LEITFADEN KRYPTOWERTE

RECHTSLAGE IN ÖSTERREICH

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

Stadler Völkel Rechtsanwälte GmbH
Seilerstätte 24 | 1010 Wien
T 01 997 10 25 | F 01 997 10 25 99
E office@sv.law | W http://www.sv.law
Autor: Dr. Oliver Völkel, LL.M.

Oktober 2024

Index

Sie wollen mehr Informationen?
Dann schauen Sie auch in unsere

Wissensdatenbank!

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

Wichtiger Hinweis

Nachdem unterschiedliche Regulierungsansätze lange Zeit zu Unsicherheit und Inkonsistenzen in Bezug auf die Nutzung und rechtliche Behandlung von Kryptowerten geführt hatten, trat am 29. Juni 2023 mit der EU-Verordnung über Märkte für Kryptowerte (MiCAR) ein einheitlicher aufsichtsrechtlicher Rahmen in Kraft. Auch wenn es Ziel der Verordnung ist, Rechtssicherheit zu gewährleisten, bleiben weiterhin strittige bzw fehlende Aussagen. Je nach Geschäftsmodell ist eine Gewerbeberechtigung oder Zulassung oder Konzession durch die Finanzmarktaufsichtsbehörde (FMA) notwendig (siehe Informationen dazu auf www.fma.gv.at). Trotz der europäischen Regulierung ist zu beachten, dass die Rechtslage zu Kryptowerten einer laufenden Weiterentwicklung unterliegt und daher nicht alle künftigen Entwicklungen abschätzbar sind.

Ihre Anfragen richten Sie daher direkt an:

- **FMA**, wenn eine Konzession oder Zulassung für Ihr Geschäftsmodell notwendig sein könnte, 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 Tätigkeit innerhalb und außerhalb der MiCAR in Betracht gezogen wird.

- **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

1.1. Was ist eine Blockchain?

Der Begriff Blockchain bezeichnet eine Datenbankstruktur zur Speicherung von Transaktionen, die nur (blockweise) um neue Einträge ergänzt werden kann. Bereits bestehende Einträge bzw Blöcke in der Struktur sind unveränderlich in dem Sinne, dass jede Änderung die Datenintegrität zerstört und ein Manipulationsversuch sofort auffallen würde. Die Blockchain kann technisch als 'append-only'-Datenbank beschrieben werden, also eine Datenbank, deren Datenstruktur nur durch das Anfügen neuer Daten veränderlich ist.

Neben dieser technischen Erläuterung lässt sich der Begriff aber auch aus einem anderen Blickwinkel erklären, nämlich im Hinblick auf ihren Einsatzzweck. Die Blockchain wird dazu verwendet, um unter einer Gruppe an Personen (den Minern oder Validatoren) Einigkeit darüber herzustellen, (a) ob Ereignisse stattgefunden haben (etwa Transaktionen oder Berechnungen) und (b) in welcher Reihenfolge. 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. Dieses Gedankenexperiment finden Sie angeschlossen in Anhang 1.

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“.

1.2. Was sind Bitcoins?

Die Bitcoin-Blockchain war die erste funktionierende technische Implementierung eines Distributed-Ledger Systems, bei dem Transaktionen der Werteinheit 'Bitcoin' direkt zwischen den Teilnehmern dieses Systems erfolgen. Jeder kann an dem System teilnehmen, es bedarf dazu keiner Zulassung durch eine zentrale Stelle. Bitcoin ist eine Kryptowährung (siehe Punkt 1.4), eine virtuelle Währung (siehe Punkt 1.5) und ein Kryptowerte (siehe Punkt 1.6).

1.3. Was sind (Alt-)Coins und Token?

Coins sind die Wertträger, die in der jeweiligen Blockchain von Anbeginn an vorgesehen sind. Man könnte auch sagen, Coins sind der jeweiligen Blockchain immanent. Der Begriff Coin wird daher für Kryptowerte wie Bitcoin oder Ether verwendet. Manchmal wird der Begriff Altcoin für alle Coins außer Bitcoin verwendet.

Coins werden in aller Regel nicht von einer zentralen Stelle (wie etwa einer Zentralbank oder anderen öffentlichen Stelle) erzeugt, sondern verteilt im Netzwerk von denjenigen Personen, die am Netzwerk der jeweiligen Blockchain teilnehmen. Neue Coins werden dabei nicht nach Belieben neu geschaffen. Das Protokoll einer Blockchain sieht stattdessen vor, dass neue Einheiten nur von denjenigen erschaffen werden können, die eine bestimmte für das Netzwerk wichtige Aufgabe erfüllen.

Der Begriff Token wird demgegenüber für Wertträger verwendet, die der jeweiligen Blockchain nicht immanent sind. Das bedeutet, dass Token im Protokoll der jeweiligen Blockchain nicht von Anbeginn an vorgesehen sind, sondern erst später durch die Benutzer der Blockchain neu

hinzugefügt werden. Token sind daher auf einer bestehenden Blockchain aufsetzende Wertträger.

Nicht jede Blockchain unterstützt Token. Ein Beispiel für eine Blockchain, die Tokens unterstützt, ist Ethereum. Auf Basis der Ethereum-Blockchain können Benutzer unter anderem nachträglich neue Wertträger (Token) schaffen und deren Übertragung von einer Person an eine andere über die Ethereum-Blockchain abwickeln. Gleichzeitig verfügt Ethereum mit dem Coin „Ether“ aber auch über einen dieser Blockchain immanenten Wertträger. Für die Nutzung der Ethereum Blockchain und die damit verbundene Belastung des Netzwerks wird von den Teilnehmern eine gewisse Leistung in Form von Ether erbracht, etwa auch für die Aufzeichnung der Transaktionen von Token.

1.4. Was ist eine Kryptowährung?

Anfänglich verwendete die Kryptobranche nicht die Begriffe 'Kryptowerte' oder 'Krypto-Asset', sondern sprach meist allgemein von Kryptowährungen. Der Begriff wurde verwendet, um die Vielzahl an Blockchain-basierten Coins zusammenzufassen (wie etwa Bitcoin, Ether, Ripple, Solana, etc). Der Begriff ist mittlerweile aus der Mode gefallen, hat aber Eingang im Einkommensteuerrecht gefunden. Dort wird der Begriff in § 27b Abs 4 EStG gesetzlich definiert. Die Definition entspricht jener der 'virtuellen Währung', die aus anderen Gesetzen bekannt ist (dazu weiter unten).

Dass die Kryptobranche anfänglich von einer 'Währung' sprach, ist auf Bitcoin zurückzuführen, der ersten Implementierung einer dezentralen DLT (Distributed-Ledger Technologie). Der Anspruch von Bitcoin war (und ist es), ohne zentralen Intermediär den Austausch von Werten zu ermöglichen ("*A Peer-to-Peer Electronic Cash System*" laut dem Whitepaper von Satoshi Nakamoto). Dass sich mit DLT weit mehr als eine 'Währung' erreichen lässt, war damals noch nicht absehbar. Die Verwendung des Begriffs sorgte dennoch für viele Missverständnisse; es handelt sich bei Bitcoin, Ether und anderen Kryptowerten jedenfalls nicht um Währungen im Rechtsinn.

Wichtig: Der Begriff 'Kryptowährung' hat im Einkommensteuerrecht zentrale Bedeutung und entspricht dort inhaltlich dem Begriff der 'virtuellen Währung'. Kryptowährung ist keine Währung im Rechtssinn.

1.5. Was ist eine virtuelle Währung?

Der Begriff 'virtuelle Währung' ist (derzeit noch) in § 2 Z 21 FM-GwG gesetzlich definiert. Die Definition basiert auf der 5. EU-Geldwäsche-Richtlinie. Eine virtuelle Währung ist demnach *„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“*.

Die Verfasser dieser Legaldefinition hatten in erster Linie Bitcoin als archetypisches Beispiel einer virtuellen Währung vor Augen. Dennoch enthält die zitierte Definition keinerlei Elemente, die auf den Einsatz einer bestimmten Technologie zugeschnitten sind. Ganz im Gegenteil, die Legaldefinition ist auffallend technologieneutral.

Im Wirtschaftsleben wird Bitcoin und vergleichbaren Kryptowerten wegen bestimmter Eigenschaften vertraut. Diese Eigenschaften haben ihren Ursprung alle in der eingesetzten Technologie, die sicherstellt, dass durchgeführte Transaktionen aufgezeichnet werden, nicht nachträglich veränderlich sind und Kryptowerte nicht gegen den Willen ihrer Inhaber weiterübertragen werden können. Gerade wegen dieser Eigenschaften werden virtuelle Währungen überhaupt als Tauschmittel akzeptiert. Der europäische Gesetzgeber hat diese Eigenschaften in der

Legaldefinition dennoch nicht berücksichtigt. Hierbei handelt es sich aber nur scheinbar um einen Widerspruch. Anstatt Merkmale zu definieren, die für die Akzeptanz einer virtuellen Währung sorgen, verlangt die Definition stattdessen pointiert, dass sie "*als Tauschmittel akzeptiert [wird]*". Weshalb sie als Tauschmittel akzeptiert wird, darauf soll es nicht ankommen.

Wichtig: Ohne sich zu weit in Details zu verlieren: Der Akzeptanz als Tauschmittel kommt eine zentrale Bedeutung bei der Frage zu, ob es sich bei einem Coin oder Token um eine virtuelle Währung handelt; ebenso für die Frage, ob eine Kryptowährung unter dem EstG vorliegt.

1.6. Was ist ein Kryptowert?

Der Begriff 'Kryptowert' (oder *crypto-asset*) hat sich im Laufe der Zeit als Überbegriff für eine ganze Reihe an Phänomenen in der Kryptowelt entwickelt. Es sollte damit auch klar zum Ausdruck gebracht werden, dass die Funktion als Wertträger im Vordergrund steht.

Der Begriff ist in der EU-Verordnung über Märkte für Kryptowerte (MiCAR) gesetzlich definiert. Die Definition ähnelt jener der 'virtuellen Währung'. Kryptowert ist eine "*digitale Darstellung eines Wertes oder Rechtes, die unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden kann*".

Diese Definition ist einerseits enger und andererseits weiter als jene der virtuellen Währung. Sie ist enger, weil sie eine bestimmte Technologie voraussetzt (DLT oder damit vergleichbare Technologie). Sie ist weiter, weil neben digitalen Darstellungen von Werten (wie bei der virtuellen Währung) auch digitale Darstellungen von Rechten erfasst sind.

Darstellung eines Wertes umfasst auch einen nicht intrinsischen Wert, der einem Coin oder Token von den betroffenen Verkehrskreisen beigelegt wird. Der Wert kann rein subjektiv und etwa lediglich nachfrageseitig durch das Interesse jener Personen begründet sein, die den fraglichen Kryptowert erwerben möchten. Dieses weite Wertverständnis dient dazu, um auch Phänomene wie etwa Bitcoin als Kryptowert zu erfassen, die (vergleichbar mit historischen Münzen, Briefmarken oder Sammelkarten) gerade kein Recht, keinen Anspruch, gegenüber einer anderen Person einräumen.

Was genau unter Darstellung eines Rechtes zu verstehen ist, lässt sich anhand einzelner Bestimmungen der MiCAR ableiten. Es geht um eine Art Verknüpfung im weitesten Sinne, wie etwa das Erfordernis, einen Token zu besitzen oder zu präsentieren, um ein bestimmtes Recht auszuüben. Viele Rechte können auf diese Weise 'tokenisiert' werden, etwa das Recht auf Herausgabe einer hinterlegten Sache oder Lieferung einer bestimmten Ware.

Weil der Begriff so weit ist, erfasst er auch zB 'tokenisierte' Finanzinstrumente. Also Finanzinstrumente, bei denen die Ausübung des Rechts an den Besitz eines DLT-basierten Tokens geknüpft ist. Es handelt sich bei diesen (und anderen) tokenisierten Instrumenten zwar um Kryptowerte, die MiCAR ist aber dennoch nicht auf sie anwendbar. Stattdessen gelten andere einschlägige Vorschriften wie etwa MiFID II (WAG 2018) oder die Prospekt-VO.

Wichtig: Der Begriff 'Kryptowert' ist ausufernd weit. Nicht jeder Kryptowert unterliegt der EU-Verordnung über Märkte für Kryptowerte (MiCAR). Teilweise unterliegen die Kryptowerte anderen Bestimmungen wie zB der MiFID II (WAG 2018) oder der Prospekt-VO.

1.7. Was sind E-Geld Token, vermögenswertreferenzierte Token und Utility Token

MiCAR legt besondere Regeln für bestimmte Arten von Kryptowerten fest, nämlich für E-Geld Token, vermögenswertreferenzierte Token und Utility Token. Diese ersten beiden Kategorien werden aufgrund ihrer englischen Bezeichnungen (E-Money Token, Asset-referenced Token) teils auch als EMT oder ART bezeichnet.

- **E-Geld Token** sind Kryptowerte, deren Wertstabilität unter Bezugnahme auf den Wert einer amtlichen Währung gewahrt werden soll. Gemeint sind damit Stablecoins wie bspw USDC oder USDT.

- **Vermögenswertereferenzierte Token** sind Kryptowerte, die kein E-Geld-Token sind und deren Wertstabilität durch Bezugnahme auf einen anderen Wert oder ein anderes Recht oder eine Kombination davon, einschließlich einer oder mehrerer amtlicher Währungen, gewahrt werden soll. Es handelt sich also um einen Token, der seinen Wert stabil hält (wenn auch nur vorgeblich), indem ein oder mehrere Werte oder Rechte (Vermögenswerte) als Bezugsgrundlage verwendet werden.

- **Utility-Token** ist ein Kryptowert, der ausschließlich dazu bestimmt ist, Zugang zu einer Ware oder Dienstleistung zu verschaffen, die von seinem Emittenten bereitgestellt wird. Die Kategorie des Utility-Tokens ist gegenüber den anderen Kryptowerten subsidiär. Ist ein Token nicht ausschließlich dazu bestimmt, Zugang zu einer Ware oder Dienstleistung zu verschaffen, sondern kann er etwa auch in eine amtliche Währung getauscht werden oder soll sein Wert stabil zu bestimmten Referenzwerten sein, so greifen stattdessen die Regeln über E-Geld-Token oder vermögenswertreferenzierte Token.

1.8. Was sind Security Tokens und was ist Tokenisierung?

Security Tokens sind tokenisierte übertragbare Wertpapiere oder sonstige tokenisierte Finanzinstrumente iSd MiFID II (WAG 2018), bei denen nicht Papier, sondern Blockchain-basierte Token zum Einsatz gelangen. Beispiele von Security Token sind tokenisierte Anleihen, also Anleihen, die nicht auf Papier gedruckt werden, sondern bei denen ein Blockchain-basierter Token ein Stück repräsentiert. Security Tokens sind zwar Kryptowerte, sie unterliegen aber aufgrund einer ausdrücklichen Ausnahme nicht dem Anwendungsbereich der MiCAR. Stattdessen ist auf sie das für alle anderen Finanzinstrumente anwendbare Regime anwendbar.

Tokenisierung bezeichnet dabei die Verknüpfung Blockchain-basierter Token mit Vermögenswerten aller Art wie beispielweise Forderungsrechten oder körperlichen Sachen; und zwar dergestalt, dass zur Ausübung des Rechts am jeweiligen Vermögenswert die Innehabung des dazugehörigen Tokens notwendig ist. Die Tokenisierung verfolgt dabei zwei Hauptziele: Erstens zielt sie darauf ab, Intermediäre zu reduzieren oder zu vermeiden. Zweitens soll die Liquidität des tokenisierten Vermögenswerts erhöht werden.

Sowohl körperliche als auch unkörperliche Vermögenswerte können mit Token verknüpft werden. Beispiele für körperliche Vermögenswerte sind Gold oder Kunstwerke. Zu den unkörperlichen Vermögenswerten gehören vorwiegend Finanzinstrumente (zB Aktien, Anleihen und Fonds-Anteile) und geistige Eigentumsrechte (etwa bei NFTs). Kern der Tokenisierung ist die rechtliche Verknüpfung zwischen dem Vermögenswert und dem Token.

1.9. Was sind NFTs?

NFT steht für 'Non-Fungible Token' und bedeutet lose übersetzt 'nicht mit anderen Stücken fungibler (austauschbarer) Token'. Ihren ersten Anwendungsfall hatten NFTs im Zusammenhang mit digitaler Kunst. Was ein NFT auszeichnet, ist wegen der rechtlichen Folgen der Einordnung bedeutend. MiCAR ist nämlich nicht auf Kryptowerte anwendbar, die einmalig und nicht mit anderen Kryptowerten fungibel sind. Die Pflichten unter MiCAR treffen also auf echte NFTs nicht zu.

Was ist aber ein echtes NFT? Um die Brücke zur analogen Welt zu schlagen: Blockchain-basierte Token, die 'technisch' nach einem NFT-Standard erstellt wurden (technische NFTs) können mit

durchnummerierten Bögen Papier verglichen werden. Diese können durch die Seriennummer individuell voneinander unterschieden werden. Für die Frage, ob sie fungibel oder austauschbar sind, ist aber nicht die Nummerierung ausschlaggebend, sondern der Einsatzzweck. Werden die Bögen mit unterschiedlichen Kunstwerken bemalt oder bedruckt, so sind sie nicht fungibel; werden sie für die Ausgabe durchnummerierter Wertpapiere, Eintrittskarten, Gutscheine oder Geldscheine mit demselben Gegenwert verwendet, so sind sie trotz Seriennummer dennoch fungibel. Dasselbe gilt für die digitale Implementierung dieses Gedankens auf DLT-Basis.

1.10. Was ist eine Wallet, was sind Adressen, private Schlüssel & Co?

Um zu erklären, was eine Wallet ist, muss eine Reihe anderer Begriffe erklärt werden. Nachfolgend wird daher der Versuch einer möglichst kompakten, aber dennoch vollständigen technischen Erklärung der Begriffe Wallet, Blockchain, Adresse, Privater Schlüssel, Transaktionswunsch und Transaktion sowie Block unternommen.

- **Wallet** ist die Kombination aus Adresse und privatem Schlüssel. Man unterscheidet:
    - **Wallet-Software** ist eine Software (App/Programm) zur Verwaltung von Wallets und zum Erstellen, Signieren und Übermitteln von Transaktionswünschen an die Teilnehmer der jeweiligen Blockchain.
    - **Cold Wallet** ist ein physisches Trägermedium wie beispielsweise Papier, Plastik oder Metall, auf dem eine Adresse und der dazugehörige private Schlüssel festgehalten sind.
    - **Paper Wallet** ist ein Unterfall der Cold Wallet, bei dem Papier als Trägermedium dient.
    - **Hot Wallet** bezeichnet eine Software, die mit dem Internet verbunden ist, und die zur Verwaltung von Adressen und privaten Schlüsseln verwendet wird, um Transaktionswünsche an die Teilnehmer einer Blockchain zu übermitteln.
    - **Non-custodial Wallet** oder **Self-custodial Wallet** ist eine Wallet, bei der niemand außer dem Nutzer selbst Zugriff auf die privaten Schlüssel hat.
    - **Custodial Wallet** ist eine Wallet, bei der die Verwahrung der privaten Schlüssel nicht durch den Nutzer selbst erfolgt (zB bei Exchanges).
- **Blockchain** bezeichnet eine Datenbankstruktur zur Speicherung von Transaktionen, die nur (blockweise) um neue Einträge ergänzt werden kann. Bereits bestehende Einträge bzw Blöcke in der Struktur sind unveränderlich in dem Sinne, dass jede Änderung die Datenintegrität zerstört und ein Manipulationsversuch sofort auffallen würde. Die Blockchain kann technisch als 'append-only'-Datenbank beschrieben werden, also eine Datenbank, deren Datenstruktur nur durch das Anfügen neuer Daten veränderlich ist.
- **Adresse** bezeichnet eine Zeichenfolge, die verwendet wird, um die Quelle oder das Ziel einer Transaktion auf einer Blockchain oder einen Smart Contract eindeutig zu identifizieren. Adressen werden erzeugt, indem bestimmte vorab festgelegte mathematische Schritte befolgt werden. Dies geschieht ohne Interaktion mit der Blockchain und ohne Anschluss an das Internet. Bei der Erzeugung neuer Adressen wird durch Einhaltung der

jeweiligen mathematischen Schritte ein passender privater Schlüssel erzeugt.

- **Privater Schlüssel** bezeichnet eine alphanumerische Zeichenfolge, die benötigt wird, um einen Transaktionswunsch so zu signieren, dass die darin beschriebene Verfügung über eine Adresse auf der Blockchain von Nodes des jeweiligen DLT-Netzwerks als authentisch akzeptiert wird, um schließlich als Transaktion in einem Block aufgenommen zu werden.

- **Transaktionswunsch** bezeichnet die gültig signierte und korrekt aufgebaute technische Instruktion zur Übertragung von Coins von bestimmten Adressen (Absender-Adressen) auf eine oder mehrere andere Adressen (Empfänger-Adresse), oder zur Interaktion mit einem Smart Contract, etwa das Aufrufen bestimmter Funktionen.

- **Transaktion** bezeichnet einen Transaktionswunsch, der in einem Block aufgenommen und damit Teil der Blockchain wurde.

- **Block** bezeichnet eine Zusammenstellung von Transaktionen. Durch die Aufnahme eines Transaktionswunsches in einen Block in der Blockchain wird dieser zur bestätigten Transaktion.

1.11. Was ist ein 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, sind dauerhaft auf der Blockchain gespeichert. Ein Smart Contract ist nach österreichischem Recht nicht automatisch auch ein zivilrechtlicher Vertrag.

1.12. Was ist Mining?

Mining ist der Versuch, Transaktionswünsche in einem Block zu bestätigen. Gleichzeitig versteht man unter Mining den Prozess, mit dem neue Einheiten eines bestimmten Kryptowerts auf einer Blockchain erzeugt werden. Beides ist korrekt und bezeichnet letztlich denselben Vorgang. Personen, die Mining betreiben, werden auch als Miner bezeichnet. Wer im Rahmen des Proof of Work oder Proof of Stake einen neuen Block mit Transaktionsdaten erzeugen darf, kann für sich selbst eine bestimmte Menge neuer Kryptowerte in die Blockchain einpflegen (Block Reward).

1.13. Was ist ein Konsensmechanismus?

Ein Konsensmechanismus ist ein Set an Regeln, nach denen sich bestimmt, welcher Miner oder welcher Staker (dazu sogleich) als nächstes einen Block mit Transaktionen der Blockchain anfügen darf. Es gibt hierzu verschiedene Verfahren; am bekanntesten sind Proof of Work sowie Proof of Stake.

1.13.1. Was ist Proof of Work?

Bei Bitcoin und vergleichbaren Blockchains bestimmt sich die Frage, wer als nächstes einen Block erzeugen darf, durch das Lösen eines komplexen mathematischen Problems. Derjenige, dem es als erstes gelingt, das Problem zu lösen, darf Transaktionen in einem neuen Block festhalten. Die Natur dieses mathematischen Problems bringt es mit sich, dass eine große Zahl verschiedener Lösungsmöglichkeiten durchprobiert werden muss, um eine Lösung zu finden. Je mehr Rechenkraft eine Person in einem solchen System aufwendet, desto besser sind die Chancen dieser Person, eine Lösung zu finden. Wem es letztlich gelingt, das Problem zuerst zu lösen,

kann jedoch nicht vorhergesagt werden, sondern hängt vom Zufall ab. Wurde eine Lösung gefunden, dann kann diese Lösung jedoch mit sehr geringem Aufwand von anderen Teilnehmern der Blockchain verifiziert werden.

Nur wegen dieses zufälligen Elements eignet sich das Verfahren für den Einsatz in der Blockchain. Und weil das Finden einer Lösung eine rechenintensive Angelegenheit ist, wird es auch als „Proof of Work“ bezeichnet – wer eine Lösung des Problems präsentiert, beweist damit, dass er Rechenzeit und Energie (also Arbeit, "Work") aufgewendet haben muss.

Das Proof of Work Verfahren dient also lediglich dazu, unter den Teilnehmern in der Blockchain Einigkeit darüber herzustellen, wer einen Block erzeugen darf. Je mehr Personen an diesem Prozess teilnehmen, je mehr Rechenleistung dem System also insgesamt zur Verfügung steht, desto schwieriger wird das mathematische Problem und desto rechenintensiver wird das Finden einer Lösung.

1.13.2. Was ist Proof of Stake?

Proof of Stake bezeichnet einen Konsensmechanismus, an dem nur teilnehmen kann, wer bereit ist, seine Regeltreue durch das Einsetzen eines Einsatzes (eines "Stakes") zu bekräftigen, wobei zur Entscheidung über die Frage, wer als nächstes eine für das Fortbestehen der Blockchain wesentliche Aufgabe wahrnehmen darf, zunächst eine Mehrzahl an Validatoren eine gemeinsame Zufallszahl generieren, auf deren Basis aus der Liste an Validatoren die nächste zuständige Person bestimmt wird.

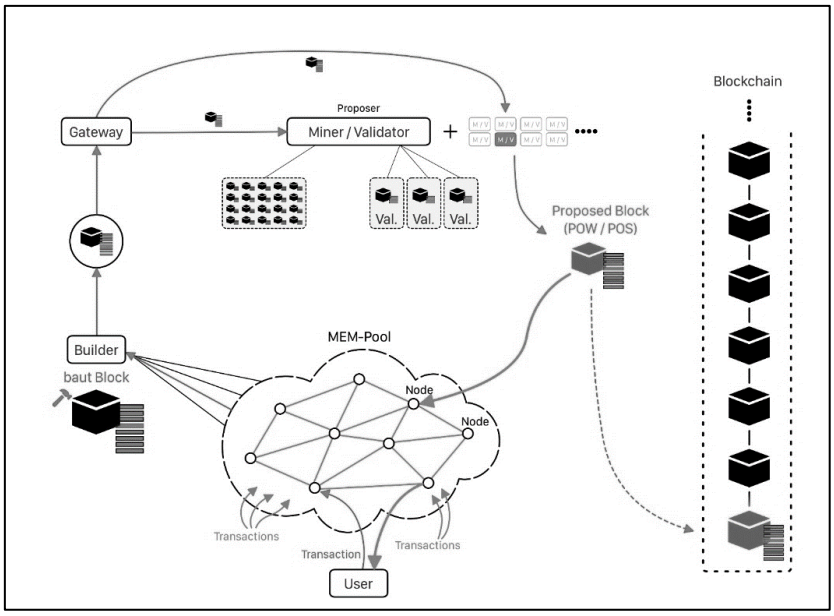
Validator ist eine Person, die nach Leisten des Stakes in die Liste der Validatoren aufgenommen wird, um neue Blöcke vorzuschlagen (proposing) oder die Gültigkeit eines vorgeschlagenen Blocks zu belegen (attesting). Bei Ethereum und vergleichbaren Blockchains müssen Personen hierzu zunächst Ether als Einsatz (Stake) hinterlegen. Bei Ethereum muss eine Mindestmenge von 32 Ether hinterlegt werden. Sobald der Stake hinterlegt ist, kann die Person einen Validator-Knoten betreiben. Hierbei handelt es sich um Hard- und Software, die mit dem Internet verbunden ist.

Wer als nächste Person aus der Liste an Validatoren ausgewählt wird, um einen Block zu erzeugen oder Blöcke zu attestieren, hängt vom Zufall ab. Konkret erzeugen eine Vielzahl von Validatoren jeweils eine eigene Zufallszahl. Diese Zufallszahlen werden in verschlüsselter Form den anderen Validatoren bekanntgegeben; nach einer gewissen Zeit reichen die Validatoren die Codes zur Entschlüsselung nach. Die dann entschlüsselten einzelnen Zufallszahlen bilden die Basis um einerseits (a) den nächsten Validator auszuwählen, der als nächstes einen Block erzeugen darf, und andererseits (b) die nächsten Validatoren auszuwählen, die gemeinsam nach demselben Muster eine neue Zufallszahl erzeugen. Verstoßen Validatoren gegen den Konsensmechanismus, etwa beim Falschvalidieren von Transaktionen, können sie einen Teil des Stakes verlieren (Slashing).

1.14. Welche Akteure spielen bei der Blockchain eine Rolle?

Bei der Antwort auf die Frage, welche Akteure bei der Blockchain eine Rolle spielen kann zunächst zwischen solchen Personen unterschieden werden, die zum Erhalt des Systems einen eigenen Beitrag leisten – Miner oder Validatoren – und solchen Personen, die das System nutzen und nicht zu seinem Erhalt beitragen. Darüber hinaus haben sich über die letzten Jahre weitere Rollen entwickelt, die eine Zwitterstellung einnehmen.

Zum besseren Verständnis der Rollen kann das nachfolgende Diagramm dienen:



Nutzer (User) übermitteln laufend neue Transaktionswünsche (Transactions) an das Netzwerk. Dort verbreiten sie sich im Pool unbestätigter Transaktionswünsche (MEM-Pool) unter allen Teilnehmern. Bei Bitcoin (Proof of Work) sind es die Miner bzw bei Ethereum (Proof of Stake) die Validatoren, die aus dem Pool unbestätigter Transaktionswünsche Blöcke bündeln und versuchen, diese unter Beachtung des jeweiligen Konsensmechanismus zum Teil der Blockchain zu machen.

Daneben haben sich jedoch weitere Rollen entwickelt. Ein Builder analysiert die Blockchain und öffentliche Transaktionswünsche dahingehend, ob Möglichkeiten bestehen, zusätzlich zu Transaktionsgebühren weitere Erträge zu erwirtschaften, etwa durch das Ausnutzen von Arbitragemöglichkeiten durch Interaktion mit verschiedenen Smart Contracts. Entdeckt der Builder eine günstige Gelegenheit, so versucht er, eigene Transaktionen – gegebenenfalls statt den öffentlichen Transaktionswünschen – in den Block einzupflegen.

Als Reaktion darauf hat sich als eigenes Geschäftsfeld das Anbieten privater Kommunikationskanäle etabliert, über die Nutzer mit Minern, Validatoren oder Buildern kommunizieren können. Der Nutzer übermittelt den Transaktionswunsch über diese privaten Kanäle, wobei nach dem gemeinsamen Verständnis der Transaktionswunsch nicht für eigene Zwecke analysiert, sondern direkt im Block aufgenommen wird. Dafür erhält der Miner, Validator bzw Builder vom Nutzer unter Umständen ein Entgelt.

Ein Builder kann nun versuchen, Blöcke, die er aus öffentlichen sowie privaten Transaktionswünschen zusammenstellt, selbst durch Beachtung des jeweiligen Konsensmechanismus zum Teil der Blockchain zu machen. Übernimmt der Builder diese Aufgabe selbst, so wird er auch Miner (bei Proof of Work) oder Validator (bei Proof of Stake) genannt.

Da selten einzelne Personen über ausreichend Rechenleistung bzw einer ausreichenden Anzahl an Validatoren verfügen, um regelmäßig neue Blöcke in die Blockchain einzupflegen, hat sich das System der sogenannten Builder/Proposer Separation entwickelt. Der Builder versucht dabei nicht mehr selbst, einen neuen Block in die Blockchain einzupflegen, sondern er bedient sich dazu des Proposers (Miners bzw Validators). Diese stellen ihre Rechenleistung bzw Validatoren zur Verfügung, um durch Beachtung des jeweiligen Konsensmechanismus den Block zum Teil der Blockchain zu machen.

Damit Miner bzw Validatoren als Proposer an diesem Prozess teilnehmen, ist allerdings ein ökonomischer Anreiz erforderlich. Schließlich könnten sie auch selbst öffentlich verfügbare Transaktionswünsche zu einem Block zusammenstellen und bestätigen. Hier kommen Gateways als Intermediäre zwischen Builder und Proposer ins Spiel. Gateways analysieren Blöcke, die sie von Buildern erhalten, und leiten sie an Proposer (also Miner oder Validatoren) weiter, wenn sie besonders hohe Transaktionsgebühren für den Proposer vorsehen. Kann ein Builder nicht nur aus dem öffentlichen Pool an Transaktionswünschen Blöcke zusammenstellen, sondern auch privat übermittelte Transaktionen berücksichtigen, so haben sie in der Regel einen Vorteil bei der Erstellung wirtschaftlich wertvollerer Blöcke gegenüber jenen Minern oder Validatoren, die nur aus dem öffentlichen Pool unbestätigter Transaktionswünsche eine Auswahl treffen können. Für Validatoren ist es daher wirtschaftlich sinnvoller über einen Gateway Blöcke von Buildern zu erhalten, als selbst Blöcke zusammenzustellen.

Zusammenfassend lassen sich die Funktionen beschreiben wie folgt:

- **Nutzer**: Person, die Transaktionswünsche an das jeweilige DLT-Netzwerk übermittelt, um mit der Blockchain auf die eine oder andere Weise zu interagieren, etwa um virtuelle Währungen zu übertragen, oder um mit Smart Contracts zu interagieren.

- **Proposer**: Person, die durch Befolgung des jeweiligen Konsensmechanismus versucht, die jeweilige Blockchain um einen neuen Block an Transaktionsdaten zu erweitern. Bei Proof of Work wird der Proposer auch Miner genannt, bei Proof of Stake wird der Proposer auch Validator genannt.

- **Builder**: Person, die aus dem Pool unbestätigter Transaktionswünsche, sowie anderen (über nicht-öffentliche Kanäle empfangene) Transaktionswünschen einen Block zusammenstellt. Im Rahmen der Builder/Proposer Separation übermittelt der Builder den Block mittels Gateways an den Proposer. Außerhalb der Builder/Proposer Separation fällt die Funktion des Builders und jene des Proposers beim **Miner** (Proof of Work) bzw beim **Validator** (Proof of Stake) zusammen.

- **Gateway**: Person, die von einer Mehrzahl an Buildern Blöcke entgegennimmt, um sie nach inhaltlicher Prüfung an Proposer weiterzuleiten. Ein Gateway ist somit ein Intermediär zwischen Builder und Proposer.

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

- **Miner:** 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.

- **Validator:** 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).[1]

Die **Blockchain-Technologie** kann und wird auch in anderen und unterschiedlichen Bereichen eingesetzt zB im Derivatehandel (Nasdaq-Initiative) oder Energiebereich (Direktvermarktung

[1] *Völkel* in *Piska/Völkel (Hrsg)*, Blockchain rules (2024), Rz 1.142 ff.

bei Solarenergie). Auch im behördlichen Bereich sind Varianten denkbar (Datennachweise, Ersatz behördlicher Register, Vereinfachung von Behördenverfahren).[2]

2. Grundlagen der EU-Verordnung über Märkte für Kryptowerte (MiCAR)

Am 30. Dezember 2024 tritt die europäische Verordnung über Märkte für Kryptowerte (abgekürzt oft als 'MiCA', 'MiCAR' oder auch 'MiCA-VO') in Kraft und wird in allen Mitgliedstaaten der EU unmittelbar gelten. Mit MiCAR besteht nun erstmals ein unionsweit einheitlicher Rechtsrahmen für das öffentliche Angebot von Kryptowerten und das Anbieten von Kryptowerte-Dienstleistungen. Neben umfangreichen Regeln zu diesen beiden Aspekten finden sich in der Verordnung auch Bestimmungen über die Verhinderung von Marktmissbrauch und Insiderhandel.

2.1. Anwendungsbereich

MiCAR erfasst alle natürlichen und juristischen Personen, die in der Europäischen Union Kryptowerte ausgeben, öffentlich anbieten, zum Handel zulassen möchten, oder wenn sie Dienstleistungen im Zusammenhang mit Kryptowerten erbringen möchten:

- Ausgabe ist der erstmalige Verkauf oder das sonstige erstmalige Inverkehrbringen eines Kryptowerts durch einen Emittenten. Das kann, muss aber nicht im Rahmen eines öffentlichen Angebots erfolgen.

- Ein öffentliches Angebot liegt rasch vor: Jede Mitteilung ist ein öffentliches Angebot, also zB auch der Inhalt einer Website, wenn sie ausreichend Informationen über die Angebotsbedingungen und die anzubietenden Kryptowerte enthält, um eine Kaufentscheidung zu ermöglichen. Ein öffentliches Angebot kann also nicht nur vom Emittenten, sondern von jedem gemacht werden, der den Kryptowert (weiter-)verkauft.

- Zulassung zum Handel bedeutet, dass der Kryptowert an einer Handelsplattform in der Union gelistet werden soll. MiCAR kann somit selbst dann einschlägig sein, wenn weder der Emittent seinen Sitz in der Union hat (keine Ausgabe) noch ein öffentliches Angebot in der Union erfolgt.

- Dienstleistungen sind die Verwahrung und Verwaltung von Kryptowerten, der Betrieb einer Handelsplattform, der Tausch von Kryptowerten gegen Geld oder andere Kryptowerte, die Ausführung von Aufträgen, die Platzierung, die Annahme und Übermittlung von Aufträgen sowie die Beratung und die Portfolioverwaltung.

Der Anwendungsbereich erfasst somit ein weites Spektrum der am Markt bekannten Tätigkeiten. Greift eine Ausnahme vom Anwendungsbereich, oder ist eine Tätigkeit nicht in MiCAR reguliert, so ist die Verordnung nicht einschlägig. Solche Tätigkeiten können also ohne Beachtung der Bestimmungen in MiCAR ausgeübt werden (allenfalls sind aber andere Bestimmungen einschlägig, wie etwa MIFID II bzw das WAG 2018).

MiCAR bezeichnet die Anbieter von Dienstleistungen auch sperrig als 'Kryptowerte-Dienstleister'; abgekürzt wird dies in aller Regeln mit dem Akronym 'CASP' (Crypto Asset Service Provider).

2.2. Allgemeine Anforderungen an alle CASPs

Alle CASPs treffen bestimmte allgemeine Pflichten. Hierzu zählt einerseits die Pflicht zu ehrlichem, redlichem und professionellem Handeln im besten Interesse des Kunden. Auch die Pflicht

[2] *Raschauer, N./Silbernagl, R.*: Grundsatzfragen des liechtensteinischen „Blockchain-Gesetzes“ – TVTG, in ZFR 1/2020, S 11.

zu redlichem, eindeutigen und nicht irreführenden Marketingmitteilungen und der Warnung vor Risiken gelten für alle CASPs.

Daneben sieht MiCAR gewisse Mindestkapitalanforderungen vor und enthält Regeln zur Unternehmensführung. Zudem verlangt MiCAR als allgemeinem Grundsatz von allen CASPs, dass sie Kryptowerte und Geldbeträge sicher aufbewahren, und zwar auf eine Weise, dass im Falle der Insolvenz des CASPs die Kryptowerte und Gelder der Kunden geschützt sind. Für Österreich bedeutet dies, dass ein Aus- oder Absonderungsanspruch existieren muss.

Alle CASPs müssen darüber hinaus über ein funktionstüchtiges Beschwerdemanagement verfügen und über angemessene Verfahren, um Interessenskonflikte zu erkennen, zu vermeiden und gegebenenfalls offenzulegen. Auslagerungen dürfen ausschließlich entsprechend den Vorgaben der MiCAR vorgenommen werden, und jeder CASP muss über einen Plan verfügen, wie seine Geschäfte ordnungsgemäß abgewickelt werden können, sollte er seine Tätigkeit einstellen.

Neben diesen allgemeinen Pflichten schreibt MiCAR eine Reihe an besonderen Pflichten vor, die jeweils die Anbieter bestimmter Dienstleistungen betreffen. Aufgrund des Umfangs dieser Anforderungen, werden diese hier nicht dargestellt.

3. Öffentliches Angebot von Kryptowerten

3.1. Grundlagen

MiCAR legt allgemeine Anforderungen für das öffentliche Angebot von Kryptowerten fest. Ein öffentliches Angebot kann dabei sehr rasch vorliegen. Jede Mitteilung ist ein öffentliches Angebot, also zum Beispiel auch der Inhalt einer Website, wenn sie ausreichend Informationen über die Angebotsbedingungen und die anzubietenden Kryptowerte enthält, um eine Kaufentscheidung zu ermöglichen. Auch Empfehlungen von Influencern in Videobotschaften oder auf Veranstaltungen können ein öffentliches Angebot darstellen. Es kann potentiell jeder Vertrieb erfasst sein. Wer Kryptowerte öffentlich anbietet, der wird auch als Anbieter bezeichnet.

Die weiter unten dargestellten Anforderungen an das öffentliche Angebot von Kryptowerten gelten aber nicht in jedem Fall. Wird ein Kryptowert:

- kostenlos angeboten (echte Airdrops; das heißt keine Gegenleistung, nicht einmal die Nennung persönlicher Daten), oder
- handelt es sich um einen schürfbaren Kryptowert (zB Bitcoin oder Ether) oder
- betrifft das Angebot Utility-Tokens für bestehende Produkte oder Dienstleistungen,

so ist der gesamte Abschnitt über das öffentliche Angebot von Kryptowerten unter MiCAR nicht anwendbar. Das heißt aber nicht, dass MiCAR insgesamt unanwendbar wäre. Die Regeln für Dienstleister gelten dennoch. So müssen CASPs etwa auch für solche Kryptowerte ein Whitepaper bereitstellen. Für Kryptowerte, die im Rahmen eines begrenzten Netzes genutzt werden, sieht MiCAR eine Reihe an Detailregeln vor.

Eine Besonderheit gilt für die hier vorgestellten ausgenommenen Kryptowerte (kostenlos, schürfbar, Utility-Token), wenn sie nicht an einem Handelsplatz gelistet sind. In diesem Fall ist auch für die Dienstleistungen des Verwahrens und Verwaltens sowie die Transferdienstleistung keine Zulassung unter MiCAR notwendig. Damit sollen etwa unternehmensinterne Kryptowerte von MiCAR gänzlich ausgenommen werden.

Die nachfolgend vorgestellten allgemeinen Grundsätze gelten also nur dann, wenn der Kryptowert nicht kostenlos angeboten wird, nicht schürfbar ist, oder im Fall eines Utility-Tokens das Produkt oder die Dienstleistung noch nicht besteht:

- Nur juristische Personen dürfen in der Union solche Kryptowerte öffentlich anbieten, also etwa eine Aktiengesellschaft oder Gesellschaft mit beschränkter Haftung, Das ist kein Widerspruch zum oben vorgestellten Anwendungsbereich von MiCAR, wonach auch Einzelpersonen erfasst sind. Auch diese werden von MiCAR erfasst, ihnen ist aber das öffentliche Angebot der hier gegenständlichen Kryptowerte untersagt.

- Ein Whitepaper muss vor dem öffentlichen Angebot des Kryptowerts erstellt, an die zuständige Aufsichtsbehörde übermittelt und auf der Website des Anbieters veröffentlicht werden. Dort muss es so lange verfügbar sein als Personen den Kryptowert halten, also potentiell zeitlich unbeschränkt. Soll ein vermögenswertereferenzierter Token öffentlich angeboten werden, muss das Whitepaper darüber hinaus von einer Aufsichtsbehörde genehmigt worden sein.

- Wird Marketing betrieben, so müssen die Marketingmitteilungen eindeutig als solche erkennbar sein, redlich, eindeutig und nicht irreführend sein, mit den Informationen im Whitepaper übereinstimmen, auf das Whitepaper verweisen und bestimmte in MiCAR festgelegte Disclaimer und Erklärungen enthalten. Zu Dokumentationszwecken sind die Marketingmitteilungen ebenfalls auf der Website des Anbieters zu veröffentlichen. Vor der Veröffentlichung des Whitepapers darf kein Marketing betrieben werden.[3]

Darüber hinaus müssen alle Anbieter bestimmte allgemeine Grundsätze erfüllen, siehe unter anderem Punkt 2.2.

3.2. Das Whitepaper

MiCAR übernimmt die Usance der Branche, ein Whitepaper zu erstellen und schreibt vor, welchen Inhalt es aufzuweisen hat. Neben Informationen über den Anbieter (oder die Person, die die Zulassung zum Handel beantragt) muss das Whitepaper Informationen über den Emittenten enthalten (wenn es nicht dieselbe Person ist), Informationen über den Betreiber der Handelsplattform (wenn dieser das Whitepaper erstellt), Informationen über das Projekt, das öffentliche Angebot, den Kryptowert, über die mit dem Kryptowert verknüpften Rechte und Pflichten, Informationen über die zugrundeliegenden Technologien, Informationen über Risiken und Informationen über klima- und umweltbezogene Auswirkungen des verwendeten Konsensmechanismus. Der letzte Punkt ist der Kompromiss einer Debatte, die wohl auch zum gänzlichen Verbot des Proof of Work auf europäischer Ebene hätte führen können.

Das Whitepaper muss redlich und eindeutig verfasst sein; es darf folglich nicht irreführend sein. Es darf keine wesentlichen Aspekte auslassen und muss in knapper und verständlicher Form vorgelegt werden. Es muss bestimmte Erklärungen und Disclaimer enthalten und darf keine Aussagen über einen künftigen Wert des angebotenen Kryptowerts enthalten.

Das Whitepaper darf grundsätzlich nur von demjenigen für ein öffentliches Angebot verwendet werden, der es erstellt hat. Führen andere Personen ebenso ein öffentliches Angebot desselben Coins oder Tokens durch, so dürfen diese Personen das Whitepaper nur nutzen, wenn dafür eine ausdrückliche Zustimmung vorliegt.

[3] *Völkel* in *Piska/Völkel*, Blockchain rules (2024), Rz 13.14 ff.

Das Whitepaper muss der zuständigen Aufsichtsbehörde (FMA, BaFin etc) spätestens 20 Arbeitstage vor dem Tag der Veröffentlichung (und damit auch vor dem Start des öffentlichen Angebots) übermittelt werden. Marketingmitteilungen müssen nur über Anforderung an die Aufsichtsbehörde übermittelt werden. Einer vorherigen Genehmigung des Whitepapers bedarf es im Allgemeinen nicht. Etwas anderes gilt nur im Fall von vermögenswertereferenzierten Tokens, und auch nur dann, wenn nicht eine Ausnahme greift (siehe weiter unten).

Nach der Veröffentlichung des Whitepapers dürfen die Kryptowerte (sofern gewünscht und der Aufsichtsbehörde zuvor mitgeteilt) in der gesamten Union angeboten werden. Die für den Token zuständige Aufsichtsbehörde übernimmt die Kommunikation diesbezüglich mit den Aufsichtsbehörden anderer Mitgliedstaaten. Es gibt für das öffentliche Angebot von Kryptowerten also einen unionsweiten Pass.

Mit der einmaligen Veröffentlichung des Whitepapers ist es aber noch nicht getan. Das Whitepaper muss aktuell gehalten werden, solange das öffentliche Angebot dauert oder die Kryptowerte zum Handel zugelassen sind. Treten neue Umstände ein, oder sind Fehler oder Ungenauigkeiten im Whitepaper vorhanden, muss es aktualisiert werden, wenn dies die Bewertung der Kryptowerte beeinflussen kann. Das geänderte Whitepaper ist der Behörde sieben Arbeitstage vor Veröffentlichung zu übermitteln. Alte Versionen des Whitepapers und von Marketingmitteilungen sind mindestens zehn Jahre lang auf der Website der Emittentin zu veröffentlichen.

Bei Utility Tokens für Waren oder Dienstleistung, die noch nicht bestehen bzw noch nicht erbracht werden, darf das öffentliche Angebot nicht länger als zwölf Monate dauern. Für das Whitepaper vermögenswertereferenzierter Token und von E-Geld-Token bestehen bestimmte Besonderheiten.

Ein Whitepaper ist dann nicht notwendig, und Marketingmitteilungen müssen nicht auf der Website dokumentiert werden, wenn:

- ein Angebot an weniger als 150 Personen erfolgt (Achtung: Nicht die Anzahl der Käufer ist entscheidend, sondern die Anzahl individueller Personen, denen ein Angebot gelegt wird); oder

- innerhalb von zwölf Monaten der Gesamtgegenwert aller ausgegebenen Kryptowerte höchstens 1 Million Euro beträgt; oder

- sich das Angebot ausschließlich an qualifizierte Anleger richtet und nur diese die Kryptowerte halten dürfen. Qualifizierte Anleger sind zum Beispiel beaufsichtigte Unternehmen, besonders große Unternehmen, öffentliche Einrichtungen oder institutionelle Anleger.

Die oben vorgestellten Ausnahmen laden freilich zum Missbrauch ein. Darum gilt nach MiCAR eine Gegenausnahme: Die genannten Ausnahmen gelten nicht, wenn der Anbieter (oder eine andere Person) die Absicht kundtut, den Kryptowert an einem Handelsplatz listen zu wollen. Wer also zum Beispiel einen Bitcoin-Hardfork durchführt, Coins pre-mined und diese verkauft, für den gilt die Ausnahme vom Anwendungsbereich. Wird aber zusätzlich in Aussicht gestellt, den Coin an einer Exchange listen zu wollen, so gilt die Ausnahme nicht und es ist ua ein Whitepaper zu erstellen.

Wer freiwillig ein Whitepaper erstellt, obwohl er es nicht müsste, der muss sich dennoch an die Vorgaben der MiCAR zum Inhalt des Whitepapers halten.[4]

[4] *Völkel* in Piska/Völkel, Blockchain rules (2023), Rz 13.22 ff.

4. Zugang: Zulassung, Konzession oder Gewerbe?

4.1. 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 Kryptowerten wie Bitcoin vorsehen, abhängig von der konkreten Ausgestaltung im Einzelfall, eine konzessionspflichtige Tätigkeit darstellen können. Insbesondere können Geschäftsmodelle im Zusammenhang mit Mining von Kryptowerten, sofern sie im Übrigen alle Kriterien eines AIF erfüllen, vom Anwendungsbereich des AIFMG erfasst sein (FAQ September 2024 zur Anwendung des AIFMG).[5]

Zur steuerlichen Beurteilung verweisen wir auf unseren Artikel zur Besteuerung von Kapitalvermögen im Privatvermögen.

4.2. Zulassung von Anbietern von Kryptowerte-Dienstleistungen (CASPs)

MiCAR unterscheidet zwischen zwei Gruppen, die Kryptowerte-Dienstleistungen erbringen dürfen. Entweder erwirbt ein Unternehmen eine eigene Zulassung unter der MiCAR oder es handelt sich um ein bereits beaufsichtigtes Unternehmen; konkret nennt MiCAR die Kreditinstitute, Zentralverwahrer, Wertpapierfirmen, Marktbetreiber, E-Geld-Institute, OGAW-Verwaltungsgesellschaften oder Verwalter alternativer Investmentfonds.

Juristische Personen bzw Unternehmen müssen eine Zulassung bei der zuständigen Behörde des Mitgliedstaats beantragen, wenn sie ihre Dienste an die breite Öffentlichkeit in der Union anbieten möchten. Um zugelassen zu werden, müssen Anbieter einen Antrag stellen, über einen Sitz in einem Mitgliedstaat verfügen, in dem sie zumindest einen Teil der Dienstleistungen ausführen und mindestens ein Geschäftsführer muss in der Union ansässig sein. Ähnlich wie Emittenten von Token werden zugelassene Anbieter im Rahmen der MiCAR mit der Zulassung über „Passporting"-Rechte verfügen; damit können sie mit nur einer Lizenz in der gesamten Union ihre Leistungen erbringen.

5. Vorteile und Risiken von Kryptowerten bzw Blockchain-Technologie

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

[5] https://www.fma.gv.at/wp-content/plugins/dw-fma/download.php?d=4879&nonce=999617385cac701b.

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.

Autoren:
Dr. Oliver Völkel, LL.M., Gründungspartner und Rechtsanwalt bei Stadler Völkel Rechtsanwälte
Dr. Alexander Kern, MSc, Geschäftsführer Fachverband Finanzdienstleister (WKO)

Anhang 1: Eine Erklärung der Blockchain

Piska/Völkel (Hrsg), Blockchain rules (2. Aufl., 2024) Rz 1.54 ff.

III. Die öffentliche Blockchain

A. Zweck der öffentlichen Blockchain

1.54 Wer von Distributed Ledger oder Blockchain spricht, meint damit zu allermeist die Technologie, die den bekannten virtuellen Währungen wie Bitcoin oder Ether zugrunde liegt. Doch hinter dem Schlagwort Blockchain verbergen sich in der Regel viele verschiedene Technologien, und neue Technologien werden laufend entwickelt.

1.55 Gemein ist den öffentlichen Blockchains 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 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.

1.56 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.

1.57 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. 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. Jeder notiert also seinen eigenen Punktestand.

1.58 Leider hat sich in die Gruppe ein unredlicher 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 unredlich handelt?

1.59 Die Gruppe entscheidet daher, dass alle Teilnehmer auf ihrem eigenen Stück Papier nicht nur die eigene Anzahl an Punkten notieren, sondern auch das Startguthaben aller anderen neunzehn Teilnehmer und die Transaktionen aller anderen. Möchte eine Person Punkte übertragen, solle sie das so laut in den Raum rufen, 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.

1.60 Diese Idee scheint gut zu funktionieren. Als A dem B fünf Punkte übertragen möchte, ruft er dies laut in den Raum und alle notieren 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 alle Rufe, manche missverstehen sie, 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.

1.61 Das Notieren jeder Transaktion durch alle Teilnehmer war eine gute Idee, in der Praxis aber zu fehleranfällig. Die Gruppe entscheidet daher, doch eine einzelne Person als „Aufzeichner“ zu bestimmen. Der Aufzeichner soll jedoch laufend abgelöst werden und am Ende seiner Funktionsperiode alle von ihm aufgezeichneten Übertragungen vorlesen. Alle anderen in der Gruppe schreiben diesen Block an Transaktionen mit und kontrollieren, ob die eigenen Transaktionen richtig aufgezeichnet sind. Bemängelt kein Teilnehmer den Block, so darf der Aufzeichner als Belohnung seinen eigenen Punktestand um eine vorab vereinbarte Menge erhöhen, was ebenfalls von allen in der Gruppe notiert wird. Macht der Aufzeichner hingegen einen Fehler, so wird der gesamte Block von allen Teilnehmern ignoriert. Neue Punkte erhält der Aufzeichner dann nicht. In einem solchen Fall müssen alle gewünschten Transaktionen eben dem nächsten Aufzeichner nochmals gesagt werden.

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

1.63 Das System ist freilich kompliziert. Denn um festzustellen, welchen Punktestand eine Person hat, genügt es nicht, einen einzelnen Zahlenwert zu kontrollieren. Stattdessen müssen die Teilnehmer, ausgehend von den ursprünglichen 100 Punkten alle Übertragungen nachvollziehen um den Punktestand der einzelnen Personen zu ermitteln. Dabei fällt den Teilnehmern aber noch ein Problem auf: Nicht nur der Aufzeichner kann Fehler machen, sondern auch die Gruppenmitglieder, wenn sie den vom Aufzeichner am Ende seiner Funktionsperiode vorgelesenen Block mitschreiben. Außerdem könnten die Teilnehmer der Versuchung unterliegen, vergangene Übertragungen zu verändern oder unter den Tisch fallen zu lassen. Nicht nur der Aufzeichner, sondern auch die anderen Teilnehmer könnten unredlich agieren. Wer entscheidet in so einem Fall, welcher Aufzeichnungsstand die wahren Geschehnisse wiedergibt?

1.64 Die Teilnehmer könnten sich darauf einigen, dass die Mehrheit entscheidet; Sicherheit würde dies aber nicht bieten. Stattdessen entscheiden sich die Teilnehmer für eine komplizierte, dafür sichere Lösung. Ausgehend von den aufgezeichneten Übertragungen (z.B. 5 von A an B; 7 von C an B; 2 von B an D) soll der Aufzeichner jeden Buchstaben in seinen Notizen durch einen Zahlenwert ersetzen, der seiner Position im Alphabet entspricht. Die Zahlen werden danach abwechselnd addiert und subtrahiert. Das Ergebnis dieser Berechnung nennt der Aufzeichner den Teilnehmern als Prüfwert zusätzlich zu den aufgezeichneten Übertragungen.

1.65 Berechnen die Teilnehmer denselben Prüfwert wie der Aufzeichner, so haben sie die Aufzeichnung richtig übernommen. Das Problem fehlerhafter Aufzeichnungen ist damit gelöst. Doch auch das Problem des unredlichen Teilnehmers lässt sich auf diese Weise lösen,

indem der nächste Aufzeichner bei der Berechnung des Prüfwerts für den nächsten Block den Prüfwert des vorherigen Blocks als Ausgangspunkt nimmt. Auf diese Weise werden die Prüfwerte aller Blöcke miteinander verbunden und es bildet sich eine Kette. Möchte ein unredlicher Teilnehmer eine Transaktion in einem Block ändern, so ändert dies den Prüfwert des Blocks; und weil der Prüfwert auch Teil des nächsten Blocks ist, ändert dies auch den Prüfwert des nächsten Blocks (usw). Ein Manipulationsversuch fällt damit sofort auf.

1.66 Die Teilnehmer in diesem Gedankenexperiment haben einen Mechanismus gefunden, der alle eingangs genannten Zwecke einer Blockchain erfüllt. Sie stellen Konsens darüber her, ob Übertragungen ihrer eigenen virtuellen Währung stattgefunden haben und in welcher Reihenfolge. Der Aufzeichnungsstand ist unveränderlich bzw würde jede Änderung der Historie wegen der Verknüpfung der Blöcke mittels Prüfwert sofort auffallen. Außerdem kommt das System ohne eine vertrauenswürdige zentrale Stelle aus.

1.67 Das System ist bereits sehr robust. Ein Problem gilt es aber noch zu lösen: Nach welchen Regeln sollen die Teilnehmer 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 Welt dieses Gedankenexperiments bieten sich viele 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 freilich weit schwieriger zu lösen.