Inhaltsverzeichnis

WhitePaper Krypto-Assets

EXECUTIVE SUMMARY

Krypto-Assets haben ein schwieriges Jahr hinter sich. Nach den Rekordhochs im November 2021 und einer Marktkapitalisierung von 3 Trillionen US-Dollar war mit dem Ende des Quantitative Easing auch der Höhenflug am Krypto-Markt vorbei. Der Kollaps der Krypto-Börse FTX sorgte für einen weiteren Tiefpunkt. Viele der Ereignisse in den letzten Monaten erinnern an die Dotcom-Blase zu Beginn des Jahrtausends. Umso wichtiger ist der genaue Blick auf die Chancen und Risiken dieser Assetklasse.

Der Round Table Asset Management hat in den zurückliegenden Sitzungen die verschiedenen Facetten des Krypto-Markts genauer untersucht. Die Diskussionsrunden haben gezeigt, dass sowohl Praktiker im Asset Management als auch Experten aus Wirtschaft und Wissenschaft der Blockchain-Technologie weiterhin riesiges Potenzial zuschreiben. Erwartet wird aber, dass sich die Krypto-Welt einschneidend verändert – sowohl auf regulatorischer als auch monetärer Ebene. Auch werden sich bei dauerhaft höheren Zinsen nur noch die Projekte durchsetzen, die einen substanziellen Mehrwert versprechen.

ÜBERBLICK ZUR REGULATORIK

Die Diskussionen im Round Table Asset Management wurden mit Unterstützung von Dr. Christoph Wronka, Jens Hermann Paulsen und Nils-Philipp Böhm (alle Deloitte) in vorliegendem Positionspapier zusammengefasst. Nach einem Überblick zur geltenden und einem Ausblick auf die kommende Regulatorik wird aufgezeigt, wie genau die Technologie hinter Krypto-Assets funktioniert. Zudem werden unterschiedliche Anwendungsfälle durch die Verwendungen von Blockchain-Technologien aufgezeigt. Auch die Handlungsmöglichkeiten sich für die Finanzwelt, insbesondere Asset Manager, werden analysiert. Es folgt eine intensive Auseinandersetzung mit den Implikationen fürs Risikomanagement und die Nachhaltigkeitsaspekte bei Krypto-Assets.

HERZSTÜCK BLOCKCHAIN

Die Blockchain-Technologie als eine dezentrale verteilte Datenbank mit ihrer Eigenschaft der Unveränderlichkeit von Einträgen ist das Herzstück hinter jedem Krypto-Asset. Chancen ergeben sich vor allem aus der Möglichkeit des vertrauensvollen Handels zwischen zwei oder mehr Parteien ohne die Notwendigkeit zur Einbindung Dritter. Ein Beispiel macht dies deutlich: Die Aufgaben eines Notars bei Immobilientransaktionen könnten in Zukunft von Smart Contracts übernommen werden. Das ist ein auf einer Blockchain ausgeführter Programmcode. Sobald der Käufer die entsprechende Summe für den Hauskauf zur Verfügung stellt, übersendet der Smart Contract das Geld an den Verkäufer und überschreibt dem Käufer das Eigentum an der Immobilie. Das lässt Transaktionen durch den Wegfall von Intermediären nicht nur kosteneffizienter, sondern auch schneller werden.

CHANCEN FÜR DIE FINANZBRANCHE

Gesamthaft betrachtet könnten die Finanzmärkte effizienter, transparenter und liquider werden. Chancen bieten sich auch für Asset Manager. Beispielsweise könnten Abhängigkeiten von Intermediären wie Banken oder Brokern beim Vertriebsprozess entfallen. Für Asset Manager. bieten sich vielfältige Möglichkeiten, bestehende Produkte zu erweitern oder neuartige Produkte auf den Markt zu bringen. Auch das Investieren in Start-ups würde sich vereinfachen, wenn Start-ups über einen ICO (Initial Coin Offering) ihren Investoren Anteile in der Form von Tokens anbieten. In der Folge ließe sich das Produktportfolio unter anderem um ICO-Fonds und Krypto-Fonds erweitern. Kurzum: Es bieten sich große Chancen für die gesamte Finanzbranche.

GESETZGEBER GEFORDERT

Gleichzeitig entstehen bei der Integration von Krypto-Assets in das Geschäftsumfeld neue Risiken. So wird immer wieder diskutiert, wie Krypto-Assets vor fremden Zugriffen geschützt und sicher verwahrt werden können. Auch die Frage der Übertragungsrisiken und wie der einhergehende Verlust der Coins mitigiert werden kann, ist für die Risikoabwägung entscheidend. Zudem geht es um Haftungsrisiken für Dienstleister. Der Gesetzgeber ist an vielen Stellen gefordert, auch um zukünftig einen Kollaps, wie der der Krypto-Börse FTX im November 2022, zu verhindern.

Mit der kommenden „Markets in Crypto-Assets"-Verordnung auf europäischer Ebene sollen die Krypto-Branche strenger überwacht und Verbraucherinnen und Verbraucher geschützt werden – ohne dabei die Innovationskraft zu rauben. Damit versucht die Europäische Union, einen Milliardenmarkt zu erschließen. Denn erst durch ausreichende Regulierung wird eine tiefergehende Adaption durch Endverbrauchende und breite Teile der Finanzbranche möglich werden.

STÄRKUNG DER INNOVATIONSKRAFT

Die deutsche Gesetzgebung hat mit dem elektronischen Wertpapiergesetz (eWpG) und der Krypto-Fondsanteile-Verordnung (Krypto-FAV) erste Schritte unternommen, die Finanzbranche zu digitalisieren und in ihrer Innovationskraft zu stärken. So können Fondsanteile elektronisch begeben werden und nach Worten des Finanzministeriums soll dies in dieser Legislaturperiode auch für Aktien möglich werden. Weiterhin könnte es auch für Publikumsfonds einfacher werden, direkt oder indirekt in Krypto-Assets zu investieren.

In diesem Whitepaper werden wir auf die folgenden Punkte eingehen:

- Überblick über die geltende Regulatorik und einen Ausblick auf die kommende
- Wie die Technologie hinter Krypto-Assets genau funktioniert
- Welche unterschiedlichen Anwendungsfälle sich durch die Verwendungen von Blockchain-Technologien ergeben
- Eine Klassifierzierung von NFTs und anderen Tokenarten
- Implikationen für die Finanzwelt, insbesondere für Asset-Manager
- Implikationen für das Risikomanagement
  Der Nachhaltigkeitsaspekt bei Krypto-Assets

Kapitel I – Bitcoin als erster Use Case

Derzeit existiert wohl keine Technologie, welcher ein höheres Potenzial nachgesagt wird, das Anlageuniversum zu verändern. Dabei handelt es sich um die die Blockchain und die daraus resultierenden Möglichkeiten. Ob eine direkte Investition wie z. B. in Krypto-Währungen und NFT´s oder die Möglichkeit der Emission digitaler Fondsanteile: Die neuen Möglichkeiten und Potenziale sind grenzenlos.

Um einen ersten Überblick über die Funktionsweise der Technologie zu erhalten, springen wir zum 31.10.2008 zurück, wo eine bis heute unbekannte Person oder Gruppe unter dem Pseudonym Satoshi Nakamoto ein White Paper mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System" an einen kleineren Kreis von Krypto-Graphen gesendet hat.

Dies war der Startschuss für die heute bekannteste Krypto-Währung der Welt – Bitcoin – auf dessen Technologie alle nachfolgenden Krypto-Währungen basieren. In den letzten Jahren stieg das Interesse privater Anleger zu den oben aufgeführten Themen stetig, sodass diese immer mehr Platz in der aktuellen Berichterstattung einnahmen. Es zeigt sich, dass der anfängliche Krypto-Trend eine wesentliche gesellschaftliche Rolle eingenommen hat, weshalb sich nicht nur Politiker sowie Experten aus Wirtschaft oder Technik, sondern auch Asset Manager mit diesem Thema auseinandersetzen müssen um den Implikationen auf die zukünftige Entwicklung der Finanzbranche gerecht zu werden.

Krypto-Währungen funktionieren auf Basis der Blockchain- und Distributed Ledger Technologie (DLT). Hierbei handelt es sich um ein dezentrales System zur Dokumentation von Transaktionen, welches ein zentral geführtes Hauptbuch ersetzt, indem die gespeicherten Informationen vielen verschiedenen Parteien vorliegen, und von diesen verwaltet werden. Seither werden dieser Technologie revolutionäre Ansprüche zugewiesen, die über viele Branchen und Bereiche hinweg disruptive Veränderungen hervorbringen können. So ist die Finanzbranche in der Lage durch frühe Adaption der Technologie sowie dem Aufbau eines entsprechenden Produktportfolios eine Vorreiterrolle einzunehmen und die Transformation im Hinblick auf bspw. den Zahlungsverkehr voranzutreiben.

Neben der medialen Berichterstattung lässt sich die Entwicklung durch die ansteigende Marktkapitalisierung sowie der stetig steigenden Anzahl an Krypto-Währungen quantifizieren:

Während im Jahr 2013 nur 26 verschiedene Krypto-Währungen verfügbar waren, stieg diese Anzahl bis 2019 auf rund 2.380 an. Heutzutage werden bereits mehr als 10.500 Krypto-Währungen, mit einer gesamten Marktkapitalisierung von ca. 1,95 Billionen EUR, gehandelt. Davon entfällt ca. 40 % der Marktkapitalisierung auf den Bitcoin. Daher steht dieser, trotz der steigenden Relevanz anderer Krypto-Währungen, weiterhin im Mittelpunkt.

Der Bitcoin kann durch Fragmentierung in kleinere Einheiten umgerechnet werden. Die kleinste Einheit ist ein Satoshi, angelehnt an den Erfinder. Dieser Wert beträgt 0,00000001 BTC. Bitcoin lassen sich auf verschiedenen Websites, dazu zählen unter anderem Binance, Coinbase Pro, OKEx, Kraken, Huobi Global und Coinmarketcap, gegen eine Zahlung von klassischen Währungen wie EUR oder USD erwerben. Der erste Handel wurde im Frühjahr 2010 durch zwei Privatpersonen durchgeführt. Bei diesem wurden zwei Pizzen zu einem Preis von 10.000 BTC erworben. Der erste Währungstausch erfolgte kurze Zeit später, indem 10.000 BTC gegen 50 USD getauscht wurde. Seitdem stieg der BTC-Preis bis zu seinem All-Time-High von rund 68.789,63 USD im Oktober 2021 an. Danach folgte jedoch ein ebenso schneller Kursverfall, sodass der aktuelle Kurs lediglich rund 21.000 USD beträgt. (Stand Nov. 2022)

Die Bitcoin-Blockchain ist eine Datei welche kontinuierlich wächst und bereits eine Größe von 420.590 MB erreicht hat. Diese wächst aufgrund der weiteren Transaktionen stetig. Die aneinandergereihten Blöcke sind durchschnittlich rund 1,2 MB groß, bauen aufeinander auf und beinhalten sowohl die Informationen des vorherigen Blocks als auch die Informationen der aktuell ausgeführten Transaktion. Diese Informationen sind öffentlich zugänglich und werden in einem dezentralen Hauptbuch, dem Distributed Ledger gespeichert. Öffentlich bedeutet, dass jeder Teilnehmer des Netzwerkes die Blockchain jederzeit einsehen kann, jedoch können die Teilnehmer als solche anonym bleiben, solange ihre „digitale Bankadresse" (Wallet) nicht offengelegt wird. Wird eine Transaktion ausgeführt, so wird die Information über Käufer, Verkäufer und Anzahl der gehandelten Bitcoin so lange im Netzwerk verteilt, bis jeder Teilnehmer diese verifiziert hat und der Eigentumsübertrag vollzogen ist. Dieser Vorgang wird als Konsensmechanismus bezeichnet, da er für eine konsistente Daten- und Informationslage zwischen allen Netzwerkteilnehmer sorgt.

Seit der Erzeugung des ersten Bitcoin im Januar 2009 sind bis heute rund 19,2 Millionen BTC im Netzwerk verteilt worden. Neue Bitcoin wurden während des Konsensmechanismus erstellt, als Belohnung für das Verifizieren von Transaktionen (mehr dazu in Kapitel III). Die maximale Menge an Bitcoin ist auf 21 Millionen beschränkt. Die Begrenzung soll als Sicherheitsmechanismus vor Inflation schützen. Nach aktuellem Kenntnisstand wird der letzte Bitcoin voraussichtlich im Jahre 2140 im Netzwerk verteilt. Schätzungen zu Folge sind aktuell rund 30 % der bestehenden Bitcoin aufgrund der fehlenden Zugangsberechtigung zur eigenen Wallet verloren gegangen.

Aufgrund des Bitcoin ist die Idee vom Internet of Information (IoI) über das Internet of Payment (IoP) zu einem Internet of Value (IoV) zu gelangen entstanden. Beim IoI geht es um die Nutzung des Internets für einen schnellen Wissenstransfer. Der Gedanke des Wertetransfers blieb hierbei außenvor. Im Rahmen des IoP geht es um das Abwickeln von Zahlungen im Internet über entsprechende Dienstleister. Diese fungieren dabei als Intermediäre und nehmen für die Zahlungsabwicklung, im Sinne des Vertrauens zwischen den Parteien, eine tragende Rolle ein.

Im Gegensatz zum IoP schafft das IoV die Möglichkeit des direkten Wertetransfers. Hierbei steht die Lösung des Double-Spending-Problems im Vordergrund, welches bisher durch den Einsatz von Zahlungsabwicklern und nun durch die Blockchain gelöst werden kann. Double-Spending beschreibt die doppelte Ausgabe von gleichen Einheiten einer Währung.

Folglich können mit Hilfe der fortschreitenden Verbreitung des IoV sichere Transaktionen, ohne Beteiligung eines Zahlungsdienstleisters, dezentral durchgeführt werden.

Dieses Whitepaper soll in den folgenden Kapiteln ein Grundverständnis für die Blockchain-Technologie, die verschiedenen Anwendungsmöglichkeiten sowie mögliche disruptive Veränderungen für die Asset Management Industrie schaffen. Zusätzlich wird sowohl auf die aktuellen Entwicklungen am Krypto-Markt, als auch auf die Risiken und Chancen der Krypto-Assets eingegangen. Das Whitepaper dient darüber hinaus als Einstieg für anschließende Vertiefungen der Thematik vor dem Hintergrund des Risikomanagements.

Kapitel II – Krypto-Graphie und Signaturen

Wer tiefgehend verstehen möchte, welche bedeutenden Möglichkeiten sich aus der Blockchain Technologie für die Zukunft ergeben, muss sich mit zwei wesentlichen Themen auseinandersetzen: Krypto-Graphie & Signaturen.

Krypto-Graphie findet heutzutage bei nahezu der gesamten Kommunikation im Internet Anwendung. Für die sichere Übertragung von Nachrichten oder auch Passwörtern und zum Schutz gegen zunehmendes Cyber-Crime ist die Verschlüsselung von Nachrichten schlicht unabdingbar geworden. Bei Krypto-Währungen respektive DLT-Technologien finden Krypto-Graphische Verfahren in sehr vielen Funktionen Anwendung. Am eindrücklichsten ist jedoch die Verwendung als Zugang zum digitalen Konto. Mit Krypto-Graphie wird sichergestellt, dass nur der tatsächliche Besitzer Zugriff auf die auf der Blockchain auf ihn gesicherten Werte hat.

Grundsätzlich beschränken sich im Zusammenhang mit Blockchain-Technologien wichtige krypto-graphische Verfahren auf sogenannte „asymmetrische Verschlüsselungsverfahren". „Asymmetrisch" bedeutet, dass das Verschlüsseln und Entschlüsseln von Nachrichten jeweils mit einer anderen Zahlenfolge/einem anderen Schlüssel geschieht. Eines der bekanntesten Prinzipien im heutigen Internet ist das sogenannte Rivest–Shamir–Adleman Verfahren (RSA-Verfahren), welches im Folgenden zur Erklärung dient.

Private und Public Key: Alice möchte ihrem Freund Bob eine verschlüsselte Nachricht zukommen lassen. Dafür erzeugt Alice zunächst über ein mathematisches Verfahren, welches auf der zufälligen Auswahl und anschließenden Multiplikation zweier Primzahlen besteht, einen sogenannten „Private Key" (privaten Schlüssel). Der Schlüssel wird deswegen als „privat" bezeichnet, weil Alice diesen Schlüssel für sich unbedingt geheim halten sollte.

Aus dem mathematischen Verfahren ergibt sich anschließend ein sogenannter „Public Key" (öffentlicher Schlüssel), der das Schlüsselpaar komplettiert. Diesen öffentlichen Schlüssel teilt Alice ihrem Freund Bob mit. Es gilt: Nachrichten, die mit Private Key verschlüsselt wurden, können nur mit dem zugehörigen Public Key entschlüsselt werden, und andersherum (**Abbildung 1**).

Trotz des mathematischen Zusammenhangs zwischen beiden Schlüsseln, ist es für Bob auf Basis des ihm bekannten Public Keys, nicht möglich, den privaten Schlüssel von Alice herzuleiten. Um Alice eine vertrauliche Nachricht zu senden, würde Bob die von ihm verfasste Nachricht mit dem ihm bekannten öffentlichen Schlüssel verschlüsseln. Ist die Nachricht bei Alice angekommen, kann sie die Nachricht mit ihrem zugehörigen privaten Schlüssel entschlüsseln und die Nachricht lesen. Da nur Alice den privaten Schlüssel besitzt, das gleiche aber nicht unbedingt für den von ihr geteilten Public Key gelten muss, besteht absolute Vertraulichkeit nur, wenn Bob wie im Beispiel eine Nachricht an Alice sendet. Daher wird bei der Kommunikation im Internet häufig sowohl von Alice als auch von Bob ein Schlüsselpaar erstellt und daraufhin jeweils der öffentliche Schlüssel ausgetauscht.

Hash Funktionen: Der Begriff einer Hash-Funktion umfasst jegliche Arten von Funktionen, die eine beliebige Größe an Daten bzw. Bits auf eine festgelegte Größe abbilden. Rückgabewerte einer Hash-Funktion werden unter anderem „Digest", „Hashwert" oder auch einfach „Hash" genannt.

Beispielsweise bildet die Hashfunktion SHA 256 Dateien oder Bitfolgen beliebiger Größe stets auf einen Hashwert mit der Länge von 256 Bits ab. Die gleiche Datei resultiert dabei immer

Abbildung 1 – Nachrichten ver- bzw. entschlüsseln

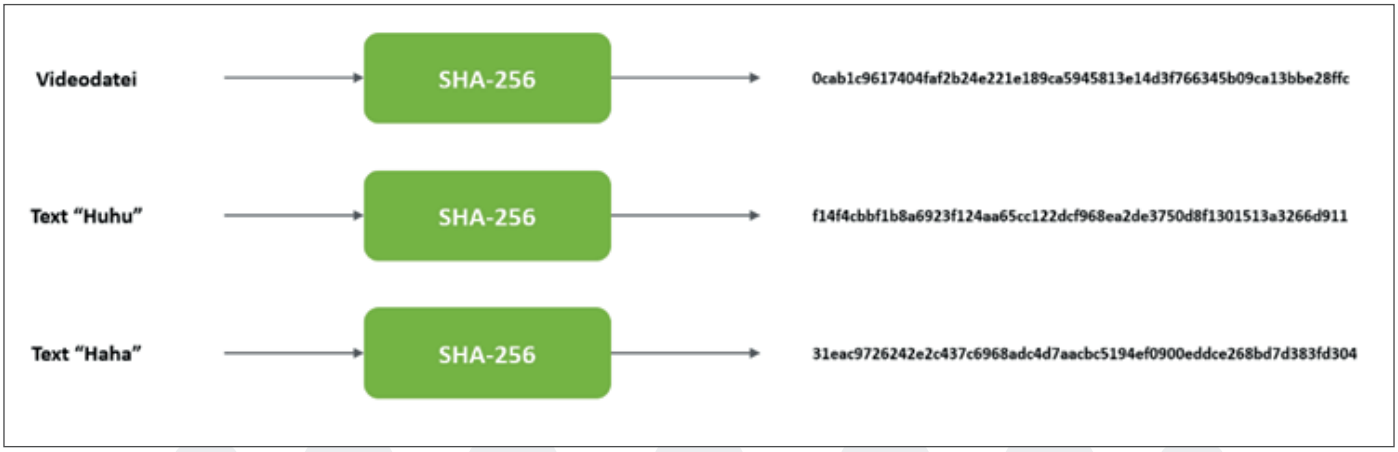
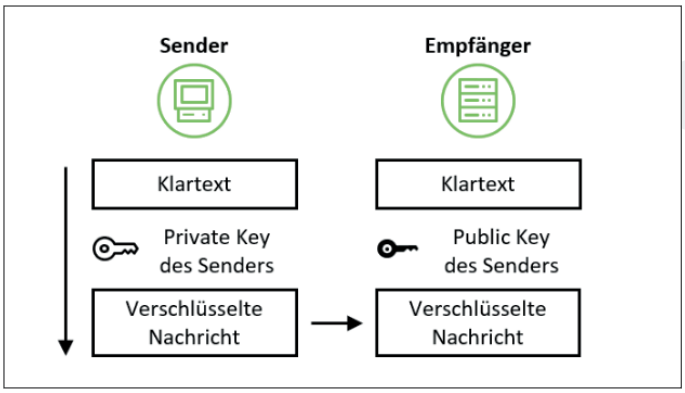


Abbildung 2 – Umwandlung von Texten in Hashwerte



im gleichen Hashwert. Kleinste Änderungen am Eingabewert der Hash-Funktion resultieren allerdings in einer deutlichen Veränderung des Ausgabewertes. Hash-Funktionen sind deshalb so nützlich, weil sie nicht umkehrbar sind. Es ist nicht möglich aus einem Hashwert den vorausgegangenen Eingabewert zu rekonstruieren (**Abbildung 2**).

DIGITALE SIGNATUREN:

Digitale Signaturen vereinen das Wissen aus Hash-Funktionen und den asymmetrischen Verschlüsselungsverfahren. Über

digitale Signaturen wird sichergestellt, dass ausschließlich der Besitzer des Private Keys eine Nachricht verschickt, bzw. eine Transaktion veranlasst hat. Eine digitale Signatur ist vereinfacht eine fälschungssichere Unterschrift oder eine Art Siegel in der digitalen Welt.

Das Bitcoin-Netzwerk bringt in seiner Funktionsweise die Konzepte der Hash-funktionen, der Krypto-Graphie und der digitalen Signaturen zusammen. Darauf wird im Folgenden näher eingegangen.

Kapitel III – Technologie hinter den Krypto-Assets

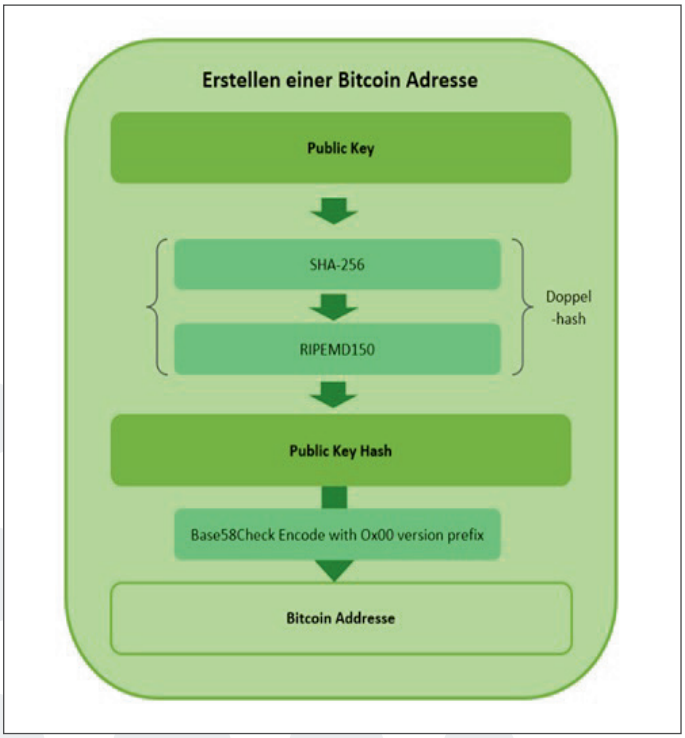
WALLET-ADRESSEN UND IHR ZUGEHÖRIGER KEY

Wallets sind die digitalen Bankkonten für Krypto-Währungen. Wie jedes Bankkonto benötigen auch Wallets eine eigene Adresse, um Transaktionen zu empfangen oder zu versenden. Im Folgenden wird erklärt, wie man eine Wallet Adresse erzeugt.

Um die im Wallet hinterlegten Werteinheiten zu transferieren benötigt man einen Zugangsschlüssel. Diese Aufgabe übernimmt eine digitale Signatur, die sich aus dem zum Wallet zugehörigen Private Key erzeugen lässt. Auf einer Blockchain werden keine Kontostände gespeichert. Die zur Verfügung stehenden Währungseinheiten ergeben sich aus der Menge der an die Wallet transferierten Einheiten, abzüglich der bereits ausgegebenen Einheiten. Es können niemals mehr Einheiten ausgegeben werden, als zuvor eingenommen wurden.

Um eine Bitcoin-Wallet-Adresse zu erzeugen, muss zunächst ein Public Key generiert werden. Im Gegensatz zur vorausgegangen vereinfachten Darstellung anhand des RSA-Verfahrens, spielt beim Bitcoin, für die Erzeugung des Schlüsselpaars, die sogenannte Elliptische-Kurven-Krypto-Grafie eine tragende Rolle. Für die Erzeugung des Schlüsselpaars wird zunächst eine 256-Bit große Zufallszahl generiert, welche den Private Key darstellt. Dass beim Verfahren jemals zwei gleiche Zufallszahlen generiert werden, ist nahezu ausgeschlossen. Zum Vergleich, die Menge an möglichen resultierenden Zufallszahlen (2^256) ist größer als die Menge der Atome im für die Menschen sichtbaren Universum (Schätzung 10^80). Nach der zufälligen Generierung des Private Key wird mit Hilfe elliptischer Kurven Multiplikation (ECM) der zugehörige Public Key generiert. Hier gilt ebenfalls, dass der Public Key nicht aus dem Private Key hergeleitet werden kann. Anschließend wird der Public Key zweifach gehashed und nachträglich mit Hilfe des Base58-Verfahrens encoded. Die Wallet-Adresse ist erstellt und das digitale Bitcoin-Konto erzeugt (**Abbildung 3**).

Abbildung 3 – Erstellen einerBitcion-Adresse



BLOCKCHAIN: HASH-KETTE:

Die Eigenschaften der Unveränderlichkeit und Fälschungssicherheit bei Blockchain Systemen resultieren aus der nicht nur bildlichen Verkettung jedes Blockes mit seinem Vorgänger. Dabei macht sich die Technologie die Eigenheiten von Hashfunktionen zu Nutze. Vereinfacht ausgedrückt hat jeder Block seinen eigenen Hashwert. Dieser Hashwert ergibt sich wiederum aus drei weiteren Hashwerten, dem Hashwert des vorangegangenen Blocks, dem Nonce des Blockes, und dem Merkle Root (**Abbildung 4**).

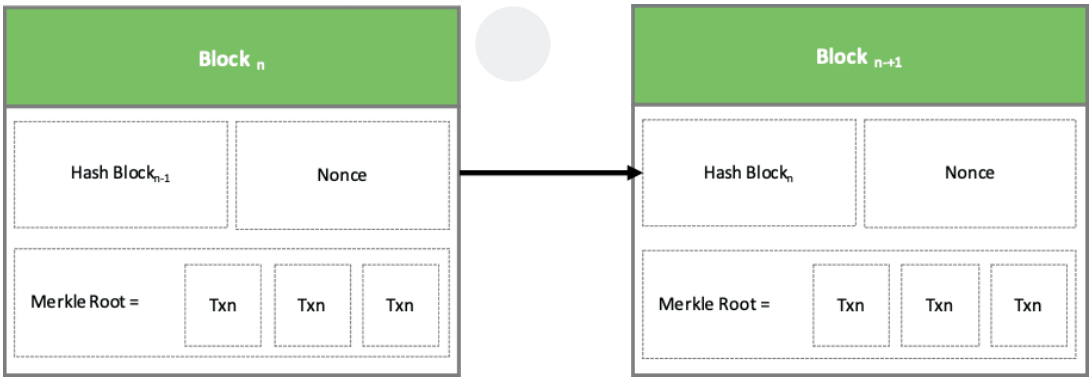


Abbildung 4 – Zusammensetzung eines neuen Blocks

Letzteres ist nichts anderes als der Hashwert einer baumartigen Verkettung aller Transaktionen innerhalb des Blockes.

Maßgeblich ist, dass die Veränderung von nur einem dieser Werte, den Hashwert des Blockes an sich verändert. Durch eine Veränderung des Block-Hashwerts, der als Eingabewert für den Hashwert des Folgeblockes dient, ginge eine Veränderung aller nachfolgenden Blöcke einher. Dies hat zur Folge, dass sobald der Hashwert eines Blockes einmal im Verlauf festgelegt ist, der Wert nicht mehr verändert werden kann, ohne dass dies sofort sichtbar für andere Netzwerkteilnehmer wäre. Eine nachträgliche Veränderung von Transaktionen oder ganzen Blöcken ist damit ausgeschlossen, die Blockchain ist somit sowohl unveränderlich als auch fälschungssicher.

KONSENS IN DEZENTRALEN SYSTEMEN:

Mit dem Verzicht auf zentrale Instanzen muss deren Kontoführungsrolle ein verteiltes Kassenbuch übernehmen. Es speichert keine Kontostände, sondern alle jemals erfolgten Zahlungstransaktionen und wird im Falle der Krypto-Währung Bitcoin als Blockchain auf den Rechnern der Teilnehmer (Knoten) redundant gespeichert. Die Rechner sind über das Web in einem öffentlichen Peer-to-Peer-Netzwerk verbunden, wie man es von Napster oder BitTorrent kennt. Dort wie hier gibt es im System per Definition keine zentrale Autorität und keine Zugangskontrollen oder andere Barrieren. Das Bitcoin-Netzwerkprotokoll gleicht die Datenstände der Nutzer automatisch ab und sorgt dafür, dass die Blockchain nur korrekte Daten, also gültige Transaktionen enthält. Das Protokoll verhindert, dass Nutzer bereits verbrauchtes Geld ausgeben (Double-Spending) oder Geld (mittels Signaturen) transferieren, welches ihnen gar nicht gehört. Der Konsensalgorithmus ist das Herzstück jeder Krypto-Währung.

Es wird im Wesentlichen in zwei verschiedene Konsensalgorithmen unterschieden: Proof-of-Work (PoW) und Proof-of-Stake (PoS).

PROOF-OF-WORK:

Der beim Bitcoin angewendete PoW Algorithmus ist darauf ausgerichtet, dass sich etwa alle 10 Minuten ein neuer Block bildet. Der neu gebildete Block umfasst alle validierten Transaktionen, die sich seit der Fertigstellung des vorangegangenen Blocks ergeben haben. Die Bildung eines Blockes läuft folgendermaßen ab:

I. Nutzer erzeugen eine Überweisung mit ihrer Wallet. Die Adresse zu der Wallet des Zahlungsempfängers haben sie z. B. mit Hilfe eines QR-Codes erfasst. Neue Zahlungstransaktionen werden von der Software an alle Knoten im P2P-Netzwerk verteilt.

II. Jeder Knoten, der aktiv an der Konsensfindung teilnimmt, fasst die im Netzwerk propagierten Transaktionen zu einem Block zusammen. Vor der Aufnahme in den Block prüft er zunächst die Gültigkeit der Transaktion: ist das Geld nicht bereits ausgegeben? Stimmt die digitale Signatur des Zahlers?

III. Zusätzlich zur Validierung und der Sammlung an Transaktionen, muss der Knoten für die Fertigstellung des Blockes, den Block um eine Zahl ergänzen (Nonce), sodass der Hash-Wert des geformten Blockes eine vorgegebene Anzahl führender Nullen aufweist. Dieses Hash-Puzzle ist nur durch Ausprobieren lösbar, die genaue Dauer der Lösungsfindung lässt sich nicht prognostizieren, sie folgt einer Bernoulli-Verteilung. Im Durchschnitt beträgt sie 10 Minuten und gibt damit die Bitcoin-Konsenszykluszeit vor. Das Lösen des Rätsels erfordert dabei Rechenleistung (Work), um innerhalb kürzester Zeit möglichst viele Zufallswerte auszuprobieren. Dieser Prozess wird als „Mining" bezeichnet.

IV. Die Knoten aus Schritt II stehen bei der Lösung des Hash-Puzzles im Wettbewerb. Der Sieger des Rennens ist rein zufällig. Der neu gebildete Block des Siegers ist der erste und einzige, der im Netz verteilt wird.

V. Die anderen Knoten akzeptieren den neuen Block nur dann, wenn alle enthaltenen Transaktionen gültig sind.

VI. Die Akzeptanz des neuen Blocks führt dazu, dass er an die Blockchain angehängt wird. Und zwar an den Block, den der blockbildende Knoten zu Beginn seines Hash-Puzzles als den letzten in der Kette betrachtete. Die Knoten verfolgen immer den längsten Pfad in der Kette. Kinderlose Verzweigungen werden von der Software abgeschnitten.

Die Verwendung einer Zufallszahl bzw. das Lösen eines Rätsels für die Bestimmung des nächsten Blockes hat mehrere Gründe:

1. Aus spieltheoretischer Sicht ist es für einen Angreifer nicht prognostizierbar, welcher Block als nächster in die Kette aufgenommen wird. Der Angreifer kann sich also keinen Knoten zur Manipulation aussuchen

2. Die Lösung des Rätsels erfordert das Einbringen von Rechenleistung, um überhaupt die Chance zu haben, den nächsten Block bestimmen zu dürfen.

3. Wie bereits erläutert, ist der Hashwert des vorangegangenen Blocks auch ein Bestandteil für den Hashwert des Nachfolgers. Möchte ein Angreifer einen Block in der Blockchain verändern, müsste er also nicht nur den Nonce des zu manipulierenden Blockes errechnen, sondern auch für alle Folgenden. Das ist mit der heutzutage zur Verfügung stehenden Rechenleistung ein unmögliches Vorhaben.

Der PoW Algorithmus macht es für Angreifer sehr schwer, das Netzwerk zu sabotieren und wird daher als äußerst sicher angesehen. Allerdings bringt der Algorithmus entscheidende Nach-

teile mit sich. Dadurch, dass die Teilnehmer des Netzwerks vielfältig die gleiche Menge an Transaktionen validieren, bzw. jeweils versuchen für den gleichen Block als Erstes das Rätsel zu lösen, ist ein Netzwerk mit PoW zum einen sehr energieintensiv und zum anderen auch nicht skalierbar. Das Erscheinen neuer Teilnehmer führt ausschließlich zum Verbrauch von mehr Energie und nicht zur Validierung von mehr Transaktionen. Das Bitcoin-Netzwerk (Layer I) kann nur ca. 3 Transaktionen pro Sekunde (tps) bestätigen und ist daher im Vergleich zu den Kreditkartensystemen (mehr als 10.000 tps) nicht konkurrenzfähig. Die Layer II, auf welchen im weiteren Verlauf des Kapitels eingegangen wird, kann jedoch ähnliche Leistung wie das Kreditkartensystem erzielen, weshalb ein Vergleich grundsätzlich schwierig ist. Aufgrund der gestiegenen Anzahl an Nutzern und der schlechten Skalierbarkeit haben sich in der Vergangenheit zeitweise Transaktionskosten von über 10 EUR pro Transaktion ergeben. Dies macht das Überweisen kleinerer Beträge unwirtschaftlich.

PROOF-OF-STAKE:

PoS ist im Vergleich zum PoW Algorithmus zentralisierter. Das Validieren von Transaktionen und Formen neuer Blöcke obliegt beim PoS ausschließlich einer eingeschränkten Menge an Netzwerkteilnehmern, sogenannten „Validatoren".

Wie lässt sich nun die Dezentralität aufrechterhalten und Vertrauen zu Validatoren herstellen? Dies wird gelöst indem bis auf eine kleine Einstiegsbarriere jeder einen eigenen Validator-Knoten starten kann. Zusätzlich können Netzwerkteilnehmer durch Delegation ihrer Coin („Staking") einem Validator ihr Vertrauen aussprechen. Als Anreiz für die Delegation werden Netzwerkteilnehmer anschließend prozentual an den erwirtschafteten Transaktionsgebühren beteiligt. Um einen Validator-Knoten starten zu können, benötigt es bspw. beim ETH 2.0 Netzwerk eine Summe von 32 ETH. Dies ist beim Ethereum Netzwerk die Barriere, um dem Validator ein Eigeninteresse an der Korrektheit seiner Validierungen zu bescheinigen.

Aufgrund des Wettbewerbs zwischen den verschiedenen Krypto-Projekten, die sicherste, schnellste und dezentralste Lösung anzubieten gibt es viele unterschiedliche PoS-Algorithmen und Ansätze. Bisher ist nicht absehbar, welche Verfahren sich langfristig durchsetzen werden.

SMART-CONTRACTS:

Smart-Contracts sind die Grundlage für die sich ergebenden Chancen bei der Verwendung von Blockchain Technologien und ein wesentliches Argument für den Einstieg von Investoren in den Krypto-Markt. Lange Zeit benötigte es eine dritte Partei, um Vertrauen zwischen zwei Parteien (bspw. Käufer und Verkäufer) herzustellen. Die Rolle des vertrauenswürdigen Dritten, der das Geschäft überwacht, übernimmt beim Häuserkauf bspw. der Notar und beim Verkauf von gebrauchten Waren über das Internet eine Plattform wie Ebay. Smart-Contracts machen diesen Dritten durch ihren Programmcode überflüssig.

Überweist der Käufer das Geld an die vom Smart-Contract überwachte Adresse, wird automatisch der Grundbucheintrag für das Haus geändert. Dabei sind der Programmierung fast keine Grenzen gesetzt. So lassen sich Smart-Contracts wiederum mit weiteren Smart-Contracts verbinden, um damit kleine Programme auf der Blockchain zu erzeugen. Smart-Contracts bekommen analog zu Wallets eine eigene Adresse auf der Blockchain. Zusätzlich zum hinterlegten Programmcode gibt es auch die Möglichkeit Zustände und Daten zu speichern. So können auch neue virtuelle Einheiten erschaffen und ihre zugehörigen Eigentümer innerhalb des Smart Contracts hinterlegt werden. Für das Erzeugen neuer virtueller Einheiten (Token) bietet die Ethereum Blockchain verschiedene Standards als Vorlage. Die Standards dienen dazu, das Emittieren neuer Tokens einfacher zu gestalten und auf der Blockchain Interoperabilität zu ermöglichen. Die bekanntesten Standards sind der ERC-20, der ERC-721, der ERC-777 und der ERC-1155 Token Standard (**Abbildung 5**).

Name des Standards	Verwendungszweck	Einführungsdatum
ERC-20	Standard für das Erstellen von Fungible Tokens. Bietet Basisfunktionalitäten, wie das transferieren von Tokens...	19.11.2015
ERC-721	Standard für das Erstellen von NFTs	24.01.2018
ERC-777	Standard, der es ermöglicht im Auftrag einer anderen Adresse, eines Vertrags oder Accounts Tokens versenden	20.11.2017
ERC-1155	Ein Standard für Smart Contracts, die mehrere Token Typen verwalten	17.06.2018

Abbildung 5 – Erläuterung der bekanntesten Etheruim-Standards

UNTERSCHIEDLICHE LAYER BEI BLOCKCHAIN TECHNOLOGIEN:

Alle bisher dargestellten Grundprinzipien und Funktionalitäten auf Blockchain-Systemen sind wesentlich für die Layer I eines Blockchain-Ökosystems. Layer I gilt als Rückgrat oder auch als Herzstück eines Blockchain-Systems. Hier werden sowohl fundamentale Operationen dargelegt, Programmiersprachen festgelegt und der Konsensalgorithmus definiert. Grundsätzlich gilt, die Layer I einer Blockchain führt die einzige finale Version der verteilten Datenbank.

Wenn Blockchain-Systeme in Zukunft Basis für eine Vielzahl von Transaktionen des alltäglichen Lebens werden sollen, bedarf es einer hohen Skalierbarkeit. Wenn Millionen Micro-Transaktionen die Blockchain sekündlich für sich beanspruchen, kommt es zu einer starken Belastung. Verzögerungen oder hohe Transaktionskosten könnten die Folge sein. Um Last von der Haupt-Chain (Layer I) abzunehmen wurde deshalb beispielsweise beim Bitcoin (Bitcoin Lightning Netzwerk) sowie dem Ethereum Netzwerk eine zweite Blockchain (sog. Layer II) auf Basis der Layer I aufgesetzt. Layer II und Layer I befinden sich in ständigem Austausch. Layer II hat die Aufgabe Transaktionen zu bündeln und zu validieren, bevor diese dann auf der Layer I final Teil der Blockchain werden. Dies skaliert und beschleunigt das Blockchainsystem. Für die Funktionsweise von Layer II Blockchains gibt es verschiedene Lösungsansätze. Häufig werden Channels oder sogenannte „Optimistic Rollups" verwendet. Immer häufiger wird auch von einer Layer III Blockchain gesprochen. Der Ethereum Mitbegründer Vitalik Buterin sieht für eine Layer III Blockchain verschiedene Anwendungsfälle. Ein Layer III könnte laut ihm „maßgeschneiderte Funktionalitäten" wie z.B. datenschutzbasierte Anwendungen übernehmen.

Für andere in der Krypto-Branche sind Layer III bereits als Anwendungsebene präsent. Die Anwendungsebene bezieht sich auf alle Arten von Anwendungen, die auf Smart Contracts basieren und den Nutzern der Blockchain Benutzeroberflächen zur Verfügung stehen. Eine einheitliche Definition der Layer III bleibt bisher offen.

Kapitel IV – Abgrenzung der verschiedenen Tokenarten

Wie bereits zum Ende des vorangegangenen Kapitels eingeleitet, kann ein Token als eine Werteinheit innerhalb eines Ökosystems einer technischen Plattform definiert werden. Die Ausgabe von Tokens geschieht meistens mit der Hilfe von Smart-Contracts auf einer Blockchain. Die der Blockchain zugrundeliegende Währung (z.B. Ethereumoder Bitcoin) wird daher zur Abgrenzung der typischen Tokens meist als „Coin" bezeichnet.

Basierend auf seinen jeweiligen Eigenschaften und unterschiedlichsten Funktionen kann ein Token in verschiedene Klassen eingeteilt werden. Die jeweilige Klassifizierung hat dabei auch Auswirkungen auf den regulatorischen Rahmen, unter den das Token fällt. Den technischen Möglichkeiten sind fast keine Grenzen gesetzt.

So können Rechte (z.B. Wahlrecht, Eigentumsrechte, Ausübungsrechte) oder auch reale Objekte in der Form von Token dargestellt werden. Der Prozess der Übertragung auf Blockchain Technologien wird als „Tokenization" bezeichnet. In Abhängigkeit der Ausgestaltung von Token, können diese zunächst in Fungible (Austauschbare) und Non-Fungible (Nicht Austauschbare) Tokens unterteilt werden. Non-Fungible Token sind der breiten Bevölkerung eher unter dem Akronym NFT bekannt.

Bezüglich der funktionalen Eigenschaften von Token wird in der Krypto-Branche typischerweise in Payment Token, Utility Token, Hybrid Token, Security Token und Stablecoin unterschieden. Aufgrund der Vielfalt unterschiedlichster Ausprägungen von Token gibt es bis dato keine einheitliche Definition für Tokenarten.

Zumindest aus regulatorischer Sicht soll es nun aber ein Rahmenwerk für die Klassifizierung und rechtliche Einordnung sämtlicher Tokenarten geben. Eine große Bedeutung für die einheitliche Entwicklung notwendiger Regulatorik wird in naher Zukunft der von der Europäischen Union geplanten Verordnung MiCa (Markets in Crpyto Assets Regulation) zukommen. Die MiCa umfasst allerdings ausschließlich fungible Token. Für die erwähnten Non-Fungible Tokens (NFTs) plant das EU-Parlament ein eigenes regulatorisches Rahmenwerk zu erstellen.

Aufgrund der Bedeutung der MiCa wird im Folgenden daher auf die wesentlichen nach MiCa definierten Tokenarten, sowie auf die Security Token eingegangen.

FUNGIBLE TOKEN:

Grundsätzlich kann zwischen Wertreferenzierte-, Nicht-Wertreferenzierte-Token, CBDCs (Central Bank Digital Currencies) und Utility Token unterschieden werden.

Utility Token sind Token, die keinen finanziellen Zwecken, sondern der Verwendung innerhalb eines Ökosystems bzw. dessen Funktionen, dienen.

Wertreferenzierte-Token (Stablecoin) verfolgen die Intention in ihrem Wert stabil zu bleiben und beispielsweise den Preis von Nominalwährungen, Waren oder Rohstoffen abzubilden. Wertreferenzierte-Token haben daher ihr Abbild oder andere Arten von Wertpapieren, Waren oder Rohstoffen als hinterlegte Sicherheit. Diese Art von Token zielt darauf ab als Zahlungsmittel oder auch Wertspeicher verwendet zu werden. Ein Beispiel

ist der von der US-amerikanischen Firma Circle herausgegebene Token USDC, der den Wert des US-Dollars abbilden soll und nach Unternehmensangaben zum Großteil mit Cash und Staatsanleihen als Sicherheiten hinterlegt ist.

Nicht-wertreferenzierte-Token haben dagegen keine hinterlegte Sicherheit und keine Kopplung an eine nationale Währung. Vielmehr sind die nicht-wertreferenzierten-Token damit ein Sammelbegriff für Token unterschiedlicher Ausprägung, die weder den vorher genannten Tokenarten zuzuordnen sind noch einem Wertpapier im aufsichtsrechtlichen Sinne entsprechen.

Payment Token wie Bitcoin oder Ethereum sind daher nach MiCa ebenfalls den Nicht-wertreferenzierten-Token zuzuordnen.

Eine weitere wichtige Unterkategorie sind die Security Token. Sie sind nicht von der MiCa umfasst, da sie im regulatorischen Kontext dem aufsichtsrechtlichen Begriff von Wertpapieren zugeordnet werden können. Ein Security Token repräsentiert meist Eigenkapital, Schulden, oder einen realen Vermögenswert auf einer Blockchain. Die erstellten Token machen einen Vermögenswert damit handelbar. Security Token können, von ihrer Funktionsweise, herkömmlichen Wertpapieren sehr ähnlich oder auch gleichzusetzen sein.

NFTS:

Bei Fungiblen Token ergibt sich kein Unterschied zwischen den jeweiligen ausgegebenen Token, weshalb sie grundsätzlich untereinander austauschbar sind. Als Beispiel eignet sich eine Ein-Euro-Münze: Zwischen Münzen verschiedenen Ursprungs wird grundsätzlich im Wert nicht unterschieden. Anders gestaltet es sich bei Immobilien, Automobilen oder auch Kunstwerken. Aufgrund der vollkommen unterschiedlichen Charakteristiken wie bspw. bei Immobilien der Lage, der Architektur, der verbauten Technik oder der Größe des Grundstücks, ergibt sich zwischen verschiedenen Objekten ein unterschiedlicher Wert. Sobald sich aus der individuellen Gestaltung einer Gruppe von Token derselben Gattung ein Wertunterschied oder spezifisches Merkmal hinsichtlich der Bereitschaft zum Tausch ergibt, ist dieser also als „Non-Fungible“ zu klassifizieren. Es handelt sich um ein NFT.

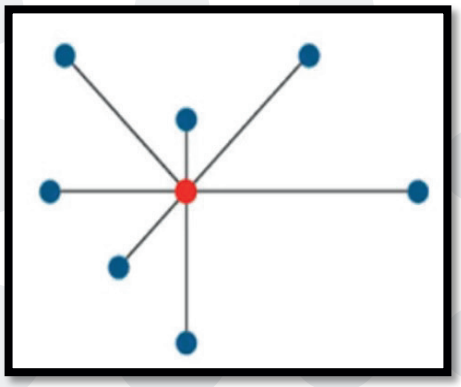
Kapitel V – Chancen und Nutzen der Tokenisierung

Bevor die Möglichkeiten und Vorteile der Tokenisierung erörtert werden, soll ein kurzer Exkurs die Unterschiede zwischen einem zentralen und dezentralen Netzwerk sowie die verschiedenen Blockchain-Arten aufzeigen, um ein tiefergehendes Verständnis für die Blockchain-Technologie zu schaffen.

ZENTRALES NETZWERK:

Betrachten wir das gesamte Internet, welches global verteilt ist und aus einer Vielzahl einzelner Rechner, Server, Netze etc. besteht. Diese Spannen in Ihrer Gesamtheit das komplette Internet auf. Demnach existieren zentrale Knotenpunkte, an denen sich einzelne Knoten zu einem Netzwerk zusammenschließen. Anhand dieser Knotenpunkte lässt sich ein zentrales Netzwerk (**Abbildung 6**) und dessen großer Schwachpunkt erläutern. Betrachten wir das folgende Netzwerk, wobei der zentrale Knotenpunkt rot dargestellt ist:

Abbildung 6 – zentrales Netzwerk

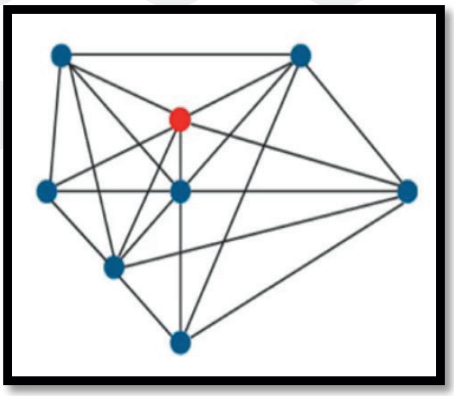


Sofern der zentrale Knotenpunkt ausfällt, kann er keine Datenübertragungen innerhalb des Netzwerks mehr gewährleisten, da jegliche Anfragen über ihn gesteuert werden und alle anderen Rechner im Netzwerk über ihn miteinander verbunden sind. Dies wird auch als Single Point of Failure bezeichnet.

DEZENTRALE NETZWERKE:

Im Rahmen eines dezentralen Netzwerks (**Abbildung 7**) wird die Kontrolle auf alle verfügbaren Knotenpunkte übertragen. Jeder einzelne Knotenpunkt ist mit den anderen Knoten innerhalb des Netzwerkes verbunden. Dafür betrachten wir das folgende Schaubild:

Abbildung 7 – dezentrales Netzwerk



Dies entspricht dem Grundgedanken der Blockchain, denn jedes Mitglied (jeder Knoten) eines Netzwerkes verfügt über eine Kopie der exakt gleichen Daten. Somit werden verfälschte bzw. veränderte Daten durch die anderen Netzwerkteilnehmer erkannt und zurückgewiesen. Zusätzlich hat jeder Knoten Zugriff auf eine gemeinsam genutzte Echtzeitansicht der geteilten Daten. Dabei können sich alle Parteien sicher sein, dass bei der Übertragung keine Daten verloren gegangen sind.

Darüber hinaus trägt die Dezentralisierung zur Optimierung der Ressourcenzuteilung bei. Zum Beispiel, indem die versprochenen Dienstleistungen mit größerer Sorgfalt und besserer Leistung erbracht werden.

Schließlich sei noch zu erwähnen, dass ausgefallene Knotenpunkte automatisch synchronisiert werden, sodass sie erneut ein Teil des Netzwerks werden, sobald sie wieder up-to-date sind. Dadurch können alle Datenverluste, Manipulationen und sogar erfolgreiche Hacking-Angriffe nahezu vollständig ausgeschlossen werden.

Nachdem wir uns nun ein Bild über die verschiedenen Netzwerke gemacht haben, werden wir auf die verschiedenen Blockchain-Arten eingehen.

ÖFFENTLICHE BLOCKCHAIN:

Die Blockchain Technologie bietet ihrem Ursprung nach das höchste Maß an Transparenz. Auf einer öffentlichen Blockchain ist jedem freigestellt, sich an dem Netzwerk zu beteiligen. Die integrierten Prozesse, ihre Daten und Transaktionen sind für alle Teilnehmer einsehbar und unveränderbar gespeichert. In der konkreten Anwendung könnten bspw. Lieferketten auf der Blockchain dokumentiert, nachverfolgt und somit das Vertrauen in die Herkunft von Produkten gestärkt werden.

Allerdings ist hundertprozentige Transparenz nicht immer gewünscht. Für den Schutz sensibler Daten kann es notwendig sein, Daten nur einem ausgewählten Teilnehmerkreis offenzulegen. Auch dafür bietet die Blockchain entsprechende Lösungen.

PRIVATE BLOCKCHAIN:

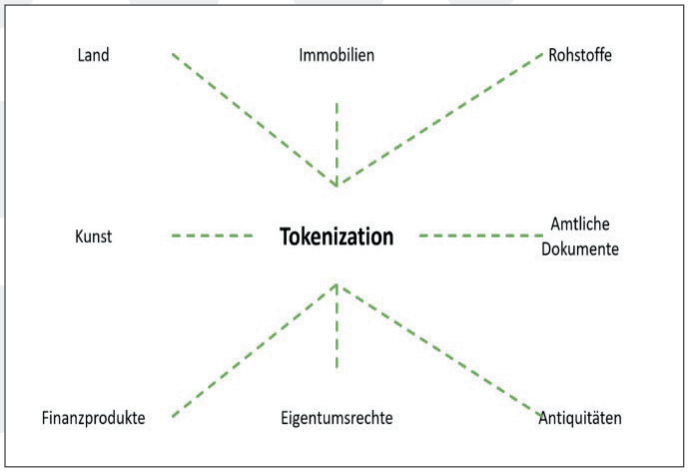
Private Blockchains sind nicht öffentlich zugängig. Dabei wird durch eine Gruppe von Initiatoren der Teilnehmerkreis festgelegt. Die Gruppe der Initiatoren bilden ein sogenanntes Konsortialnetzwerk. Dadurch ist zum einen das Modell und zum anderen das Betreiben des Netzwerks dezentraler gestaltet. Veränderungen und Updates des Quellcodes müssen durch die beteiligten Parteien im Rahmen einer vereinbarten und akzeptierten Form (Konsensus) bestätigt werden. Dazu zählt auch die Erweiterung des Netzwerkes durch die Aufnahme weiterer Teilnehmer. Das Schlüsselkonzept der privaten Blockchain sind Berechtigungen. Damit wird sichergestellt, dass nur ausgewählte Teilnehmer Lese- und Schreibrechte für die relevanten Inhalte erhalten.

HYBRID BLOCKCHAIN:

Das Netzwerk innerhalb einer hybriden Blockchain ist einerseits für interne Inhalte geschlossen, andererseits problemlos erweiterbar. Dabei können ausgewählte Transaktionen öffentlich und andere privat in einem anonymen Umfeld abgewickelt werden.

Aufgrund des erweiterten Verständnisses der verschiedenen Netzwerk- bzw. Blockchain-Arten, können wir nun auf die zahlreichen Vorteile, die sich durch das Abbilden realer Vermögenswerte auf der Blockchain ergeben, eingehen (**Abbildung 8**).

Abbildung 8 – Möglichkeiten der Tokenisierung



OPERATIVE EFFIZIENZ:

Durch die vollständig digitale Abwicklung von Transaktionen über Blockchain Technologien und das Wegfallen von Intermediären werden Transaktionskosten signifikant reduziert. Durch Automatisierung ergeben sich zusätzlich Vorteile hinsichtlich der Geschwindigkeit bei der Abwicklung von Transaktionen. Bezogen auf die Finanzindustrie könnten Settlement-Prozesse beschleunigt und damit Finanzmarkttransaktionen effizienter werden. Laut Roland Berger ergeben sich bei hoher Adaption in der Finanzindustrie bis 2030 Kostenvorteile in Höhe von 4,6 Mrd. EUR.

TEILBARKEIT:

Durch die Blockchain Technologie wird es möglich Vermögenswerte zu teilen. Das heißt konkret, dass bspw. mehrere Parteien sich an der gleichen Wohnung beteiligen können. Das ist unter

anderem in der aufkommenden Sharing-Economy interessant, wo der Gebrauch und das Teilen von Vermögenswerten den Besitz immer häufiger ersetzt.

Ein weiterer Vorteil ergibt sich hinsichtlich Einstiegsbarrieren. Während bspw. das Kaufen einer Ferienwohnung in New York für eine einzelne Familie vorerst nicht erschwinglich gewesen ist, ist es im Bund mit zwei weiteren Familien dann vielleicht doch möglich. Hohe Mindestbeträge für Investments lassen sich somit eliminieren, was die Idee des „Inclusive Finance" unterstützt und zugleich den Markt für weitere Teilnehmer öffnet.

Dadurch, dass öffentliche Blockchains globale Netzwerke sind, fallen auch geografische Einschränkungen für Investoren weg.

Weitere Marktteilnehmer, kleinere Mindestbeträge und die Schnelllebigkeit von Transaktionen lassen damit vormals illiquide Vermögensgegenstände liquide werden.

SINGLE POINT OF TRUTH:

Das Prinzip des Single-Point-of-Truth (SPOT) beschreibt die Idee einen zentralen Ort als verlässliche Quelle konsistenter Daten zu haben. Unternehmen haben im vergangenen Jahrzehnt riesige Mengen an Daten generiert. Durch den Wandel von Technologien und das Entstehen von Datensilos wird es für Unternehmen zunehmend schwieriger diese Daten miteinander zu verbinden, zu sortieren und damit zu nutzen. Eine private Blockchain, auf der alle Daten und auch jegliche Vermögenswerte für einen bestimmten Teilnehmerkreis gespeichert werden können, könnte das Risiko für Datenverlust sowie erfolgreiche Cyberangriffe verringern.

Gleichzeitig ergeben sich weitere Möglichkeiten für das Austauschen von Daten. Durch das Verwenden hybrider Blockchains könnten Geschäftspartner Daten einfacher teilen und auf Basis dieser Daten interagieren. Durch das Einbinden von Akteuren in den Datenfluss von Unternehmen ließe sich auch die Effizienz entlang ganzer Wertschöpfungsketten verbessern.

Kapitel VI – Neue Regulatorik als Enabler für eine neue Kapitalmarktstruktur

Die dynamischen Entwicklungen in den Bereichen Blockchain, Tokenization und Krypto-Währung stellt auch für den Regulator eine neue Herausforderung dar. In diesem Kapitel werden die zentralen Gesetze und Regularien, welche auf Krypto-Assets Anwendung finden, skizziert und die entsprechenden Implikationen beschrieben.

KRYPTO-VERWAHRGESCHÄFT (KWG)

Das Krypto-Verwahrgeschäft wurde durch das Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie (Änderungsrichtlinie) vom 12. Dezember 2019 (Umsetzungsgesetz) als Finanzdienstleistung eingeführt. Das Umsetzungsgesetz, wie auch die Änderungsrichtlinie, sehen u.a. eine Erweiterung des geldwäscherechtlichen Verpflichtetenkreises, insbesondere im Bereich sog. „virtueller Währungen", vor.

Dienstleistungsanbieter, die den regelmäßigen Umtausch von virtuellen Währungen in gesetzliche Zahlungsmittel und umgekehrt sowie in andere Krypto-Werte anbieten, sind bereits Finanzdienstleistungsinstitute und damit müssen sie die Geldwäscherechtlichen Bestimmungen einhalten, da Krypto-Werte, je nach Ausgestaltung, Finanzinstrumente im Sinne des § 1 Abs. 11 Satz 1 Nr.10 KWG sein können. Der Umtausch von Finanzinstrumenten in Krypto-Werte im Sinne des KWG fällt in den Katalog der Bank- oder Finanzdienstleistungsgeschäfte nach § 1 Abs. 1 Satz 2, Abs. 1a Satz 2 KWG.

Den gesetzlichen Tatbestand des Krypto-Verwahrgeschäftes erfüllt, wer:

- Krypto-Werte oder private krypto-grafische Schlüssel, die dazu dienen, Krypto-Werte zu halten, zu speichern oder zu übertragen
- für andere
- verwahrt, verwaltet und sichert.

KRYPTO-WERTPAPIERE, (EWPG)

Der Gesetzentwurf dient der Modernisierung des deutschen Wertpapierrechts und des dazugehörigen Aufsichtsrechts. Zentraler Bestandteil ist die Einführung des neuen Gesetzes über elektronische Wertpapiere – eWpG. Nach aktueller Rechtslage sind Finanzinstrumente, die zivilrechtlich als Wertpapiere gelten, in einer Urkunde zu verbriefen. Die Papierurkunde ist Anknüpfungspunkt für die sachenrechtlichen Übertragungstatbestände und trägt u.a. dem Verkehrsschutz potenzieller Erwerber Rechnung. Um die Verkehrsfähigkeit von Wertpapieren und den rechtssicheren Erwerb gleichwohl zu gewährleisten, bedarf es eines geeigneten Ersatzes der Papierurkunde, z.B. durch Eintragung in ein Register auf Basis der Blockchain-Technologie.

KRYPTO-WERTPAPIERREGISTER (AN STELLE VON CLEARSTREAM) EWPG

§4 Abs.3 Nr. 2 eWpG: Ein Krypto-Wertpapier ist ein elektronisches Wertpapier, das in ein Krypto-Wertpapierregister eingetragen ist.

§16 Abs. 1 eWpG: Ein Krypto-Wertpapierregister muss auf einem fälschungssicheren Aufzeichnungssystem geführt werden, in dem die Daten in der Zeitfolge protokolliert und gegen unbefugte Löschung sowie nachträgliche Veränderungen geschützt gespeichert werden.

Die BaFin führt gemäß § 20 Abs. 3 eWpG eine öffentliche Liste („Krypto-Wertpapierliste“) im Internet über ihr nach § 20 Abs. 1 S. 2 eWpG mitgeteilte Veröffentlichungen bezüglich der Eintragung von Krypto-Wertpapieren im Bundesanzeiger. Die Veröffentlichung dieser Liste soll es dem Rechtsverkehr unkompliziert ermöglichen, eine einfache Übersicht über die mit einem Krypto-Wertpapier verbundenen Veröffentlichungen zu erhalten. Die Angaben in der Liste beruhen auf den von den Emittenten vorgenommenen Veröffentlichungen im Bundesanzeiger. Sie enthält eine Auflistung mit Angaben zum Emittenten, zur registerführenden Stelle, zum entsprechenden Krypto-Wertpapier, zum Datum der Eintragung im Krypto-Wertpapierregister sowie im Fall einer Änderung das Datum der Änderung und den wesentlichen Inhalt der jeweiligen Änderung.

ACCOUNTING

WIRTSCHAFTSGUT NACH HGB

Einheiten einer virtuellen Währung oder sonstige Token sind nicht abnutzbare Wirtschaftsgüter materieller Art, die nach den allgemeinen bilanzsteuerrechtlichen Grund-sätzen dem Anlage- oder Umlaufvermögen zuzuordnen sind. Sie sind bei Zuordnung zum Anlagevermögen unter Finanzanlagen im Sinne des § 266 Absatz 2 A. III. Handelsgesetzbuch (HGB) und bei Zuordnung zum Umlaufvermögen unter sonstige Vermögensgegenstände im Sinne des § 266 Absatz 2 B. II. 4. HGB auszuweisen.

ZUGANGSBEWERTUNG NACH HGB

Die für die Blockerstellung sowie als Transaktionsgebühr zugeteilten Einheiten einer virtuellen Währung oder sonstigen Token werden angeschafft (tauschähnlicher Vorgang). Die Anschaffungskosten entsprechen dem Marktkurs im Zeitpunkt der Anschaffung der Einheiten einer virtuellen Währung oder sonstigen Token (Ableitung aus § 6 Absatz 6 Satz 1 EStG). Wenn ein Börsenkurs vorhanden ist, ist dieser als Marktkurs zu Grunde zu legen. Bei fehlenden Börsenkursen kann ein Kurs von einer Handelsplattform (z. B. Kraken, Coinbase und Bitpanda) oder einer webbasierten Liste angesetzt werden.

FOLGEBEWERTUNG NACH HGB

Die Folgebewertung erfolgt je nach Einstufung als Umlauf- oder Anlagevermögen zum strengen oder gemilderten Niederstwertprinzip (§ 253 Abs 4 S 1, Abs 3 S 5). Da Krypto-Währungen eine unbegrenzte Nutzungsdauer aufweisen, scheidet eine planmäßige Abschreibung aus; § 253 Abs 3 S 3 ist nicht einschlägig. Neben einer Einzelbewertung dürfte für eine konkrete Krypto-Währung auch die Anwendung der Gruppen- bzw. Durchschnittsbewertung (§ 240 Abs 4) zulässig sein, sofern man immaterielle VG unter bewegliche VG subsumiert; eine Zusammenfassung verschiedener Krypto-Währungen kommt angesichts unterschiedlicher inhaltlicher Ausgestaltung und Preise im Hinblick auf das Gleichartigkeits- bzw. Gleichwertigkeitsgebots (→ § 240 Rn. 136 f.) nicht in Betracht.

Kapitel VII – Digitale Assets: Übersicht und Verwendung

Für digitale Assets gibt es bisher keine eindeutige Definition. Um eine Übersicht verschiedener digitaler Assets geben zu können, benötigt es ein einheitliches Verständnis für den grundlegenden Begriff des „digitalen Assets“. Dieses Whitepaper beschränkt die Definition digitaler Assets daher auf jegliche Vermögenswerte, die in einem binären digitalen Format mit Nutzungsrechten existieren (d. h. Stimmen, Waren, Zertifikate, Identität, Belohnungen, Token, usw.). Eine Übersicht der erläuterten Assets findet sich in **Abbildung 9**.

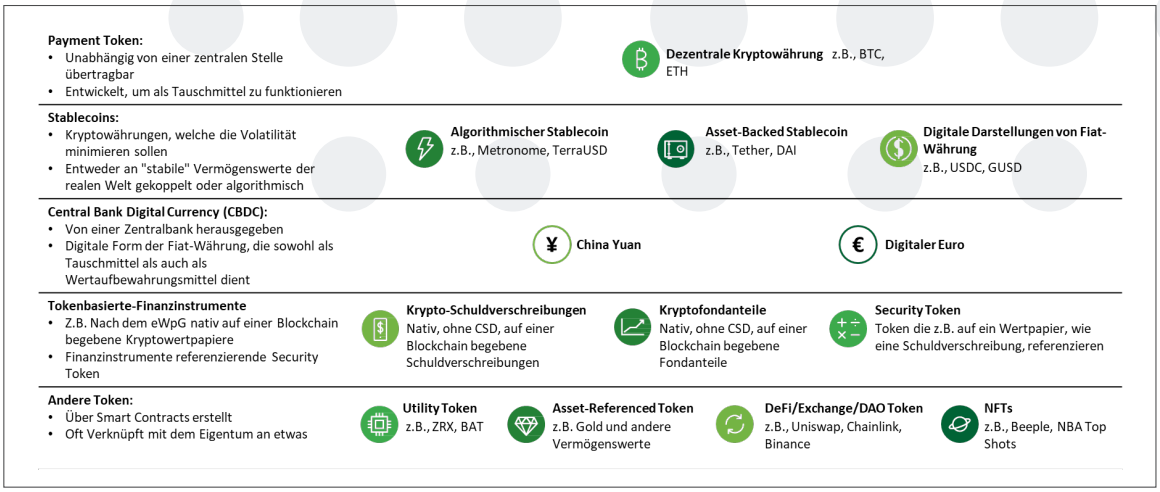


Abbildung 9 – Überblick über die verschiedenen Tokenarten

Zusätzlich ist es wichtig zu erwähnen, dass das Exposure zu digitalen Assets nicht zwangsweise an das Halten digitaler Assets geknüpft ist. Aufgrund der digitalen Komponente ist für das Halten digitaler Assets stets eine digitale Infrastruktur notwendig. Daher ist für das Halten digitaler Assets entweder eine entsprechende Infrastruktur oder ein externer Dienstleister unabdingbar (z.B. eine zentrale Krypto-Börse, wie BSDEX, Binance, Crypto.com oder Coinbase). Mittlerweile ist eine Investition in digitale Assets indirekt über klassische Assets möglich. So gibt es bereits verschiedene entsprechende Investmentmöglichkeiten wie Spezial-AIFs oder Exchange Traded Notes (ETNs), die ein Exposure in das Digitale ermöglichen. Mehr dazu in Kapitel VIII.

Im Folgenden wird eine Übersicht verschiedener digitaler Assets aufgezeigt. Einzelne Beispiele werden erläutert, um die große Bandbreite verschiedener Anwendungsfälle aufzuzeigen.

Die größte Marktdurchdringung eines digitalen Assets haben bisher die sog. Payment Token wie bspw. Bitcoin und Ethereum erreicht. Darüber hinaus haben auch die Stablecoin in letzter Zeit eine hohe Aufmerksamkeit erfahren und wurden explizit von der MiCa-Regulatorik aufgegriffen (siehe Kapitel IV).

Als weiteres digitales Asset seien auch CBDC erwähnt, welche von einer zentralen Stelle, meistens Zentralbanken, herausgegeben werden. CBDCs könnten das heutige Papiergeld ersetzen. Erste Vorbereitungen sind bereits getroffen. So wird in der MiCa-Regulatorik bereits dezidiert auf CBDCs eingegangen. Auf europäischer Ebene sind derzeit zwei unterschiedliche Arten in der Ausarbeitung. Insbesondere der sog. CBDCs können dabei für Asset Manager im Rahmen der Erzielung von Effizienzgewinnen interessant sein. Allerdings befindet sich der Digitale Euro, wie der CBDC von der EZB genannt wird, noch relativ am Anfang, sodass genauere Details erst in den kommenden Jahren zu erwarten sind. Auch die derzeitigen Design-Entscheidungen sind noch nicht final, weshalb der digitale Euro in näherer Zeit noch keine Aussicht auf konkrete Anwendungsfälle bietet.

Tokenbasierte Finanzinstrumente bilden klassische Finanzinstrumente als Token ab. Dies bringt Vorteile- wie z. B. einen einfacheren Zugang durch die Fraktionalisierung und die Möglichkeit der komplett automatischen Abwicklung mit sich. Diese Security Token fallen regelmäßig regulatorisch als Finanzinstrument in die MiFID II. Hinzu kommen in Deutschland die Krypto-Wertpapiere, welche durch das eWPG ermöglicht werden. Es ergeben sich unter Umständen interessante Vorteile, insbesondere im Zusammenspiel mit Stablecoin oder CBDCs. So könnten Wertpapiere darüber atomar, also ohne Counterparty Risiko, komplett automatisiert, 24/7 und mit atomarem Delivery versus Payment (DVP) gehandelt werden. Das eWpG ermöglicht bereits heute Schuldverschreibungen und Fondsanteile in der Form von Krypto-Assets rein digital zu emittieren. Es wurde darüber hinaus bereits angekündigt, dass Aktien sehr bald folgen sollen.

Zu unterscheiden ist dabei explizit zwischen Security Token und Krypto-Wertpapieren nach dem eWpG. Der Vorteil der Krypto-Wertpapiere gegenüber dem Security Token liegt darin, dass dieser nativ auf der Blockchain emittiert wurde. Es ist keine Referenz auf ein Asset in der realen Welt, sondern stellt eine eigene Assetklasse dar.

„Andere Token" ist ein Sammelbegriff für eine Vielzahl weiterer Anwendungsfälle. Die angeführten Beispiele sind keineswegs als abschließende Liste zu verstehen. Beispiele sind u. A. Utility Token, Asset-referenced Token, Decentralized Autonomous Organization (DAO) Token und NFTs.

Utility Token geben dem Eigentümer gewisse Nutzungsrechte oder Privilegien.

Die PSG Fan Token erlauben beispielsweise die Teilnahme an Umfragen um Entscheidungen bzgl. des Teams zu beeinflussen. Asset-referenced Token sind an bestimmte Assets gebunden. Sie verkörpern das Recht an einem Asset in der realen Welt wie z. B. Gold oder Öl.

DAO Token sind als eine Art Unterkategorie der Utility Token zu verstehen. Sie sind eng mit der Interaktion mit verschiedenen Decentralized Finance-Protokollen (DeFi) verknüpft. DAOs (Decentralised Autonomous Organisations) sind Konstrukte, um die bereits heute existierenden Formen von Gesellschaften und Körperschaften zu dezentralisieren bzw. zu digitalisieren. Je nach Ausgestaltung eines DAOs können Algorithmen dafür bestimmt sein, innerhalb der digitalen autonomen Gesellschaften Entscheidungen bzgl. der Geschäftssituation zu treffen. Häufig gehen mit den Token von DAOs jedoch lediglich Stimmrechte für die weitere Entwicklung der Technologie einher. So werden einige Protokolle direkt von DAOs gesteuert und haben keine andere zentrale Kontrollinstanz / Institution mehr. Dadurch werden die DAO Token-Halter, und damit in vielen Fällen die Nutzer des Protokolls, dessen Eigentümer und können über Entscheidungen und die Zukunft des Protokolls mitbestimmen.

Als letztes Beispiel Asset in dieser Kategorie sind NFTs zu benennen (bereits in Kapitel IV erläutert). Die Berichterstattung sowie die Marktkapitalisierung von NFTs haben zuletzt wieder abgenommen, dennoch bleiben interessante Anwendungsfälle. NFTs könnten besonders aufgrund ihres Sammelcharakters, der potenziellen Abbildung von Rechten oder Eigentumsbescheinigungen in den Bereichen der Kunst, Musik, der Veranstaltungbranche, POAP (Proof of Attendance Protocol) und im generellen Marketing disruptive Veränderungen mit sich bringen.

Die Produktvielfalt entwickelt sich ständig weiter und immer neue Produkte ergänzen die bereits bestehende Produktpalette. Die dynamische Entwicklung der Regulatorik wirkt hierbei als zentraler Beschleuniger.

Kapitel VIII – Geschäftsmodelle & Investmentmöglichkeiten für Asset Manager in der Praxis

Die zunehmende Verbreitung und Akzeptanz von Krypto-Assets eröffnet Asset Managern nicht nur neue Investmentmöglichkeiten abseits etablierter Vermögenswerte, sondern bietet ihnen auch die Gelegenheit, neue Produkte zu lancieren sowie bestehende Produkte, um zusätzliche Komponenten zu ergänzen. Somit kann zum einen der potenzielle Kundenstamm ausgebaut und zum anderen auf Anforderungen und unterschiedliche Risikoprofile bestehender Kunden besser eingegangen werden. Kundenwünsche nach mehr Risikodiversfikation oder ein allgemeines Exposure in Krypto-Assets wird möglich.

Die Investitionsmöglichkeiten in Krypto-Assets sind vielfältig. Neben direkten Anlage-möglichkeiten sind auch indirekte Anlagemöglichkeiten mittels ETPs (Exchange-Traded-Products) möglich, bspw. in Form von Exchange Traded Notes.

Das Investieren in Krypto-Assets bedeutet jedoch nicht notwendigerweise, auf ein Exposure in traditionelle Anlagen verzichten zu müssen. Security Token erlauben es Asset Managern Investition in Krypto-Assets mit traditionellen Anlagen zu verbinden. Ein Investment in illiquide Vermögensgegenstände wie bspw. Gemälde lässt sich über NFT´s realisieren. Darüber hinaus bieten ICOs (Initial Coin Offering) Asset Managern die Möglichkeit, in Start-ups zu investieren, welchen der Weg über einen Börsengang derzeit verwehrt ist.

Wie bereits einleitend beschrieben, kann durch die Krypto-Welt traditionellen Asset-Managern auch die Möglichkeit bieten, neue Produkte anzubieten. Solche reinen Krypto-Fonds können zum Beispiel in Krypto-Währungen wie Bitcoin oder direkt in Bitcoin Miners investieren. Eine weitere Möglichkeit ergibt sich, indem Investitionen in klassische Anlagen (Aktien, Anleihen, Immobilien) um Krypto-Assets ergänzt und dann als hybride Fonds vermarktet werden. Alternativ oder auch ergänzend hierzu bieten sich auch STO-Fonds an (Security Token Offering), welche in durch Tokens repräsentierte Aktien und Bonds investieren.

Die Auflegung neuer Produkte bzw. die Ergänzung bestehender Produkte um eine Krypto-Komponente, ist jedoch nicht der einzige Bereich, der das Geschäftsmodell von Asset Managern beeinflussen kann. Auch Vertriebsprozesse lassen sich anders gestalten. Krypto-Fonds können beispielsweise als ICO-Fonds aufgelegt werden, d.h. Fondsanteils-scheine werden als Bitcoin emittiert und nicht in klassische Währungen. Traditionelle Vertriebswege nehmen unter Umständen an Wichtigkeit ab, d. h. Banken und unabhängige Broker werden als Vertriebskanäle durch Krypto-Plattformen in Teilen substituierbar und die Beziehung zwischen Asset Manager und Kunde wird direkter.

Für Asset Manager, welche sich in die Krypto-Welt wagen, ergeben sich auch aus operativer Sicht Veränderungen. So gehen mit der Nutzung der DLT einige Effizienzgewinne einher.

Die Abwicklung von Transaktionen und Settlement-Prozesse werden derzeit von Dienstleistern oder Verrechnungsstellen durchgeführt, dies dauert in der Regel eine gewisse Zeit. Bei der Anwendung der DLT hingegen wird der Abrechnungsprozess durch das Schreiben von Transaktionen in die zugrunde liegende Blockchain abgeschlossen, der Abwicklungsprozess kann also theoretisch in nahezu Echtzeit durchgeführt werden.

Die Abwicklungsgeschwindigkeit von Transaktionen sowie Settlement-Prozesse wird durch Automatisierung (d.h. mit Smart Contracts, automatisierte Auftragsbücher und Handelsgeschäfte) und den Wegfall von Intermediären beschleunigt. Durch die Reduktion von Intermediären verringern sich Transaktionskosten und die Komplexität der Prozesse wird signifikant reduziert.

Auch die Datentransparenz und -sicherheit wird gewährt. Transaktionen sind öffentlich einsehbar und sicher in der Blockchain hinterlegt und für alle Teilnehmer nachvollziehbar bzw. nachverfolgbar. Die Notwendigkeit, einige Prozesse zu „duplizieren", um eine ordnungsgemäße Abwicklung von bspw. Wertpapiergeschäften zu gewährleisten, so wie es manche institutionelle Marktteilnehmer mit hohem technischem Aufwand betreiben, besteht also nicht mehr. Backoffice Tätigkeiten können also reduziert und somit auch hier Kosten eingespart werden.

Auf welcher regulatorischen Basis stehen Investitionsmöglichen in Krypto-Assets für Asset Manager? Krypto-Assets sind keine zulässigen Vermögensgegenstände nach §§ 193-198, 219, 221, 261 KAGB. Hieraus folgt, dass Krypto-Assets als Investitionsmöglichkeit für Privatanleger über OGAW (Organismen für gemeinsame Anlage in Wertpapieren) sowie Publikums-AIFs (Alternative Investmentfonds) derzeit nicht möglich ist. Eine Ausnahme stellen hierbei Krypto-Wertpapiere dar, welche nach eWpG ausgegeben wurden (s.a. Kapitel VI). Das im Juni 2021 in Kraft getretene eWpG erlaubt zum Beispiel Unternehmen, digitale Aktienzertifikate in begrenztem Umfang oder auch digitale Inhaberschuldverschreibungen auszugeben.

Eine mögliche Alternative stellen geschlossene sowie offene Spezial-AIFs dar. Nach § 285 bzw. § 282 KAGB liegen hier keine Einschränkungen bezogen auf zulässige Vermögensgegenstände vor. Die Bewertbarkeit des Vermögens-gegenstandes, also des Krypto-Assets, muss jedoch gewährleistet sein (Bestimmbarkeit des Verkehrswerts, § 285 Abs. 1 KAGB). Im Falle offener Spezial-AIFs gilt es zusätzliche Anforderungen an die Risikomischung zu berücksichtigen gemäß § 282 Abs. 2 KAGB. Für professionelle Anleger bzw. Asset Manager besteht also mittlerweile die Möglichkeit, in Krypto-Assets zu investieren.

Kapitel IX – Überblick der aktuellen Entwicklungen am Krypto-Markt (DeFi-Sektor)

Der Begriff Decentralized Finance beschreibt ein System aus mittlerweile vielen Anwendungsgebieten des FSI-Sektors und mehreren hundert Millionen Wallets. In diesem Ökosystem bedarf es streng genommen keinem Intermediär wie einer Bank oder einem Finanzdienstleister, da Transaktionen „Peer-to-Peer" in einem dezentralen Netzwerk durchgeführt werden. Die Implementierung der DeFi-Anwendung erfolgt durch einen Smart Contract, der alle Funktionen der Applikation als Programmcode enthält und den Intermediär damit ablöst. Die finanziell größten Protokolle, die Smart Contracts im Rahmen von DeFi verwalten, sind unter anderem Ethereum (64 %), Tron (8 %) und die Binance Smart Chain (5 %).

Das Spektrum der DeFi-Anwendungen orientiert sich an den traditionellen Finanzsystemen im Bereich der Handelsplattformen, Kreditvergabe und Krypto-Token in Form von Stablecoin, Derivaten und Versicherungen. Darüber hinaus entwickeln sich angesichts der zugrunde liegenden Blockchain Technologie neue Anwendungsszenarien. Diese umfassen unter anderem das Staking zur Konsensfindung und Validierung von PoS basierten Netzwerken. Ebenso sind Oracles, die als Schnittstelle zwischen der isolierten Blockchain und der „Außenwelt" agieren, um Daten auszutauschen zu nennen sowie die Tokenisierung realer oder digitaler Assets mittels NFTs oder Anteilsscheinen einer Decentralized Autonomous Organization.

Die ersten DeFi-Projekte entstanden bereits im Jahr 2015 im Anschluss an die Entwicklung des Ethereum-Netzwerks. Eine umfassende Nutzung ereignete sich im Jahr 2021. Der Total Value Locked (TVL), der den gesamten Wert definiert, der in DeFi-Anwendungen enthalten ist, stieg innerhalb dieses Jahres von ca. 15 Milliarden USD bis zu einem Höchstwert von über 180 Milliarden USD. Analog dazu verhielt sich die Anzahl einzelner Adressen, die mit DeFi-Applikationen interagierten. Diese erhöhten sich im selben Zeitraum von 1,3 Millionen auf 4,2 Millionen.

Der DeFi-Sektor verfügt noch über diverse Risiken, welche aufgrund dessen, dass die Anwendungen Vermögen verwalten, zu großen finanziellen Schäden führen können. Durch eine effektive Regulierung können positive Entwicklungen und weitere Innovationen auch im traditionellen Finanzsystem Einfluss finden. Darüber hinaus besteht die Möglichkeit, dass Finanzbereiche in Zukunft explizit durch DeFi-Anwendungen abgewickelt werden. Dieser Trend lässt sich auch anhand der Personalfluktuation darstellen. Seit einigen Jahren wechseln die Mitarbeiter namhafter Unternehmen der traditionellen Finanzwirtschaft vermehrt in den Krypto-Markt.

Kapitel X – Ausblick

DIGITALE ASSETS AUS DER NACHHALTIGKEITSPERSPEKTIVE

Der Energieverbrauch einer Blockchain-Technologie hängt fast ausschließlich vom zugrundeliegenden Konsensalgorithmus ab. In den letzten Jahren wurde deshalb häufig der hohe Energieverbrauch des Bitcoin-Netzwerks kritisiert. Auch im Europa Parlament wurde im Zusammenhang mit der MiCa zeitweise sogar über ein Verbot des PoW Algorithmus diskutiert. Der exakte Energieverbrauch von Blockchain-Technologien kann nicht genau nachverfolgt werden, da die Energieabrechnungen der Mining-Teilnehmer nicht offenliegen. Der Verbrauch lässt sich allerdings approximieren. Der Gesamtverbrauch von Blockchain-Technologien weltweit, gemessen in

Kilowattstunden (Kwh), soll bei etwa 120 bis 240 Billionen Kwh liegen (**Abbildung 10**). Das entspricht bis zu 1% des weltweiten Energiekonsums. Dabei gehen wegen des vorliegenden PoW, der Marktkapitalisierung und der Netzwerk-teilnehmer etwa 60% bis 80% auf das Bit-

Abbildung 10 – Jährlicher Energieverbrauch (inkl. Schätzung des Energieverbrauchs einiger Kryptoassets)

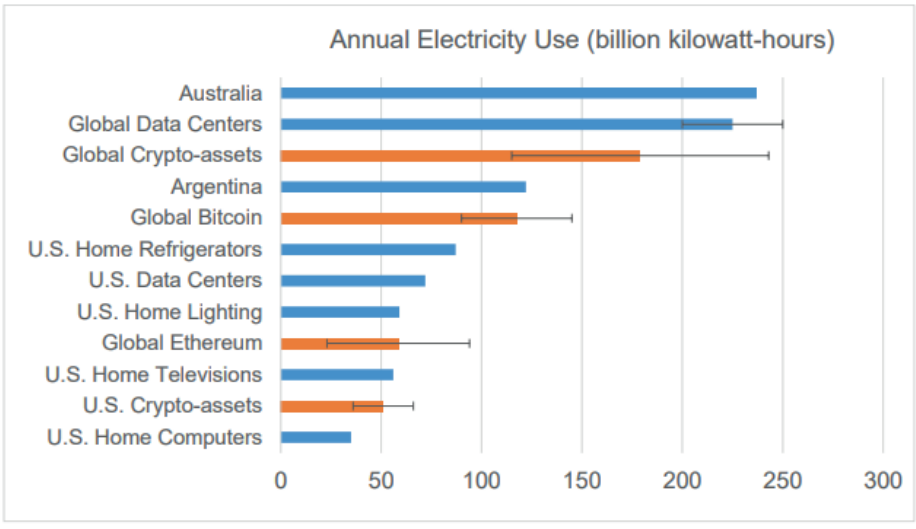


Figure 2.1: Comparison of Annual Electricity Use of Several Examples and the Best Estimates for Crypto-assets, as of August 2022, with error bars representing the best range of values.[80,81]

coin-Netzwerk zurück. Ethereum verbraucht mit PoW etwa 20% bis 40%. Die beiden größten Krypto-Währungen vereinen also nahezu den gesamten Energieverbrauch auf sich. Mit dem Wechsel von Ethereum auf PoS im September 2022 wird sich der Energieverbrauch des Ethereum Netzwerks drastisch reduzieren. Die verbliebenen Krypto-Währungen, größtenteils basierend auf PoS-Algorithmen, benötigen nur einen Bruchteil an Energie gegenüber den PoW Algorithmen. Ihr Energieverbrauch wird auf weniger als 0,001% des weltweiten Energieverbrauchs geschätzt, was etwa 0,28 Billionen kWh pro Jahr entspricht. PoS Algorithmen sind aufgrund ihrer Architektur also deutlich ressourcensparender. In Verbindung mit den im Kapitel V genannten Chancen durch die Verwendung von Krypto-Technologien (Prozesseffizienz, Vermeiden von Datensilos) ergeben sich schlussendlich mehr Vor- als Nachteile. Damit haben Blockchain-Technologien das Potenzial unsere Welt nicht nur effizienter, sondern auch nachhaltiger zu gestalten.

DIGITALE ASSETS AUS DER RISIKOMANAGEMENTPERSPEKTIVE

Mit der Verwendung und dem Investieren in Blockchain-Technologien gehen auch neue Risiken einher. Für das operative Geschäft von Vermögensverwaltern und Fonds ergeben sich Fragen hinsichtlich der Verwahrung von Private Keys für Wallet-Adressen. Dabei stehen IT-Risiken besonders im Fokus. Eine zusätzliche Herausforderung stellt die Tatsache dar, dass den Krypto-Assets zumeist keine Fundamen-taldaten oder Sicherheiten zugrunde liegen. Schwierigkeiten ergeben sich schlussendlich auch bei der Bewertung und Modellierung dieser Risiken. Damit braucht es aufgrund der inhärenten Risiken für die Früherkennung und Beurteilung von kurz- sowie mittelfristigen Risiken und Preisprognosen möglicherweise neue Ansätze. Neben den herkömmlich verwendeten Indikatoren und Tools zur Messung von Risiken könnten also auch auf Krypto-Assets spezifizierte Instrumente für das Portfolio- und Risikomanagement zum Einsatz kommen.

Potenzielle Risiken beim Investieren in Krypto-Assets:

EMP-ANGRIFF:

Durch einen elektromagnetischen Impuls besteht das Risiko eines Totalverlustes der Inhalte der Blockchain durch einen vollständigen Ausfall der Netzwerke.

HARD-FORK-RISIKO:

Der sogenannte „Hard-Fork" einer Blockchain ist die Aufteilung dieser in zwei nicht zueinander kompatiblen Versionen mit neuen Anforderungen der Verwahrung.

ÜBERTRAGUNGSFEHLER:

Fehlerhafte Eingaben der Ziel-Adressen bzw. Public Keys bei einem Krypto-Asset-Transfer, können zu einem unwiderruflichen Verlust der Krypto-Assets führen.

EINSTELLUNG ODER UNTERBRECHUNG DER MINING-TÄTIGKEIT:

Die Funktionsfähigkeit der jeweiligen Blockchain hängt maßgeblich von der Fähigkeit und Bereitschaft ihrer Miner ab. Eine signifikante Reduktion der Miner kann zu der Einstellung der Transkationen führen.

SOFTWARE-/ PROGRAMMCODEFEHLER:

Fehler in der Software und der Verschlüsselungstechnologie können zu unbefugtem Zugriff von Dritten auf die Krypto-Assets führen oder die gesamte Blockchain beeinträchtigen

MANIPULATIONSRISIKO:

Unzureichende Sicherheit der krypto-grafischen Verfahren können die gesamte Funktionsfähigkeit der Blockchain gefährden, beispielsweise durch neue, nicht ausreichend getestete Hash-Funktionen.

VERWAHRRISIKO:

Cyber- oder physische Angriffe auf die Verwahrstelle der Krypto-Assets.

MEHRHEITSANGRIFF 50+1:

Zerstörung des Validierungsprozesses oder des Vertrauens in die Blockchain durch eine Instanz oder Gruppierung, die die Mehrheit aller Validator-Nodes kontrolliert und damit das Netzwerk manipulieren kann.

LIQUIDITÄTSRISIKO:

Starke Abnahme der Liquidität oder Einschränkung des Handels durch ein Stressszenario (bspw. Verkaufspanik bei Terra Luna).

MARKTPREISRISIKO:

Der Marktpreis bestimmt sich aus Angebot und Nachfrage. Das Risiko eines Preisverfalls ist durch keinen inneren Wert beschränkt.

Kapitel XI – Risiken und Nutzen von Krypto-Assets und der Blockchain-Technologie

Krypto-Assets besitzen meist eine hohe Volatilität. Dies kann für Trader von großem Vorteil sein, da sich die hohen Schwankungen ausnutzen lassen Für Investoren hingegen besteht die Gefahr, dass das Portfolio stark negativ tendiert und gegebenenfalls (Buch-)Verluste über längere Zeit hingenommen werden müssen. Des Weiteren dienen Krypto-Währungen nur bedingt als zusätzliche Anlageklasse, da ihre Korrelation zu den Aktienmärkten insbesondere im Jahr 2022 sehr hoch war.

Angesichts dessen, dass es sich bei Krypto-Assets um finanzielle Vehikel handelt und der Umgang im Vergleich zu herkömmlichen Investmentklassen komplexer ist, gibt es diverse Betrugsschemata, die eingesetzt werden, um an die Gelder unwissender Anleger zu gelangen. Aus diesem Grund ist es essenziell, dass sich der Krypto-Investor umfassend mit der sicheren Handhabung vertraut macht.

Ein übliches Risiko in Bezug auf Krypto-Assets ist der Verlust des Zugangs zu dem privaten Schlüssel. Diese Situation kann insbesondere bei der persönlichen („non-custodial") Verwahrung eintreten. Infolgedessen hat der Nutzer keinen Zugriff mehr auf seine Krypto-Assets. Die Risiken hinsichtlich der Verwahrung werden im weiteren Verlauf erneut aufgegriffen.

Nach dem Start des Bitcoin im Jahr 2009 und dessen Erfolg wurden immer mehr Projekte initiiert, die diesen imitierten oder von eigenen Verbesserungen und neuen Versprechungen berichteten. Mittlerweile gibt es eine große Menge an Krypto-Währungen und täglich kommen neue hinzu, wobei jedes einzigartig sein möchte. Für den Anleger ist es dabei unabdingbar, das Projekt zu verstehen, in das er investiert. Weitere relevante Indikatoren, die ein seriöses Projekt kennzeichnen, können ein öffentlich einsehbarer Programmiercode, der freie Zugang zum Netzwerk und die Bekanntheit der Initiatoren sein. Häufig werden Investoren durch das Versprechen hoher Gewinne für das Projekt begeistert. Einige vermeintlich seriöse Projekte erwiesen sich rückblickend als Schneeballsysteme, wie es auf Onecoin zutraf.

Eine weitere große Gefahr für jedes Projekt geht von Fehlern im eigenen Programcode aus, die trotz umfassender Audits unentdeckt bleiben. Aufgrund der Vernetzung verschiedener Projekte kann sich die Sicherheitslücke eines Netzwerks auf andere auswirken. Die nordkoreanische Hackergruppe Lazarus konnte beispielsweise mittels eines Angriffs auf die Blockchain-Brücke „Ronin" über 600 Millionen USD aus dem NFT-Spiel „Axie Infinity" erlangen.

Schließlich liegen der Art der Verwahrung, für die sich der Nutzer entscheidet, weitere Risiken zugrunde. Zunächst werden die Verwahrungsmodelle privater Schlüssel in die Kategorien „custodial" und „non-custodial" unterteilt.

Für das erstere Modell können Nutzer die Dienste eines Treuhänders (z. B. Krypto-Börse oder spezieller Dienstleister) in Anspruch nehmen, der die privaten Schlüssel entsprechend verwahrt. Der Vorteil dieser Services ist es, dass die Handhabung einfach ist, da die Online-Dienste von überall zugänglich sind und nutzerseitig nichts installiert werden muss. Zudem können die Krypto-Währungen meist direkt gehandelt werden, ohne dass es zuvor einer Transaktion auf der Blockchain bedarf. Der Treuhänder stellt jedoch einen „Honeypot" dar, da ein großes monetäres Vermögen durch diesen verwaltet wird. Der Nutzer muss dem Verwahrer folglich vertrauen, dass der Online-Service entsprechende Sicherheitsvorkehrungen aufweist und der Dienstleister sich selbst ordnungsgemäß verhält.

Bei Lösungen, die als „non-custodial" klassifiziert werden, ist der Nutzer selbst für die Verwahrung des privaten Schlüssels verantwortlich. Das bedeutet, dass der Nutzer sich umfangreich mit der individuellen Verwahrung auseinandersetzen muss. Verliert er den Zugang, sind die verwalteten Werte ebenfalls verloren. Diese Art der Speicherung entspricht dem ursprünglichen Gedanken der Blockchain-Technologie, da bei der Verwahrung kein Intermediär involviert ist. Trotzdem muss der Nutzer weiterhin auf die bereitgestellte Soft- bzw. Hardware vertrauen.

Es wird hierbei zwischen Hot- und Cold-Storage unterschieden. Ersterer ist „heiß", da das Gerät, auf dem die Verwahrung erfolgt, eine Verbindung zum Internet aufweist. Das Risiko von externen Angriffen ist demnach höher. Zu dieser Kategorie zählen Software-Wallets, die auf Smartphones oder dem Computer ausgeführt werden.

Bei dem Cold-Storage handelt es sich um die Aufbewahrung des privaten Schlüssels ohne Internetzugang. Dies erfolgt meist mittels entsprechender Hardware, kann aber auch durch einen einfachen QR-Code auf Papier geschehen. Da letzteres ein hohes Risiko aufgrund von Alterung und Zerstörung besitzt, ist es weniger gebräuchlich. Hardware-Wallets besitzen sehr hohe Sicherheitsstandards und sind dementsprechend teurer als die meist kostenlosen Software-Lösungen. In der Handhabung sind sie weniger bequem, da die Geräte zunächst mit einem internetfähigen Gerät gekoppelt werden müssen, um Transaktionen durchführen zu können. Der private Schlüssel verlässt das Gerät hierbei nicht, da lediglich das Signieren der Transaktion erfolgt.

Ein Risiko aufgrund der Zerstörung des Geräts, das die privaten Schlüssel verwaltet, besteht zunächst nicht. Der private Schlüssel kann aus einer Kombination aus 12 bzw. 24 Wörtern („Seed-Phrase") wiederhergestellt werden. Bei der Erstellung eines Wallets bzw. dem privaten Schlüssel werden diese angezeigt, damit der Nutzer sie notieren kann. Die Gefahr der Zerstörung

oder des Verlusts der notierten Seed-Phrase besteht hingegen weiterhin.

Trotz der beschriebenen Risiken wird der Blockchain-Technologie auch ein großer Nutzen zugesprochen. Das grundlegende Ziel ist es, von einem zentralen System – in dem es einen „Single Point of Failure" gibt – zu einem dezentralen System zu wechseln. Dadurch können die Funktionen des Netzwerks auch garantiert werden, wenn einzelne Knoten böswillig oder fehlerhaft sind oder diese komplett ausfallen. Ursprünglich mussten die Nutzer ihr Vertrauen einer zentralen Instanz geben. In einem dezentralen Netzwerk wird dieses auf ein Protokoll übertragen, das die Regeln zur Teilnahme und Interaktion beschreibt und von jedem Nutzer eingehalten werden muss.

Blockchains sind in der Regel transparente Systeme, die die Privatsphäre der Teilnehmer mittels einer Pseudonymisierung schützen. Das bedeutet, die Adressen der Nutzer lassen sich ohne weiteres nicht mit der realen Identität in Verbindung bringen. Gleichzeitig kann jedoch jede Transaktion in der Blockchain nachvollzogen werden. Diese öffentliche Einsehbarkeit ermöglicht es, dass betrügerisches Verhalten verhindert wird.

Um Fälschungen der Blockchain vorzubeugen, werden kryptografische Hashfunktionen eingesetzt. Die einzelnen Blöcke werden dabei verknüpft, sodass bei einer Veränderung nachfolgende Blöcke ebenfalls invalide werden.

Aufgrund der bereits genannten Eigenschaften der Blockchain ergeben sich neue Geschäftsmodelle. Sofern das Netzwerk eigenständig funktioniert, sind diese nicht mehr an bestimmte Zugangszeiten gebunden, sondern können Transaktionen rund um die Uhr durchführen. Diese Automatisierung von Prozessen kann durch die Blockchain bisher unerreichbare Ebenen ermöglichen.

AUTOREN:

Christoph Wronka
Director
+49 69 756956037
cwronka@deloitte.de

Jens Paulsen
Senior Manager
+49 40 320804255
jpaulsen@deloitte.de

Nils-Philipp Böhm
Senior Consultant
+49 40 320804129
nboehm@deloitte.de