts- und Meldepflichten im Bereich der Prävention von Geldwäscherei und Terrorismusfinanzierung zu beachten haben, im Konkreten:

- Pflicht zur Feststellung und Überprüfung der Kundenidentität und des wirtschaftlichen Eigentümers (Know-Your-Customer-Prinzip): Eine der wichtigsten Pflichten der Dienstleistungserbringer besteht darin, die Identität des Kunden oder des wirtschaftlichen Eigentümers festzustellen und zu überprüfen. Die Worte "feststellen" und "überprüfen" beschreiben zwei verschiedene Prozesse. Zunächst muss die Identität festgestellt und erst dann überprüft werden. Feststellung der Identität" bedeutet, Daten zu sammeln. Dies kann auf unterschiedlichste Weise erfolgen, mündlich, schriftlich, automationsgestützt oder auch durch Dritte. Die anschließende "Überprüfung der Identität" beschreibt die Verifizierung der erhobenen Daten anhand von Dokumenten, Daten oder Informationen, die aus einer glaubwürdigen und unabhängigen Quelle stammen. Nach den Vorstellungen des Gesetzgebers soll die Identitätsprüfung z.B. grundsätzlich durch die persönliche Vorlage eines amtlichen Lichtbildausweises erfolgen. Viele Dienstleister haben aufgrund ihres Geschäftsmodells über das Internet keine Möglichkeit, ihre Kunden persönlich zu identifizieren. Hierfür bietet das FM-GwG einige Absicherungen an, z.B:

⁵⁰ § 32a FM-GwG.

- Referenzkonto-Methode: Eine solche Sicherheitsmaßnahme ist die so genannte Referenzkonto-Methode, d.h. die erste Zahlung über ein Referenzkonto. Umgangssprachlich wird das Verfahren auch als penny check bezeichnet. Bei der Referenzkontomethode wird die erste Zahlung des Kunden über ein Konto abgewickelt, das - vereinfacht ausgedrückt - bei einem Kreditinstitut mit Sitz in der EU oder mit Sitz in einem Drittland, das die gleichen Verpflichtungen wie europäische Kreditinstitute hat, eröffnet wurde.
- Biometrisches Identifikationsverfahren: Eine weitere Sicherheitsmaßnahme ist das biometrische Identifikationsverfahren. Biometrische Identifikationsverfahren sind Verfahren zur Online-Identifikation, bei denen die gesamte Online-Identifikation oder einzelne Schritte davon ohne Beteiligung eines Mitarbeiters im Rahmen eines automatisierten elektronischen Verfahrens durchgeführt werden. Damit wurde einer langjährigen Forderung von Finanzdienstleistern entsprochen.
- Bewertung der Geschäftsbeziehung: Dienstleister haben den Umfang der Sorgfaltspflichten gegenüber Kunden auf risikoorientierter Grundlage zu bestimmen. Es sind daher im Rahmen einer „Customer due diligence“ (CDD) umfassende Informationen über den Kunden sowie das zu erwartende Transaktionsverhalten einzuholen. Auf diese Informationen basierend ist ein Risikoprofil des Kunden zu erstellen und jeder Kunde einer Risikoklasse zuzuteilen. Das Risikoprofil gibt Aufschluss darüber, welche Maßnahmen der Dienstleister in Bezug auf virtuelle Währungen zu setzen hat und ob etwa eine bestimmte Geschäftsbeziehung begründet, fortgeführt oder beendet werden sollte. Bei jeder Risikobewertung sind die in Anlage I des FM-GwG genannten Risikovariablen zu berücksichtigen. Diese umfassen den Zweck eines Kontos oder einer Geschäftsbeziehung, die Höhe der von einem Kunden eingezahlten Vermögenswerte oder den Umfang der ausgeführten Transaktionen sowie die Regelmäßigkeit oder Dauer der Geschäftsbeziehung. Darüber hinaus müssen auch stets die Risikovariablen der Anlage III des FM-GwG berücksichtigt werden, um allfällige Hochrisikokunden als solche identifizieren zu können und in weiterer Folge verstärkte Sorgfaltspflichten anzuwenden. Sollen auf einen Kunden lediglich vereinfachte Sorgfaltspflichten angewendet werden, so müssen außerdem die Risikovariablen der Anlage II des FM-GwG miteinbezogen werden.
- Laufende Überwachung der Transaktionen und Geschäftsbeziehung: Dabei werden die im Rahmen der Geschäftsbeziehung getätigten Transaktionen daraufhin überprüft, ob sie mit den Kenntnissen des Verpflichteten über den Kunden, seine Geschäftstätigkeit und sein Risikoprofil, ggf. auch über die Herkunft der Mittel, übereinstimmen.
- Einholung und Überprüfung von Informationen über die Herkunft der verwendeten Mittel: Die Verpflichteten müssen den Kunden fragen, wo und wie er die virtuellen Währungen und das verwendete Fiat-Geld erworben hat (Einholung von Informationen), und sie müssen auch den Nachweis dafür verlangen (Überprüfung der erhaltenen Informationen). Die Herkunft der Gelder des Kunden muss vollständig plausibel gemacht werden. Für Fiat-Transaktionen und Zahlungen mit Visa-Karten usw. sind Software-Tools zu verwenden, die Informationen über frühere und künftige Transaktionen liefern. Bei virtuellen Währungen müssen ebenfalls Software-Tools eingesetzt werden, um die Herkunft der virtuellen Währungen und die zukünftigen Transaktionen von der Wallet-Adresse aus zu ermitteln. Darüber hinaus müssen auch manuelle Kontrollen durchgeführt werden, insbesondere im Falle von Anomalien.
- Regelmäßige Überprüfung: Alle erforderlichen Informationen, Daten und Dokumente müssen regelmäßig auf Vollständigkeit und Aktualität überprüft werden. Anschließend sind risikoorientiert Fragen an den Kunden zu stellen und Nachweise zu erbringen.

- Bestellung eines Geldwäschebeauftragten: Zur Überwachung der Einhaltung der Bestimmungen zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung ist ein Geldwäschebeauftragter zu bestellen. Die FMA prüft den Geldwäschebeauftragten auf seine Eignung und Zuverlässigkeit.⁵¹ Der Geldwäschebeauftragte ist der zentrale Ansprechpartner für alle Angelegenheiten der Geldwäsche- und Terrorismusfinanzierungsprävention. Er führt die folgenden Tätigkeiten aus:
 - Erstellung und laufende Aktualisierung der Risikoanalyse;
 - Einführung und Weiterentwicklung von angemessenen und geeigneten Richtlinien, Kontrollen, Verfahren und IT-Systemen zur Einhaltung und Überprüfung der Sorgfaltspflichten des AML-Gesetzes;
 - Einführung und Weiterentwicklung von konzernweiten Richtlinien und Verfahren sowie deren Überprüfung;
 - Erarbeitung und Weiterentwicklung von internen Regelungen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung;
 - Überprüfung der getroffenen Maßnahmen und implementierten Prozesse auf ihre Eignung, die Einhaltung der Vorschriften zur Verhinderung von Geldwäsche und Terrorismusfinanzierung zu gewährleisten;
 - Umsetzung eines Maßnahmenkatalogs für die Anwendung der verstärkten Sorgfaltspflichten;
 - Sicherstellung einer verstärkten Überwachung von Geschäftsbeziehungen;
 - Überprüfung, Bewilligung oder Ablehnung von neu aufzunehmenden Geschäftsbeziehungen sowie Stopp und Bewilligung von Transaktionen;
 - Behandlung von Auffälligkeiten und Durchführung der zu deren Klärung erforderlichen Untersuchungen;
 - Veranlassung, dass in Zweigstellen oder Tochtergesellschaften in anderen Mitgliedstaaten das jeweilige nationale Recht angewendet wird und in Drittstaaten die Anforderungen des AML-Gesetzes erfüllt werden;
 - Entwicklung, Organisation und Durchführung von Schulungsmaßnahmen;
 - Einreichung von Verdachtsmeldungen und Berichten gemäß der Verordnung (EU) 2015/847 und Erledigung von Anträgen auf Genehmigung einer Transaktion;
 - Entwicklung und Einrichtung eines Systems zur raschen Meldung an die Geldwäschemeldestelle oder die Finanzmarktaufsicht in Österreich;
 - Regelmäßige Berichterstattung an den Vorstand;
 - Durchführung von Kontrollen hinsichtlich der laufenden Compliance;
 - Entwicklung und Pflege von Systemen zur langfristigen Aufbewahrung der Dokumente und Daten.
- Meldepflicht bei Verdachtsfällen
- Risikoanalyse/-bewertung: Dienstleister sind zur Erstellung einer Risikoanalyse auf Unternehmensebene. Dabei müssen die potentiellen Risiken der Geldwäscherei und Terrorismusfinanzierung, denen das Unternehmen ausgesetzt ist, auf Basis von Daten und Informationen unter Berücksichtigung sämtlicher relevanten Risikofaktoren ermittelt und bewertet werden. Es sind jedenfalls Risikofaktoren in Bezug auf Kunden, Länder oder geografische Gebiete, Produkte, Dienstleistungen, Transaktionen und Vertriebskanäle sowie sonstigen neuen oder sich entwickelnden Technologien zu ermitteln und zu bewerten. Die Aufzeichnungen sind mindestens jährlich in regelmäßigen Abständen zu aktualisieren und müssen der FMA auf Anfrage übermittelt werden.

⁵¹ Farahmandnia, Die persönliche Zuverlässigkeit von Geschäftsleitern eines Krypto-Unternehmens, RdW 2021/266.

Achtung: Auch wenn Wallet-Provider nun verpflichtet werden, den Kunden zu identifizieren, ist eine „anonyme“ Transaktion weiterhin möglich, da Nutzer diese auch ohne regulierte Wallet-Anbieter durchführen können.⁵²

Die FMA prüft grundsätzlich die Einhaltung der Bestimmungen des FM-GwG sowie der Geldtransfer-VO. Für jene Dienstleistungen in Bezug auf virtuelle Währungen, die nicht im Inland erbracht werden, sind die jeweiligen nationalen Bestimmungen zu berücksichtigen.

11. EU-Rechtsrahmen über Märkte in Kryptowerte („MiCA“)

Die Europäische Kommission hat am 24.9.2020 im Rahmen des Digital Finance Packages ein umfassendes Rahmenwerk zur Regulierung und Stärkung der digitalen Widerstandsfähigkeit des Finanzsektors präsentiert.

Darunter findet sich auch ein [Vorschlag für eine Verordnung über Märkte für Kryptowerte und zur Änderung der Richtlinie \(EU\) 2019/1937](#). Die geplante Verordnung durchläuft das ordentliche Gesetzgebungsverfahren und befindet sich nach aktuellem Stand⁵³ in der Phase der förmlichen Annahme durch den Rat der EU und das Parlament. Das Inkrafttreten der MiCA wird für das Jahr 2023 erwartet.

Dieser Legislativvorschlag soll jene Kryptowerte regeln, die bisher keinen Bestimmungen unterliegen sind, stellt Emittenten unter strenge Anforderungen und schafft insbesondere Sicherheitsvorkehrungen (Eigenkapitalanforderungen, Verwahrung von Vermögenswerten, Beschwerdeverfahren etc.). Auch ein verpflichtendes White-Paper für Kryptowerte wird eingeführt. Zusätzlich ergeht ein Vorschlag für eine Pilotregelung für Marktinfrastrukturen, mit denen angestrebt wird, Transaktionen mit Finanzinstrumenten in Form von Kryptowerten zu tätigen und abzuwickeln.

Wichtig: Der Legislativvorschlag umfasst auch die Beratung von Kryptowerten als regulierte Krypto-Dienstleistung (aktuelles siehe unter Stichwort Krypto-Asset in der [Wissensdatenbank](#).)

Autoren:

Dr. Oliver Völkel, Gründungspartner und Rechtsanwalt bei Stadler Völkel Rechtsanwälte

Mag.a Leyla Farahmandnia, Partnerin und Rechtsanwältin bei Stadler Völkel Rechtsanwälte

Mag. Philipp Ley, Rechtsanwaltsanwärter bei Stadler Völkel Rechtsanwälte

Andreas Ramprecht, LL.M. (WU), Rechtsanwaltsanwärter bei Stadler Völkel Rechtsanwälte

Dr. Alexander Kern, MSc, Geschäftsführer beim Fachverband Finanzdienstleister (WKO) und bei der Fachgruppe Finanzdienstleister Wien (WKW)

Mag. Sandra Pfaffenlehner, Referentin beim Fachverband Finanzdienstleister (WKO)

Disclaimer/Haftung: Sämtliche Angaben in diesem Artikel und im Anhang erfolgen trotz sorgfältiger Bearbeitung und Kontrolle ohne Gewähr. Eine etwaige Haftung der Autoren, des Fachverbands Finanzdienstleister oder von Stadler Völkel Rechtsanwälte aus dem Inhalt dieses Artikels und dem Anhang ist ausgeschlossen.

⁵² Siehe auch *Piska, Chr./ Völkel, O.: Kryptowährungen und AML - smart regulation in Sicht*.

⁵³ September 2022.

Literaturverzeichnis

- [1] *Aigner*, Das Pfandrecht und die Blockchain, ÖBA 2019, 816 f.
- [2] *Anderl*, #Blockchain in der Rechtspraxis (2019)
- [3] *Artmann, E./Bieber, T./Mayrhofer, M./Schmidt, N./Tumpel, M. (Hrsg)*, Crypto Assets, Linde Verlag Ges.m.b.H., 2022
- [4] *Bernsteiner, C.*: Kryptowährungen und Gewerberecht, in: Kryptowährungen: Krypto-Assets, ICOs und Blockchain. Kirchmayr-Schliesselberger, S., Klas, W., Miernicki, M., Rinderle-Ma, S. & Weilingner, A. (eds.). Facultas Verlags- und Buchhandels AG, Wien, 2019, S 463-487.
- [5] *Buchleitner, C./Rabl, T.*: Blockchain und Smart Contracts (ecolex - Heft 1/2017), Manz, 2017.
- [6] *Gerdes, I./Feiler, L.*: Bitcoin: Virtuelles Geld im rechtsfreien Raum?
- [7] *Hanzl, M./Pelzmann, H./Schragl, M.*, Handbuch Digitalisierung, Linde Verlag, 2021.
- [8] *Hanzl/Rubey*, Smart Contracts - die intelligente Art Verträge zu schließen?, Zak 2018, 238 ff.
- [9] *Heine/Stang*, Weiterverkauf digitaler Werke mittels Non-Fungible-Token aus urheberrechtlicher Sicht MMR 2021, 756-
- [10] *Hoeren/Sieber/Holznapel/Guggenberger*, Handbuch Multimediarecht, 55. EL Mai 2021
- [11] *Kirchmayer-Schliesselberger, S./Klas, W./Miernicki, M./Rinderle-MA, S./Weilingner, A.*, Kryptowährungen, Facultas Verlags- und Buchhandels AG, Wien, 2019.
- [12] *Kresbach, G./Zhang, E.*, Urheberrechtliche Aspekte von Non-Fungible Token, MMR 2021, S 194 ff.
- [13] *Petriz M/Grimmer D.*: Initial Coin Offering - eine neue Art der Unternehmensfinanzierung und steuerliche Auswirkungen, in taxlex 2017, Ausgabe 12/2017, S 382 ff.
- [14] *Petriz M/Wimmer/Deichsel*, Kryptosteueruide 2021, Linde Verlag, 2021.
- [15] *Piska, Ch. / Völkel, O.*: Blockchain rules, MANZ'sche Verlags- und Universitätsbuchhandlung, Wien, 2019.
- [16] *Piska, Ch./ Völkel, O.*: Kryptowährungen und AML - smart regulation in Sicht, in Ecolex 2018, 671 ff.
- [17] *Piska, Ch.*: Kryptowährungen und ihr Rechtscharakter - eine Suche im Bermuda-Dreieck, Ecolex 2017, S 632 ff, 2017.
- [18] *Polivanova-Rosenauer, T.*: Kryptowährung - eine weitere Anlageklasse oder ein Wirtschaftsgut Sui generis, in taxlex 2017, Ausgabe 12/2017, S 376 ff.
- [19] *Raschauer, N./Silbernagl, R.*: Grundsatzfragen des liechtensteinischen „Blockchain-Gesetzes“ - TVTG, in ZFR 1/2020, S 11-17.
- [20] *Rauer/Bibi*, Non-fungible Tokens - Was können sie wirklich?, ZUM 2022, 22.
- [21] *Rirsch, R./ Dämon, R./ Tomanek, S.*: PRIIP-VO - Der vergessene Anwendungsbereich, in ÖBA 1/20, S 37-45
- [22] *Schnell/Schwaab*, Vertragsgestaltung beim Einsatz von Smart Contracts zur Automatisierung von Lieferbeziehungen, BB 2021, 1091
- [23] *Schmidt, N.*, Kryptowährungen und Blockchains: Technologie, Praxis, Recht, Steuern (2019)
- [24] *Schock, S.*: Virtuelle Währungen - Ein Blick über die Grenzen, Ecolex 2017, S 636ff, 2017.
- [25] *Smets/Kapeller*, Smart Contracts: Vertragsabschluss und Haftung, ÖJZ 2018, 293
- [26] *Stadler, A./Chochola, T.*: Kryptowährungen: Aufklärungspflichten im Verhältnis Unternehmer - Verbraucher, Ecolex 2017, S 641 ff, 2017.
- [27] *Steiner, Ch.*: Krypto-Assets und das Aufsichtsrecht, Finanzverlag, Wien, 2019.
- [28] *Varro, D.*: Bitcoin-Mining: nicht steuerbares Glücksspiel?, in taxlex 2017, 399, Ausgabe 12/2017.
- [29] *Völkel, O.*: Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, in ZTR 2017, 103, Ausgabe 3/2017, S 103 ff.
- [30] *Völkel, O.*: Privatrechtliche Einordnung virtueller Währungen, ÖBA 2017, 385..
- [31] *Völkel, O.*: Privatrechtliche Einordnung der Erzeugung virtueller Währungen, Ecolex 2017, S 639 ff, 2017.

- [32]Völkel, O.: Mining von virtuellen Währungen als Alternativer Investmentfonds?, ZFR 2018, 317.
- [33]Völkel, O.: Zum Begriff „virtuelle Währung“, ZFR 7/2019, 346.
- [34]Völkel, O.: Zur Bedeutung der Dezentralität von Blockchains im Privatrecht, ZFR 12/2019, 601.
- [35]Völkel, O.: Vertrauen in die Blockchain und das Sachenrecht, ZFR 2020/218.
- [36]Welten/Ozsvar in Binder Grösswang, Digital Law² (2020) Zivilrecht, 15 f.
- [37]Zeinzinger, T.: Das Internet der Werte - Blockchain Technologie & Kryptowährungen als Basis der neuen Wirtschaft, Graz, 2016.

Links:

- [1] [BaFin: Bitcoins - Aufsichtliche Bewertung und Risiken für Nutzer](#)
- [2] BMDW - Parlamentarische Anfragebeantwortung (GZ: [BMDW 10.101/0280 IM/a/2018](#))
- [3] BMF - Parlamentarische Anfragebeantwortung (GZ: [BMF-310205/0115-I/4/2014](#))
- [4] [BMF - Steuerliche Behandlung von Kryptowährungen](#)
- [5] BMWFW - Parlamentarische Anfragebeantwortung (GZ: [BMWFW-10.101/0250-IM/a/2014](#))
- [6] EBA-Pressemitteilung 1: [Hinweis zu virtuellen Währungen der Europäischen Bankaufsicht \(EBA\)](#)
- [7] EBA-Pressemitteilung 2: <http://www.eba.europa.eu/-/eba-proposes-potential-regulatory-regime-for-virtual-currencies-but-also-advises-that-financial-institutions-should-not-buy-hold-or-sell-them-whilest-n>
- [8] FMA: Information zu Bitcoin: <http://www.fma.gv.at/de/sonderthemen/information-zu-bitcoin.html>
- [9] Liste von aktuellen Kryptowährungen: <http://coinmarketcap.com/>
- [10][Zeinzinger, T.: Blockchain - Das Internet der Werte, Graz, 7.11.2016](#) (get know howww - UBIT Steiermark)

12. Anhang: Auszug - Was ist die Blockchain?

Zur besseren Verständlichkeit und Veranschaulichung des Blockchainprozesses folgt ein Auszug aus:

PWC: Kurzstudie für die Verbraucherzentrale NRW, Düsseldorf, 26.7.2016 (S 3 f)

(entspricht dem Proof-of-Work-Algorithmus)

„Wenn ein Anbieter und ein Nachfrager eine Transaktion vereinbaren, legen sie die Variablen einer Transaktion fest, unter anderem Empfänger, Sender und Höhe der Transaktion. Die Informationen der einzelnen Transaktion werden mit anderen Transaktionen im gleichen Zeitraum als Datenblock zusammengefasst. Dies ist vergleichbar mit dem Versenden von E-Mails, auch dort werden die E-Mails in Datenblöcke zerlegt. Bei Blockchain besteht der Unterschied darin, dass der Vorgang eine einzelne standardisierte Transaktion beinhaltet.

Diese Transaktion wird verschlüsselt auf vielen einzelnen Computern verteilt (Peer-to-Peer) und auf diesen lokal gespeichert. Die Mitglieder des Netzwerkes bestätigen (Validierung) automatisch die Transaktionen, die auf den verschiedenen Computern gespeichert sind.

Die Validierung innerhalb eines Blocks erfolgt durch Algorithmen, welche den Blöcken einen einzigartigen Hash anhängen. Ein Hash ist eine auf allen in dem Block gespeicherten Informationen basierende Serie von Zahlen und Buchstaben. Wird nur eine Information innerhalb einer Transaktion durch Manipulation oder Übertragungsfehler nachträglich verändert, beispielsweise die Höhe des jeweiligen Transaktionsbetrags, errechnet der Algorithmus des veränderten Blockes nicht mehr den korrekten Hash und erstellt eine Fehlermeldung. Diese Zahlen- und Zifferkombinationen werden laufend auf ihre Korrektheit geprüft und die einzelnen Blöcke zu einer gesamten Datenblock-Kette zusammengefügt - der Blockchain.

Die in der Blockchain gespeicherten Informationen sind durch eine Verknüpfung der Zahlen- und Zifferkombinationen nicht (oder nur mit sehr hohem Aufwand) manipulierbar. Dieser andauernde Prüfungsprozess (das sogenannte Mining) wird durch Mitglieder der Blockchain geleistet, welche hierfür abhängig von der von ihnen eingebrachten Rechenleistung entlohnt werden.

Die Blockchain kann durch diesen Validierungsprozess durch alle Mitglieder befüllt, aber nicht nachträglich verändert werden. Dies ermöglicht direkte Peer-to-Peer-Transaktionen zwischen Personen oder Organisationen, für die vormals immer ein Intermediär nötig war, der die Transaktion legitim dokumentierte. Ist für eine Geldtransaktion zwischen zwei Parteien normalerweise eine Bank als Intermediär notwendig, so kann diese Transaktion mithilfe der Blockchain-Technologie direkt zwischen den beiden Parteien stattfinden und dokumentiert werden.“

13. Anhang 2: Eine alternative Erklärung der Blockchain

Eine alternative Erklärung der Blockchain bietet der folgende Auszug aus:

Piska/Völkel (Hrsg), Blockchain rules (2019) Rz 1.1 ff.

"Wer heute von Blockchain spricht, meint damit zu allermeist die Technologie, die den bekannten virtuellen Währungen wie Bitcoin, Ether, Dash oder Litecoin zugrunde liegt. Doch hinter dem Schlagwort Blockchain verbergen sich in der Regel viele verschiedene Technologien, und neue Technologien werden laufend entwickelt. Gemein ist den Blockchain-Technologien ihr Zweck: Unter einer Gruppe an Personen soll Einigkeit darüber hergestellt werden, (a) ob Ereignisse stattgefunden haben (etwa Transaktionen oder Berechnungen) und (b) in welcher Reihenfolge diese Ereignisse stattgefunden haben. Diese Ereignisse sollen (c) auf eine Weise aufgezeichnet werden, die unveränderlich ist - oder zumindest auf eine Weise, die es jedem ermöglicht, sofort zu erkennen, dass nachträglich Veränderungen vorgenommen wurden. Zuletzt - und das ist das Alleinstellungsmerkmal der Technologie - soll (d) der gesamte Prozess ohne eine vertrauenswürdige zentrale Stelle auskommen.

Gerade der letzte Punkt - das Fehlen einer vertrauenswürdigen zentralen Stelle - bereitet in der Regel das größte Kopfzerbrechen für jene, die sich zum ersten Mal mit der Technologie beschäftigen. Als erster Einstieg bietet sich zum Verständnis der Technologie als Gedankenexperiment die Vorstellung einer Blockchain in der analogen Welt an. Stellen Sie sich eine Gruppe von 20 Personen in einem Raum vor. Die Gruppe entscheidet, dass sie untereinander nicht mehr mit Geld handeln möchte, sondern stattdessen mit einer eigenen Währung. Diese Währung soll aber nicht physisch existieren, sondern nur auf dem Papier. Um die Wirtschaft rund um diese virtuelle Währung in Gang zu bringen, wird entschieden, dass alle Personen mit einem Betrag von 100 starten sollen. Zu diesem Zweck notiert jede Person für sich selbst ein Startguthaben von 100 Punkten auf einem eigenen Stück Papier. Wird Handel betrieben, so wird in der Gruppe vereinbart, dass sich jede Person notiert, welche Anzahl an Punkten sie von einer anderen Person erworben oder an eine andere Person abgegeben hat.

Leider hat sich in die Gruppe ein unehrlicher Teilnehmer eingeschlichen, der nicht notiert, wenn er Punkte abgeben sollte. Die Gruppe erkennt schnell, dass ihre virtuelle Währung auf diese Weise nicht funktionieren kann. Schließlich kann im Nachhinein nicht mehr mit Sicherheit bestimmt werden, welche der beteiligten Personen die Übertragungen korrekt aufgezeichnet hat. Eine einzelne Person zu bestimmen, die für alle anderen die Aufzeichnungen führt, kommt aber aus genau demselben Grund nicht in Betracht - was wenn diese zentrale Stelle Fehler macht oder unehrlich handelt?

Die Gruppe entscheidet also, dass alle Teilnehmer auf ihrem eigenen Stück Papier nicht nur ihre eigene Anzahl an Punkten notieren, sondern zunächst auch das Startguthaben aller anderen neunzehn Teilnehmer. Möchte eine Person an eine andere Punkte übertragen, solle sie das so laut sagen, dass alle anderen in der Gruppe es hören. Jeder notiert auf dem eigenen Stück Papier die Übertragung. Auf diese Weise sollte immer jeder in der Gruppe genau wissen, wem wie viele Punkte zustehen.

Diese Idee scheint zunächst gut zu funktionieren. Als Person A der Person B fünf Punkte übertragen möchte, ruft er dies laut in den Raum und alle notieren sich die Übertragung. Das Problem scheint gelöst und die Teilnehmer im Raum beginnen die neue virtuelle Währung immer eifriger zu nutzen. Irgendwann jedoch wird genau dies zum Problem. Es wird laut durcheinandergerufen. Nicht jeder Teilnehmer hört noch alle Rufe, manche missverstehen die Rufe, und manche Teilnehmer sind schlicht nicht schnell genug beim Notieren. Schon nach kurzer Zeit unterscheiden sich die Aufzeichnungen der Teilnehmer

erheblich. Es besteht in der Gruppe keine Einigkeit mehr darüber, welche Übertragungen tatsächlich stattgefunden haben und in welcher Reihenfolge. Ein neues System muss gefunden werden.

Das Notieren jeder einzelnen Transaktion durch alle anderen war eine gute Idee, in der Praxis aber zu anfällig für Fehler. Die Gruppe entscheidet daher, doch eine einzelne Person als „Aufzeichner“ zu bestimmen. Der Aufzeichner soll jedoch laufend abgelöst werden und dann alle von ihm aufgezeichneten Übertragungen in einem Block vorlesen. Alle anderen in der Gruppe schreiben den Block mit und kontrollieren, ob die eigenen Transaktionen richtig aufgezeichnet sind. Fällt keinem Teilnehmer ein Fehler auf, so darf der Aufzeichner als Belohnung seinen eigenen Guthabensstand um ein paar Punkte erhöhen, was ebenfalls von allen in der Gruppe notiert wird. Macht der Aufzeichner hingegen einen Fehler, so soll der gesamte Block ignoriert werden, neue Punkte erhält der Aufzeichner dann auch nicht. Übertragungen müssen in so einem Fall eben dem nächsten Aufzeichner nochmals angesagt werden.

Dieses System löst gleich mehrere Probleme auf einmal. Zunächst besteht auf diese Weise immer Einigkeit in der Gruppe, welche Übertragungen stattgefunden haben. Gleichzeitig besteht aber auch ein Anreiz, sich an die Regeln des Systems zu halten. Wer den sicherlich mühsamen Prozess des richtigen Aufzeichnens fehlerfrei erledigt, der darf sich selbst belohnen. Wer hingegen versucht zu betrügen, wird entlarvt und hat die schwierige Aufgabe des Aufzeichnens umsonst erledigt.

Die Teilnehmer entscheiden sich für dieses System, erkennen jedoch unmittelbar ein neues Problem. Nach welchen Regeln sollen sie entscheiden, wer der nächste Aufzeichner sein darf? Da mit dieser Aufgabe nun eine Belohnung verbunden ist, haben alle in der Gruppe ein Interesse daran, selbst möglichst oft Aufzeichner zu sein. In der analogen Welt dieses Gedankenexperiments bieten sich dafür freilich viele verschiedene Lösungsmöglichkeiten an. Die Gruppe könnte etwa würfeln; wer die höchste Augenzahl würfelt, ist der nächste Aufzeichner. In der digitalen Implementierung von Blockchains ist dieses Problem hingegen weit schwieriger zu lösen.

Die Teilnehmer in diesem Gedankenexperiment haben einen Mechanismus gefunden, Konsens darüber herzustellen, welche Übertragungen ihrer eigenen virtuellen Währung stattgefunden haben und in welcher Reihenfolge. Außerdem kommt das System ohne eine vertrauenswürdige zentrale Stelle aus. Lediglich das letzte, oben unter Rz 1.1 genannte Merkmal - die unveränderliche Aufzeichnung - kann dieses System nicht abschließend gewährleisten. Auf welche Weise die digitale Implementierung der Blockchain-Technologie alle vier Anforderungen erfüllt, wird an späterer Stelle erörtert."