IDW KNOWLEDGE PAPER

KRYPTOWÄHRUNGEN

STAND 05.05.2022

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER

INHALT

1. VORBEMERKUNGEN

Der rasante Anstieg und die hohe Volatilität von Kryptowährungen haben zu einem gestiegenen globalen Interesse und einer zunehmenden Kontrolle durch Organisationen, Investoren, Aufsichtsbehörden, Regierungen und andere Institutionen geführt.

Ende April 2022 beträgt die Marktkapitalisierung von Kryptowährungen rund 1,9 Bill. USD.[1] Die bedeutend höhere Preisvolatilität von Kryptowährungen im Vergleich zu herkömmlichen Fiatwährungen[2] und traditionellen Anlageklassen verdeutlicht den risikoreichen Charakter von Kryptowährungen.

Die am meisten verbreitete Kryptowährung ist der Bitcoin (BTC) mit einem wertmäßigen Marktanteil von rd. 41%.[3] Es sind mittlerweile jedoch über 19.000[4] verschiedene Kryptowährungen im Umlauf, darunter weitere bekannte wie z.B. Ether, Litecoin und Ripple. Jede dieser Kryptowährungen unterliegt ihren eigenen Regeln, kryptografischen Protokollen und Konsensmechanismen. Ein Umstand, der das Verständnis von Kryptowährungen besonders herausfordernd und auch eine Beschäftigung mit der dahinterstehenden Technik erforderlich macht.

Die Anzahl der Unternehmen, die Kryptowährungen halten bzw. Transaktionen mit Kryptowährungen eingehen, nimmt stetig zu. Gleichzeitig ist der Erfahrungsschatz der Unternehmen sowie ihrer Berater und Prüfer mit diesem Thema möglicherweise noch recht gering, so dass sie sich der Risiken und Herausforderungen ggf. noch nicht vollumfänglich bewusst sind.

Geschäftsleitung, Aufsichtsräte, Wirtschaftsprüfer und sonstige Interessierte sollen mit dem Knowledge Paper unterstützt werden, ein Grundverständnis über Kryptowährungen und die damit assoziierten Risiken und Herausforderungen zu erlangen.

Die Ausführungen in diesem Knowledge Paper reflektieren den Erkenntnis- und Diskussionsstand im Mai 2022 und erheben in der schnelllebigen Welt der Kryptowährungen und Blockchain-Technologie keinen Anspruch auf Vollständigkeit.

1. GRUNDLAGEN VON KRYPTOWÄHRUNGEN

1.1. Definition, Ein- und Abgrenzung

1.1.1. Virtuelle Währungen/Kryptowährungen im engeren Sinne

Unter virtuellen Währungen (auch Currency- oder Payment-Token bzw. Coins) werden digital dargestellte Werteinheiten von Währungen verstanden, die von keiner Zentralbank oder öffentlichen Stelle emittiert oder garantiert werden und grundsätzlich[5] nicht den gesetzlichen Status einer Währung oder von Geld besitzen, aber deren Werteinheiten von natürlichen oder juristischen Personen als Tauschmittel akzeptiert werden und auf elektronischem Wege übertragen, gespeichert und gehandelt werden können.[6] Virtuelle Währung hat keinen immanenten Wert; der Wert entsteht allein durch das Vertrauen der Nutzer und bestimmt sich über Angebot und Nachfrage[7].

Virtuelle Währungen zeichnen sich durch ein meist dezentrales, stets verteiltes und kryptografisch abgesichertes Zahlungssystem aus und werden deswegen auch als Kryptowährungen bezeichnet.[8] Die kryptografischen Kontrollen sollen sicherstellen, dass virtuelle Währungseinheiten nur von ihrem jeweiligen Eigentümer bzw. Berechtigten und nur einmal verwendet werden können. Die Schaffung von und Geschäftsvorfälle mit Kryptowährungen basieren auf der Blockchain- bzw. Distributed Ledger-Technologie.[9]

Kryptowährungen ermöglichen Einzelpersonen und Unternehmen, direkt miteinander Geschäfte zu tätigen (Peer-to-Peer), ohne einen Vermittler wie eine Bank oder ein anderes Finanzinstitut einzuschalten und ohne, dass die handelnden Parteien ihre „wahren“ Identitäten offenlegen müssen. Die handelnden Parteien treten lediglich mit ihren Wallet-Adressen bzw. öffentlichen Schlüsseln (vgl. Abschn. 1.2.2.) als Pseudonym nach außen in Erscheinung. Diese Pseudonyme können in einer öffentlichen Blockchain aufgrund der Festschreibung und Offenlegung der gesamten Transaktionshistorie nachverfolgt werden. Ohne Kenntnis einer Zuordnung der „echten“ bzw. „realen“ Namen zu Pseudonymen bleibt die „wahre“ Identität der dahinterstehenden Personen verborgen. Der im Kontext von Kryptowährungen verwendete Begriff der **Pseudonymität** ist jedoch nicht mit Anonymität zu verwechseln oder gleichzusetzen, bei der keine Nachverfolgung oder Identifizierung der handelnden Personen möglich ist.

Aus der Nutzerperspektive bietet die Pseudonymität den Vorteil, dass Transaktionen (relativ) unbeobachtet durchgeführt werden und bspw. von Personen, die in irgendeiner Form Verfolgung oder Repression ausgesetzt sind, als Zahlungsweg genutzt werden können (z.B. Whistleblower im Exil oder für Menschenrechte kämpfende Dissidenten). Andererseits sind Kryptowährungen durch die nicht zwingende Identifizierung auch bei (Cyber-)Kriminellen beliebt und werden z.B. für Lösegeldzahlungen bei Ransomware-Attacken, zur Geldwäsche aus kriminellen Aktivitäten, zur Finanzierung von Terrorismus und anderen illegalen Handlungen missbraucht.

1.1.2. Abgrenzung: Digitales Zentralbankgeld

Kryptowährungen sind nicht zu verwechseln mit digitalem Zentralbankgeld eines Landes, das einer digitalen Verbindlichkeit der Zentralbank entspricht und dessen Stabilität durch geld- und fiskalpolitische Maßnahmen von Zentralbanken und Regierungen gesteuert wird, die die Geldmenge nach eigenem Ermessen ausweiten können. Bei Kryptowährungen wie bspw. dem Bitcoin existiert keine Steuerung der Geldmenge durch eine zentrale Stelle. Die vorgegebene Inflation bei diesen Kryptowährungen ist durch einen individuellen Algorithmus zu Beginn bestimmt und kann nur durch einen Mehrheitsentscheid mit Wirkung für die Zukunft angepasst werden. Hierfür ist ein Konsens der Netzwerkteilnehmer notwendig; dies muss in einer demokratischen Wahl der Miner und/oder der Knoten des Netzwerkes (fullnodes) festgelegt werden. Somit folgen Kryptowährungen einer anderen Philosophie als digitales Zentralbankgeld und sind in dieser Hinsicht nicht mit diesem vergleichbar.

Digitales Zentralbankgeld befindet sich noch in einem frühen Entwicklungsprozess; derzeit setzen sich die Zentralbanken zahlreicher Länder mit der Einführung von digitalem Zentralbankgeld auseinander. Vereinzelt wurden und werden Pilotprojekte (z.B. in der Volksrepublik China) durchgeführt. Die Untersuchungsphase des Pilotprojekts der EZB zum digitalen Euro hat im Oktober 2021 begonnen.[10]

1.1.3. Kryptowerte im weiteren Sinne

Die Bezeichnung Kryptowährungen bildet mit der o.g. Definition bzw. der Beschränkung auf Tauschmittel nur eine Teilmenge der am Markt befindlichen digitalen Werteinheiten ab, die zumeist als Token oder Coins bezeichnet und unter dem Begriff der Kryptowerte zusammengefasst werden.

Kryptowerte können nach ihrer Funktionalität in Token und Coins unterschieden werden. Der Begriff „Coin“ bezeichnet üblicherweise Kryptowerte, deren Zweck auf ihre Funktion als Tauschmittel gerichtet ist. Unter „Token“ werden dagegen Kryptowerte verstanden, die dem Eigentümer zusätzliche Funktionalitäten bzw. Nutzen verleihen.[11] In der Praxis werden diese Begriffe mangels einer gesetzlichen oder in der Literatur einheitlichen Definition jedoch häufig synonym verwendet.

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) unterscheidet folgende Grundarten von Kryptowerten hinsichtlich ihres Hauptzweckes:[12]

- **Zahlungs-Token** (auch Payment-Token oder virtuelle Währung): digitale Token bzw. Coins auf der Basis der Blockchain-Technologie, die tatsächlich oder der Absicht des Organisators nach als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen akzeptiert werden oder der Geld- und Wertübertragung bzw. als Wertaufbewahrungsmittel dienen sollen. Siehe hierzu auch die Definition von Kryptowährungen i.e.S. in Abschn. 1.1.1. Ist der Wert eines Zahlungs-Tokens an eine nationale Währung oder andere Vermögenswerte gebunden, spricht man auch von **Stablecoins**. Kryptowährungen vermitteln keine Ansprüche gegenüber einem Emittenten.

- **Wertpapier(ähnliche) Token** (auch Asset-, Equity-, Security- oder Investment Token): Token, die ihren Inhabern mitgliedschaftliche Rechte oder schuldrechtliche Ansprüche vermitteln, welche mit denen eines Aktieninhabers oder Inhaber eines Schuldtitels vergleichbar sind.

- **Nutzungs-Token** (auch Utility- oder App-Token): Token, die Zugang zu einer digitalen Nutzung oder Dienstleistung vermitteln sollen, welche auf oder unter Benutzung einer Blockchain-Infrastruktur erbracht wird. Bei Nutzungs-Token wird häufig der Vergleich zu Gutscheinen oder Lizenzen gezogen. Sie berechtigen zum Bezug bestimmter Waren oder Dienstleistungen und verfügen über einen Emittenten, der zur Erbringung der Leistung verpflichtet ist.[13] Wenn Nutzungs-Token nur zur Einlösung gegenüber dem Emittenten berechtigen, nicht handelbar sind und aufgrund ihrer Ausgestaltung keine Erwartungen an ihre Wertentwicklung oder Unternehmensentwicklung des Emittenten abbilden, werden sie nach der Gesetzgebung und der BaFin-Verwaltungspraxis nicht als Kryptowerte und damit auch nicht als Finanzinstrumente eingeordnet.[14]

Kryptowerte können auch Kombinationen aus den o.g. Kategorien darstellen (**hybride Token**).

Während bei Kryptowährungen die eigene Blockchain die Basis bildet, bedienen sich Nutzungs- und Anlage-Token in der Regel bereits bestehender Blockchains als Basis.[15]

In der jüngsten Vergangenheit hat die sogenannte „Tokenisierung“ von Vermögenswerten der digitalen und realen Welt einen rasanten Aufschwung genommen. Hierbei werden (vergleichbar mit der Verbriefung in einer Urkunde) alle möglichen Rechte „greifbar" und handelbar gemacht, wobei Inhaber eines bestimmten Rechts nur ist, wer Inhaber des korrespondierenden Tokens ist. Hiernach können Kryptowerte auch nach ihrer Austauschbarkeit in

- fungible, d.h. austauschbare Token (wenn ein Vermögenswert in mehrere, gleichartige Token zerlegt wird) und

- nicht-fungible, d.h. nicht austauschare Token (entweder wenn es zu einem bestimmten Vermögenswert nur genau einen Token gibt oder wenn ein Vermögenswert in mehrere, unterschiedliche Token zerlegt wird)

unterschieden werden. Den intensiven Diskussionen in Fachkreisen folgend sind die rechtlichen Fragen beim Einsatz von sogenannten NFT (Non-Fungible Token) derzeit besonders vielfältig. Der Fokus des Knowledge Papers liegt nachfolgend auf Kryptowährungen (im engeren Sinne) und somit auf fungiblen Token.

1.2. Der Erwerb von Kryptowährungen

1.2.1. Erwerbsarten

Neben dem Erwerb gegen Fiatwährungen oder im Tausch gegen andere Kryptowährungen, z.B. auf Handelsplattformen, können Kryptowährungen auch auf andere Arten erworben bzw. hergestellt werden. Nachfolgend werden weitere gängige Arten der Erlangung von Kryptowährungen beschrieben.

Beim **Mining** wird im Rahmen des Konsensmechanismus Proof-of-Work Rechnerleistung zur Validierung von Transaktionen und der Erzeugung von Blöcken bereitgestellt. Als Gegenleistung erhält der erfolgreiche Miner, also derjenige, der den Block erstellt, Einheiten der virtuellen Währung gutgeschrieben.

Beim Konsensmechanismus Proof-of-Stake werden Nutzer für das langfristige Halten von Einheiten einer virtuellen Währung belohnt (**Staking**). Dabei werden vom Staker Einheiten der virtuellen Währung über einen bestimmten Zeitraum gesperrt. Während der Sperrzeit kann der Staker auf diese Einheiten der virtuellen Währung nicht zugreifen. Nach Ablauf der Sperrzeit erhält der Staker eine Belohnung in Form von zusätzlichen Einheiten der virtuellen Währung.

Fork (auch Split) bezeichnet die Gabelung oder Aufspaltung virtueller Währungen. Dazu kann es kommen, wenn das Protokoll der zugrundeliegenden Blockchain verändert wird, z.B. um neue Funktionen hinzuzufügen oder Sicherheitslücken zu beheben. Da Kryptowährungen maßgeblich auf der Open-Source-Idee beruhen, kann das Protokoll grundsätzlich von jedem eingesehen, heruntergeladen und verändert werden. In der Folge kann es zu Meinungsverschiedenheiten innerhalb des Nutzer- und Entwicklernetzwerkes zur weiteren Ausgestaltung der Blockchain kommen, die grundsätzlich im Konsens gelöst werden müssen. Wird kein Konsens gefunden, führt dies zur Aufspaltung der Blockchain. Dadurch entsteht eine zusätzliche Version der Kryptowährung, welche fortan neben der ursprünglichen Version der Kryptowährung existiert.

Kryptowährungen können auch bei einem **Initial Coin Offerings** (ICO) erworben werden. Ein ICO ist eine auf der Blockchain-Technologie beruhende Form der Finanzierung. Unternehmen sammeln – wie beim Crowdfunding oder Crowdinvesting – über Online-Plattformen Kapital – als Kryp-

towährung oder Fiatwährung – von vielen Anlegern ein. Anders als beim Börsengang (IPO – Initial Public Offering) erhält der Anleger bei einem ICO keine Aktien des Unternehmens, sondern Token, denen je nach Ausgestaltung unterschiedliche Funktionen zukommen können. Details zu der konkreten Ausgestaltung der Token sowie Informationen zum geplanten Geschäftszweck und den handelnden Personen finden sich in der Regel im zugrundeliegenden **White Paper**.[16] Die Ausführung erfolgt über **Smart Contracts**, in Blockchain implementierte Programmcodes, welche spezifische Aktionen in Abhängigkeit vom Eintritt vordefinierter Ereignisse oder Bedingungen automatisiert ausführen.[17]

Bei einem **Airdrop** („aus der Luft fallend") werden unentgeltlich (zusätzliche) Einheiten einer Kryptowährung an die Halter dieser Kryptowährung oder an die Öffentlichkeit gewährt. Sie werden häufig als Marketinginstrument oder zur Datensammlung eingesetzt.

1.2.2. Digitale Schlüssel und Signaturen

Der Besitz von Kryptowährung wird über digitale Schlüssel und digitale Signaturen geregelt. Digitale Schlüssel treten paarweise in Form eines privaten und eines hieraus abgeleiteten öffentlichen Schlüssels auf (Public-Key-Kryptographie).

Der **öffentliche Schlüssel** dient als Empfangsadresse für die Transaktion, vergleichbar mit der IBAN oder einer E-Mail-Adresse.

Der **private Schlüssel** ist nur dem Inhaber bekannt und dient als Passwort bzw. der Erzeugung digitaler Unterschriften zur Autorisierung von Kryptowährungs-Transaktionen. Er ist vergleichbar mit der PIN zu einem Bankkonto oder dem Passwort zu einem E-Mail-Account. Nur der private Schlüssel ermöglicht (zusammen mit dem öffentlichen Schlüssel) den Zugang zu den Einheiten einer virtuellen Währung, die auf der Blockchain gespeichert werden.

Öffentlicher und privater Schlüssel sind in einer mathematisch einzigartigen Weise derart verknüpft, dass ein öffentlicher Schlüssel einem privaten Schlüssel zugeordnet ist, jedoch durch die Einwegfunktion der mathematischen Beziehung aus dem öffentlichen Schlüssel praktisch[18] keine Rückschlüsse auf den privaten Schlüssel oder gar seine Rückrechnung möglich sind (**asymmetrische Kryptographie**).[19] Derjenige, der über den zum öffentlichen Schlüssel passenden privaten Schlüssel verfügt, kann gegenüber den anderen Teilnehmern der Blockchain unwiderlegbar nachweisen, dass ihm das Recht zusteht, die der Adresse zugeordneten Kryptowährungs-Bestände zu transferieren. Er weist dies nach, indem er die betreffende Transaktion mit seinem privaten Schlüssel signiert. Das Netzwerk kann anhand des öffentlichen Schlüssels und ohne die Offenlegung des privaten Schlüssels die Echtheit dieser **digitalen Signatur** prüfen. Geht der private Schlüssel, z.B. aufgrund eines Crashs oder Hacking verloren, sind die damit verbundenen Rechte für den Inhaber und das Netzwerk verloren. Denn dann kann niemand mehr den Nachweis erbringen, dass ihm die Berechtigung zu einem Transfer zusteht.

1.2.3. Kryptowährungs-Wallets

Um Kryptowährungs-Transaktionen durchführen und diese verfolgen zu können, benötigen Nutzer eine Wallet (digitale oder auch analoge Brieftasche oder Geldbörse). Bei Wallets handelt es sich um Anwendungen zum Erzeugen, Verwalten und Speichern privater und öffentlicher Schlüssel.

Wallets können wie folgt kategorisiert werden:

- **Online Wallets** (auch Web Wallets) sind auf einem fremden Server gehostet und werden von einem Wallet-Anbieter verwaltet. Dabei übernimmt häufig der Wallet-Anbieter die Kontrolle über die Schlüssel der Nutzer.
- **Software Wallets** befinden sich auf dem eigenen Computer bzw. Server (Desktop Wallet) oder auf dem Smartphone (Mobile Wallet).
- **Hardware Wallets** sind Geräte, die eine eigenständige Wallet auf spezieller Hardware (z.B. USB-Sticks wie Ledger Nano) betreiben und die bei Bedarf mit dem Internet verbunden werden.
- **Paper Wallets** sind Papieraufzeichnungen[20] der privaten Schlüssel. Wenn der Computer oder andere verwendete Geräte (Smartphone, Drucker) offline sind, wird eine Software verwendet, um einen Satz privater und öffentlicher Schlüssel mit den dazugehörigen Adressen für eine Cold Wallet zu generieren. Die öffentlichen und privaten Schlüssel der Wallet werden auf Papier ausgedruckt bzw. notiert.

Weiter wird zwischen Hot Wallets und Cold Wallets unterschieden. Hot Wallets sind permanent mit dem Internet verbunden, was zu einer schnelleren Verfügbarkeit der Token, aber auch zu einem größeren Risiko einer unautorisierten Entwendung führt. In Cold Wallets wird der private Schlüssel dagegen offline gespeichert und nur bei Bedarf mit dem Internet verbunden. Im Fall einer Paper Wallet ist für einen Transfer der damit verbundenen Kryptowährungen der private Schlüssel in eine Hot Wallet einzugeben. Für die kurze Zeit, die der Versand der Kryptowährung benötigt, ist der private Schlüssel der Paper-Wallet nicht mehr „kalt" und somit z.B. Viren und anderer Malware ausgesetzt.

2. DAS KRYPTOWÄHRUNGS-ÖKOSYSTEM

In den bisherigen Erläuterungen wurde bereits erkennbar, dass das Kryptowährungs-Ökosystem aus zahlreichen Teilnehmern und Dienstleistern besteht. Abbildung 1 gibt einen Überblick über diese Teilnehmer und Elemente des Kryptowährungs-Ökosystems.

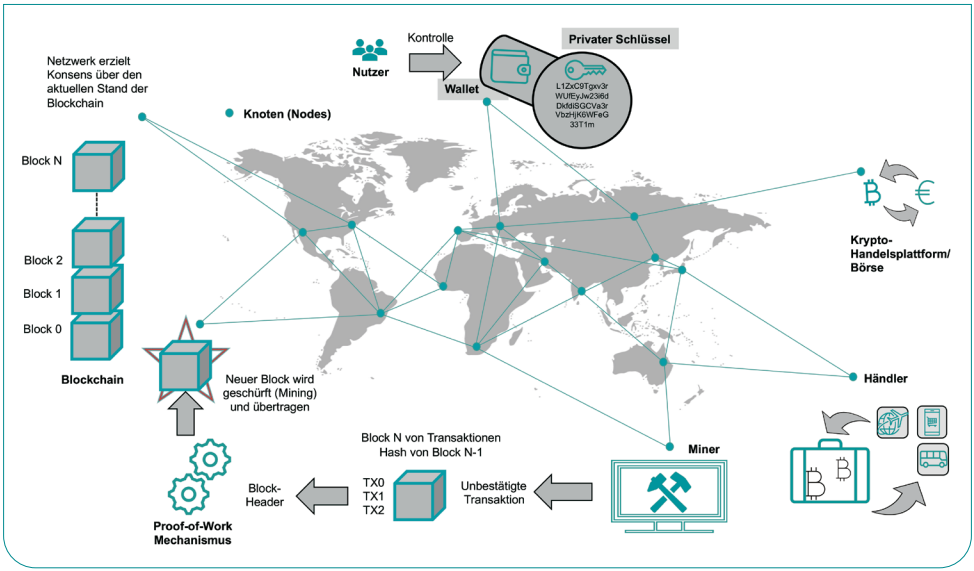

Abb. 1: Das Kryptowährungs-Ökosystem am Beispiel von Bitcoin (Quelle: Andreas M. Antonopoulos (2018): 2. Auflage, Bitcoin & Blockchain – Grundlagen und Programmierung – Die Blockchain verstehen, Anwendungen entwickeln)

2.1. Nutzer

Als Nutzer werden Privatpersonen und Unternehmen bezeichnet, welche Kryptowährungs-Transaktionen ausführen. Dies geschieht selten direkt (Peer-to-Peer) mittels eigenständig betriebenem Netzwerkknoten (Node), sondern meist über Dritte wie Kryptowährungs-Handelsplattformen oder -Börsen. In beiden Fällen werden in der Regel Leistungen von Wallet-Anbietern in Anspruch genommen.

2.2. Kryptowährungs-Handelsplattformen/-Börsen

Kryptowährungs-Handelsplattformen bzw. -Börsen sind rein digitale Plattformen, die einerseits einen Marktplatz für den Kauf und Verkauf bzw. die Übertragung von Kryptowährungen bieten, andererseits häufig eine reine Erwerbsplattform für Kryptowährungen darstellen. Inzwischen bieten viele Kryptowährungs-Börsen Schnittstellen zu klassischen Fiatwährungen, etwa durch die Option, Kryptowährungen per Kreditkartenzahlung zu erwerben.

Einige Handelsplattformen ermöglichen es den Benutzern, Kryptowährungen in einer Wallet auf der Plattform zu speichern. Dies ist eine wichtige Unterscheidung zwischen zwei Haupttypen von Kryptowährungs-Handelsplattformen:

- **Verwahrende Handelsplattformen** ermöglichen es den Nutzern, ihre Kryptowerte innerhalb der Plattform zu speichern; dadurch haben sie Zugriff auf ihre Gelder und können schnell handeln und Transaktionen durchführen. Die Verwahrung umfasst den Schutz der Kryptowerte innerhalb des Systems der Handelsplattform.
- **Nicht verwahrende Handelsplattformen** nehmen die Kryptowerte eines Benutzers nicht in Verwahrung, indem sie eine plattformeigene Wallet für sie unterhalten; vielmehr können Benutzer mehrere verschiedene Wallet-Technologien verwenden, um Transaktionen persönlich digital zu signieren und somit zu autorisieren.

Eine weitere Unterscheidung ist:

- **Zentralisierte Handelsplattformen** ermöglichen den Erwerb von Kryptowährungen gegen Fiatwährung. Ein weiteres Merkmal ist, dass es Transaktionen gibt, die nur auf der Plattform, aber nicht auf der Blockchain stattfinden (Bsp. Binance, Coinbase oder Kraken).
- **Dezentralisierte Handelsplattformen** bringen Käufer und Verkäufer zusammen und ermöglichen so den direkten Austausch zwischen den beiden Parteien (Peer-to-Peer), ohne selbst dabei als Vermittler aufzutreten[21] (bspw. UniSwap, SushiSwap).

2.3. Wallet-Anbieter

Wallet-Anbieter sind auf die Entwicklung und den Betrieb von kryptografischen Schlüsselverwaltungslösungen spezialisiert, um hochsensible private Schlüssel, die mit öffentlichen Blockchain-Adressen verbunden sind, vor Diebstahl oder Zerstörung zu schützen.

2.4. Verwahrer

Das Kryptoverwahrgeschäft wird im Kreditwesengesetz (KWG) als die Verwahrung, die Verwaltung und die Sicherung von Kryptowerten oder privaten kryptografischen Schlüsseln, die dazu dienen, Kryptowerte zu halten, zu speichern und zu übertragen definiert. Ähnlich wie

Depotbanken für Aktienwerte verwahren Kryptoverwahrer die Kryptowerte oder die privaten Schlüssel im Auftrag von Nutzern wie Hedgefonds, Vermögensverwaltern und anderen Unternehmen.

Die Verwahrfunktion wird häufig auch von Handelsplattformen oder Wallet-Anbietern wahrgenommen (z.B. blocknox GmbH für Bison/BSDEX – von Börse Stuttgart).

2.5. Miner

Das Erstellen neuer Blöcke und damit die Verifikation der durchgeführten Transaktionen erfolgt über ein Konsensverfahren, welches von der jeweiligen Blockchain vorgegeben ist.[22] Beim Proof-of-Work-Konsensmechanismus (z.B. Bitcoin) wird dieser Prozess Mining genannt. Als Miner werden Computer oder Computergruppen bezeichnet, die hierfür Rechnerkapazität bereitstellen.

Aufgrund der steigenden Rechnerleistung, die benötigt wird, um die Transaktionsdaten zu verarbeiten, bündeln Miner ihre Rechnerleistung mitunter in zentralen **Mining-Pools**. Zudem betreiben Cloud Mining-Dienste **Serverfarmen**, die auf Mining spezialisiert sind und ihre Kapazitäten an Kunden verkaufen oder vermieten.

2.6. Staker

Neben dem Mining im Proof-of-Work-Verfahren ist Staking im Proof-of-Stake-Verfahren (Bsp. Ether) als Konsensmechanismus anzuführen.

Jeder Teilnehmer eines solchen Blockchain-Netzwerkes kann seine Token „at stake" halten. Diese sind dadurch eingefroren und können über einen definierten Zeitraum nicht für Transaktionen genutzt werden. Im Gegenzug erhält der Staker proportional zur Menge der "at stake" befindlichen Kryptowerte die Möglichkeit, eingehende Blockchain-Transaktionen zu validieren und dafür Staking-Rewards in Form von weiteren Kryptowerten zu verdienen.

3. RECHTLICHE UND REGULATORISCHE EINORDNUNG

Aufgrund einer fehlenden allgemeingültigen Legaldefinition von Kryptowerten ist eine pauschale rechtliche Einordnung nicht möglich. Diese richtet sich vielmehr nach der konkreten Ausgestaltung der Kryptowerte und bringt teilweise Auslegungsfragen mit sich. Nachfolgend werden entsprechend dem Fokus dieses Papiers lediglich reine Kryptowährungen (Currency Token) betrachtet. Weil eine klare zivilrechtliche Einordnung als Sachen oder Rechte in der Regel nicht möglich ist, ist z.B. ein gutgläubiger Erwerb oder das Erlangen von „rechtlichem Eigentum" fraglich. Zur (aufsichts-)rechtlichen Einordnung von Kryptowährungen hat sich die BaFin in Mitteilungen und Hinweisen geäußert.[23] Ein Großteil der rechtlichen Einordnung wird derzeit darauf gestützt, weil sie Indikatoren zur rechtlichen Einordnung liefern können. Zur Herstellung von Rechtssicherheit ist letztlich der Gesetzgeber bzw. die höchstrichterliche Rechtsprechung gefordert.

Kryptowährungen stellen rechtlich stets Zahlungsmittel dar.[24] Sie haben allerdings grundsätzlich nicht den Status einer gesetzlichen Währung[25] oder von Geld i.e.S., weil sie digitale Abbildungen von Werten sind, die von keiner Zentralbank oder öffentlicher Stelle emittiert oder garantiert werden.[26] Ferner erfüllen reine Zahlungstoken weder die Merkmale eines Wertpapiers nach dem Wertpapierhandelsgesetz (WpHG) noch die eines elektronischen Wertpapiers nach dem elektronischen Wertpapiergesetz (eWpG), weil sie keine Rechte gegenüber dem Emittenten vermitteln. Sie stellen nach Auffassung der BaFin regelmäßig Recheneinheiten i.S.d. KWG dar.[27] Seit dem 1.1.2020 handelt es sich bei Kryptowerten um Finanzinstrumente i.S.d. KWG.[28]

Kryptowährungen sind regelmäßig kein E-Geld i.S.d. Zahlungsdiensterechts (ZAG), weil es an einer Forderung gegenüber einem Emittenten fehlt.

Kryptowährungen sind auch grundsätzlich keine Vermögensanlagen i.S.d. Vermögensanlagengesetzes, weil es (auch hier) an einem Anteil oder Forderung gegenüber einem Emittenten fehlt und für gewöhnlich keine anderen vermögenswerten Vorteile gewährt oder in Aussicht gestellt werden.

Die Qualifizierung als Finanzinstrument hat zur Folge, dass bei Betreiben bestimmter Geschäfte die Vorschriften des KWG zur Anwendung kommen und u. a. folgende Tätigkeiten einer Erlaubnispflicht gem. § 32 KWG der BaFin und weiteren Pflichten[29] unterliegen:

- Betrieb eines multilateralen Handelssystems (Kryptobörsen) (je nach Ausgestaltung Bankgeschäft oder Finanzdienstleistung)
- Aufstellen von Krypto-Automaten, an denen Kryptowährungen veräußert oder erworben werden können
- Kryptoverwahrgeschäft

Keiner Erlaubnispflicht unterliegen dagegen grundsätzlich:

- Ausgabe oder Mining von Token (Mining-Pools hingegen sind nach Auffassung der BaFin „in der Regel erlaubnispflichtig tätig")[30]
- Technische Hilfeleistungen (Bereitstellung von Wallets, Serverbereitstellung, Programmierung von Smart Contracts)[31], es sei denn, es handelt sich um Kryptoverwahrgeschäfte (vgl. oben)

4. RISIKEN UND HERAUSFORDERUNGEN

Aus der Art und den Eigenschaften der jeweiligen Kryptowährung bzw. der ihr zugrundeliegenden Blockchain-Technologie können sich Risiken ergeben, die in den folgenden Abschnitten dargestellt werden.

4.1. Technologie-/IT-Risiken

Kryptowährungen nutzen zur technischen Abbildung maßgeblich die Blockchain-Technologie, was bedeutet, dass hier ein Betriebsmodell mit rein digitalem Charakter besteht.

Hieraus resultieren spezifische IT-Risiken aus der eingesetzten Technik bzw. aus der Blockchain (z.B. Netzwerksicherheit, Datenintegrität, Vertraulichkeit) sowie (organisatorische) Risiken, die der Anwender selbst durch Kontrollen abdecken muss (bspw. Key Management).

Risiken aus der Nutzung der Blockchain
Öffentliche (public) Blockchains zeichnen sich dadurch aus, dass die Transaktions-Historie der Nutzer jedem zugänglich ist (Transparenz), der die Datenbasis herunterlädt. Zwar kann es für Dritte schwierig sein, einen Teilnehmer der

Blockchain zu identifizieren, sobald dieser aber identifiziert worden ist, ist seine gesamte Transaktions-Historie öffentlich, d.h. transparent und lückenlos verfolgbar.

Bei der Nutzung von Blockchain-Lösungen stellt der Datenschutz eine große Herausforderung dar, weil die Blockchain keine technische Möglichkeit bietet, die Daten nach gewisser Zeit zu löschen. Alle Transaktionen sind in der Blockchain öffentlich verfügbar. Insofern ist das Risiko zur inkonsistenten oder nicht vorhandenen Implementierung eines angemessenen Datenschutzes oder technischen Maßnahmen groß.

Ein weiteres Risiko kann in der unklaren oder nicht eindeutigen digitalen Identität bestehen. Die Blockchain-Technologie ermöglicht dem Benutzer, über den privaten Schlüssel Zugriff auf Blockchain-Netzwerke zu bekommen. Allerdings sind die digitalen Identitäten auf Blockchains oftmals nicht klar definiert (z.B. Dateneigentümer, Custodians, Betreuer, Prüfer). Durch die Pseudonymität ist die Zuordnung der Person zur digitalen Identität unzureichend definiert. Hiermit besteht das Risiko für ungenaues und inkonsistentes On-Chain-Tracking. Diesem kann man mit der Nutzung einer regulierten Kryptobörse/-handelsplattform oder eines Kryptoverwahrers entgegentreten.

Darüber hinaus kann die Datenintegrität innerhalb des gesamten Blockchain-Netzwerks durch nichtsichere Zugriffspunkte und unsicheren Netzwerkverkehr gefährdet werden (z.B. unzureichende Interoperabilität usw.). Die Integrität der Daten kann weiterhin in der Blockchain nicht gewährleistet werden, wenn unangemessene Änderungen an den Blockchain-Daten nicht durch die Blockchain-Transaktionen, sondern anhand anderer Mittel vorgenommen werden (z.B. durch 51%-Angriffe[32], Forks, unzureichenden Schutz und Integritätsprüfung (Proof-of-Work) externer Datenquellen).

Die Netzwerksicherheit spielt eine wichtige Rolle und kann ein wesentliches Risiko zur Datenintegrität darstellen. Weitere mangelhafte Blockchain-Sicherheitsmaßnahmen (z.B. Überwachung, Krisenmanagementverfahren, fehlende Sicherheitsstandards, schwache Netzwerkarchitektur, unsichere Implementierung oder Anpassung des Konsensmechanismus, unzureichender Schutz vor Blockchainspezifischen Angriffen, unzureichender Schutz vor allgemeinen Cyberangriffen usw.) können dazu führen, dass die Währung doppelt ausgegeben werden kann, oder es kann zur kompletten Spaltung des Netzwerks kommen.

Die Fortschritte der letzten Jahre in den Blockchain-Technologien haben neue „Second Layer"-Lösungen[33] notwendig gemacht. Eine solche Technologie ermöglicht dem Entwickler, in ein bestehendes Blockchain-Netzwerk neue Funktionalitäten zu implementieren oder bestehende Funktionalitäten zu verbessern oder zu erweitern. Ein Beispiel dafür ist das Ethereum-Netzwerk. Allerdings bringen die neuen Lösungen auch neue Risiken mit sich. Eine unangemessene Nutzung und Entwicklung von Smart Contract-Anwendungen könnte dazu führen, dass die alten Konditionen des Netzwerks nicht mehr greifen und ein einfacherer Weg gesucht wird, um die Transaktionszeit und die Effizienz zu erhöhen. Das könnte dazu führen, dass die bessere Leistung zu Lasten der Netzwerksicherheit erzielt wird.

Weiter spielt die Leistung der Blockchain eine wichtige Rolle. Die Netzwerkarchitektur wirkt sich negativ auf die Performance des Netzwerks aus. Das bedeutet, dass die Transaktionen mehrmals bestätigt werden müssen und es dadurch in kurzer Zeit zu erheblichen Verzögerungen der Transaktionen kommen kann, was ggf. konträr zu den Geschäftsanforderungen steht.

Weiterhin werden immer wieder neue Second Layer-Lösungen entwickelt, die den Austausch unterschiedlicher Kryptowährungen über Cross-Chain-Plattformen vereinfachen. Allerdings können durch die Komplexität und neue technische Erweiterungen Kryptowährungen bei dem Cross-Chain-Austausch verloren gehen.

Spezifische Kryptowährungsrisiken
Ein zentrales Risiko aus dem Einsatz einer Kryptowährung ist der Verlust oder Diebstahl des privaten Schlüssels, da dies zum irreversiblen Verlust oder Diebstahl des betroffenen Bestandes der Kryptowährung führt. Nur der private Schlüssel gewährt den Zugang zu den Einheiten einer virtuellen Währung und ist daher unbedingt vor Verlust oder Kompromittierung zu sichern. Eine Wiederherstellung des privaten Schlüssels ist nicht möglich. Daher ist ein adäquates Key Management unerlässlich.

Das Key Management sollte sich dabei auf die Einrichtung geeigneter und wirksamer Kontrollen über den gesamten Lebenszyklus privater Schlüssel (von der Sicherung bei der Erstellung über den Transport bis hin zur Aufbewahrung und zur Benutzung) erstrecken. Sofern die Verwahrung der Schlüssel von Dienstleistern übernommen wird, sind dessen Kontrollen zu überwachen und ggf. zu ergänzen.

Dieses impliziert auch, dass angemessene Maßnahmen in Bezug auf Cyber-Risiken umzusetzen sind, um ein mögliches Hacking bzw. Diebstahl von Kennwörtern und privaten Schlüsseln zu verhindern.

4.2. Risiken aus der Mitwirkung Dritter

Das Kryptowährungs-Ökosystem entwickelt sich schnell weiter. Die Verwendung von Kryptowährungen im Unternehmen wird daher in einer arbeitsteiligen Organisation in Bezug auf die Nutzung von IT-technischen und fachlichen Ressourcen sowie unter Effizienzgesichtspunkten häufig mit der Interaktion mit externen Dienstleistern wie Krypto-Handelsplattformen, -Verwahrern und Wallet-Anbietern einhergehen. Auch wenn bestimmte Aufgaben von externen Dienstleistern übernommen werden, verbleiben die mit den Kryptowährungen verbundenen Risiken dennoch im Unternehmen oder entstehen erst aus der Mitwirkung Dritter. Häufige Dienstleistungen sind:

- die Nutzung und Verwaltung kryptografischer Schlüssel,
- Verwahrung, Aufzeichnung, Auftragsausführung und Kundentransaktionen sowie
- Sicherheitsmaßnahmen der IT-Infrastruktur.

Es liegt in der Verantwortung der Geschäftsführung, angemessene Kontrollen über die von der Drittpartei erbrachten Dienstleistungen einzurichten. Dies kann die Etablierung von Prozessen

und Kontrollen für die Auswahl der Dienstleistungsunternehmen, die Einholung und Würdigung von Bescheinigungen über die Angemessenheit und Wirksamkeit des internen Kontrollsystems beim Dienstleistungsunternehmen, z.B. nach *IDW PS 951 n.F. (03.2021)*[34], und die Einrichtung von ergänzenden Kontrollen beim auslagernden Unternehmen umfassen.

Aufgrund der Art der Technologie werden die Dienstleistungen in den meisten Fällen komplexer sein als die eines traditionellen Drittanbieters. Ferner weisen die Dienstleister häufig einen eher geringen Reifegrad und bei entsprechendem Unternehmenserfolg ein schnelles Wachstum der Geschäftstätigkeit auf. Unternehmensstrukturen, Prozesse und Kontrollen inkl. deren Dokumentation werden häufig nicht in der gleichen Geschwindigkeit angepasst, woraus sich (temporäre) Prozess- und Kontrollrisiken ergeben können. Neben Art und Umfang der Dienstleistung sowie des Reifegrads des Unternehmens wird auch zu berücksichtigen sein, ob bzw. in welchem Ausmaß der Dienstleister regulatorischen Vorschriften unterliegt und ob über die Einhaltung entsprechender Vorschriften aussagekräftige und verlässliche Informationen, wie z.B. Zertifikate, Bescheinigungen oder Prüfungsberichte verfügbar sind.

4.3. Rechtliche und regulatorische Risiken

Der aktuelle Stand der rechtlichen und regulatorischen Einordnung von Kryptowährungen ist in Abschn. 3. beschrieben. Risiken ergeben sich vor allem aus der bestehenden Rechtsunsicherheit und aus der erwarteten Zunahme nationaler sowie internationaler Regulierungsbestrebungen.

Rechtsunsicherheit besteht darin, dass sich (bislang) bei Rechtstheoretikern und Rechtsanwendern in Teilen keine deutlich erkennbare herrschende Meinung hinsichtlich der rechtlichen Einordnung der Kryptowährungen und Token herausgebildet hat. Dies wird durch die Vielzahl an Kryptowerten sowie die Geschwindigkeit ihres Entstehungsprozesses zusätzlich erschwert. Damit sind Anspruchsgrundlagen aller Beteiligten bei der Ausführung einzelner Transaktionen und Dienstleistungen innerhalb sich derzeit etablierender Geschäftsmodelle (z.B. Übertragung von Kryptowährungen oder deren Verwahrung) unklar und Gegenstand verschiedener Auslegungen.

Die Globalisierung digitaler Infrastrukturen ermöglicht es, Kryptowährungen unabhängiger von (einzelnen) nationalen Legislativen zu halten und zu transferieren. Unterschiede in der Effektivität der nationalen Aufsicht eröffnen tendenziell den Anreiz, regulatorische Arbitrage zu betreiben. Dies führt wiederum zu einer verstärkten Regulierung in oder für (kryptotechnologisch) besser aufgestellten Länder.

Die Kryptowertetransferverordnung verpflichtet bspw. Kryptowertedienstleister dazu, Namen, Anschrift und Kontonummer der am Transfer beteiligten Parteien zu übermitteln und zu speichern. Diese Aufgabe der Pseudonymität gegenüber dem Kryptowertedienstleister ist im ursprünglichen Bitcoin-Whitepaper nicht vorgesehen (gewesen). Bei Nicht-Einhaltung drohen dem Dienstleister hohe Strafen.

Risiken aus der unklaren Mittelherkunft
Wie in Abschn. 1.1.1. dargelegt, ist eine Zuord-

nung von Pseudonymen zu den „wahren“ Identitäten der dahinterstehenden Organisationen oder Personen nicht vorgesehen.

Das bedeutet, verfügt man über Token, die in ihrer Transaktionshistorie Teil von Geschäften fragwürdiger Herkunft waren, wird man durch seine eigene Verfügung über diese Token ein Teil dieser Transaktionshistorie.

Durch die Offenlegung des vollständigen Transaktionsregisters allen Teilnehmern gegenüber (damit jedem Teilnehmer die Überprüfung der Integrität der Blockchain möglich ist) lässt sich (wenn auch mit erheblichem Aufwand) jeder Block in seine Bestandteile zerlegen und jede Transaktion lückenlos zurückverfolgen. Damit ist eine Anonymität, wie sie z.B. beim Börsenhandel[35] möglich ist, nicht gegeben.

Das heißt auch, dass die Identifikation der Beteiligten fragwürdiger Transaktionen der Vergangenheit jedem (anderen) Teilnehmer möglich ist.

Das birgt neben Reputationsrisiken (der eigene Name könnte unbemerkt in Zusammenhang mit fragwürdigen Transaktionen gebracht werden) auch strafrechtliche Risiken (bspw. Verdacht der Geldwäsche). Möglicherweise kann dem durch die Einrichtung von Compliance-Vorkehrungen entgegengewirkt und hierdurch der Nachweis einer ordnungsgemäßen Geschäftsorganisation erbracht werden.

Schließlich erschwert die Pseudonymität die Einhaltung von Transparenzanforderungen in vielen Bereichen, bspw. bei der Erfüllung von Sanktionsregimes- oder Meldepflichten oder Ermittlung und Darstellung von Beziehungen zu nahestehenden Personen.

4.4. Volatilität und Bewertung

Kryptowährungen verfügen, wie in Abschn. 1.1.1. festgestellt, über keinen inneren Wert, der Wert bestimmt sich allein über Angebot und Nachfrage ihrer Nutzer. Die Vergangenheit hat gezeigt, dass Kryptowährungen einer außergewöhnlich hohen **Preisvolatilität** unterliegen. Halter von Kryptowährungen sollten sich des Risikos eines Werteverlusts bewusst sein, im Extremfall bis hin zum Totalverlust, und die Wertentwicklung sowie ggf. identifizierte (Frühwarn-)Indikatoren laufend überwachen.

Aus der Preisvolatilität ergeben sich auch Herausforderungen für die **Bewertung** von Kryptowährungen. Da Kryptowährungen nicht unmittelbar Zahlungsströme generieren bzw. im Regelfall nicht mit Basiswerten unterlegt sind, aus denen sich solche ergeben, können üblicherweise keine Bewertungsmodelle herangezogen werden. Vielmehr resultiert die Wertfindung aus Angebot und Nachfrage. Maßgeblicher Aspekt der Wertfindung ist daher die Auswahl relevanter Handelsdaten von bspw. Kryptobörsen.

Schwierigkeiten bereitet dabei die Fragmentierung des Marktes in u.a. zentrale oder dezentrale Handelsplätze. Das Spektrum reicht dabei von Börsen mit Sitz in San Francisco (Coinbase oder

Kraken), Deutschland (JustTrade, BSDEX, TradeRepublic, Scalable Capital, Bison, Nuri) zu Antigua und Barbuda (FTX[36]) oder gänzlich unbekannt (Binance). Aufgrund der sehr unterschiedlich ausgeprägten Regulierungsniveaus gibt es üblicherweise keine Transparenz über den jeweiligen Preisfindungsmechanismus.

Zur Festlegung des relevanten Marktes sind Kriterien wie Handelsvolumen je Kryptowährung und Anzahl der Marktteilnehmer zu berücksichtigen.

Aus den genannten Risiken ergibt sich für Unternehmen die Notwendigkeit, interne Kontrollen einzurichten bzw. Kontrollen einbezogener Dienstleister zu überwachen oder zu ergänzen.

4.5. Nachhaltigkeitsaspekte

Im November 2021 betrug der monatliche Stromverbrauch für das Mining von Bitcoin 9,52 TWh, dies entspricht mehr als einem Viertel des Nettostromverbrauchs der Bundesrepublik in einem durchschnittlichen Monat des Jahrs 2019[37]. Es ist daher nachvollziehbar, dass mit zunehmender Popularität des Bitcoin der enorme Stromverbrauch stärker in die Kritik geraten ist, vor allem unter Berücksichtigung der Besonderheit des Mining, bei welcher der Großteil der aufgewendeten Rechnerleistung nicht zur Bestätigung genutzt wird und verpufft.

Demgegenüber ist zu erwarten, dass angesichts der zunehmenden Bedeutung von Umweltaspekten Konzepte wie bspw. Proof-of-Stake wichtiger werden, zumal sie ohne einen rechenintensiven Mining-Prozess auskommen.

Sollte es gelingen, durch effizientere Verfahren den Energieverbrauch drastisch zu reduzieren und so den ökologischen Aspekt der Nachhaltigkeit zu verbessern, können auch die positiven Argumente und Aspekte der Nachhaltigkeitsbilanz von Kryptowährungen stärker ins Gewicht fallen.

5. AUSWIRKUNGEN AUF DEN BERUFSSTAND

5.1. Auswirkungen auf die Abschlussprüfung

Mit der zunehmenden Zahl von Unternehmen, die Kryptowährungen besitzen oder unterschiedliche Arten von Transaktionen mit Kryptowährungen durchführen, steigt auch die Bedeutung in der Abschlussprüfung. Nachfolgend werden exemplarisch nur einige Besonderheiten bei der Prüfung von Kryptowährungs-Beständen bzw. -Transaktionen dargestellt.

Bereits bei der Frage der **Auftragsannahme bzw. -fortführung** kann es notwendig sein, dass sich der Abschlussprüfer auf der Grundlage seiner vorläufigen Kenntnisse über den Auftrag u.a. mit folgenden Fragestellungen beschäftigt:

- Prüfungsbereitschaft des (potenziellen) Mandanten inkl. Ausgestaltung, Implementierung und Dokumentation geeigneter Kontrollen sowie die Verfügbarkeit weiterer notwendiger Prüfungsnachweise. Insbesondere bei einer Beauftragung nach dem Abschlussstichtag kann es sinnvoll sein, im Vorfeld der Auftragsannahme zu klären, ob wesentliche Kryptowährungen zwischen Abschlussstichtag und Zeitpunkt der Abschlussprüfung transferiert wurden und ob für die Prüfung des Vorhandenseins der Kryptowährungen und das Innehaben der Verfügungsmacht über diese jeweils zum Abschlussstichtag Prüfungsnachweise erlangt werden können (vgl. Ausführungen weiter unten). Wenn ein Unternehmen keinen Prozess zur Nachverfolgung seiner Kryptowährungs-Transaktionen eingerichtet hat, können sich für die Prüfung besondere Herausforderungen bis hin zu einem möglichen Prüfungshemmnis ergeben.
- Der mit den Kryptowährungs-Transaktionen verfolgte Geschäftszweck einschließlich der Integrität des (potenziellen) Mandanten. Hierbei kann es notwendig sein, u.a. der Frage nachzugehen, ob Hinweise auf Beteiligung an Geldwäsche oder anderen kriminellen Aktivitäten vorliegen.
- Kenntnisse des (potenziellen) Mandanten im Hinblick auf den Besitz sowie die Transaktion von Kryptowährungen und Einrichtung eines geeigneten IKS. Sind die entsprechenden Voraussetzungen nicht gegeben, könnte möglicherweise ein Prüfungshemmnis bestehen.

- Ob das vorgesehene Prüfungsteam insgesamt über die für die Durchführung des Auftrags notwendigen Fach- und Branchenkenntnisse verfügt, relevante Erfahrungen vorliegen oder erlangt werden können und erforderlichenfalls Sachverständige zur Verfügung stehen.[38]

Bei der **Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen** kann es sein, dass der Abschlussprüfer Risiken im Zusammenhang mit dem Einsatz von Kryptowährungen identifiziert (z.B. die in Abschn. 4. genannten Risiken) und diese dann nach den Grundsätzen ordnungsmäßiger Abschlussprüfung (GoA) zu beurteilen hat, um die weiteren Prüfungshandlungen so zu planen, dass diese die beurteilten Risiken entsprechend behandeln.

Bei der **Prüfungsdurchführung** werden in der Regel die Prüfung des Vorhandenseins der Kryptowährungen sowie das Innehaben der Rechte an diesen, jeweils zum Abschlussstichtag, besondere Prüfungsschwerpunkte darstellen. Folglich werden als diesbezüglich relevante Aussagen der Rechnungslegung das „Vorhandensein" sowie „Rechte und Verpflichtungen" sein. Aufgrund der Volatilität von Kryptowährungen werden darüber hinaus oftmals der „Ausweis" sowie die „Genauigkeit, Bewertung und Zuordnung" relevante Aussagen in der Rechnungslegung darstellen.

Die Zuordnung einer bestimmten Anzahl von Kryptowährungen zu einer öffentlichen Adresse ist in der Regel aus der Blockchain ersichtlich. Hier wird es oft notwendig sein, dass der Abschlussprüfer, wenn nicht andere Informationen (z.B. Bestätigung Dritter) verfügbar sind, die Verlässlichkeit von Informationen aus der Blockchain als Prüfungsnachweis beurteilt. Dabei kann auch die Quelle der gewonnenen Informationen (öffentlich zugänglicher Block-Explorer, eigen- oder fremdentwickelte IT-Anwendungen, Betrieb eines eigenen Knotens) zu berücksichtigen sein. Als Nachweis für das Innehaben der Rechte an den Kryptowährungen wird die Kontrolle des Unternehmens über den zugehörigen privaten Schlüssel zu beurteilen sein. Dies kann bspw. über Mikrotransaktionen oder Sign-Message-Verfahren erfolgen. Hierdurch kann allerdings jeweils nur zum Prüfungszeitpunkt Verfügungsmacht nachgewiesen werden. Wenn zwischen Abschlussstichtag und Prüfungszeitpunkt Kryptowährungen transferiert wurden, stellt sich die Frage, wie das Innehaben der Rechte an diesen zum Abschlussstichtag retrograd nachgewiesen und geprüft werden kann. Zudem bedeutet das Innehaben der Verfügungsmacht über den privaten Schlüssel nicht zwangsläufig auch, dass das Unternehmen exklusiv über die Rechte an den zugehörigen Kryptowährungen verfügt. Der Abschlussprüfer wird sich hierfür üblicherweise nicht allein auf aussagebezogene Prüfungshandlungen stützen können, um ausreichende geeignete Prüfungsnachweise zu erzielen. Das Unternehmen sollte geeignete und wirksame Kontrollen über das Management des gesamten Lebenszyklus der privaten Schlüssel eingerichtet haben, auf die sich der Abschlussprüfer nach entsprechenden Angemessenheits- und Funktionsprüfungen stützen kann.

In Abschn. 4.2. wurden Risiken für das Unternehmen bei der Auslagerung auf Dienstleistungsunternehmen aus dem Kryptowährungs-Ökosystem aufgezeigt. In der Abschlussprüfung ist der Abschlussprüfer nach den GoA verpflichtet, diesbezüglich zu entscheiden, ob es sich bei dem

Dritten um ein Dienstleistungsunternehmen i.S.d. *IDW PS 331 n.F.*[39] bzw. des *(ISA [DE] 402)*[40] handelt. Um im Folgenden die Risiken zu beurteilen und weitere Prüfungshandlungen planen zu können, hat sich der Abschlussprüfer ein ausreichendes Verständnis von Art und Bedeutsamkeit der von dem Dienstleister erbrachten Dienstleistungen und von deren Auswirkungen auf die für die Abschlussprüfung relevanten internen Kontrollen der auslagernden Einheit zu verschaffen. Dazu hat er auch ein Verständnis darüber zu erlangen, wie das Unternehmen im Rahmen seiner Geschäftstätigkeit ausgelagerte Dienstleistungen in Anspruch nimmt. Es kann wichtig sein, dass sowohl das auslagernde Unternehmen als auch der Abschlussprüfer sich dabei bewusst sind, dass die an Krypto-Dienstleister delegierten Aufgaben in der Regel komplexer sein werden als sonstige typische ausgelagerte Dienstleistungen, wie z.B. die Lohnbuchhaltung. Ferner sind die Prozesse der Dienstleistungsunternehmen, ihre Kontrollsysteme und die Gestaltung angemessener Kontrollen möglicherweise noch nicht in dem Maße ausgereift, dass sie den korrespondierenden Prüfungsanforderungen vollumfänglich entsprechen. Der Prüfer wird bei seinen Überlegungen in der Regel auch den Umstand berücksichtigen, ob bzw. in welchem Ausmaß das Dienstleistungsunternehmen regulatorischen Vorschriften oder einer eigenständigen Prüfungspflicht unterliegt.

5.2. Erbringung von Assurance- und Beratungsdienstleistungen

Wirtschaftsprüfer können als vertrauensschaffende und unabhängige „Partei" Assurance-Dienstleistungen im Zusammenhang mit Kryptowährungen erbringen.

Neben Fragen, die sich unmittelbar auf die Darstellung von Kryptowährungen im Jahresabschluss und Lagebericht beziehen, ergeben sich zusätzliche Fragestellungen zur Funktionsweise und Zuverlässigkeit der den Kryptowährungen zugrundeliegenden Blockchain.[41] Daneben kommen folgende weitere Assurance- und Beratungsdienstleistungen in Betracht:

- Dienstleistungen zur Sicherstellung der ordnungsgemäßen Durchführung der Key Ceremony. Ein Unternehmen, welches Kryptowährungen für sich selbst verwahren möchte, sollte eine spezielle IT-Infrastruktur betreiben, bei der kryptographische Schlüssel zum Einsatz kommen. Diese Schlüssel werden bei der sogenannten Key-Ceremony erstellt und sind geheim zu halten. Diese Prozedur kann von einem Wirtschaftsprüfer begleitet werden.

- Darüber hinaus können Dienstleistungen zur Erstellung oder Prüfung des Internen Krypto-Kontrollsystems erbracht werden. Eine solche Prüfung könnte z.B. auf der Grundlage des *ISAE 3000 Revised*[42] oder im Falle eines Dienstleisters nach *ISAE 3402*[43] *bzw. IDW PS 951 n.F. (03.2021*) erfolgen.

- Sofern ein Unternehmen Smart Contracts, bspw. im Bereich Decentralized Finance (DeFi) oder für NFT nutzt, können vom Wirtschaftsprüfer Assurance-Dienstleistungen erbracht werden, bei welchen der Code auf

Schwachstellen beurteilt wird (Code Review). Dies ist vor allem für DeFi von Relevanz, da kleinste Fehler im Code zum Verlust der Kryptowährungen führen können.

- Von großer Relevanz im Bereich Kryptowährungen ist die Einhaltung von Anforderung zur Prävention von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen. Hierzu kann der Wirtschaftsprüfer ebenfalls mit Assurance-Dienstleistungen tätig werden[44].

- Ein neuer Bereich, welcher mehr und mehr an Bedeutung gewinnt, ist das Thema ESG. Kryptowährungen sind hiervon insofern betroffen, weil das Mining von speziellen Kryptowährungen, wie z.B. der Bitcoin, signifikante CO_2-Emissionen produziert. Unternehmen, welche solche Kryptowährungen produzieren, halten oder als Zahlungsmittel akzeptieren, könnten in Zukunft bei ESG-Ratings schlechter gestellt werden, wodurch sich ihre Refinanzierungskosten erhöhen könnten. Bestätigungsleistungen rund um das Thema ESG-konformes Mining können helfen, negativen Konsequenzen vorzubeugen.

6. AUSBLICK

Die in diesem Knowledge Paper aufgeführten Erläuterungen sollen die Basis dafür bilden, die zukünftige Entwicklung bei den Kryptowährungen oder anderen Kryptoprodukten besser einordnen zu können sowie das Bewusstsein für die damit zusammenhängenden Risiken für Unternehmen und deren Berater zu schärfen.

Die Märkte für Kryptoassets entwickeln sich rasant und auch in Zukunft ist mit vielen **neuer Kryptowährungen und -produkte** zu rechnen (z.B. Bitcoin-backed-Notes, Kryptowertpapiere, Utility-Token), welche neue Eigenschaften aufweisen und neue Herausforderungen mit sich bringen werden.

Während die **rechtliche Einordnung** mittlerweile etablierter Kryptowährungen künftig durch Gesetzesinitiativen und Gerichtsurteile konkretisiert werden wird, ist zu erwarten, dass neue Kryptowährungen und -produkte auch zu neuen Rechts-/Auslegungsfragen führen.

Mit dem rapiden Anstieg des Kryptomarkts nehmen auch die **Warnungen von Regulierungsbehörden** zu. Während früh vor Risiken für Verbraucher beim Kauf von Kryptowährungen gewarnt wurde[45], stuften viele die Risiken für die Finanzstabilität aufgrund der anfänglich geringen Marktkapitalisierung noch als nicht wesentlich ein[46]. Dies hat sich nun geändert: Der Finanzstabilitätsrat äußerte wegen des rasanten Wachstums im Kryptomarkt im Februar 2022 die Besorgnis, dass der Kryptomarkt bald einen Punkt erreicht haben könnte, an dem er wegen seines Umfangs, der strukturellen Anfälligkeit und der zunehmenden Verflechtung mit dem traditionellen Finanzsystem eine Bedrohung des globalen Finanzsystems darstellt.[47]

Zukünftig ist also mit einer deutlichen **Ausweitung der Regulierung** zu rechnen. Auf EU-Ebene soll die „Markets in Crypto-Assets" (MiCA) getaufte Regulierung für EU-weit einheitliche Regelungen im Krypto-Bereich sorgen. Ein aktueller Entwurf zur Anpassung der „Transfer of Funds Regulation" der EU sieht zudem Verschärfungen für Anti-Geldwäschemaßnahmen von Krypto-Dienstleistern bei bestimmten Krypto-Transaktionen vor[48], welche als „de facto"-Verbot von sogenannten „unhostet" Wallets gewertet werden könnten.

Das im Entwurf der MiCA-Regulierung zunächst vorgesehene Verbot für die Erbringung von Krypto-Dienstleistungen, die auf „ökologisch nicht nachhaltigen Konsensmechanismen" beruhen und somit ein drohendes Verbot für Kryptowährungen, die wie der Bitcoin auf dem Proof-of-Work-Verfahren basieren, wurde zwar in der Abstimmung im Wirtschaftsausschuss des EU-Parlaments im März 2022 von einer knappen Mehrheit abgelehnt; hierzu steht die Endabstimmung im Parlament jedoch noch aus. In jedem Fall wird unter **Nachhaltigkeitsaspekten** die Etablierung alternativer Verfahren wie z.B. Proof-of-Stake und die Suche nach neuen Verfahren zu erwarten sein, welche neue Herausforderungen bergen werden.

Angesichts der zunehmenden Ausbreitung von Kryptowährungen und der befürchteten Auswirkungen auf die Finanzmarktstabilität setzen sich derzeit auch die Zentralbanken zahlreicher Länder mit der Einführung von digitalem Zentralbankgeld intensiver auseinander. In der im Oktober 2021 gestarteten Untersuchungsphase zum digitalen Euro hat die EZB im März 2022 erstmals Studienergebnisse veröffentlicht, welche die Zahlungsgewohnheiten der Bürger und ihre Einstellung zu digitalen Zahlungen betreffen. Diese Ergebnisse werden in die weiteren Untersuchungen einfließen, an deren voraussichtlichem Ende im Oktober 2023 die Entscheidung steht, ob ein digitaler Euro entwickelt und eingeführt wird.

FUSSNOTEN

1 Vgl. www.coinmarketcap.com (Abruf: 26.04.2022).

2 Unter Fiatwährungen werden die von einer Regierung festgelegte Zahlungsmittel, die, anders als Gold- oder Silbermünzen (sog. Warengeld), über keinen inneren Wert verfügen, verstanden.

3 Vgl. www.coinmarketcap.com (Abruf: 26.04.2022).

4 Vgl. www.coinmarketcap.com (Abruf: 26.04.2022).

5 Eine Ausnahme bildet El Salvador, wo Bitcoin seit September 2021 als offizielles Zahlungsmittel zugelassen ist.

6 In Anlehnung an die Richtlinie (EU) 2018/843 vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/948 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU (ABl. L 156 vom 19. Juni 2018, S. 43-74).

7 A. Varmaz/N. Varmaz/Günther/Podding (2021) in: Omlor/Link (Hrsg), Handbuch Kryptowährungen und Token, Frankfurt a.M., Kap. 1, Rn. 53.

8 Vgl. https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160 (Abruf: 23.11.2021).

9 Eine Einführung in die Blockchain-Technologie und die damit verbundenen Implikationen für die Abschlussprüfung finden Sie in dem *IDW Knowledge Paper „Auswirkungen der Blockchain-Technologie auf Wirtschaftsprüfer"* aus Oktober 2019; https://www.idw.de/blob/119712/5773f7606aa432aab26d34ebbf1e8e14/down-knowledgepaper-blockchain-data.pdf (Abruf: 14.03.2022).

10 Siehe https://www.ecb.europa.eu/paym/digital_euro/html/index.de.html (Abruf: 21.03.2022).

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

12 Vgl. BaFin, Merkblatt Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token, WA-51-Wp 7100-2019/0011 und IF 1-AZB 1505-2019/0003, S. 5 f.

13 Vgl. Omlor (2021) in: Omlor/Link (Hrsg), Handbuch Kryptowährungen und Token, Frankfurt a.M., Kap. 6, Rn. 17.

14 Vgl. Schwennicke (2021) in: Omlor/Link (Hrsg), Handbuch Kryptowährungen und Token, Frankfurt a.M., Kap. 8, Rn. 34.

15 Vgl. BMF-Entwurf „Einzelfragen zur ertragsteuerrechtlichen Behandlung von virtuellen Währungen und von Token", abrufbar unter: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Einkommensteuer/2021-06-17-est-kryptowaehrungen.pdf?__blob=publicationFile&v=3 (Abruf: 17.03.2022).

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

17 Vgl. *IDW Knowledge Paper „Auswirkungen der Blockchain-Technologie auf Wirtschaftsprüfer"*, S. 12 f. (Abruf 24.05.2022).

18 In der Theorie kann der zu einer öffentlichen Adresse zugehörige private Schlüssel mittels Brute-Force-Suche, d.h. dem Ausprobieren aller potenziellen Kombinationen, herausgefunden werden. Praktisch ist dies auf Grundwegen des immensen Aufwands mit dem derzeitigen Stand der Technologie jedoch nahezu unmöglich.

19 Vgl. Müller, Bitcoin, Blockchain und Smart Contracts, Technische Grundlagen und mögliche Anwendungsbeispiel in der Immobilienwirtschaft, in: ZfIR 2017, S. 604.

20 Grundsätzlich ist auch die Aufzeichnung auf anderen Materialien wie Holz oder Metall denkbar.

21 Vgl. https://www.blockchain-insider.de/dezentralisierte-marktplaetze-dexes-und-was-sie-leisten-a-879522/ (Abruf: 30.05.2022).

22 Erläuterungen zu den Konsensmechanismen siehe z.B. *IDW Knowledge Paper „Auswirkungen der Blockchain-Technologie auf Wirtschaftsprüfer"* (Abruf: 30.05.2022).

23 Vgl. z.B. BaFin, Virtuelle Währungen/Virtual Currency (VC), geändert am 18.09.2020; BaFin, Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, vom 19.12.2013.

24 Vgl. Omlor, JZ 2017, S. 754, 760.

25 Eine Ausnahme bildet bislang die Republik El Salvador, in der im Juni 2021 ein entsprechendes Gesetz verabschiedet wurde, mit der auch Bitcoins als Zahlungsmittel akzeptiert werden.

26 Vgl. Omlor (2021) in: Omlor/Link (Hrsg), Handbuch Kryptowährungen und Token, Frankfurt a.M., Kap. 6, Rn. 24 ff.

27 Vgl. BaFin, Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, vom 19.12.2013. Diese Auffassung hat das KG Berlin, Urt. v. 25.9.2018, BKR 2018, 473 nicht geteilt.

28 Eingeführt mit dem Gesetz zur Umsetzung der Änderungsrichtlinie zur 4. Geldwäscherichtlinie vom 12.12.2019 BGBl. I, S. 2602.

29 So löst die Erbringung erlaubnispflichtiger Dienstleistungen regelmäßig auch eine gesetzliche Prüfungspflicht des Abschlusses aus, die auch die Prüfung der Einhaltung der aufsichtsrechtlichen Anforderungen durch den Abschlussprüfer einschließt.

30 Vgl. BaFin, Virtuelle Währungen/Virtual Currency (VC), geändert am 18.09.2020; eine Erlaubnispflicht verneinend: Schwennicke (2021): in Omlor/Link (Hrsg), Handbuch Kryptowährungen und Token, Frankfurt a.M., Kap. 8, Rn. 76 ff.

31 Vgl. Schwennicke (2021): in Omlor/Link (Hrsg), Handbuch Kryptowährungen und Token, Frankfurt a.M., Kap. 8, Rn. 87 ff.

32 Die Funktionsweise der Blockchain erfordert Konsens um Transaktionen zu bestätigten oder hinzuzufügen. Gelingt es einem Miner oder einer Gruppe von Minern, über 50% der Arbeits- bzw. Rechenleistung im Netzwerk zu kontrollieren, so kann dieser Umstand im Proof-of-Work-Verfahren dazu missbraucht werden, die Blockchain zu manipulieren, da er oder sie die „Mehrheit" im Konsensmechanismus abbilden.

33 Second-Layer-Lösung ist eine Plattform außerhalb der Blockchain, die eine Peer-to-Peer-Transaktion zwischen zwei zustimmenden Parteien und einer dritten, überwachenden Partei beinhaltet, die den Wert der Transaktion garantiert. Lösungen der zweiten Schicht sind wie Zahlungskanäle mit umfangreichen Transaktionsraten und blitzschnellen Verarbeitungsfähigkeiten, aber sie sind immer noch mit der Blockchain verbunden. Am Ende der Transaktionen in der zweiten Schicht schreibt das System den Wert zurück in die Hauptkette/Blockchain.

34 *IDW Prüfungsstandard „Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen" (IDW PS 951 n.F. (03.2021))*.

35 Unter Einschaltung eines zentralen Kontrahenten, https://www.xetra.com/xetra-de/handel/handelsmodelle/fortlaufender-handel-mit-auktionen (Abruf: 04.02.2022).

36 Quelle: https://about.ftx.com (Abruf 20.12.2021).

37 Im Jahr 2019 betrug der Stromverbrauch 439,8 TWh, und damit 36,6 TWh pro Monat, im Jahr 2020 418,6 TWh (vorläufig) [Quelle: Stromabsatz und Erlöse der Elektrizitätsversorgungsunternehmen nach Abnehmergruppen; https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Energie/Verwendung/Tabellen/stromabsatz-haushalt.html; Abruf: 20.12.2021].

38 Vgl. *IDW QS 1*, Tz. 75.

39 *IDW Prüfungsstandard: „Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen" (IDW PS 331 n.F.)*.

40 International Standards on Auditing [DE]: „Überlegungen bei der Abschlussprüfung von Einheiten, die Dienstleister in Anspruch nehmen" (ISA [DE] 402).

41 Vgl. *IDW Knowledge Paper „Auswirkungen der Blockchain-Technologie auf Wirtschaftsprüfer"*.

42 International Standards on Assurance Enagements „Assurance Engagements other than Audits or Reviews of Historical Financial Information" (ISAE 3000 Revised).

43 ISAE „Assurance Reports on Controls at a Service Organization" (ISAE 3402).

44 Vgl. z.B. *IDW Entwurf eines Praxishinweises „Ausgestaltung und Prüfung eines Compliance Management Systems zur Prävention von Geldwäsche und Terrorismusfinanzierung gemäß IDW EPS 980 n.F. (10.2021)“.*

45 Vgl. z.B. die gemeinsame Warnung der europäischen Aufsichtsbehörden für Wertpapiere (ESMA), Banken (EBA) und Pensionen (EIOPA) aus Februar 2018, https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-risks-in-buying-virtual-currencies (Abruf: 18.03.2022).

46 So z.B. noch der Finanzstabilitätsrat im Juli 2018, vgl. https://www.fsb.org/2018/10/fsb-sets-out-potential-financial-stability-implications-from-crypto-assets/ (Abruf: 18.03.2022).

47 Vgl. https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/ (Abruf: 18.03.2022).

48 Siehe Entwurf vom 21.04.2022 unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8293_2022_INIT&qid=1650982770259&from=EN (Abruf: 26.04.2022).

Dieses IDW Knowledge Paper wurde von der IDW Arbeitsgruppe „Kryptowährungen“ entwickelt.

Wir freuen uns über Ihre Anmerkungen: Sie können sie direkt an Frau Valerie Wachter, Institut der Wirtschaftsprüfer in Deutschland e.V., Postfach 320580, 40420 Düsseldorf oder an valerie.wachter@idw.de senden.

INSTITUT DER WIRTSCHAFTSPRÜFER IN DEUTSCHLAND E.V.
WIRTSCHAFTSPRÜFERHAUS

Tersteegenstr. 14
40474 Düsseldorf

Postfach 32 05 80
40420 Düsseldorf

Telefon: +49 (0) 211/4561-0
Telefax: +49 (0) 211/4561097

E-Mail: info@idw.de
Web: www.idw.de

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER