Dieses Knowledge Paper wurde vom Fachausschuss Informationstechnologie (FAIT) des IDW verabschiedet.

Ansprechpartnerin:

WP StB Grit Baum
Institut der Wirtschaftsprüfer in Deutschland e.V.
Postfach 320580
40420 Düsseldorf

Wir freuen uns über Ihre Anmerkungen. Sie können diese direkt an das Institut der Wirtschaftsprüfer in Deutschland e.V., Postfach 320580, 40420 Düsseldorf, oder an digitales@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

KNOWLEDGE PAPER

AUSWIRKUNGEN DER **BLOCKCHAIN-TECHNOLOGIE** AUF WIRTSCHAFTSPRÜFER

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER

INHALT

VORBEMERKUNGEN

Das Thema Blockchain ist eines der bewegenden Themen in der Wirtschaftswelt. Die Blockchain-Technologie wird als eine der großen Innovationen im Bereich der Informationstechnologie gesehen, ein neues „Internet der Werte“. Das disruptive Potenzial der Blockchain-Technologie für die Art und Weise, wie zukünftig der Transfer und die Aufzeichnung von Werten und Rechten organisiert werden kann, wird nicht weniger als „revolutionär“ für die Geschäftswelt der Zukunft eingestuft. In der öffentlichen Wahrnehmung ist das Thema auch aufgrund der Kryptowährung Bitcoin in den breiten Fokus gerückt.

Unternehmen unterschiedlichster Branchen ergründen momentan das Potenzial der Blockchain-Technologie für die bestehenden und für neue Geschäftsmodelle. Erste Piloten und Anwendungen werden entwickelt, die auf einer Blockchain basieren. Auch wenn betriebswirtschaftlich sinnvolle Anwendungsfälle derzeit noch nicht so weit verbreitet sind, wie anzunehmen wäre, werden Blockchains unweigerlich auch aus der Perspektive der Wirtschaftsprüfung an Bedeutung gewinnen.

Dieses Knowledge Paper soll die Grundprinzipien der Blockchain-Technologie näher beleuchten und der Frage nachgehen, warum diese dazu geeignet sein können, solch eine Wirkung zu entfalten. Neben einer Erläuterung der Grundlagen der Blockchain-Technologie (Kap. 1) geht es der Frage nach, welche Anforderungen erfüllt sein müssen, damit die Blockchain-Technologie als Lösung in Frage kommt, zeigt praktische Anwendungsmöglichkeiten auf (Kap. 2), stellt die mit der Technologie derzeit verbundenen Risiken und Herausforderungen dar (Kap. 3) und betrachtet die Auswirkungen auf den Berufsstand (Kap. 4).

Wirtschaftsprüfer, Aufsichtsräte, Geschäftsleitung und sonstige Betroffene und Interessierte sollen mit dem Knowledge Paper unterstützt werden, in der heutigen schnelllebigen Zeit den Überblick zu bewahren.

Die Ausführungen in diesem Knowledge Paper reflektieren den Erkenntnis- und Diskussionsstand zum Zeitpunkt seiner Veröffentlichung im Oktober 2019 und erheben in dem inzwischen breiten Feld der Blockchain-Technologie keinen Anspruch auf Vollständigkeit.

1. GRUNDLAGEN DER BLOCKCHAIN-TECHNOLOGIE

1.1. Grundprinzipien eines „shared“ und „distributed“ Ledger

Das Standardmodell der Blockchain wurde erstmals 2008 im Bitcoin-Whitepaper beschrieben. Dieses Standardmodell stellt die Basis für alle darauffolgenden Blockchain-Modelle dar.

Unter Blockchain versteht man im Allgemeinen ein System eines gemeinsamen (shared), verteilten (distributed) Grundbuchs (ledger).

Gemeinsam bedeutet, dass nur ein Grundbuch genutzt wird, in dem die Transaktionen aller Teilnehmer erfasst werden. Dabei kann jeder Teilnehmer das Grundbuch jederzeit einsehen.

Verteilt bedeutet, dass das Grundbuch mit den kompletten Buchungen auf allen beteiligten Rechnern („nodes“) einer Blockchain im Rahmen eines peer-to-peer Netzwerkes gespeichert ist. Dies hat zur Folge, dass es keine zentrale Instanz gibt. Vielmehr ist eine Vielzahl von Teilnehmern/Rechnern gleichberechtigt und hat dieselben Information vorliegen. Somit hat auch der Ausfall eines oder mehrerer Rechner im Blockchain-Netzwerk keine Auswirkungen auf die Integrität der Daten.

Die Blockchain ist eine gemeinsam genutzte und verteilt gespeicherte Datenbank, die die aktuellen Besitzverhältnisse an einer genau bezeichneten Sache sowie alle historischen Besitzwechsel bzw. Transaktionen in Bezug auf diese Sache enthält.

Hinsichtlich der mit der Blockchain dokumentierten Rechte und Pflichten ist somit allen Beteiligten der Blockchain transparent, wer wann welche Rechte und Pflichten eingegangen ist und wie diese sich über die Zeit entwickelt haben.

Der Begriff Blockchain bezeichnet dabei das logische und technische Verfahren zur Erfassung, Verifizierung und Speicherung von Transaktionen (Werten) und zur Fortschreibung der Datenbank, die im Wesentlichen auf mathematischen Modellen und deren informationstechnologischen Umsetzung basiert.

Transaktionen können zwischen Personen, zwischen Personen und Unternehmen, zwischen Unternehmen und Personen, zwischen Unternehmen und Unternehmen, staatlichen Institutionen oder direkt zwischen Maschinen ablaufen.

Bei den transferierten Werten kann es sich sowohl um Werte monetärer als auch nichtmonetärer Art handeln.

Wird eine Transaktion im Blockchain-Netzwerk angestoßen, wird jeder Teilnehmer im Netzwerk darüber informiert, dass eine neue Transaktion zur Verifizierung bereitsteht. Jede Transaktion wird nach bestimmten festgelegten Regeln durch die Netzwerkteilnehmer validiert. Durch die Kombination von kryptographischen Methoden, asymmetrischer Verschlüsselung und Hashfunktionen können der Absender und die Integrität von Transaktionen in der Blockchain bestätigt werden. Dabei wird mit Hilfe einer Hashfunktion der Hashwert (zufällige Zeichenkette) für eine Transaktion erzeugt. Dadurch wird der übermittelten Transaktion eine Art Fingerabdruck beigefügt, welcher sich bei einer nachträglichen Veränderung der Transaktion ebenfalls ändern würde und somit eine Manipulation deutlich werden ließe.

Der Absender verschlüsselt diesen Hashwert mit seinem privaten, nur ihm bekannten Schlüssel. Der Empfänger entschlüsselt dann wiederum diese Signatur mit dem öffentlichen, bekannten Schlüssel des Absenders und prüft dabei, ob diese dem Hashwert der empfangenen Transaktion entspricht. Dadurch lässt sich sowohl der Absender bestätigen als auch verifizieren, dass der Teilnehmer die notwendigen Rechte/Werte besitzt, um die Transaktion anzustoßen und dass diese unverändert übermittelt wurde. Der öffentliche Schlüssel erlaubt sozusagen den Einblick in das Konto des Teilnehmers, in dem seine Besitzverhältnisse an den in der Blockchain abgebildeten Werten erfasst sind.

Die Validierung von Transaktionen und das Erzeugen von Blöcken, in die die Transaktionen geschrieben werden, wird als „Mining“ bezeichnet. Dabei werden Transaktionen zu einem in sich abgeschlossenen Gebilde, einem Block, zusammengefasst. Hat dieser Block seine vorgesehene Größe erreicht, wird dieser geschlossen, mit dem Vorgänger verbunden, und der nächste Block entsteht. Die Erzeugung eines Blocks, die Validierung der darin enthaltenen Transaktionen, das Verschließen des Blocks und die Verknüpfung mit den Vorgängerblöcken erfolgt über kryptografische Verfahren (Hash-Algorithmen). Dabei umfasst der letzte Block der Kette eine Hash-Information (Prüfsumme) des Vorgängerblocks.

Ist ein Block gespeichert, also abgeschlossen und verkettet, können die Transaktionen in diesem Block nicht mehr unbemerkt verändert oder neue Transaktionen hinzugefügt werden, da jede Veränderung bezüglich einer Transaktion an alle aktiven Netzwerkteilnehmer übermittelt und von ihnen validiert wird. Dieser Umstand macht eine nachträgliche Veränderung der Blockchain unmöglich. Wird versucht, einen Block in der Kette zu ändern, so werden auch die Hash-Werte des Blocks und der nachfolgenden Blöcke geändert. Die anderen Nodes (Knoten) werden diese Manipulation erkennen und den Block von der Hauptkette ausschließen.

Sobald also ein Geschäftsvorfall aufgezeichnet worden ist, kann dieser nicht mehr geändert werden („Unveränderbarkeit“). Sollte wider Erwarten tatsächlich ein Geschäftsvorfall fehlerhaft aufgezeichnet worden sein, kann dieser nur mit Zustimmung aller Beteiligten wieder „storniert“ werden, um dann den korrigierten Geschäftsvorfall in der Blockchain zu erfassen. Alle drei Vorgänge sind jedoch in der Blockchain abgebildet.

Das Erstellen neuer Blöcke und damit die Verifikation der durchgeführten Transaktionen erfolgt über ein Konsensverfahren der beteilig-

ten Nodes. Über kryptografische Verfahren wird die Richtigkeit einer Transaktion verifiziert und über den Konsens im Netzwerk unveränderlich bestätigt. Das Konsensverfahren bestätigt dezentral die Integrität der Transaktionen. Das populärste Konsensverfahren ist hierbei die Proof-of-Work-Methode[1]; es bestehen jedoch zahlreiche andere Formen, Konsens herzustellen (Proof-of-Stake[2], Proof-of-Capacity[3] und weitere).

Die Dokumentation von Geschäftsvorfällen in einer Blockchain erfordert somit die Zustimmung aller Beteiligten („Konsensus"). Das bedeutet, dass Geschäftsvorfälle nur dann aufgezeichnet werden, wenn die Beteiligten sich darüber einig sind, dass diese auch Gültigkeit besitzen.

Die einzelnen Blöcke reihen sich nach und nach zu einer fest miteinander verbundenen Kette aneinander. Dabei wird stetig eine Kopie der Blockchain an alle aktiven Netzwerkteilnehmer übermittelt.

Die Blockchain ist also eine Kette von Blöcken, die alle durchgeführten Transaktionen enthalten und über die verlinkten Hashes miteinander verknüpft sind. Sie stellt damit ein dezentrales Transaktionsregister dar, das eine weitestgehend fälschungssichere Buchführung (Aufzeichnung von Transaktionen) ermöglicht.

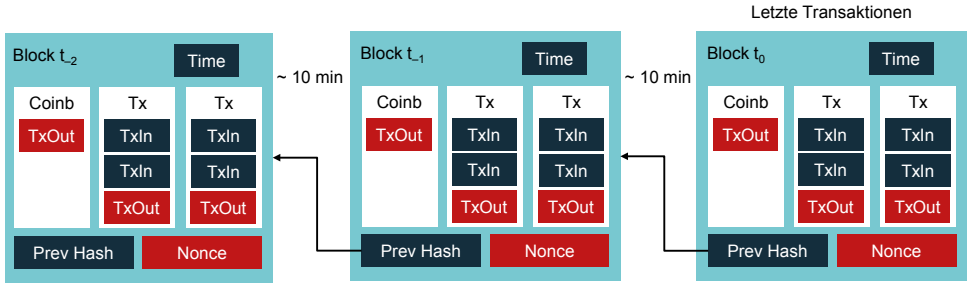

Abbildung 1: Schematische Darstellung einer Blockchain: Transaktionsdatensätze werden in Blöcken gespeichert, die in einer Reihe miteinander verkettet sind (vereinfachte Darstellung); Quelle: Laschewski, Der Blockchain-Algorithmus, WPg 07/2017, S. 359

1 Konsensverfahren, bei dem durch den Algorithmus derjenige Teilnehmer (Miner) belohnt wird, der durch das Lösen einer komplizierten kryptografischen Aufgabe Transaktionen validiert und somit neue Blöcke der Blockchain erzeugt.

2 Konsensverfahren, bei dem der wertmäßige Anteil des Teilnehmers am Netzwerk in die Berechnung einfließt, welcher Teilnehmer eine Transaktion validieren darf.

3 Konsensverfahren, bei dem der zur Verfügung gestellte Speicherplatz entscheidend ist.

1.2. Arten von Blockchains

1.2.1. Permissionless Blockchains

Bei der permissionless Blockchain (oder auch public Blockchain) kann jeder am Netzwerk ohne Einschränkungen teilnehmen. Alle Teilnehmer sind anonym, gleichberechtigt und können Transaktionen senden, empfangen, einsehen und an der Blockchain-Fortschreibung mitwirken. Bei der permissionless Blockchain gibt es keine Zentralinstanz zur Verwaltung und keine kontrollierende Drittpartei. Die Verwaltung der Blockchain funktioniert autonom allein durch die sich gegenseitig regulierende anonyme Masse der Teilnehmer. In der Regel wird dabei ein Proof-of-Work-Verfahren als Konsensfindung verwendet. Gebühren und Entlohnung kommen unabhängigen Transaktions-Prozessoren zugute. Die Regeln der Blockchain werden durch den öffentlich bekannten Code, also die Programmierung der Blockchain, vorgegeben. Dieser ist „open source" und somit frei zugänglich für die Entwickler-Community. Auch der Code kann nur im Konsens der Teilnehmer geändert werden.

Nachteil dieser Ausgestaltung ist die Geschwindigkeit, mit welcher die Blockchain fortgeschrieben werden kann, als auch ihr Ressourcenbedarf, insbesondere an Strom und Rechnerhardware (bedingt durch aufwendigere Konsensverfahren, die künstlich erschwerte Berechnungen beinhalten, um die Sicherheit und Integrität der Blockchain zu gewährleisten). Vergleicht man das Bitcoin-Netzwerk z.B. mit der etablierten Infrastruktur des VISA-Netzwerks, so kommt das Bitcoin-Netzwerk auf eine Verarbeitung von ca. 7 Transaktionen pro Sekunde, demgegenüber kommt das VISA-Netzwerk auf eine Verarbeitung von ca. 56.000 Transaktionen pro Sekunde. Allein der Strombedarf für das Mining von Bitcoins war in 2017 höher als der jährliche Stromverbrauch einiger Länder.[4]

Permissionless Blockchains sind vor allem im Bereich von virtuellen Währungen verbreitet. Beispiele sind die Bitcoin-Blockchain und die Ethereum-Blockchain.

4 *https://www.lsp.de/de/good2know, visa-vs-coins*, abgerufen am 19.09.2019. *https://www.businessinsider.de/bitcoin-stromverbrauch-miner-2017-11,* abgerufen am 10.09.2019.

1.2.2. Permissioned Blockchains

Im Gegensatz zu einer permissionless Blockchain, bei der es keine zentrale Verwaltungsinstanz gibt, jeder teilnehmen kann und alle Teilnehmer gleichberechtigt sind, gibt es bei der permissioned Blockchain eine zentrale Instanz bzw. eine zentrale Gruppe, die bei der Initiierung der Blockchain die Regeln definiert hat sowie festlegt, wer an dem Blockchain-Netzwerk teilnehmen darf und welche Teilnehmer sich am Konsensfindungsprozess beteiligen dürfen (also als nodes mit Mining-/Verifizierungs-Berechtigung agieren). Darüber hinaus ist eine

Art Schiedsrichter erforderlich, der die Berechtigung hat, Geschäftsvorfälle im Blockchain-Netzwerk zu beobachten. Typischerweise ist der Schiedsrichter selbst von der Nutzung der Blockchain ausgeschlossen.

Um an einer permissioned Blockchain teilnehmen zu können, benötigt man eine Einladung oder Erlaubnis. Dabei gibt es verschiedene Varianten, wie oder wer über neue Teilnehmer entscheidet: Dies kann eine zentrale Verwaltungsinstanz sein, die Teilnahmelizenzen ausgibt oder ein Konsortium, das über die Aufnahme neuer Teilnehmer entscheidet.

Permissioned Blockchains lassen sich nochmals unterteilen in private Blockchains und hybride (Konsortium-)Blockchains.

Private Blockchains werden meist zu internen Zwecken durch ein einzelnes Unternehmen aufgesetzt. Die Verwaltung und Steuerung liegen dabei bei einer zentralen Instanz. Dies setzt aber gerade einen der wesentlichen Vorteile der Blockchain außer Kraft, nämlich die Verifizierung der Integrität von Transaktionen durch eine große Anzahl unabhängiger Akteure und die damit verbundene Sicherheit und Unveränderbarkeit.

Bei der privaten Blockchain ist der Zugang beschränkt und die Identität der Teilnehmer bekannt (wie auch bei der hybriden Blockchain). Neben der bekannten Identität der Teilnehmer ist ein weiteres Kennzeichen der privaten Blockchain, dass Funktionen (wie das Mining) und der Zugriff auf die Informationen in der Blockchain über Berechtigungen gesteuert werden.

Ein Vorteil ist, dass ein Konsensmechanismus in einer privaten Blockchain, bei der jegliche Teilnehmer bekannt sind, nicht die gleiche Komplexität benötigt wie in einem System, bei dem alle Teilnehmer unbekannt sind. Dadurch können mehr Transaktionen mit höheren Geschwindigkeiten und weniger Energieeinsatz verarbeitet werden als bei einer öffentlichen Blockchain.

Eine private Blockchain stellt dabei eher einen alternativen Ansatz zur Nutzung herkömmlicher ERP-Systeme und anderer Datenbank-Technologien *(„Blockchain as a tool")* dar.

Ein Beispiel hierfür bildet das Hyperledger Framework, auf dessen Basis private Blockchains aufgesetzt werden können.

Hybride (Konsortium-)Blockchains werden meist von Akteuren aufgesetzt, die gemeinsam von einem Shared-Ledger-System profitieren können. Die Teilnahme am Konsensfindungsprozess wird auf bestimmte Akteure eingeschränkt. Das bedeutet, dass die Sicherstellung der Integrität der durchgeführten Transaktionen durch eine definierte Gruppe erfolgt. Hierbei kann vorab festgelegt werden, dass eine Transaktion nur als wahr angenommen wird, wenn diese von einer bestimmten Mehrheit der beteiligten Blockchain-User bestätigt wird (Konsenserzielung durch die Mehrheit der Konsortium-Teilnehmer). Dieses ist auch ein wesentliches Abgrenzungsmerkmal zur privaten Blockchain, wo die Autorität und die Validierung von Transaktionen bei nur einer zentralen Instanz liegt, die das Blockchain-Netzwerk kontrolliert. Die hybride Blockchain bietet durch den eingeschränkten Kreis und die Bekanntheit der Identität der Teilnehmer einige Vorteile privater Blockchains, wie beispielsweise eine höhere Prozess- und Interaktionsgeschwindigkeit, überlässt hierbei jedoch die Verantwortung nicht einem einzigen Akteur (der in der Lage wäre, die Blockchain zu manipulieren). Insbesondere die Kooperation zwischen Unternehmen und Institutionen bietet vielfältige Einsatzmöglichkeiten für diesen Typ der Blockchain.

Hybride Blockchains eignen sich für geschäftliche Aktivitäten mit bekannten Akteuren, um geschäftliche und rechtliche Transaktionen effizienter durchführen zu können. Ein Beispiel ist die R3 Konsortium Blockchain Plattform im Finanzbereich.

2. POTENZIELLE PRAKTISCHE ANWENDUNGSMÖGLICHKEITEN

2.1. Voraussetzungen für einen sinnvollen Einsatz

Zehn Jahre nach der Einführung der Blockchain-Technologie und Investments, die global längst die Grenze von einer Milliarde Euro überschritten haben, sind die praktischen Anwendungsfälle für den Einsatz der Technologie jenseits von potenziellen Ideen, Prototypen und vereinzelten Anwendungen noch nicht soweit gediehen, wie es der Aufwand und die Präsenz in der öffentlichen Diskussion vermuten lässt.

Insofern stellt sich die Frage, warum das so ist oder anders formuliert:

Welche Anforderungen müssen erfüllt sein, damit die Blockchain-Technologie im Gegensatz zu millionenfach eingesetzten herkömmlichen Datenbanktechnologien als Lösung in Frage kommt?

Prinzipiell handelt es sich bei einer Blockchain um eine Datenbank

- zur Speicherung von Transaktionen in Bezug auf eine definierte Sache (z.B. Besitzverhältnisse an einem definierten Vermögenswert), wobei die Transaktionen voneinander abhängig sind;
- deren Nutzer sich gegenseitig nicht vertrauen, aber zur Fortschreibung dieser Datenbank berechtigt sind.

Im Kontext einer Kryptowährung als originärem Anwendungsfall der Blockchain-Technologie dient eine Blockchain dazu, die Gültigkeit von Transaktionen im Sinne der Fortschreibung von Besitzverhältnissen an einer eindeutig identifizierbaren Einheit der jeweiligen Kryptowährung zu gewährleisten und somit das erforderliche Vertrauen der teilnehmenden Wirtschaftssubjekte in die Gültigkeit der Transaktionen zu rechtfertigen.

Da für alle Teilnehmer an der Blockchain jederzeit vollständige Transparenz über alle verfügbaren Einheiten der Kryptowährung als auch der entsprechenden Besitzverhältnisse an jeder einzelnen Einheit erlangt werden kann, da jeder Teilnehmer über eine identische Version der Blockchain verfügt, kann der Einsatz einer zentralen Regelungsinstanz bzw. eines Intermediärs bei gleichzeitiger Anonymität der teilnehmenden Wirtschaftssubjekte vermieden werden.

Ein betriebswirtschaftlich sinnvoller Anwendungsfall für den Einsatz der Blockchain-Technologie jenseits des Anwendungsfalls der Kryptowährung liegt also immer dann vor, wenn es für die Verwaltung von Transaktionen in Bezug auf einen Vermögenswert sinnvoll ist, eine vertrauensbegründende zentrale Regelungsinstanz bzw. einen Intermediär durch eine Blockchain zu ersetzen bzw. zu vermeiden.

Sinnvoll ist dies grundsätzlich immer dann, wenn die Transaktionsverarbeitung auf der Basis der Blockchain-Technologie schneller, zuverlässiger, einfacher oder kostengünstiger als durch einen Intermediär gesteuert erfolgen kann und somit die Anonymität der teilnehmenden Wirtschaftssubjekte auch gegenüber einem Intermediär sichergestellt sein soll.

Bei dieser Abwägung sind darüber hinaus zwei der Blockchain-Technologie immanente Aspekte zu beachten:

1. Im Anwendungsfall der Kryptowährungen ergibt sich die Existenz des verwalteten Vermögenswertes aus der Blockchain selbst. Es kann insofern keine Diskrepanz zwischen dem „digitalen" Vermögenswert und seiner realen Existenz geben. Sofern die mit einer Blockchain verwalteten Vermögenswerte sogenannte „digital twins" zu realen Vermögenswerten (immateriell oder physisch) darstellen, sind entsprechende Abstimmprozesse erforderlich.
2. Im Anwendungsfall der Kryptowährungen erfolgt die Bestätigung der Validität von Transaktionen durch definierte Konsensverfahren, die von den teilnehmenden Wirtschaftssubjekten als maßgeblich akzeptiert werden. Insofern ist das Verfahren zur Bestätigung der Validität einer Transaktion, welches jeweils zum Einsatz kommen soll, entscheidend für die Akzeptanz der Blockchain in ihrem konkreten Anwendungsfall.

Voraussetzungen für einen sinnvollen Einsatz der Blockchain-Technologie sind also:

1. Es sollen Besitzverhältnisse an einer genau definierten Menge von Vermögenswerten verwaltet werden. Wenn Veränderungen an den Besitzverhältnissen bei Vorliegen definierter Bedingungen automatisch vollzogen werden, wird dies durch sogenannte „smart contracts" vollzogen, bei denen es sich um programmierte Ausführungsbedingungen handelt, auf die sich die beteiligten Wirtschaftssubjekte geeinigt haben.
2. Die beteiligten Wirtschaftssubjekte verzichten auf einen Intermediär zur Abwicklung der Transaktionen und der Verwaltung der Menge der Vermögenswerte.
3. Die Wirtschaftssubjekte einigen sich im Zuge der Initiierung der Blockchain auf den verwendeten Mechanismus zur Validierung von Transaktionen.
4. Die Wirtschaftssubjekte einigen sich auf ein Verfahren zur Sicherstellung der Kongruenz der „digital twins" in der Blockchain mit den tatsächlich existierenden Vermögenswerten.

Sofern diese Voraussetzungen nicht erfüllt werden, ist der sinnvolle Einsatz einer Blockchain als zu verwendende Datenbank-Technologie grundsätzlich zu hinterfragen. Sofern alle Voraussetzungen vorliegen, ist darüber hinaus abzuwägen, ob es sich hierbei um eine Technologie handelt, die im konkreten Fall tatsächlich die „einfachere" Lösung gegenüber dem Einsatz eines Intermediärs sowie herkömmlicher Datenbank-Technologien ist.

2.2. Smart Contracts aus technischer und rechtlicher Sicht

Viel beachtet ist der Einsatz der Blockchain für Smart Contracts. Bei Smart Contracts handelt es sich um einen Programmcode, der dezentral in einer Blockchain gespeichert ist und der spezifische Aktionen automatisiert durchführt, sobald ein bestimmtes Set von definierten Bedingun-

gen greift. Es sind in erster Linie verteilte Programme („distributed Apps"), die primär dazu genutzt werden, Transaktionen in der Blockchain automatisiert anzustoßen und durchzuführen. Der Begriff Smart Contract leitet sich daraus ab, dass der Programmcode im Prinzip einen Vertragstext darstellt, der sich basierend auf Parametern und Konditionen, auf die sich die beteiligten Akteure vorab geeinigt haben, selbst ausführt.

Smart Contracts fixieren – in Form von Programmcodes – dasjenige, worauf sich die Parteien geeinigt haben. Das wirft vielfältige juristische Fragen auf, die bislang mehrheitlich ungeklärt sind. Inwieweit müssen beide Parteien den Programmcode „verstehen", um diesen „wollen zu können"? Wem ist die Erklärung juristisch zuzurechnen, wenn der Smart Contract maschinell generiert bzw. „abgeschlossen" wird? Welche Anforderungen sind an die „Akzeptanz" durch eine Vertragspartei zu stellen (insbesondere bei Blockchain-basierten Smart Contracts wird der Smart Contract als solcher nur von einem Teilnehmer „initiiert")? Die entscheidende Frage aus rechtlicher Sicht ist allerdings, was geschieht, wenn der Smart Contract, so wie er gestaltet ist, etwas anderes (rechtserhebliches) „macht" als das, was das Rechtssystem sich vorstellt. Verträge können angefochten werden, ihre Regelungen können gegen AGB-Recht verstoßen (und damit unwirksam sein), sie können nicht vollstreckbar sein, sie können so oder so ausgelegt werden, gesetzliche (d. h. im Vertrag nicht ausdrücklich niedergelegte) Regelungen können den Vertrag „auffüllen" (etwa im Bereich der Gewährleistung) – die Liste ließe sich noch verlängern. Im Rechtssystem hat das unmittelbare Auswirkungen auf den „Vertrag": Der Vertrag ist bzw. wird anders als das, was ursprünglich niedergelegt wurde. Er ist anders zu „lesen" bzw. es bedarf zusätzlicher Informationen als nur der ursprünglichen Fixierung oder zusätzlicher rechtlicher Einsichten, um ihn juristisch vollständig verstehen zu können. Dieses Auseinanderdriften von rechtlicher Sichtweise und Niederlegung in Programmform kann dazu führen, dass der Vertrag automatisch etwas „tut", was er „nicht tun soll". Die Realität, die der Smart Contract „selbstausführend und selbstvollstreckend" schafft – etwa das Bewirken von Zahlungen –, muss dann eventuell aus rechtlichen Gründen „zurückgedreht" werden. Juristisch sind das etwa Rückabwicklungen, Bereicherungsansprüche und sonstige (nachträgliche) Ausgleichsmechanismen. Hier dürfte in Zukunft in der Praxis die größte juristische Herausforderung für das Konzept des schnellen Smart Contracts liegen.

Eine der derzeit bedeutendsten Anwendungsplattformen für Smart Contracts bietet die Blockchain-Technologie von „Ethereum". Diese war von Beginn an darauf angelegt, die Erstellung, Verwaltung und Ausführung von dezentralen Programmen in eine Blockchain einzubetten. Vor allem ist „Ethereum" für die Kryptowährung „Ether" bekannt, welche als Zahlungsmittel für Transaktionsverarbeitungen innerhalb der Smart Contracts verwendet wird.

Einige der Vorteile, die Smart Contracts durch ihre Sicherung auf einer Blockchain mit sich bringen, sind die Unveränderbarkeit, jederzeitige Transparenz (was allerdings auch gleichzeitig ein Problem sein kann, da nicht jeder wünscht, dass bestimmte Bedingungen eingesehen werden sollen) und der Schutz vor fremdem Zugriff. Sobald alle festgelegten Bedingungen erfüllt sind, werden Transaktionen durch Smart Contracts automatisiert durchgeführt. Dies bringt den Vorteil mit sich, dass Gegenleistungsrisiken und Transaktionskosten durch diese Art von Verträgen gesenkt werden.

BEISPIEL

Ein konkretes Anwendungsbeispiel ist das „Brooklyn Microgrid" des US-Unternehmens LO3 Energy in Zusammenarbeit mit Siemens Digital Grid und next47. Diese haben ein lokales Stromnetz in Brooklyn aufgebaut, wo private Solarstrom-Erzeuger (sogenannte „Prosumer": Producer and Consumer) ihren Strom direkt mit privaten Haushalten in der Umgebung handeln können. Die Abrechnung und Buchhaltung der erzeugten und verkauften Mengen erfolgt dabei über die Blockchain.

Als Basis nutzt LO3 die „Ethereum"-Blockchain, mit der Möglichkeit der Integration von Smart Contracts. Über ein SmartMeter (also einen „intelligenten" Stromzähler) wird der täglich produzierte Strom erfasst, der ins Stromnetz eingespeist wird. Das „SmartMeter" gibt die Information über die eingespeiste Strommenge an die Blockchain. Hier wird ein Smart Contract ausgelöst, der einen Token für den Erzeuger produziert („EnergyCredit"). Dieser Token stellt die Menge der eingespeisten kW-Stunden dar. Beim Kauf der Energie wird über ein „SmartMeter" beim Verbraucher die verbrauchte Menge erfasst und automatisiert über die Blockchain verrechnet. Der Verbraucher hält vorher in einem Smart Contract die Einkaufsbedingungen fest, z.B. welcher Anteil an lokalem Strom enthalten sein soll und bis zu welchem Preis er bereit ist, diesen abzunehmen. Im Hintergrund findet eine automatische Auktion statt, in der automatisiert der Preis anhand der vorab hinterlegten Rahmenbedingungen und externen Marktpreise als Informationsbasis ermittelt wird.

Die Ausführung und Abrechnung erfolgt dann über Smart Contracts automatisiert im Hintergrund: der „EnergyCredit" des Produzenten verringert sich um die verkaufte Menge, dafür erhält er als Gegenleistung einen entsprechenden „ValueCredit", der dann ge-

gen reale Währung abgerechnet und ausgezahlt werden oder als Crypto-Token (hier in Form von „Ether“) gehalten werden kann.

Der dezentral erzeugte Strom und der Verbrauch von Strom werden somit direkt zwischen privaten Kleinanlagenbetreibern und Konsumenten gehandelt. Zwischenhändler oder große Energiekonzerne sind hierbei nicht mehr notwendig, wodurch nicht nur Zeit, sondern auch Transaktionskosten gespart werden können.

2.3. Fixed Assets

Ein häufig diskutiertes Beispiel der Anwendung der Blockchain-Technologie ist die sogenannte „Tokenization“ von Vermögensgegenständen. Um die dahinterliegende Idee kurz zu beschreiben, ziehen wir eine Landmaschine, etwa einen Mähdrescher, als Beispiel heran. Die Anschaffung eines Mähdreschers ist mit sehr hohen Investitionen verbunden (lassen wir es 300.000€ sein), gleichzeitig ist aber dessen Nutzung in der Regel auf wenige Tage im Jahr begrenzt. Dadurch ist diese unerlässliche Anschaffung für einen Landwirt allein unattraktiv. Mit Tokenization bezeichnet man nun die Umwandlung der Besitz- oder Nutzungsrechte an einem Gut, hier an dem Mähdrescher, in eine feste Anzahl digitaler Token. Der Begriff Token kann in diesem Zusammenhang im deutschen wohl am ehesten mit „Wertmarke“ verglichen werden. In unserem Beispiel könnte man die Rechte am Mähdrescher z.B. in 100 Token aufteilen. Nennen wir diese Token MäT. Der Besitz eines MäT repräsentiert also den Besitz eines 1%igen Anteils am Mähdrescher. Die Herausgabe der MäT erfolgt auf einer geeigneten öffentlichen oder privaten Blockchain, wo er beliebig getauscht, verkauft und eingekauft werden kann. Mit einer entsprechenden vertraglichen Vereinbarung würde der Besitz eines MäT auch einen rechtlich bindenden Besitzanspruch auf den Mähdrescher gewähren. In jedem Fall aber wäre bereits heute durch die Unveränderlichkeit und Überprüfbarkeit der Blockchain der vereinbarte Besitzanspruch dokumentiert. So können große Investitionen wie etwa die Anschaffung eines Mähdreschers zur gemeinschaftlichen Nutzung auf viele Schultern entlastet werden. Die Verankerung der Besitzansprüche in öffentlichen (digitalen, evtl. auch Blockchain basierten) Registern könnte über Smart Contracts geregelt werden, womit wie oben erwähnt, eine enorme Entbürokratisierung einhergehen würde. Konkret könnte der Besitz eines MäT im Beispiel des Mähdreschers außerdem die Nutzungsdauer regeln, sofern – ebenfalls per Smart Contract – die Freischaltungsdauer der Maschine an den Besitz von MäT gekoppelt wäre. Die tatsächliche Nutzung der Maschine inklusive Zeitstempel und etwaigem Nutzungsverhalten könnte per Blockchain als digitales, vollautomatisches und unabänderliches Fahrtenbuch gespeichert werden. Dies könnte sowohl für die Kostenteilung notwendiger Instandhaltungsmaßnahmen als auch als Versicherungsnachweis bei eventuellen Streitigkeiten dienen.

Die Tokenization lässt sich beliebig auf andere Fixed Assets wie Immobilien, PKW u.v.m. ausweiten.

2.4. Mehrwertsteuer 2.0

Basierend auf der Blockchain-Technologie ist aus der Sicht der Umsatzsteuer folgendes Anwendungsbeispiel denkbar: Jede Ausgangsrechnung läuft elektronisch über die Blockchain und wird dort digital erfasst. Hierzu wird die Rechnung elektronisch generiert und an die digitale Informationskette übertragen. In der praktischen Umsetzung erfolgt dies mit der gleichen technischen Selbstverständlichkeit, wie das Versenden einer E-Mail. Soweit sich aus der Rechnung eine Umsatzsteuerschuld ergibt, wird diese unmittelbar über die bereits bestehende Bitcoin-Technologie an den Fiskus abgeführt. Das Ergebnis ist eine Steuererhebung in Echtzeit, bei welcher jede Transaktion unveränderbar digital aufgezeichnet wird („Audit-Trail“). Zugleich wäre eine technische Zuordnung („Mapping“) zum Vorsteuerabzugsberechtigten möglich, dem zugleich via Bitcoin der korrespondierende Vorsteuerbetrag gutgeschrieben werden könnte. Das Besondere ist, dass nur in der Blockchain registrierte Umsatzsteuerzahlungen letztlich eine Vorsteuererstattung legitimieren würden. Damit würde nicht nur ein Großteil der bekannten Betrugsszenarien obsolet, es könnten zugleich zahlreiche umsatzsteuerrechtliche Formerfordernisse entfallen. Konsequent zu Ende gedacht würde dies ggf. sogar eine Belegvorhaltepflicht beim Leistungsempfänger entbehrlich machen, denn dessen Existenz ergäbe sich bereits zweifelsfrei aus der Blockchain. Das Ergebnis dieses Gedankenspiels könnte eine Entbürokratisierung sein, welche die Kosten für die erforderliche Infrastruktur innerhalb kürzester Zeit einspielen könnte. Das bestehende Mehrwertsteuerrecht müsste nicht nennenswert modifiziert werden, das grundsätzliche System der fraktionierten Zahlung bliebe erhalten. Die Gewinner einer solchen Digitalisierung des Mehrwertsteuerrechts wären damit Unternehmen, Fiskus und Finanzverwaltung gleichermaßen. Einen ersten Schritt in diese Richtung hat zum 1. Januar 2019 Italien vollzogen und die elektronische Rechnung verpflichtend für alle inländischen Wirtschaftsakteure eingeführt. Im Kern sind die entsprechenden Rechnungen über ein elektronisches Austauschsystem an den Rechnungsempfänger zu übermitteln. Damit geht letztlich wohl auch die Hoffnung des italienischen Fiskus einher, bekannte Betrugsszenarien auszuschließen und damit das Umsatzsteueraufkommen zu sichern. So wird es über den verpflichtenden Versand von E-Rechnungen insbesondere möglich, die entsprechende Umsatzsteuerschuld exakt zu berechnen und mit den Angaben der Umsatzsteuer-Voranmeldung abzugleichen. Zugleich wird dadurch die Datengrundlage geschaffen, den Vorsteuerabzug an die korrespondierend gemeldete Umsatzsteuerschuld zu koppeln. Der nächste logische Schritt wäre, den jeweiligen Vorsteueran-

spruch auf Rechnungs- bzw. Transaktionsebene mit der gemeldeten Umsatzsteuerschuld abzugleichen. Die Auszahlung des jeweiligen Vorsteuervergütungsanspruchs könnte dann faktisch an die Anmeldung bzw. Abführung der korrespondierenden Umsatzsteuerschuld geknüpft werden. Nutzt man hier zudem die sich aus der Blockchain-Technologie ergebenden Möglichkeiten, den Zahlungsverkehr über Kryptowährungen abzubilden, ließe sich ein intrinsisches System bestehend aus Real-Time-Deklaration und permanenter Steuerentrichtung etablieren. Sollte das italienische Modell zum Erfolg führen und zugleich administrierbar sein, ist es eine Frage der Zeit, bis andere Länder wie auch Deutschland nachziehen und ebenfalls auf das „Clearance-System" umstellen werden.

3. RISIKEN UND HERAUSFORDERUNGEN

Wie bei allen neuen Technologien stehen auch bei der Blockchain-Technologie den mit ihr verbundenen Chancen und Potenzialen einige technologieimmanente Risiken und Herausforderungen gegenüber, die es gilt, im Auge zu behalten und für die entsprechende Lösungen gefunden werden müssen.

Da alle Daten einer Blockchain bei allen Teilnehmern parallel gespeichert und über mehrere Netzwerke hinweg synchronisiert werden, ist die Nutzung einer Blockchain-Technologie mit enormen Datenmengen verbunden, die gespeichert und heruntergeladen werden müssen. Darüber hinaus benötigt die Blockchain hohe Rechenressourcen, was sich insgesamt auf die Skalierbarkeit auswirkt und die Performance des Gesamtsystems beeinträchtigen kann.

Auch die Vielfalt der Blockchain-Techniken kann sich als problematisch erweisen. In der Praxis wirft dies Fragen nach der Ausprägung von Schnittstellen oder der Migration von Blockchain-Anwendungen und Plattformen auf, z.B. bei Unternehmenszusammenschlüssen.

Durch die Kontrolle von mehr als der Hälfte aller Netzwerkteilnehmer (sog. „51%-Angriff"), ist es möglich, eine alternative Transaktionskette zu erstellen, d.h. die Daten in der Blockchain technisch zu ändern. Diese geänderten Daten werden dann zur Realität. Ein solches Szenario ist bei der aktuell zur Verfügung stehenden Rechenkapazität für Proof-of-Work-Architekturen in großen Netzwerken relativ unwahrscheinlich. Eine nichtlinear gesteigerte Rechenkapazität, wie etwa durch die Verwendung von Quantencomputern, kann diese Voraussetzung jedoch in mittelfristiger Zukunft ernsthaft in Frage stellen. Für Proof-of-Stake-Architekturen ist, ähnlich wie bei klassischen IT-Systemen, eine adäquate Sicherung insbesondere derjenigen Netzwerkteilnehmer mit ‚hohem stake' eine kritische Voraussetzung für die Datenintegrität.

Eine zentrale Eigenschaft der Blockchain-Technologie ist die Transparenz aller getätigten Transaktionen. Damit einhergehend ergeben sich für jeden Blockchain-Nutzer individuelle Transaktions- und Interaktionsmuster, welche trotz Anonymisierung Rückschlüsse auf die Identität des Blockchain-Nutzers zulassen. Die Pseudo(!)-Anonymität der Blockchain-Nutzer darf also nicht darüber hinwegtäuschen, dass Sender und Empfänger einer Transaktion mit etwas Aufwand in der Regel zu identifizieren sind[5].

Dieser Punkt ist besonders für public Blockchains (z.B. Bitcoin, Ethereum) von Bedeutung. Für private Blockchains (z.B. Hyperledger) ist die Frage der Anonymität der Teilnehmer hinfällig, da diese ohnehin bekannt sind.

Nicht zuletzt fehlt es an einem verbindlichen rechtlichen und regulatorischen Rahmen für die Blockchain-Technologie, der auch international von Bedeutung ist, da sich Blockchain-Netzwerke über mehrere Länder hinweg erstrecken können. Ferner sind derzeit nicht alle Regelungen des Datenschutzes ohne weiteres mit der Blockchain-Technologie kompatibel, wie z.B. das „Recht auf Vergessenwerden".

5 Möser et al. 2013: An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. 10.1109/eCRS.2013.6805780

4. AUSWIRKUNGEN DER BLOCKCHAIN-TECHNOLOGIE AUF DEN BERUFSSTAND

4.1. Auswirkungen auf die Abschlussprüfung

Die Blockchain wird auch aus der Perspektive der Jahres- oder Konzernabschlussprüfung an Bedeutung gewinnen. Dies betrifft insbesondere Fallkonstellationen, in welchen das geprüfte Unternehmen Blockchain-Lösungen einsetzt, welche unmittelbaren oder mittelbaren Einfluss auf das zu prüfende Zahlenwerk des Unternehmens haben. In erster Linie betrifft dies die Verwaltung der Inventare von Vermögenswerten, die Teil der Buchführung sind. Denkbar ist aber auch bspw. die Abbildung von virtuellen Währungen und Wertpapieren bzw. Wertpapierverzeichnissen, Archivierungslösungen, Intercompany-Ledger, elektronischen Rechnungen oder der Einsatz von Smart Contracts, welche die vertragliche „Ausführung" in Abhängigkeit bestimmter Prämissen bereits vorab festlegen.

In derartigen Fällen obliegt es letztlich dem Wirtschaftsprüfer, die Verlässlichkeit der Blockchain-Struktur zu beurteilen, um einen Rückschluss auf den Prüfungsgegenstand „Jahresabschluss" zu ziehen. Dabei geht es nicht nur um die Beurteilung des Outputs bzw. der niedergelegten Informationen in der Blockchain, sondern auch um eine Beurteilung der Verlässlichkeit der Blockchain-Struktur selbst. Der Wirtschaftsprüfer wird sich im Rahmen der Prüfung des Jahresabschlusses mit der Fragestellung auseinandersetzen müssen, inwieweit die zum Einsatz kommende Ausprägung der Blockchain sowie die Maßnahmen und Vorkehrungen im Internen Kontrollsystem geeignet sind, den Risiken für den Jahresabschluss aus der Nutzung der Blockchain entgegenzuwirken und somit die Einhaltung der gesetzlichen Anforderungen sicherzustellen. Im Einzelnen betrifft dies die Nachvollziehbarkeit des Rechnungslegungs- bzw. Buchführungsverfahrens und die Nachvollziehbarkeit der Abbildung der einzelnen Geschäftsvorfälle in ihrer Entstehung und Abwicklung, die Einhaltung der Aufbewahrungsvorschriften sowie die Beachtung der Grundsätze ordnungsmäßiger Buchführung und – als Voraussetzung hierfür – die Gewährleistung der IT-Sicherheit.

Die Sicherstellung der Grundsätze ordnungsmäßiger Buchführung ist in jedem Einzelfall vor dem Hintergrund der allgemein gültigen Anforderungen an die Ausgestaltung der Rechnungslegung bei Einsatz von Informationstechnologie zu beurteilen, wie sie in der Literatur und durch den *IDW RS FAIT 1* formuliert sind. Während die Beurteilung der Einhaltung der Ordnungsmäßigkeitsanforderungen stark von der konkreten Ausgestaltung der jeweiligen Anwendung abhängig ist und sich somit am Einzelfall orientieren muss, werden die die IT-Sicherheit bestimmenden Aspekte Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit durch einige grundsätzliche technologieimmanente Faktoren beeinflusst, die bei der Beurteilung durch den Wirtschaftsprüfer zu berücksichtigen sind.

Bei der **Vertraulichkeit** muss zwischen Informationen zu den Transaktionspartnern und Informationen zum Transaktionsinhalt unterschieden werden. In Bezug auf den Transaktionsinhalt, der sich in der Regel aus einem Token/Asset/Coin und einer dazugehörigen Nachricht zusammensetzt, obliegt die Sicherstellung der Vertraulichkeit dem Absender der Transaktion. Diese kann beispielsweise durch die Verwendung geeigneter Verschlüsselungsmaßnahmen erreicht werden, wodurch die Vertraulichkeit der Nachricht einer Transaktion gewährleistet ist, sofern der private Schlüssel des Absenders nur diesem zugänglich (und damit vertraulich) ist. Der Token selbst, der die Höhe bzw. den Wert der Transaktion enthält, kann nicht verschlüsselt werden. Dies ist allerdings zur Gewährleistung der Ordnungsmäßigkeit auch nicht erforderlich.

Vertraulichkeit kann also bei Transaktionen in der Blockchain für die beigefügte Nachricht sichergestellt werden, nicht aber – falls vorhanden – für die Höhe der Transaktion und die Identität der beteiligten Partner.

Integrität ist die zentrale Eigenschaft einer Blockchain. Das Risiko der Gefährdung der Integrität der Blockchain ist sehr gering, da Daten einer Blockchain grundsätzlich technisch nicht abgeändert werden können. Allerdings ist zu berücksichtigen, dass durch einen „51%-Angriff" die Beeinträchtigung der Datenintegrität sehr wohl möglich ist.

Da Blockchains als dezentrale Datenspeicher generell nicht auf einzelne Server, Services o.ä. angewiesen sind, besteht auch für die **Verfügbarkeit** der Daten einer Blockchain nur ein sehr geringes Risiko. Da alle Daten bei allen Teilnehmern parallel gespeichert werden, kann beim Ausfall der Daten eines Teilnehmers jederzeit auf die identischen Daten eines anderen Teilnehmers zurückgegriffen werden, zusätzliche Back-Up Verfahren sind nicht notwendig.

Autorisierung bezieht sich im Blockchain-Umfeld eher auf die Frage, wer am Netzwerk teilnehmen darf (Permissioned Blockchain, private Blockchain) und weniger darauf, welche Rechte ein Teilnehmer hat. Generell gilt, dass jeder Teilnehmer prinzipiell das Recht hat, beliebige Transaktionen auszuführen. Es muss also sichergestellt sein, dass der Teilnehmer für das Unternehmen Transaktionen durchführen darf bzw. die bestehenden Genehmigungsverfahren eingehalten werden. Die Frage, ob eine solche Transaktion dann auch bestätigt wird (also ob sie dauerhaft in der Blockchain verbleibt), kann je nach Architektur der Blockchain unterschiedlich gehandhabt werden.

Hervorzuheben sind hier die Verfahren Proof-of-Work und Proof-of-Stake. Beim Proof-of-Work wird u.a. sichergestellt, dass nur Transaktionen getätigt werden können, die in einer validen Transaktionshistorie stehen, also nur Token versendet werden können, die dem Empfänger auch zur Verfügung stehen. Der Proof-of-Stake ähnelt eher dem klassischen Autorisierungsverfahren, bei dem ein oder mehrere Netzwerkteilnehmer darüber bestimmen, welche Transaktionen valide sind und damit in der Blockchain verankert werden. Über den Zugriff auf die in einer Transaktion abgebildeten Daten entscheidet, wie oben erwähnt, der Absender der betreffenden Transaktion, z.B. durch Verschlüsselung.

Transaktionen einer Blockchain können immer einem Sender und einem Empfänger eindeutig zugeordnet werden. Allerdings ist die Zuordnung eines Senders/Empfängers zu einer realen Entität durch Dritte abhängig von der Art der Blockchain.

Unabhängig von der Art der Blockchain kann aber die **Authentizität** eines auf einer Blockchain abgebildeten Geschäftsvorfalls durch den Verursacher selbst jederzeit belegt werden, indem dieser die Möglichkeit des Zugriffs auf den entsprechenden Account/die Adresse belegt.

Die **Verbindlichkeit** einer Transaktion ist generell gegeben, solange der Veranlasser einer Transaktion den Zugriff auf seinen Account/seine Adresse ordnungsgemäß unter Verschluss hält. Unter dieser Voraussetzung ist eine Transaktion nicht abstreitbar.

Die Beurteilung der Verlässlichkeit der Blockchain-Struktur in ihrer Eigenschaft als Abbildungsmedium für rechnungslegungsrelevante Daten verlangt ein entsprechend fundiertes technisches Ver-

ständnis bzw. eine spezifische Erweiterung des Kompetenzportfolios des Wirtschaftsprüfers. Die Blockchain ist insoweit nur eine Ausprägung der Entwicklung vom Wirtschaftsprüfer zum „Algorithmenprüfer", der in der Lage ist, in Software kodierte Algorithmen und Datenstrukturen zu analysieren und auf die Grenzen ihrer Funktionsfähigkeit bzw. ihres Einsatzzweckes sowie auf etwaige Schwachstellen bzw. Angriffspunkte hin zu untersuchen.

Inwieweit sich aus dem Einsatz der Blockchain Effizienzen im Rahmen von Abschlussprüfungen ergeben, kann derzeit nicht abschließend beurteilt werden. Vieles deutet darauf hin, dass weiterhin die allgemeinen Grundsätze ordnungsmäßiger Abschlussprüfung gelten werden, wenngleich sich im Hinblick auf die konkreten Prüfungsvorgehensweisen Änderungen vor dem Hintergrund des Einsatzes einer neuen Datenbank-Technologie ergeben werden. Die prüferischen Fragestellungen selbst werden aber weiterhin Gültigkeit behalten.

4.2. Steuerliche Aspekte

Ertragsteuer

Im privaten Bereich zählt ein Gewinn oder Verlust aus der Veräußerung von Kryptowährungen zu den sonstigen Einkünften aus privaten Veräußerungsgeschäften, insoweit zwischen Erwerb und Veräußerung nicht mehr als ein Jahr liegt. Außerhalb der einjährigen Haltefrist sind Gewinne aus der Veräußerung von Kryptowährungen im privaten Bereich nicht einkommensteuerpflichtig. Der Gewinn ergibt sich dabei als Differenz zwischen den Anschaffungskosten und dem Veräußerungspreis. Wurde die Kryptowährung in verschiedenen Tranchen erworben, so ist hinsichtlich der Anschaffungskosten die Fifo-Methode anzuwenden, wonach unterstellt wird, dass die zuerst angeschafften Bestände zuerst veräußert wurden. Erfolgt die Anschaffung oder Herstellung von Kryptowährungen im Rahmen einer gewerblichen Tätigkeit, so sind Ergebnisse aus der Veräußerung oder dem Tausch der Kryptowährung als Einkünfte aus Gewerbebetrieb zu erfassen. Die Kosten für das sogenannte „Mining" sind dabei als Betriebsausgaben abzugsfähig.

Umsatzsteuer

Mit Schreiben vom 27. Februar 2018 hat die deutsche Finanzverwaltung auf den boomenden Kryptowährungsmarkt reagiert und in einem ersten Schreiben zur umsatzsteuerlichen Behandlung von Bitcoins und anderen virtuellen Währungen Stellung genommen. Dabei geht es auch um steuerliche Folgefragen betreffend Umsätze im Zusammenhang mit Mining, Wallets und Handelsplattformen.

Gerade aufgrund der Mannigfaltigkeit dieses Themas ist davon auszugehen, dass dies zugleich erst den Auftakt zu weiteren Stellungnahmen der Finanzverwaltung darstellen dürfte. Bis zum Ergehen von höchstrichterlicher finanzgerichtlicher Rechtsprechung dürfte noch längere Zeit verstreichen.

4.3. Erbringung von Assurance- und Beratungsdienstleistungen

Der Wirtschaftsprüfer ist als vertrauensschaffende und unabhängige „Partei" bestens dafür positioniert, Assurancedienstleistungen im Zusammenhang mit der Blockchain zu erbringen.

> Da es bei einer Vielzahl von Blockchain Anwendungen zunächst darum geht, die jeweilige Blockchain technisch (genutzte Verfahren) und inhaltlich (z.B. Ausführungsregeln bei Smart Contracts) zu verstehen und zu bewerten, kann der Wirtschaftsprüfer hier die nötige Transparenz und das Vertrauen zwischen den beteiligten Akteuren schaffen. Dazu gehört, die rechtlichen Hintergründe einer Blockchain, ihre inter-/intrabetrieblichen Verflechtungen und weitere relevante Umstände eingehend zu prüfen und zu betrachten. Dies gilt insbesondere bei Konsortium-Blockchains.

Neben den in Kapitel 4.1. dargestellten, sich unmittelbar aus den Aussagen in der Rechnungslegung ergebenden Fragestellungen, ergeben sich zusätzliche Fragestellungen zur Funktionsweise und Zuverlässigkeit der eingesetzten Blockchain. Diese Fragestellungen hängen davon ab, ob es sich bei der Blockchain um eine permissionless oder um eine permissioned Blockchain handelt. Bei einer permissioned Konsortium-Blockchain werden sich die teilnehmenden Geschäftspartner auf eine Reihe von technischen Protokollen und Standards geeinigt haben, die maßgeblich für die Transaktionsverarbeitung in der Konsortium-Blockchain sind. Hierzu sind entsprechende interne Kontrollen einzurichten und zu überwachen, die dafür sorgen, dass die Transaktionsverarbeitung im Sinne dieser Protokolle und Standards erfolgt.

Aufgrund der Relevanz der geltenden Protokolle und Standards für die Abschlussprüfungen der einzelnen Teilnehmer des Konsortiums können zukünftig Wirtschaftsprüfer durch das Konsortium beauftragt werden, an zentraler Stelle Prüfungshandlungen durchzuführen. Ein sich hieraus ergebendes Prüfungsurteil kann sodann allen Blockchain-Teilnehmern verfügbar gemacht werden. Der Wirtschaftsprüfer als Prüfer einer Blockchain-Service-Organisation unterstützt die Teilnehmer in der Überwachung der Blockchain und schafft das erforderliche Vertrauen, welches letztendlich die Voraussetzung für die Verbreitung der Blockchain-Technologie ist.

Der Wirtschaftsprüfer kann hier als vertrauenswürdige, unabhängige dritte Partei Assurance- und Beratungsleistungen bspw. in den Bereichen Controls & Risks, Technical Assurance und Verification- und Validierungsservices erbringen.

Im Bereich Controls and Risks geht es um das Verstehen der Risiken und die Schaffung von Transparenz hinsichtlich des Einsatzes der Blockchain im Unternehmen sowie um die notwendigen Anpassung und Ausgestaltung des Internen Kontrollsystems. Dabei kann eine Beurteilung dieser Prozesse auch als Internal Control Report über die internen Kontrollen für Unternehmen erfolgen, die Blockchain-bezogene Dienste nutzen, mit ihnen interagieren, sie aufbauen oder bereitstellen.

Im Bereich Technical Assurance geht es um die Sicherstellung der Verlässlichkeit der verwendeten Plattformen, Regeln und Mechanismen. Dieses umfasst mit Smart Contracts Assurance die Prüfung von Vertragsbedingungen und deren Umsetzung. Bei Blockchain Platform & Protocol Assurance geht es u.a. um die Evaluierung der Manipulationssicherheit und Integrität der verwendeten Verfahren.

Zudem können hier auch Validation Services von Relevanz sein, also die Bereitstellung von Validierungs-, Existenz- und Assurance-Diensten für digitale Bestände, die physische Bestände in Blockchains repräsentieren. Zu den Verification Services gehört im Rahmen z.B. von Abschlussprüfungen auch die Prüfung, ob die in den Bilanzen aufgeführten Kryptowährungskonten und Bestände auch tatsächlich dem Unternehmen zuzurechnen sind.

Bei einer Zentralisierung bestimmter administrativer Funktionen der Blockchain, wie z.B. der Überwachung der Implementierung und des Betriebs der Blockchain-Protokolle, könnte das gegenseitige Vertrauen der Blockchain-Teilnehmer beeinträchtigt werden, sofern diese Funktion durch einen Node oder Blockchain-User übernommen wird. Der Wirtschaftsprüfer als sachverständiger und unabhängiger Dritter erfüllt die mit dieser Überwachungsfunktion verbundenen Anforderungen in besonderem Maße. So könnte der Wirtschaftsprüfer z.B. die Funktion der Akkreditierung neuer Blockchain-User (permissioned Blockchain) oder der Überwachung der Konsensfindung der Blockchain wahrnehmen.

Trotz der konsensbasierten Blockchain-Technologie kann es z.B. in privaten Blockchains zu Meinungsverschiedenheiten zwischen den Blockchain-Teilnehmern kommen. Der Wirtschaftsprüfer ist aufgrund seiner fachlichen Kenntnisse und Erfahrungen in besonderem Maße zur Schlichtung derartiger Kontroversen zwischen Blockchain-Teilnehmern geeignet. Eine effektive Schiedsinstanz erzeugt Rechtssicherheit und erfüllt den Bedarf der Blockchain-Teilnehmer nach einem hohen Maß an Vertragskonformität in der Blockchain (z.B. im Umfeld von Smart Contracts).

Dies ist eine Auswahl möglicher Assurance- und Beratungsleistungen im Umfeld der Blockchain. Dabei werden sich in Zukunft eine Vielzahl weiterer Gebiete herauskristallisieren, insbesondere im Rahmen von Konsortium-Blockchains.

Die Tatsache, dass die entsprechenden Informationen identisch allen Teilnehmern an der Blockchain zur Verfügung stehen, verleitet zu der Annahme, dass eine zentralisierte Prüfung der eingesetzten Blockchain Prüfungssicherheit für relevante Prüfungsaspekte der Blockchain an zentraler Stelle generiert, die analog zu *IDW PS 331 n.F.* bzw. *IDW PS 951 n.F.* von Prüfern der jeweiligen Teilnehmer verwendet werden könnte. Diese Analogie scheidet aber aufgrund des Fehlens eines Intermediärs bzw. Dienstleistungsunternehmens aus. Sofern doch eine zentrale Regelungsinstanz (vor allem bei permissioned Blockchains) existiert, gelten die allgemeinen Grundsätze, wie sie in *IDW PS 331 n.F.* bzw. *IDW PS 951 n.F.* formuliert sind.

5. AUSBLICK

Die Blockchain ermöglicht die vereinfachte und für alle Parteien transparente Vereinbarung komplexer Vertragsbeziehungen. In einer komplexer werdenden Geschäftswelt mit zunehmender Automatisierung und Digitalisierung liegen künftige Anwendungsfälle vermutlich im Bereich der Kombination unterschiedlicher (auch virtueller) Geschäftspartner, die gemeinsam Transaktionen durchführen und/oder bindende Verträge abschließen. Die gegenwärtigen Anwendungsfälle der Blockchain-Technologie deuten aber noch nicht auf eine weitreichende Umsetzung jenseits des spezifischen Einsatzes hin. Es ist zu vermuten, dass ein Grund hierfür auch in den mit der Technologie verbundenen systemimmanenten Risiken und Herausforderungen liegt. Sofern es in der Zukunft aber zu weitreichenden praktischen Anwendungsfällen der Blockchain-Technologie kommt, werden sich unweigerlich Auswirkungen auf das Kompetenz- und Leistungsportfolio des Berufsstands ergeben. Sofern Aspekte der Buchführung berührt werden, gelten weiterhin die allgemeinen Anforderungen zur Einhaltung der Grundsätze ordnungsmäßiger Buchführung.