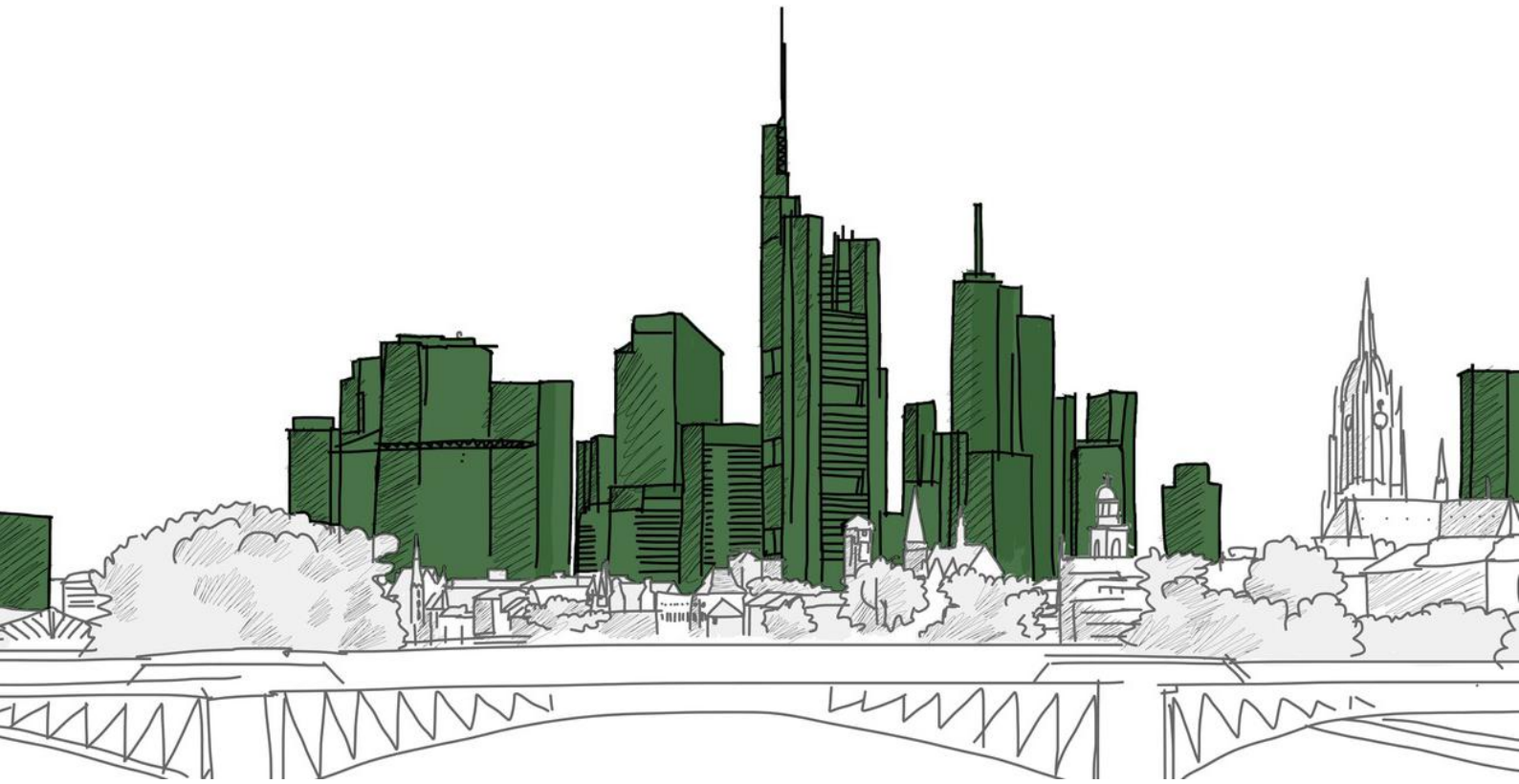
Grundlagenwissen Kryptowerte & Blockchains

Funktionsweisen, Zusammenhänge,
Chancen und Risiken



Grundlagenwissen Kryptowerte & Blockchains

Funktionsweisen, Zusammenhänge, Chancen und Risiken

Sarah Lemke und Christian Hammer

Diese Broschüre wird von der Educate Finance GmbH zu dem Zweck herausgegeben, Interessenten und Anleger über die Funktionsweise von Kryptowerten und die mit einer Vermögensanlage in Kryptowerten verbundenen Chancen und Risiken aufzuklären.

Inhaltsverzeichnis

Vorwort

Diese Broschüre macht Sie mit den wesentlichen Aspekten rund um die Themen Blockchains und Kryptowährungen vertraut. Der Hauptteil dieser Broschüre ist den Möglichkeiten, Chancen und Risiken einer Investition in Kryptowährungen gewidmet.

In dieser Broschüre werden wesentliche Begriffe und Zusammenhänge erläutert. Die meisten von Ihnen haben Begriffe wie Blockchain, Kryptowährung und Bitcoin schon gehört und auch eine Vorstellung, was sie bedeuten, aber die wenigsten wissen mit hinreichender Sicherheit, was unter diesen Begriffen tatsächlich zu verstehen ist.

Wenn Sie in Kryptowährungen investieren wollen, so sollten Sie die wesentlichen Zusammenhänge kennen, zumal sich die Kapitalanlage in Kryptowährungen erheblich von klassischen Arten der Kapitalanlage unterscheidet. Bitte beachten Sie, dass die Themen so komplex sind, dass in dieser Broschüre nicht alle Details erläutert werden können. Wir haben uns bemüht, jeweils so weit in die Tiefe zu gehen, wie es für das Grundverständnis erforderlich erscheint. Sie benötigen kein technisches Vorwissen, um diese Broschüre zu verstehen.

Die Anwendungsmöglichkeiten von Blockchains und Kryptowährungen sind in den vergangenen Jahren erheblich gestiegen und werden schon allein aufgrund der stetigen Digitalisierung auch weiter steigen. Mittels Blockchain-Technologie können alle erdenklichen Werte, Rechte und Schuldverhältnisse an materiellen und immateriellen Gütern durch sog. „Token" repräsentiert und deren Handel- und Austauschbarkeit potenziell vereinfacht werden. Welche Auswirkungen diese Entwicklung weltweit haben wird, ist noch offen. Ein verlässlicher Rechtsrahmen existiert noch nicht. Sowohl auf nationaler als auch auf europäischer Ebene werden aktuell Maßnahmen ergriffen und fortentwickelt, mit denen auch der Anlegerschutz gestärkt und weitere Maßnahmen zur Geldwäschebekämpfung in diesem Bereich eingeführt werden.

Diese Broschüre ist aufgebaut wie ein Buch, das Sie durchgehend von vorne bis hinten lesen können, wenn Sie grundsätzliches Interesse an dem Thema haben und die Grundlagen verstehen wollen. Alternativ können Sie diese Broschüre zum Nachschlagen verwenden und nach Bedarf nur einzelne Kapitel lesen. Am Ende der Broschüre finden Sie ein Glossar, in dem diverse Fachbegriffe erläutert werden.

Für Einsteiger wertvolle Informationen über die Kapitalanlage und den Finanzmarkt bietet die Broschüre „Grundlagenwissen Wertpapiere & Investmentfonds", deren Lektüre ausdrücklich empfohlen wird. Darin werden u. a. die sog. „Basisrisiken", die bei fast jeder Vermögensanlage bestehen können, erläutert.

Diese Broschüre kann sowohl in Papierform als auch als Datei vorliegen. Sie wird laufend aktualisiert und berücksichtigt die Rechtslage zum Zeitpunkt ihres Erscheinens. Das Erscheinungsdatum ist am Ende der Broschüre angegeben. Da die Gesetze und Usancen am Kapitalmarkt einem ständigen Änderungsprozess unterliegen und die technische Entwicklung laufend voranschreitet, kann nicht ausgeschlossen werden, dass die Ihnen vorliegende Broschüre nicht die aktuelle Rechtslage widergibt. In Ihrem eigenen Interesse sollten Sie stets die jeweils aktuelle Fassung dieser Broschüre verwenden. Welche dies ist, können Sie bei der fundsware GmbH oder bei der Person erfragen, von der Sie diese Broschüre erhalten haben.

Information und Aufklärung schützen Sie nicht vor finanziellen Verlusten, aber davor, von diesen mangels Risikokenntnis überrascht zu werden. Sie können die Risiken, die Sie eingehen wollen, nur bestimmen, wenn Sie diese Risiken verstanden haben.

Bitte berücksichtigen Sie, dass diese Broschüre standardisierte Informationen enthält und daher weder eine individuelle Beratung, die auf Ihre persönlichen Verhältnisse und Bedürfnisse zugeschnitten ist, noch die Lektüre der produktspezifischen und verbindlichen Verkaufsunterlagen ersetzen kann.

Die in dieser Broschüre dargestellten Kapitalanlagen bergen zum Teil erhebliche Verlustrisiken. Es handelt es sich um komplexe Produkte mit besonderen Risiken. Aufgrund ihrer Komplexität und der mit ihnen verbundenen besonderen Verlustrisiken eignen sich diese Kapitalanlagen nur für erfahrene Anleger. Die meisten der klassischen Kryptowährungen sind hoch volatil. Je nach Art des Geschäfts können neben hohen Gewinnchancen hohe Verlustrisiken – bis zum Totalverlust des eingesetzten Kapitals – bestehen. Die jeweils bestehenden Risiken sind bei der Entscheidung, ein Geschäft zu tätigen, unbedingt zu berücksichtigen!

Einleitung

A

Fast jeder, der Finanznachrichten liest, hat schon einmal von Bitcoin und Kryptowährungen gehört. Vieles von dem, was allgemein zu hören ist, sind Halbwahrheiten oder Gerüchte. Nur ein kleiner Teil der Bevölkerung kennt sich mit den Begriffen wirklich aus. Das soll und wird sich - hoffentlich - ändern. Mit dieser Broschüre wollen wir einen Teil dazu beitragen.

Bitcoin ist derzeit die weltweit führende Kryptowährung. Sie basiert auf der Blockchain-Technologie. Die Blockchain-Technologie ist eine der meistdiskutierten Innovationen der digitalen Transformation von Wirtschaft und Gesellschaft. Sie eröffnet ein weites Feld von innovativen Anwendungsmöglichkeiten und neuen Kooperationsformen und ist mehr als nur die Basis für Kryptowährungen. Nicht nur diverse Forschungs- und Wissenschaftsinstitute beschäftigen sich längst eingehend mit dem Thema, sondern auch die Bundesregierung hat bereits eine Strategie veröffentlicht, die Ziele und Prinzipien der Bundesregierung im Zusammenhang mit der Blockchain-Technologie aufzeigt und konkrete Maßnahmen enthält.

Die Blockchain-Technologie eröffnet Möglichkeiten, die weit über das Feld digitaler Währungen hinausgehen. Mit dieser Broschüre wollen wir eine Basis für das grundlegende Verständnis dieser Technologie legen, um darauf aufbauend darzustellen, welche Möglichkeiten der Kapitalanlage auf Basis dieser Technologie heute bereits bestehen.

Vielleicht haben Sie sich bislang vor dem Thema gescheut, weil Sie sich mit Computertechnologie nicht auskennen. Sie müssen aber auch kein Architekt oder Immobilienexperte sein, um erfolgreich in Immobilienaktien oder Immobilienfonds investieren zu können. Es gilt, die wesentlichen Grundlagen zu verstehen, um einschätzen zu können, welche Chancen und Risiken jeweils mit der Kapitalanlage verbunden sind. Dafür sind keine technischen Vorkenntnisse erforderlich. In dieser Broschüre werden an einigen Stellen technische Details und Zusammenhänge erläutert. Die Darstellungen sind bewusst einfach gehalten und die Chancen und Risiken der vorgestellten Kapitalanlagen können Sie auch verstehen, wenn Sie die technischen Details bei der Lektüre überspringen.

Um Bitcoin ist ein regelrechter „Hype“ entstanden, angesichts stark fallender Kurse war zwischenzeitlich aber auch von einer „Bitcoin-Blase“ die Rede. Beides möchten wir hier nicht bewerten. Neben Bitcoin existieren diverse weitere Kryptowährungen – derzeit mehrere Tausend -, von denen ein Großteil sich nicht durchsetzen konnte und bereits wieder vom Markt verschwunden ist. Daneben wurden weitere Anwendungsfelder für die Blockchain-Technologie entdeckt und auf Basis der Blockchain-Technologie wurden weitere innovative Investitionsmöglichkeiten entwickelt. Wir zeigen im Folgenden daher nicht nur auf, wie die Blockchain-Technologie funktioniert, wie Kryptowährungen entstehen und wie Sie in Kryptowährungen investieren können, sondern ein wesentlicher Teil dieser Broschüre ist innovativen Anlagemodellen gewidmet, die auf der Blockchain-Technologie basieren. Wenn Sie sich bereits mit der Vermögensanlage beschäftigt haben, werden Sie erkennen, dass einige Modelle gängigen Kapitalanlagen wie Aktien oder Anleihen ähneln.

Da die Blockchain-Technologie und hierauf basierende Anlagemodelle relativ neu am Markt sind, gibt es derzeit noch keine eigens hierfür erstellte bzw. alleinstehende gesetzliche Basis. Selbstverständlich agieren die Akteure dennoch nicht im rechtsfreien Raum. Es finden die bereits bestehenden Gesetze Anwendung und haben teilweise schon Sondervorschriften zur Regelung von Kryptowerten erhalten. Der (insbesondere europäische) Gesetzgeber arbeitet bereits an einer eigenen gesetzlichen Grundlage, die in naher Zukunft insbesondere dem Anlegerschutz und der Vermeidung von Geldwäsche dienen soll.

Header

- Versionsnummer der Software
- Hash von vorhergehendem Block
- Merkle Root
- Zeitstempel
- Ziel der aktuellen Schwierigkeit
- Nonce

Body

Transaktionen, die mit dem Block bestätigt werden sollen.

Broschüre „Blockchain-Strategie der Bundesregierung“, veröffentlicht am 18.09.2019

Basiswissen zu Währungen und Geld B

Kryptowährungen werden auch als Kryptogeld oder „das Geld der Zukunft" bezeichnet. Auf der anderen Seite wird bei der Darstellung ihrer Vorteile immer darauf hingewiesen, dass sich Kryptowährungen erheblich von „klassischen" bzw. echten Währungen unterscheiden. Um die Unterschiede zu verstehen, werden die wesentlichen Begriffe und Details im Zusammenhang mit Währungen im Folgenden erläutert.

I. Was ist eine Währung?

Eine Währung ist im weiteren Sinne die Verfassung und Ordnung des gesamten Geldwesens eines Staates oder Gebietes. Allgemein wird mit dem Begriff „Währung" auch das gesetzliche Zahlungsmittel eines Landes oder der Länder eines Währungsraums, wie z.B. einer Währungsunion bezeichnet. Der Währungsraum ist der Geltungsbereich einer Währung.

Derzeit gibt es weltweit über 160 offizielle Währungen, aber vor allem der US-Dollar und in zunehmendem Maße auch der Euro gelten als internationale Leitwährungen. Als Leitwährung wird eine Währung innerhalb eines internationalen Währungssystems bezeichnet, die als internationales Zahlungs- und Reservemittel sowie als internationale Anlagewährung verwendet wird. Sie wird auch „Ankerwährung" genannt, weil die Wechselkurse der Währungen aller anderen Länder in einer relativ stabilen Beziehung zur Leitwährung gehalten werden. Die Leitwährung dient auch als Recheneinheit zur Bestimmung des Wertes aller Währungen.

Die meisten Währungen werden an den internationalen Devisenmärkten gehandelt. Der sich dort ergebende Preis ist der Wechselkurs. Nahezu alle gängigen Währungen basieren inzwischen auf dem Dezimalsystem, das als Basis die Zahl 10 verwendet. Das heißt, eine Währungseinheit lässt sich durch die Zahl 10 teilen und ergibt dann neue Untereinheiten. Eine Untereinheit ist dabei ein dezimaler Bruchteil (i. d. R. ein Hundertstel) des Wertes der Haupteinheit. Der heutige Normalfall ist eine einzige Untereinheit, welche ein Hundertstel der Haupteinheit ausmacht, z. B. machen 100 Cents 1 Euro aus. Zur Unterscheidung von anderen Währungen spricht man anstatt von „Cents" auch von „Eurocents".

Eine Währung wird als „konvertibel" bezeichnet, wenn sie von In- und Ausländern unbegrenzt in andere Währungen umgetauscht werden darf. Volle Konvertibilität ist gegeben, wenn jede Person berechtigt ist, jede beliebige Währung gegen eine andere zu tauschen, zu transferieren oder als Guthaben zu halten. Es gibt auch Währungen mit beschränkter Konvertibilität, dabei unterscheidet man üblicherweise personenbezogen in Ausländer- und Inländerkonvertibilität. Ausländerkonvertibilität bezeichnet das Recht von Gebietsfremden (sog. Devisenausländern), Guthaben in inländischer Währung jederzeit uneingeschränkt in ausländische Währung umzutauschen, während Inländer Beschränkungen unterliegen. Inländerkonvertibilität bezeichnet demgegenüber das Recht von Gebietsansässigen (sog. Deviseninländern), jede Währung in beliebiger Menge jederzeit gegen in- oder ausländische Währung zu erwerben, während Ausländer Beschränkungen unterliegen.

Eine Währung, die im Gegensatz zu den an internationalen Devisenmärkten gehandelten Devisen nicht frei konvertierbar ist, wird als Binnenwährung bezeichnet. Ein Beispiel hierfür ist die nicht mehr existierende Mark der DDR.

Eine Währung ermöglicht als universelles Tausch- und Zahlungsmittel den Transfer von Waren und Dienstleistungen, ohne eine Gegenleistung in Form von anderen Waren und Dienstleistungen zu liefern.

II. Komplementär- und Ersatzwährungen

Neben den staatlichen Währungen gibt es Komplementärwährungen, die nur regional neben dem offiziellen Geld als Tauschmittel akzeptiert werden. Eine Komplementärwährung kann eine Ware, eine Dienstleistung oder eine geldäquivalente Gutschrift sein. Im Raum Bremen gibt es z. B. den ROLAND-Regional Wirtschaftsring e.V., der über ein Verrechnungssystem mit einer zinsfreien Währung, dem ROLAND, verfügt. Die Mitglieder des Wirtschaftsrings tauschen Waren und Dienstleistungen in ROLAND mittels Scheckgutscheinen aus. Formal stehen komplementäre Gutscheinwährungen in Konflikt mit dem Bundesbankgesetz, wonach es verboten ist, unbefugt Geldzeichen (Marken, Münzen, Scheine oder andere Urkunden, die geeignet sind, im Zahlungsverkehr an Stelle der gesetzlich zugelassenen Münzen oder Banknoten verwendet zu werden) auszugeben oder zu verwenden. Seit 2001 werden Regionalgelder auf Gutscheinbasis von der Bundesbank jedoch geduldet, da sie bislang volkswirtschaftlich keinen nennenswerten Umfang annehmen.

Eine Komplementärwährung kann auch eine ausländische, zumeist stärkere Währung sein. Diese Funktion übt etwa der US-Dollar in weiten Teilen der Welt mit schwacher einheimischer Währung aus.

III. Die Funktion von Zentralbanken

In einem Staat oder einem Währungsraum ist in der Regel die gemeinsame Zentralbank für die Geld- und Währungspolitik zuständig. Zentralbanken besitzen in nahezu allen westlichen Staaten ein großes Maß an Autonomie, das heißt die Regierung kann gar nicht oder nur in sehr geringem Maße bzw. indirekt auf die Zentralbank und deren geldpolitische Entscheidungen einwirken. Grundsätzlich richtet sich der Abhängigkeitsgrad der Notenbanken von anderen staatlichen Institutionen nach den wirtschaftlichen und politischen Verflechtungen des jeweiligen Landes.

Die Europäische Zentralbank (EZB) ist die Zentralbank der (derzeit) 19 Mitgliedstaaten der Europäischen Union, die im Sinne einer Währungsunion den Euro als gemeinsame Währung eingeführt haben. Die ausführenden Organe der EZB sind die nationalen Zentralbanken der Teilnehmerstaaten. Die EZB und die nationalen Zentralbanken der Staaten der Europäischen Union bilden das Europäische System der Zentralbanken. Die Zentralbanken der Teilnehmerstaaten sind unabhängig gegenüber Weisungen nationaler Regierungen und unterstehen nur der EZB. In Deutschland ist die nationale Zentralbank die Deutsche Bundesbank.

Eine Zentralbank hält die Währungsreserve eines Währungsraumes, refinanziert Geschäftsbanken und ggf. auch den Staat, emittiert die physischen Banknoten einer Währung und bringt diese in Umlauf. In den Zentralbankstatuten vieler Staaten ist als Hauptziel der von der Zentralbank verfolgten Geldpolitik festgelegt, die Preisniveau- und Geldwertstabilität zu wahren. Grundsätzlich muss Geld einerseits so knapp sein, dass der Geldwert nicht sinkt. Auf der anderen Seite muss die Wirtschaft ausreichend mit Geld versorgt werden, damit sämtliche Geldgeschäfte abgewickelt werden können. Zur Erfüllung ihrer Aufgaben stehen einer Zentralbank verschiedene Instrumente zur Verfügung. Das wahrscheinlich bekannteste Instrument ist die Zinspolitik. Unmittelbar beeinflussen kann eine Zentralbank nur die Zinsen im Geschäft zwischen ihr und den Geschäftsbanken (sog. Leitzins). Da die Geschäftsbanken günstigere oder ungünstigere Finanzierungsbedingungen in der Regel aber an ihre Kunden weitergeben, ändern sich in Reaktion auf die Veränderung des Leitzins auch die Zinsen am Kapitalmarkt generell und damit die geldpolitische Gesamtsituation.

IV. Was ist Geld?

Geld ist das allgemein anerkannte Tausch- und Zahlungsmittel, auf das sich eine Gesellschaft verständigt hat. Es dient als gesetzliches Zahlungsmittel zur Tilgung von Schulden mit verbindlicher Rechtswirkung, wenn man durch die Rechtsordnung verpflichtet ist, das Geld anzunehmen. Das als gesetzliches Zahlungsmittel bestimmte Geld bezeichnet man als Währung. Im Euro-Währungsraum ist Euro-Bargeld das gesetzliche Zahlungsmittel.

V. Die Funktionen von Geld

Geld hat unabhängig von seiner Form drei Funktionen. Es ist

1. Tausch- und Zahlungsmittel: Es kann gegen jede Dienstleistung und Ware eingetauscht werden.

2. Recheneinheit: Jedes Gut kann in Einheiten von Geld umgerechnet werden. Hierdurch werden alle Güter miteinander vergleichbar und addierbar gemacht. Die Verrechnung jedes Tausches erfolgt über Geldeinheiten.

3. Wertaufbewahrungsmittel: In Geld wird ein gewisser Wert „gespeichert". Es muss nicht sofort ausgegeben werden, sondern kann aufbewahrt oder angelegt werden. Verkauf und Kauf von Gütern können daher zeitlich auseinanderliegen und den Bedürfnissen des Besitzers des Geldes angepasst werden. Insofern hat Geld auch die Funktion eines Wertübertragungsmittels.

VI. Erscheinungsformen von Geld

Die Erscheinungsform des Geldes hat sich im Laufe der Zeit verändert. Früher handelte es sich bei Geld in der Regel um Warengeld, d. h. um Gegenstände aus unterschiedlichen Materialien, die einen bestimmten Marktwert haben. Das beste Beispiel hierfür sind Goldmünzen. Später kam das sogenannte Repräsentativgeld in Form von Banknoten auf. Diese konnten beim Herausgeber gegen eine gewisse Menge Gold oder Silber getauscht werden. Heute basieren moderne Volkswirtschaften auf so genanntem Fiatgeld. Dabei handelt es sich um Geld, das zum gesetzlichen Zahlungsmittel erklärt und von einer Zentralbank ausgegeben wird. Das Geldzeichen an sich hat keinen eigenen, intrinsischen (Material-)Wert, denn das für die Banknoten verwendete Papier ist im Grunde wertlos. An-

ders als Repräsentativgeld kann es gegenüber dem Herausgeber auch nicht in einen anderen Vermögenswert, z. B. eine bestimmte Menge Gold, eingetauscht werden. Es wird dennoch als Austausch für Waren und Dienstleistungen angenommen, weil aufgrund der gesetzlichen Festlegung und der Herausgabe durch eine Zentralbank allgemein darauf vertraut wird, dass der Wert des Fiatgeldes im Zeitverlauf stabil bleibt. Gelingt es Zentralbanken nicht, ihre Aufgabe, den Geldwert stabil zu halten, zu verwirklichen, besteht das Risiko, dass das Fiatgeld seine allgemeine Akzeptanz als Zahlungs- und besonders Tauschmittel und seine Attraktivität als Wertaufbewahrungsmittel verliert.

Unser heutiges Geld existiert nicht nur in physischer Form, also in Form von Münzen und Banknoten. Es kann auch als (Computer-) Eintrag auf einem Bankkonto oder als Guthaben auf einem Sparkonto existieren. Zudem gibt es bargeldlose Zahlungsformen wie Lastschriften sowie Internet- und Kartenzahlungen.

Dezentrale digitale Währungen oder virtuelle Währungssysteme, um die es in dieser Broschüre im Wesentlichen geht, gelten aus rechtlicher Sicht nicht als Geld.

VII. Zentralbankgeld

Als Zentralbankgeld wird das von der Zentralbank geschaffene Geld bezeichnet. Es existiert in Form von Sichtguthaben bei der Zentralbank oder als Bargeld in Form von Banknoten und Münzen. Geschäftsbanken unterhalten Konten bei der Zentralbank. Sie benutzen die Guthaben auf diesen Konten, um Zahlungen untereinander zu tätigen. Zudem können die Guthaben auf diesen Konten von den Geschäftsbanken jederzeit in Bargeld umgetauscht werden, falls ihre Kunden oder sie selbst Bargeld benötigen.

Zentralbankgeld wird geschaffen, indem die Zentralbank Kredite zum jeweils gültigen Leitzins und gegen die Bereitstellung entsprechender Sicherheiten an Geschäftsbanken vergibt, oder indem die Zentralbank Wertpapiere oder andere Aktiva erwirbt und im Gegenzug Guthaben gewährt. In beiden Fällen erhält die Geschäftsbank, mit der die Zentralbank das jeweilige Geschäft schließt, Zentralbankgeld auf ihr Konto bei der Zentralbank gutgeschrieben. Zahlt die Geschäftsbank ihren Kredit bei der Zentralbank zurück oder verkauft die Zentralbank die zuvor erworbenen Wertpapiere, so wird Zentralbankgeld vernichtet. Zentralbankgeld kann man sich als Forderung gegen die Zentralbank vorstellen, die erlischt, sobald sie an die Zentralbank zurückgeführt wird.

VIII. Zentralisiertes Geldsystem

Als Zentralisierung wird der Vorgang beschrieben, bei dem alle Abläufe in einem Unternehmen über einen zentralen Mittelpunkt geleitet werden. Auch das Geldsystem in Europa unterliegt dem Prozess der Zentralisierung. Zentrale Institutionen, wie die Europäische Zentralbank, haben Entscheidungsgewalt über eine Währung und sind für ein funktionierendes Geldsystem verantwortlich. Sie beeinflussen durch ihre Entscheidungsgewalt den Endkonsumenten. Bei der Kontoführung legen sie z. B. Transferlimits fest und wann der Kunde auf sein Geld zugreifen darf. Durch die Zentralisierung wird aber auch ein rapides Handeln ermöglicht und durch die zentralen Institutionen wird der Preis- und Geldwert der Währungen stabil gehalten.

Tatsächlich funktioniert unser zentralisiertes Geldsystem im Wesentlichen nicht, weil wir dem Geld aufgrund seiner ihm inhärenten Charakteristika vertrauen, sondern weil wir den zentralen Organisationen, die die Entscheidungsgewalt über unsere Währung haben, vertrauen. Die Zentralisierung von Geld wurde durch die Digitalisierung begünstigt und beschleunigt.

Das Gegenstück - die Dezentralisation - bezeichnet die organisatorische Verteilung von Aufgaben und Zuständigkeiten auf verschiedene Stellen. Es soll nicht alles „zentral" von einer Stelle geleistet werden, sondern „dezentral", also weg von einer Zentrale. Die Dezentralisierung ist eines der wichtigsten Merkmale digitaler Währungen.

Basiswissen zu Blockchains und Kryptowährungen

C

Eines der wichtigsten Merkmale digitaler Währungen ist die Dezentralisierung. Im Gegensatz zur zentralisierten Währung, wo die Zentralbank über die Geldversorgung und den Zugang zum Geld entscheidet, ist ein dezentrales System immer zugänglich und vollständig offen für jedermann. Es basiert nicht auf dem Vertrauen auf eine zentrale Organisation, sondern auf dem Vertrauen in das System als solchem. Die Geldmenge, die in Umlauf gebracht wird, ist bei Kryptowährungen zudem zumeist klar umrissen. Bei Bitcoins liegt die Obergrenze bei 21 Millionen. Das sog. Fiatgeld hingegen kann von der Zentralbank – theoretisch – unbegrenzt herausgegeben werden.

I. Kryptografie und Kryptologie

Kryptologie ist ein Teilgebiet der Informatik, das sich mit der Lehre von der Entwicklung und der Bewertung von Verfahren zur Verschlüsselung von Daten im Rahmen des Datenschutzes befasst. Kryptografie ist ein Teilgebiet der Kryptologie und befasst sich mit dem Verschlüsseln von Informationen. Mit Hilfe der Kryptografie werden unter anderem mathematische Beweise erstellt, die ein hohes Maß an Sicherheit für eine Verschlüsselung bieten.

II. Die Blockchain-Technologie

Eine Blockchain (englisch für Blockkette) ist eine kontinuierlich erweiterbare Liste von Datensätzen, die mittels kryptografischer Verfahren miteinander verkettet sind. Der einzelne Datensatz wird „Block" genannt. Jeder Block enthält einen kryptografisch sicheren „Hash" (Hashwert oder Streuwert) des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten. Hierdurch stellt eine Blockchain eine Transaktionshistorie dar, die im Nachhinein nicht mehr veränderbar - also unveränderbar - ist.

1. Hash

Der Begriff „Hash" wird in der Regel als Abkürzung für den Begriff „Hashwert" verwendet. Ein Hashwert wird durch eine Hashfunktion berechnet. Hashfunktionen reduzieren eine große Datenmenge auf eine kleinere Zeichenfolge. Daher können durch den Hash alle Daten auf der Blockchain komprimiert werden.

Es gibt für Hashes vielfältige Anwendungsbereiche. Sie werden beispielsweise bei der Verschlüsselung von Passwörtern verwendet. Passwörter sollen verschlüsselt gespeichert werden, damit sie bei einem Hackerangriff nicht im Klartext gelesen werden können. Dazu werden die Passwörter mittels einer Hashfunktion in Hashwerte umgewandelt. Gespeichert werden nur diese Hashwerte und nicht die Passwörter selbst. Gibt der Nutzer bei seiner Authentisierung sein Passwort ein, wird bei der Eingabe wieder mit derselben Hashfunktion der Hashwert berechnet und mit dem gespeicherten Hashwert verglichen. Bei Übereinstimmung gilt der Benutzer als authentifiziert.

Eine Hashfunktion ist nicht identisch mit einer „normalen" Verschlüsselung. Bei einem Verschlüsselungsalgorithmus kann der Ursprung – hier das Passwort – wieder sichtbar gemacht werden. Bei der Hashfunktion ist dies nicht gewollt. Von dem Hash wird nicht „zurückgerechnet" auf das Passwort, sondern das eingegebene Passwort wird durch den Vergleich des daraus berechneten Hashwerts mit dem gespeicherten Hashwert verglichen und ggf. verifiziert.

Der Hash ist der digitale Code, der nach Anwendung der Hashfunktion als Ergebnis herauskommt. In der Regel wird eine feste Länge für den Hash definiert, also festgelegt, wie viele Zeichen ein Hash immer hat. Bitcoin zum Beispiel verwendet den SHA-256 Algorith-

mus zur Verschlüsselung. SHA steht für „Secure Hash Algorithm“. Die Hashes des SHA-256 Algorithmus sind immer 256 Bits lang.

Das Bilden eines Hashwerts hat erst einmal nichts mit Kryptografie zu tun. Hashes werden z. B. auch genutzt, um große Datenmengen zu speichern. Nicht alle Hashfunktionen sind nach den Gesichtspunkten der Kryptografie eine kryptografische Hashfunktion. Von einer kryptografischen Hashfunktion spricht man, wenn die folgenden drei Voraussetzungen gegeben sind:

a | Irreversibilität

Vom Hashwert darf nicht auf den Ursprung geschlossen werden können, es muss sich um eine Einwegfunktion handeln. Die Umkehrung muss mindestens sehr aufwändig, im günstigsten Fall unmöglich sein. Es hat sich mit der Zeit herausgestellt, dass durch die steigende Rechenleistung doch Möglichkeiten gefunden werden, aus einem Hashwert die ursprünglichen Daten zurück zu berechnen.

b | Kollisionssicherheit

Eine sog. Kollision tritt dann auf, wenn unterschiedlichen Eingabedaten derselbe Hashwert zugeordnet wird. Bildet man z. B. die Quersumme von mehreren Zahlen, dann kann es vorkommen, dass die Quersumme mehreren Zahlenwerten entsprechen kann. Die Quersumme von 211 (2+1+1=4) ist z. B. identisch mit der Quersumme von 22 (2+2=4). Aus Sicht der Kryptografie ist die Quersummenbildung daher keine kryptografische Hashfunktion.

In der Kryptologie werden spezielle kryptologische Hashfunktionen verwendet, bei denen es praktisch unmöglich sein soll, Kollisionen absichtlich zu finden. Um die Wahrscheinlichkeit von Kollisionen zu vermeiden, werden immer bessere Verfahren verwendet, die meist längere Hashwerte erzeugen. Eine Hashfunktion wird heute als kollisionsfrei (manchmal auch passender als kollisionsresistent) bezeichnet, wenn sich Kollisionen praktisch nicht berechnen lassen.

c | Schnelligkeit - (“Agilität“)

Das Verfahren zur Berechnung des Hashwerts muss schnell (=effizient) sein.

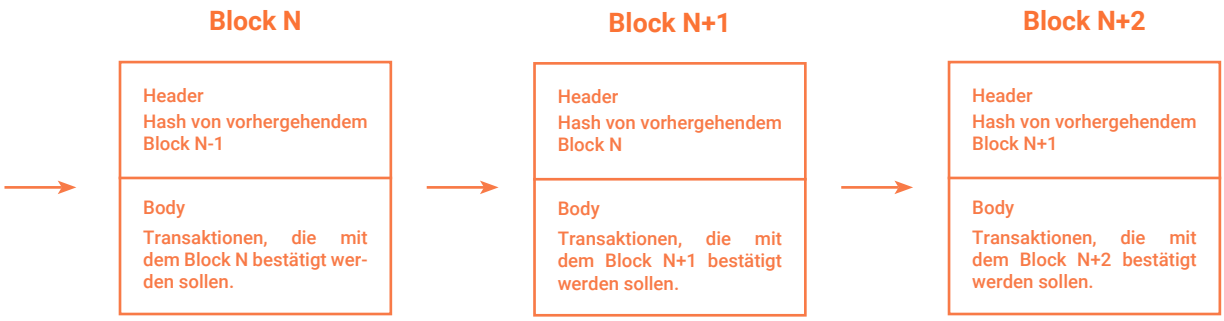
2. Die Blockchain

Die Blöcke (= Datensätze) der Blockchain bauen alle aufeinander auf, indem der Hash des vorigen Blocks im Hash des neuen Blocks enthalten ist. Ohne diese Komponente bestünde keine Verbindung und Chronologie zwischen den einzelnen Blöcken. Würde ein Block irgendwo in der Kette geändert, müsste sich auch dessen Hash im folgenden Block ändern - und dessen Hash in dessem Nachfolger und so weiter. Hierdurch ist die Blockchain im Nachhinein unveränderbar.

Jeder Block verfügt über einen Header und einen Body. In dem Header sind verschiedene Informationen enthalten, die als Metadaten bezeichnet werden, weil es sich bei ihnen um übergeordnete Daten bzw. Informationen über Daten handelt.

Im Header sind u. a. der Hash des vorigen Blocks enthalten und die sog. Nonce. In der Kryptografie wird die Bezeichnung „Nonce“ verwendet, um eine zufällig generierte Zahlen- oder Buchstabenkombination zu bezeichnen, die nur ein einziges Mal in dem jeweiligen Kontext verwendet wird. „Nonce“ ist eine Abkürzung für „used only once“ oder „number used once“. Im Body befinden sich die Transaktionen, die mit dem Block ausgeführt werden sollen.

In jedem Block sind zudem die vorigen Hashes gespeichert und die Transaktionen der vorigen Blöcke. Dadurch ergibt sich die immer weiter wachsende Kette, die Blockchain. Diese ist für jedermann einsehbar. Jeder Nutzer kann daher sehen, welche Transaktion durchgeführt wird, allerdings nicht, wer diese Transaktion durchführt.



Detailliert sieht der Inhalt eines Blocks wie folgt aus:

Header

- Versionsnummer der Software
- Hash von vorhergehendem Block
- Merkle Root
- Zeitstempel
- Ziel der aktuellen Schwierigkeit
- Nonce

Body

Transaktionen, die mit dem Block bestätigt werden sollen.

Der Header enthält auch eine sog. „Merkle Root“ Die Bezeichnung „Merkle Root“ geht auf den Wissenschaftler Ralph Merkle zurück, der sich eine Methode zur Bereitstellung einer digitalen Signatur zum Zwecke der Authentifizierung einer Nachricht hat patentieren lassen, das Konzept des sog. „Hash Baumes“ oder „Merkle Trees“. Es handelt sich dabei um eine baumförmige Struktur aus Hashwerten von Datensätzen. Die Wurzel dieses Baumes wird als „Merkle Root“ bezeichnet und enthält aufgrund der baumartigen Verknüpfung der Hashes alle Informationen über jeden einzelnen Transaktionshash, der auf dem Block existiert.

Das Ziel der aktuellen Schwierigkeit gibt an, wie klein der neue Hash sein muss, um Gültigkeit zu beanspruchen. Hierfür wird vom Netzwerk ein Schwellenwert vorgegeben, der vom Hash-Wert unterschritten werden muss. Jeder Hash hat eine Größe in Bits. Je niedriger das Ziel in Bits ist, desto schwieriger ist es, einen passenden Hash zu finden.

Dieses Verfahren der kryptografischen Verkettung in einem dezentral geführten Buchführungssystem ist die technische Basis für Kryptowährungen.

a | Mining

Das Schaffen neuer Blöcke in der Blockchain wird Mining genannt. Stark vereinfacht dargestellt läuft das Mining in zwei Schritten ab. Neben dem Wettbewerb unter den Minern, wer den Block beisteuern darf, wird geprüft, ob der von einem Miner zusammengestellte Block formal korrekt ist. Um einen neuen Block zu schaffen, muss ein Teilnehmer eine Rechenaufgabe über das Versuch-und-Irrtum-Prinzip (engl.: „trial and error“) lösen. Der Teilnehmer, der als Erster eine Lösung gefunden hat, verteilt diese sowie die Einträge des Blocks an das Netzwerk, sodass andere Teilnehmer auf diesem Block aufbauen und einen weiteren Block mit neuen Einträgen anhängen können.

Um einen neuen Block zu finden, muss ein rechenintensiver Arbeitsnachweis erbracht werden. Das mathematische Problem in jedem Block ist extrem schwierig zu lösen, aber sobald eine gültige Lösung gefunden wurde, ist es für den Rest des Netzwerks sehr einfach, die Richtigkeit der Lösung zu bestätigen.

b | Konsens

Wenn vom Mining gesprochen wird, dann heißt es häufig, dass „Konsens geschaffen“ werden muss. Als Konsensmechanismus wird

ein Algorithmus bezeichnet, der eine Einigung über den Status eines Netzwerkes zwischen seinen Teilnehmern erzielt. Hierdurch wird sichergestellt, dass alle Teilnehmer eine identische Kopie der verteilten Datenbank besitzen.

Alle herkömmlichen Zahlungssysteme haben eine zentrale Autorität oder Kontrollinstanz, die über sämtliche Transaktionen wacht. So ist es beispielsweise nicht möglich, Überweisungen von einem Konto zu tätigen, auf dem nicht das notwendige Guthaben oder ein ausreichender Kreditrahmen besteht. Bei Kryptowährungen existiert keine zentrale Autorität. Trotzdem muss irgendwie überprüft werden, ob derjenige, der eine Überweisung tätigt, über genug Kryptowährung hierfür verfügt. Eine Kryptowährung, die von jedem beliebig hergestellt und ausgegeben werden kann, hätte keinen Wert. Es muss daher Konsens im Sinne von Übereinstimmung hergestellt werden, welche Guthaben vorhanden und welche Überweisungen gültig sind und welche nicht.

c | Proof of Work (PoW)

Es gibt bei Kryptowährungen verschiedene Methoden, Konsens herzustellen. Eine der häufigsten ist die Proof-of-Work-Methode, die z. B. von der Bitcoin-Blockchain verwendet wird.

Wie oben ausgeführt, muss über ein trial-and-error-Verfahren eine Rechenaufgabe gelöst werden. Ein wesentliches Merkmal der Rechenaufgabe ist, dass sie asymmetrisch ist. Die Arbeit muss auf der Anfordererseite zwar schwer sein, aber für das Netzwerk leicht zu überprüfen. Die erforderlichen Berechnungen werden von Computern pro Sekunde milliardenfach durchgeführt. Da sich der gesuchte Input zu dem bekannten Output (Hashwert) nicht einfach errechnen lässt, wird die Lösung durch vielfaches Ausprobieren gesucht. Ist der Input erst einmal bekannt, ist es ein Leichtes, ihn durch Nachrechnen zu verifizieren.

Hinter der Proof-of-Work-Methode, die nicht erst für Kryptowährungen erfunden worden ist, steckt die Idee, dass erst ein Arbeitsnachweis (engl.: „proof of work") erbracht werden muss, bevor der Nutzer selbst den Dienst in Anspruch nehmen darf. Wenn ein gültiger Wert gefunden worden ist, ist damit auch der Nachweis erbracht, dass die notwendige Arbeit geleistet worden ist.

Tatsächlich erfordert das Lösen der komplizierten Rechenaufgaben sehr viel Zeit und durch die erforderliche Rechenkapazität ebenso viel Elektrizität und ist damit verhältnismäßig kostenintensiv. Aus diesem Grund setzen andere Kryptowährungen auf das Proof-of-Stake (PoS) Konzept.

d | Proof of Stake (PoS)

Bei der Proof-of-Stake-Methode ist der Anteil (engl.: „stake") eines Nutzers an der gesamten Menge an Tokens Grundlage des Konsens und damit ausschlaggebend dafür, welcher Nutzer einen weiteren Block der Kette erzeugen darf. Hier wird grundsätzlich mittels eines Zufallsalgorithmus der Nutzer, der den nächsten Block erzeugen darf, ausgewählt. Dabei gilt aber, je größer der Anteil eines Nutzers ist (oder gelegentlich auch je länger seine Teilnahmedauer am System), desto wahrscheinlicher ist, dass dieser Nutzer ausgewählt wird. Anders als bei der Proof-of-Work-Methode ist ein zeit- und kostenintensives Mining nicht erforderlich.

Einfach ausgedrückt werden bei der Proof-of-Stake-Methode Transaktionen auf der Blockchain validiert, indem Anteile an der Digital-Währung in einer Wallet vorgehalten und entsperrt werden, was Staking genannt wird. Das Staking der Proof-of-Stake-Methode entspricht dem Mining bei der Proof-of-Work-Methode, schließt sich damit jedoch gegenseitig aus. Der Anreiz ist jedoch identisch und besteht im Erhalt einer Einheit der Kryptowährung.

Bei der Proof-of-Work-Methode ist der Anteil an der gesamten Rechnerkapazität des Netzwerks ausschlaggebend für die Wahrscheinlichkeit, den nächsten Block erfolgreich zu minen. Bei der Proof-of-Stake-Methode ist der Anteil an den gesamten Tokens im Netzwerk ausschlaggebend für die Wahrscheinlichkeit, den nächsten Block erfolgreich zu staken.

---

e | Difficulty

Als Difficulty wird der Schwierigkeitsgrad für das Finden neuer Blocks einer Kryptowährung bezeichnet. Das Mining wird heute mit speziellen Geräten durchgeführt, die extra für diesen Zweck angefertigt werden. Der technische Fortschritt macht es einfacher, neue Blöcke zu finden. Im Idealfall würde dies bedeuten, dass sich auch der Zeitaufwand für die Erstellung eines neuen Blocks drastisch verringert und die Auszahlungen proportional steigen. Um diesem Effekt entgegenzuwirken, haben die Entwickler eine Korrelation zwischen Hash-Rate und Schwierigkeitsgrad in den Protokollen integriert. Steigt die Anzahl der Miner im Netzwerk, erhöht sich analog zu der ebenfalls steigenden Hash-Power auch die Schwierigkeit und Zeit, um einen neuen Block zu erschließen. Dadurch soll eine

gleichbleibend konstante Mining-Zeit erzielt werden. In der Regel sehen die Protokolle der Kryptowährungen bestimmte Zeiten vor, die für das „Hashing" eines neuen Blocks benötigt werden. Wären die Rechenaufgaben zu einfach, würden alle Coins einer Kryptowährung in wenigen Stunden geschürft sein.

Das Bitcoin-Netzwerk variiert seine Bitcoin Difficulty alle 2016 Blöcke, um einen konstanten Output zu gewährleisten. Wenn die Hash-Rate des Netzwerks hoch ist und die Zeit, die benötigt wird, um einen neuen Block zu entdecken, weniger als 10 Minuten beträgt, dann erhöht das Netzwerk den Schwierigkeitsgrad proportional, um die Blockerkennungszeit zu erhöhen. Wenn die Blockerkennungszeit mehr als 10 Minuten beträgt, reduziert das gleiche Protokoll den Schwierigkeitsgrad. Vorgesehen ist, dass alle 10 Minuten ein neuer Block erstellt wird.

Technisch gesehen ist die Zeit, die ein Miner benötigt, um einen neuen Block zu schürfen, direkt proportional zur gesamten Rechenleistung des Netzwerks, die als Hash-Rate bezeichnet wird.

f | Hash-Rate

Die Geschwindigkeit, mit der die vielen komplexen Rechenoperationen bei der Erschließung eines neuen Blocks durchgeführt werden, wird Hash-Rate genannt. Der Begriff wird dabei sowohl zur Bezifferung der Leistungsfähigkeit eines Computers, als auch zur Geschwindigkeitsangabe der Datenverarbeitung im Blockchain-Netzwerk verwendet und wird daher als Maßeinheit für die Rechenleistung des Bitcoin-Netzwerks angesehen. Wenn das Netzwerk eine Hash-Rate von 10 TH/s erreicht, heißt das, dass es 10 Billionen Berechnungen pro Sekunde durchführen kann. Im Bitcoin-Netzwerk liegt die durchschnittliche Hash-Rate bei 9,9 TH/s und sie wächst mit jedem neuen Miner, der sich dem Netzwerk anschließt, weiter an.

Durch die Erhöhung der Geschwindigkeit erhöhen sich auch die Kosten für die Blockbildung und die Miner werden dazu motiviert, die Leistungsfähigkeit ihrer Miningsysteme zu verbessern, um wirtschaftlich erfolgreich zu sein. Je höher die Hash-Rate, desto mehr mathematische Operationen können in der vorhandenen Zeit durchgeführt werden. Um die Hash-Rate zu erhöhen, schließen sich professionelle Miner oder Institutionen zu sogenannten Pools zusammen. Faktisch ist das individuelle Mining von Bitcoins mit den gängigen Standard-Computern heute nicht mehr möglich.

g | Funktionen des Minings

Mit dem Mining werden zwei Funktionen erfüllt. Zum einen werden durch das Mining die Transaktionen des jeweiligen Blocks validiert und so zugleich Doppelausgaben (sog. Double Spending) vermieden. Zum anderen wird neue digitale Währung erzeugt, da der Miner, der als Erster eine Lösung gefunden hat, eine Belohnung in Form der digitalen Währung erhält. Zusätzlich erhält der Miner die Summe der Gebühren aller Transaktionen, welche in seinen erfolgreich gemineten Block integriert wurden. Die Chance, sich bei der Konkurrenz durchzusetzen, wird nicht durch Zufall, sondern primär durch Hardware entschieden. Dies spiegelt sich in der Verteilung der Erlöse wieder. Arbeiten beispielsweise eine Vielzahl Miner an einem Block, bekommt der mit der höchsten Hash-Rate und den meisten Berechnungen auch den größten Teil der Blockprämie.

Mittlerweile existieren auf der Blockchain-Technologie basierende Plattformen, die anders als Bitcoin keine reine Kryptowährung darstellen, z.B. Ethereum. Durch das Mining (oder ggf. auch Staking) werden auf diesen Plattformen sog. „Smart Contracts" validiert. Für diese Smart Contracts können Transaktionsbedingungen im Vorhinein festgelegt werden, bei deren Eintritt eine Folge automatisch eintritt. Ein Beispiel ist etwa eine Zahlung, bei der das System einen Geldbetrag erst freigibt, wenn zur Freigabe führende, festgelegte Bedingungen erfüllt und validiert sind. Für Smart Contracts gibt es eine Vielzahl von denkbaren Anwendungen, unter anderem E-Voting-Systeme, virtuelle Organisationen, Identitätsmanagement und Crowdfunding.

3. Wallets

Eine Wallet (Deutsch: Geldbörse) wird oft als digitale Geldbörse bezeichnet. Tatsächlich ist eine Wallet im Zusammenhang mit Kryptowährungen zu vergleichen mit einem Passwort-Manager. In der Wallet sind keine Coins (engl.: „Münzen") gespeichert, sondern der sog. „Private Key" (hierzu unten), der Ihnen das Recht gibt, die Coins auszugeben, die in der Blockchain diesem Schlüssel zugewiesen sind.

Die Coins selbst werden nicht in der Wallet gespeichert, sondern immer in der Blockchain aufgezeichnet. Sie können daher nicht verloren gehen. Der Nutzer kann lediglich den Zugriff auf seine Coins verlieren, wenn er den Private Key verliert. Mit dem Verlust des Wallets geht daher die Zugriffsberechtigung verloren – dies entspricht einem Totalverlust.

Umgangssprachlich ist oft jedoch die Rede davon, dass die Coins in der Wallet gespeichert werden.

Jede Wallet besteht aus einer Zeichenkette, die einmalig ist. So werden die Wallets voneinander unterschieden. Grundsätzlich hat jeder, der die Zeichenkette einer Wallet kennt, Einblick darin, wie viel Guthaben in einer Wallet gespeichert ist. Persönliche Daten des Eigentümers der Wallet werden im Zusammenhang mit der Wallet allerdings nicht gespeichert. Die Wallet ist anonym, es ist also nicht ersichtlich, welcher Person die Wallet gehört. Die Wallet ist zusätzlich mit einem Passwort geschützt. Nur mit der Zeichenkette kann daher niemand auf die Wallet und das hierüber verfügbare Guthaben zugreifen.

Eine Wallet ist immer nur für eine Kryptowährung gültig. Mit einer Bitcoin Wallet können daher keine Coins einer anderen Kryptowährung, z. B. Litecoin, versendet werden. Jeder Nutzer kann so viele Wallets besitzen wie er möchte, auch für eine einzige Kryptowährung.

Im Kryptowährungsbereich werden verschiedene Arten von Wallets verwendet.

a | Soft Wallets / Software Wallets

Bei Soft Wallets bzw. Software Wallets wird der Private Key mit einem Passwort auf einem Computer oder einer App gesichert. Sie sind nutzerfreundlich, durch die Verbindung zum Internet besteht jedoch die Gefahr, dass sie gehackt werden. Für die Wallet sollte unbedingt ein extrem sicheres Passwort gewählt werden.

b | Hard Wallets / Hardware Wallets

Ein Maximum an Sicherheit bieten Hard Wallets bzw. Hardware Wallets. Diese elektronischen Geräte wurden allein zu dem Zweck der Sicherung von Kryptowährung entwickelt und programmiert. Sie sehen häufig aus wie USB-Sticks und bietet die zur Zeit höchste verfügbare Sicherheit. Anders als bei normalen USB-Sticks muss in das Gerät üblicherweise zusätzlich eine PIN eingegeben werden, damit es vom Computer angesprochen werden kann.

c | Paper Wallets

Unter einer Paper Wallet versteht man einfach ein Stück Papier, auf das man sich den Private Key notiert hat. Es handelt sich insofern um ein physisches Wallet. Mittlerweile gibt es auch die Möglichkeit, im Internet Paper Wallets erstellen zu lassen. Wesentlich bei der Paper Wallet ist, dass sie - also das Stück Papier an sich - keine Verbindung zum Internet hat und dass von dem auf ihr gespeicherten Private Key keine elektronische Kopie existiert. Wenn man Geld versendet, muss man aber online sein. Dieser Moment - das Eingeben des Schlüssels - stellt eine Sicherheitslücke dar, so dass man im Grunde genommen für jede Nutzung eine neue Paper Wallet bzw. einen neuen Private Key kreieren müsste.

d | Mind Wallets

Der englische Begriff „mind" steht für das deutsche Wort Verstand. Wenn jemand den Private Key auswendig lernt und ihn dann ausschließlich in seinem Gedächtnis abspeichert, spricht man von einer Mind Wallet. Da ein Private Keys aber sehr lang ist, ist es eher unwahrscheinlich, dass ein Nutzer in der Lage ist, seinen Private Key dauerhaft ausschließlich im Gedächtnis zu behalten.

e | Exchange Wallets

Es gibt unzählige Börsen (engl.: „exchange") für Kryptowährungen. Diese Börsen bieten sogenannte Exchange Wallets an. Hierbei verwaltet der Nutzer seinen Private Key nicht selbst, sondern lässt diesen von der jeweiligen Börse verwalten. Der Nutzer kann eine komfortable Online-Oberfläche nutzen. Diese Form der Wallet kann jedoch problematisch sein in dem Fall, dass eine Börse gehackt wird. Dann könnten Unbefugte Zugriff auf die Coins erlangen. Exchange Wallets werden auch Web Wallets genannt, weil der Zugriff darauf über das Internet geregelt wird.

f | Hot Wallets und Cold Wallets

Als Hot Wallets werden Wallets bezeichnet, die auf Endgeräten laufen, die mit dem Internet verbunden sind, z. B. Web Wallets. Als Cold Wallets werden Wallets bezeichnet, die vollständig offline sind, wie z. B. Paper Wallets.

g | Mobile und Desktop Wallets

Hierbei handelt es sich um Wallets, die in Form einer Softwarelösung auf dem PC oder in Form einer App auf dem Smartphone gespeichert sind.

4. Der Inhalt der Wallet

Wie schon beschrieben, werden in der Wallet keine Coins verwahrt, sondern Datensätze. Um Zugriff zu einer Wallet nehmen zu können, werden zwei Schlüssel benötigt, der sog. Public Key und der Private Key. Diese Schlüssel werden mittels einer Software nach dem Zufallsprinzip generiert.

a | Public Key

Der Public Key ist sozusagen die Empfangsadresse der Wallet, an die Zahlungen gesendet werden können. Der Public Key muss daher nicht geheim gehalten werden, sondern wird im Gegenteil immer dann mitgeteilt, wenn eine Transaktion in der Kryptowährung erfolgen soll. Er ist vergleichbar mit der IBAN bei einem gewöhnlichen Bankkonto.

Eine Wallet kann eine beliebige Anzahl von Public Keys verwalten und ermöglicht dem Nutzer so einen gewissen Grundschutz vor Personen, die wissen wollen, wieviel Geld sie besitzen. Daher bietet es sich an, für jeden Zahlungsempfang einen neuen Public Key zu erzeugen. Zu jedem Public Key gibt es einen Private Key, mit dem neue Transaktionen signiert werden.

b | Private Key

Jede Wallet verfügt zudem über einen Private Key. Der Private Key (privater Schlüssel) ist ein geheimer Datenblock, der über eine kryptografische Signatur Ihr Recht beweist, Coins einer bestimmten Wallet ausgeben zu dürfen. Private Keys bestehen aus einer sehr langen Folge aus Buchstaben und Zahlen. Bei Bitcoin gibt 2 hoch 256 verschiedene Variationen an Private Keys. Es ist daher quasi unmöglich, dass zwei Personen denselben Private Key haben.

Der Private Key stellt sozusagen Ihre PIN dar. Er sollte niemals preisgegeben werden, da mit ihm die Coins, die der jeweiligen Wallet zugeordnet sind, ausgegeben werden können.

Verliert der Besitzer seinen Private Key, so hat er keine Kontrolle über das Geld in der Wallet mehr!

Mittlerweile gibt es bei manchen Wallets eine Wiederherstellungsoption, für die bestimmte Authentifizierungsmerkmale erforderlich sind. In den meisten Fällen ist es allerdings so, dass der Verlust des privaten Schlüssels gleichbedeutend mit dem Verlust des Zugriffs auf das Wallet ist und somit letztendlich auch Ihre Coin-Bestände nicht mehr verfügbar sind.

c | Coins und Token

Die Begriffe „Coin“ und „Token“ werden oft synonym verwendet, obwohl sie nicht dieselbe Bedeutung haben. Ein Coin ist einfach ausgedrückt eine digitale Münze, mit der Waren oder Dienstleistungen bezahlt werden können, so z.B. ein Bitcoin. Ein Token hat eine breitere Funktionalität. Er kann als ein digitales Recht (engl.: „asset“) verstanden und z.B. wie eine digitale Aktie oder Anleihe benutzt werden.

5. Der Ablauf von Transaktionen

Wenn eine Zahlung getätigt werden soll, d.h. wenn Coins einer Kryptowährung versendet werden sollen, dann werden die Anfragen zu einem neuen Block zusammengefasst. Eine Transaktion findet erst statt, wenn dieser neue Block verifiziert wurde. Der Übertrag findet von einer Wallet in eine andere Wallet statt. Diese Transaktionen sind nicht gratis, sondern es fällt hierfür eine – in der Regel sehr kleine – Gebühr an, was in der Eingabemaske zu sehen ist. Die Überweisung ist sofort in der Wallet des Empfängers sichtbar, der Empfänger kann aber erst über den Betrag verfügen, wenn die Transaktion validiert worden ist.

III. Vorteile der Blockchain-Technologie

Die Blockchain-Technologie ist weitaus mehr als nur die Grundlage für Kryptowährungen. Sie bietet vielfältige Anwendungsmöglichkeiten, die sich aus ihren Vorteilen ergeben. Die wichtigsten Vorteile werden im Folgenden dargestellt, wobei die einzelnen Punkte sich überschneiden können.

1. Manipulationssicherheit/Integrität der Daten

Durch kryptografische Verfahren wird sichergestellt, dass die Blockchain nicht nachträglich geändert werden kann. Die Kette der Blöcke ist somit unveränderbar, fälschungs- und manipulationssicher. Würde man versuchen, die Daten irgendeines Blocks zu ver-

ändern, so wäre die ganze Blockkette ungültig. Dies liegt daran, dass sich der Hashwert des gesamten Blocks verändert und die Referenz durch den nachfolgenden Block nicht mehr stimmt. Durch das Hashing in der Blockchain wird es daher nahezu unmöglich, Daten zu ändern. Ist einmal validiert worden, sind die Daten unveränderbar und jeder Änderungsversuch kann nachvollzogen werden.

2. Transparenz/Vertraulichkeit

Die auf der Blockchain gespeicherten Daten sind von allen Beteiligten einsehbar, d.h. alle Transaktionen sind sichtbar und ihre Auswirkungen auf die verschiedenen Vertragspartner können eingesehen werden. Sie sind deshalb aber nicht unbedingt auch für alle sinnvoll lesbar, denn Inhalte können verschlüsselt abgespeichert werden. Blockchains erlauben so eine flexible Ausgestaltung des Vertraulichkeitsgrads. Zudem können zwar die Inhalte der Wallets eingesehen werden, nicht öffentlich bekannt ist aber, wem die jeweilige Wallet gehört.

3. Zuverlässigkeit

Da die Blockchain keinen zentralen Fehlerpunkt (keinen zentralen Server, Verwalter o.ä.) hat, ist es fast unmöglich, dass das System ausfallen könnte. Die Blockchain-Daten sind oft auf Tausenden von Geräten in einem verteilten Netzwerk von Knoten gespeichert. Das macht das System und die Daten sehr resistent gegen technische Ausfälle und bösartige Angriffe.

4. Nichtabstreitbarkeit

Durch die Nutzung digitaler Signaturen sind Informationen in der Blockchain speicherbar, die fälschungssicher nachweisen, dass Teilnehmende unabstreitbar bestimmte Daten hinterlegt haben, etwa Transaktionen angestoßen haben.

5. Direkte Transaktionen/Geschwindigkeit

Die Blockchain ermöglicht direkte Transaktionen zwischen zwei Teilnehmern, ohne dass ein Mittelsmann, z. B. eine Bank, eingeschaltet werden muss. Hierdurch können die Transaktionskosten reduziert und Transaktionen unter Umständen schneller durchgeführt werden.

IV. Nachteile der Blockchain-Technologie

Die Blockchain-Technologie hat neben den Vorteilen auch Nachteile.

1. Mangelnde Skalierbarkeit

Noch ist die Blockchain-Technologie nicht beliebig skalierbar, sie kann u.a. wegen des wachsenden Speicheraufwands oder der notwendigen technischen Einbindung nicht unbegrenzt wachsen. Denn konzeptionell ist grundsätzlich vorgesehen, dass jeder Teilnehmer der Blockchain jede Transaktion für das System überprüft. Die Anzahl der derzeit über Bitcoin abgewickelten Transaktionen liegt weit unter der durch herkömmliche Anbieter abgewickelten Transaktionen, wie z. B. Visa und PayPal, und das Bitcoin-System ist – anders als die anderen Systeme - damit bereits ausgelastet. Es gibt aber verschiedene Ansätze, die Transaktionsgeschwindigkeit und den Transaktionsdurchsatz zu erhöhen, z.B. mittels Erhöhung der Rechenleistung oder Vergrößerung der Anzahl der Teilnehmer.

2. Stromverbrauch

Jeder Teilnehmer, der aktiv am Netzwerk teilhaben will, muss sich viel Speicherplatz auf der Festplatte freihalten. Das Herunterladen und das Synchronisieren der Datenmenge verbrauchen viel Zeit und Kapazitäten. Bei dem Proof-of-Work-Verfahren kommt der enorme Energieverbrauch hinzu. Da die Schwierigkeit („Difficulty“) laufend angepasst wird, muss die Hardware immer mehr Rechenleistung erbringen, um einen Wert zu finden. Damit steigen der Stromverbrauch, die Kosten für die Miner und die Anforderungen an die Hardware. In Zusammenhang mit dem steigenden Stromverbrauch für Blockchain-Prozesse sieht sich diese Technik regelmäßig auch Kritik in Bezug auf Aspekte der Ökologie und der Nachhaltigkeit ausgesetzt.

3. Das Problem des Double-Spendings

Digitale Güter können leichter als reale Münzen und Scheine kopiert werden. Es besteht die Gefahr, dass digitales Geld kopiert und dann doppelt ausgegeben wird, was als „Double-Spending“ bezeichnet wird. Der Nutzer erstellt zwei Transaktionen gleichen Inhalts mit zwei verschiedenen Empfängern. Die Miner können nicht sehen, dass dasselbe Guthaben zweimal versendet werden soll. Beide Transaktionen sind gültig. Da Transaktionen aber blockweise gebündelt werden und in einem Block kein Coin doppelt ausgegeben werden kann, wird nur eine Transaktion ausgeführt. Die andere wird verworfen.

Zumindest theoretisch kann trotzdem ein Double-Spending vorkommen. Dafür müsste ein Teilnehmer 51 % der Kontrolle im gesam-

ten Netzwerk übernehmen. Angesichts der bisherigen breiten Aufstellung von Knotenpunkten wäre das ein extrem teurer und aufwändiger Versuch, weshalb es extrem unwahrscheinlich ist, dass es zu einem solchen sog. „51%-Angriff" kommt. Unabhängige Miner sind aber zusammengeschlossen in Pools. Mehr als die Hälfte der Rechenleistung für das Mining von Bitcoins ist mittlerweile im Besitz weniger Pools. Aus dieser Perspektive betrachtet ist eine Manipulation (Double-Spending oder auch das Rückgängigmachen von Transaktionen) durch böswillige Teilnehmer nicht unmöglich.

V. Blockchain-Forks und Orphan Blocks

Nicht alle Teilnehmer einer Blockchain stimmen immer mit dem überein, was der Rest der Gemeinschaft will. Es kann dann versucht werden, in der Blockchain eine Gabelung (engl.: „fork") herbeizuführen, so dass die Blockchain in zwei Strängen weitergeführt wird. Dies passiert, wenn der Konsensmechanismus bzw. das zugrundeliegende Protokoll geändert wird. Kleinere Änderungen funktionieren wie Updates. Sie sind rückwärtskompatibel und werden „Soft Fork" genannt. Durch sie entsteht in der Regel keine Gabelung. Anders ist dies bei sog. „Hard Forks". Diese sind nicht rückwärts- oder abwärtskompatibel. Die Teilnehmer müssen entweder ein Software-Update vornehmen und können der neuen Blockchain folgen, oder sie entscheiden sich dafür, bei der alten Blockchain zu bleiben. Es werden in diesem Fall beide Blockchains unabhängig voneinander weitergeführt. Bis zur „Fork" sind sie identisch, danach sind sie nicht mehr miteinander kompatibel.

Bildhaft dargestellt handelt es sich bei der Blockchain um eine Kette von Blöcken, die immer länger wird. Die Blockchain ist so programmiert, dass jeder Miner immer an dieser längsten Kette mitarbeitet. Hin und wieder kommt es jedoch vor, dass zwei Miner gleichzeitig einen neuen Block finden. Diese beiden Blöcke beinhalten verschiedene Transaktionen und sind beide valide. Sie können nicht hintereinander angehängt werden, sondern bestehen nebeneinander. Würde jetzt an beiden Blöcken weitergearbeitet werden, dann würde die Blockchain sich gabeln. Das System löst dies so, dass zunächst an beiden Blöcken weitergearbeitet wird und beim Finden des nächsten Blocks an der hierdurch dann längeren Kette weitergearbeitet wird. Die Kette wird an dem anderen Block nicht mehr weitergeführt, dieser Block „verwaist", man spricht von einem „Orphan Block". Alle seine gültigen Transaktionen werden wieder dem Pool unabgearbeiteter Transaktionen hinzugefügt und in einem der späteren Blöcke eingebettet. Der Miner, der den Orphan Block gefunden hat, erhält keine Belohnung.

VI. Dezentralisierung – Vor- oder Nachteil?

Ein wesentliches Merkmal der Blockchain-Technologie ist die Dezentralisierung. Es gibt keine zentrale, alles allein entscheidende Instanz. Dies bringt aber auch einen Nachteil mit sich. Alle Teilnehmer sind gleichermaßen berechtigt, aber nicht immer besteht Einigkeit zwischen allen Teilnehmern. Wird ein Software-Update notwendig, den ein Teil des Netzwerks jedoch ablehnt, entzweit sich die Blockchain und wird zu zwei unabhängigen Netzwerken mit derselben Historie, wie unter Ziff. V. beschrieben. Dieses Risiko der Fragmentierung führt zu einer Ungewissheit und beeinträchtigt den Nutzen dieser Technologie.

Zudem kann zwar im Prinzip jeder zu der Infrastruktur einen Teil beitragen, aber nicht immer zu einem gleichen Anteil. Alleine schon deshalb, weil die Startbedingungen aller Teilnehmer nicht gleich sein können und die Möglichkeit der Partizipation an Bedingungen wie die Leistungsfähigkeit der Hardware oder die Menge der Digital-Währung, die der Nutzer besitzt, geknüpft ist.

VII. Die Blockchain-Technologie und Datensicherheit

In öffentliche Blockchains eingespeiste Datensätze werden transparent dargestellt, die Teilnehmer sind durch die eindeutige digitale Referenz gekennzeichnet. Faktisch sind öffentliche Blockchain-Systeme nicht anonym zu nutzen. Die Nutzer hinterlassen nachverfolgbare Spuren in der Blockchain und bewegen sich im rechtlichen Sinne immer nur pseudonymisiert im System, nicht anonym. Sie treten zwar nicht mit ihrem Klarnamen auf, benötigen aber eine Adresse in dem System, um angesprochen werden zu können. Dem Transparenzprinzip der Blockchain-Technologie steht der Aspekt der Vertraulichkeit grundsätzlich diametral gegenüber.

Die Sichtbarkeit der Daten innerhalb einer Blockchain kann zudem nicht rückgängig gemacht werden. Damit stehen öffentliche Blockchains in einem Spannungsverhältnis mit dem in der Datenschutzgrundverordnung (DSGVO) verankerten Recht auf Begrenzung der Speicherdauer personenbezogener Daten bzw. dem „Recht auf Vergessenwerden".

Wie bereits ausgeführt, gibt es ein breites Spektrum an Anwendungsmöglichkeiten für Blockchains. Blockchains können öffentlich sein, wie z. B. die Bitcoin-Blockchain, oder nur einem beschränkten Nutzerkreis zugänglich gemacht werden, z.B. innerhalb eines Unternehmens. Je nach Anwendungsgebiet und Nutzerkreis können verschiedene Systeme zum Einsatz kommen, um die Rechte der Nutzer zu schützen und Datenschutzaspekte zu berücksichtigen. Um das Vertraulichkeitsproblem zu lösen, können z. B. sensible Daten nicht direkt in der Blockchain gespeichert werden, sondern nur Referenzen der Daten verwendet werden. Die Daten selbst kön-

nen z.B. in einer externen Datenbank gespeichert und dort vor unbefugter Einsichtnahme geschützt werden.

Die Vereinbarkeit öffentlicher Blockchains mit Datenschutzaspekten ist derzeit noch nicht abschließend geklärt. Derjenige, der eine öffentliche Blockchain nutzt, verstößt hiermit nicht gegen Datenschutzrecht, er kann aber nicht davon ausgehen, dass er sich in diesem System gänzlich anonym bewegt.

Auch die Miner versuchten in der Vergangenheit und versuchen bis heute möglichst unerkannt zu bleiben. Die Standorte der Rechner wurden dennoch immer wieder lokalisiert, überwiegend durch einen plötzlich auftretenden extremen Stromverbrauch.

VIII. Einsatzmöglichkeiten der Blockchain-Technologie

Hinter der Blockchain-Technologie steckt die sogenannte Distributed-Ledger-Technologie (DLT). Die Blockchain ist eine der bekanntesten Distributed-Ledger-Technologien, weshalb die Blockchain-Technologie oft als Synonym für Distributed-Ledger-Technologien verwendet wird.

1. Distributed-Ledger-Technologie

„Distributed-Ledger-Technologie" kann mit „Technik verteilter Kassenbücher" übersetzt werden. Der Begriff beschreibt eine Technik, bei der Informationen auf verschiedenen, dezentralen Systemen gehalten, verifiziert und erforderlichenfalls durch das Schaffen von Konsens angepasst werden. Die verschiedenen Distributed-Ledger-Technologien unterscheiden sich durch die Art, wie die durch Computer vernetzten Teilnehmer des Systems zu Konsens kommen, etwa durch Proof of Work oder Proof of Stake (s.o.).

Die Distributed-Ledger-Technologie kann als dezentrales Buchhaltungssystem betrachtet werden, bei dem dezentral beliebig viele prinzipiell gleichgestellte, inhaltsgleiche Kopien des Ledgers, also der Buchhaltungsdaten oder „Bücher", von unterschiedlichen Parteien unterhalten werden. Kerngedanke der Technologie ist es dabei, durch geeignete Maßnahmen sicherzustellen, dass neu hinzuzufügende Transaktionen in allen Kopien des Ledgers übernommen werden und ein Konsens über die Transaktionen und den jeweils aktuellen Stand des Ledgers besteht.

Distributed-Ledger-Technologien können öffentlich („public"), privat oder auch hybrid abgearbeitet werden. Typische Beispiele für ein Public Distributed-Ledger-System sind etwa Bitcoin, Ethereum und Litecoin. „Öffentlich" bedeutet, dass die Computer in einem Netzwerk über das Internet Informationen an Personen streuen, die diese Informationen verarbeiten und die Transaktionen verifizieren. In einem Private Distributed-Ledger-System können nur kontrollierte und zu dem Netzwerk zugelassene Systeme diese Informationen verarbeiten, z. B. firmeneigene oder auch bank- oder staatseigene Server. Hybrid Distributed-Legder sind eine Kombination aus beiden Systemen. Sie können dafür sorgen, dass die Daten über das Public Network verbreitet, bestimmte Teile jedoch nur durch verifizierte Systeme bearbeitet werden können.

Wenn die verteilte Datenstruktur nicht in Form einer Kette vorliegt, dann handelt es sich nicht um eine Blockchain. Die Blockchain ist ein Unterfall von Distributed Ledger. Einfach ausgedrückt ist jede Blockchain Distributed-Ledger, Distributed-Ledger kann aber auch in anderer Form als in Form einer Blockchain vorliegen.

Die bekannteste Anwendung von Distributed Ledger sind Kryptowährungen.

2. Kryptowährungen

Eine Kryptowährung ist eine virtuelle Währung (aber kein Geld!), die auf kryptografischen Algorithmen basiert. Hinter Kryptowährungen steht im Grunde genommen die Idee der Dezentralisierung des Finanzsystems zu verwirklichen und damit eine Abkehr und Unabhängigkeit von großen zentralistischen Einheiten, wie Banken oder Staaten, zu ermöglichen. Aktuell (Juli 2022) gibt es mehr als 10.000 verschiedene (bekannte) Kryptowährungen, von denen manche sich durchsetzen, andere verschwinden und laufend neue hinzu kommen. Bitcoin ist mit Abstand die Kryptowährung mit der derzeit höchsten Marktkapitalisierung.

Da viele Begriffe rund um Kryptowährungen und die dahinterstehenden Technologien häufig synonym verwendet werden, obwohl sie eigentlich eine andere Bedeutung haben, werden einige weitere der Begriffe im Folgenden erläutert. Die Unterschiede können relevant sein, um verschiedene Projekte zu verstehen und sie hinsichtlich ihrer Chancen und Risiken bewerten zu können.

a | Coins/Altcoins

Wie bereits oben in Grundzügen dargestellt, bezeichnet der englische Begriff „coin“ im Deutschen eine „Münze“ und ist eine Einheit einer Kryptowährung. Wesentlich ist, dass Coins eine eigene Blockchain besitzen. Da sich die erstmalige Verwendung in dieser Art zurückführen lässt auf den Bitcoin und dessen Entstehung, dürften daher genau genommen nur solche Einheiten als Coins bezeichnet werden, die ihrem Wesen nach dem Bitcoin entsprechen bzw. zugehören und auf dessen Technologie (mit eigener Blockchain, eigenen Minern und eigenen Nodes) beruhen. Coins, die diese Eigenschaften aufweisen, werden - da sie direkte Alternativen zum Bitcoin darstellen - auch als Altcoins (kurz für: alternative Coins) bezeichnet. Altcoins sind z.B. Namecoin oder Litecoin.

Coins können auch außerhalb ihrer Plattform genutzt werden - etwa als Tausch- bzw. Zahlungsmittel -, vorausgesetzt, der jeweilige Vertragspartner akzeptiert sie als Zahlungsmittel.

b | Stable Coins

Stable Coins sind – vermeintlich - stabile Werte in digitaler Form. Sie zeichnen sich durch ein festes Verhältnis zu einem Basiswert aus und sollen dessen Wertentwicklung im Idealfall exakt nachbilden. Solche Basiswerte können zum Beispiel Edelmetalle, Währungen oder ein Korb verschiedener Währungen sein. Ein Stable Coin ist ein Krypto-Derivat (lat. derivare = ableiten), also die Abbildung von einem Basiswert in Form eines Krytpowerts. Anders als ein klassischer Coin, der von anderen Werten grundsätzlich unabhängig ist und insofern einen „eigenen“ Wert hat und eigenen Schwankungen unterliegt, hat ein Stable Coin selbst keine eigene, unabhängige Wertentwicklung, sondern hängt von der Wertentwicklung des abgebildeten Basiswerts ab. Ein Stable Coin ist daher keine eigenständige, unabhängige Kryptowährung.

Bei klassischen Kryptowährungen kommt es nicht selten vor, dass Coins innerhalb weniger Stunden dramatisch an Wert verlieren, nur um dann oftmals wieder deutlich im Kurs zuzulegen. Der Stable Coin soll dieser Sorge entgegenwirken. Er ist in der Regel stabiler als eine klassische Kryptowährung, sofern der mit dem Stable Coin verbundene Wert (z.B. Gold, US-Dollar, Euro) eine entsprechende Stabilität hergibt.

Stable Coins ermöglichen es Anlegern, in der „Krypto-Welt“ zu agieren, ohne auf die etablierten Eigenschaften von Fiatgeld oder anderen traditionellen Basiswerten wie Gold verzichten zu müssen.

Fiatgeld

Als Fiatgeld wird eine nationale Währung bezeichnet, die nicht an den Preis eines Rohstoffes wie Gold oder Silber gebunden ist. Der Wert von Fiatgeld basiert größtenteils auf dem Vertrauen der Öffentlichkeit in seinen Herausgeber, d.h. die Regierung oder die Zentralbank des jeweiligen Landes. Das Gegenteil ist Warengeld, das neben seinem Geldwert auch einen eigenen Gebrauchswert besitzt. Beispiele für Warengeld sind Edelmetalle, Tee, Zigaretten oder Alkohol. Heute stellen Fiatwährungen in fast allen Gesellschaften und Lebensbereichen das vorherrschende Zahlungsmittel dar.

---

c | Token/Krypto-Token

Der wesentliche technische Unterschied zwischen Coins und Token besteht darin, dass Token keine eigene Blockchain besitzen, sondern eine bereits vorhandene Blockchain oder ein bereits bestehendes Protokoll nutzen. Sie sind dadurch einfacher zu erstellen. Es gibt Plattformen, die Standardvorlagen nutzen, mit denen Nutzer ihre eigenen Token erstellen können. Ein Token bildet zwangsläufig immer eine eigene Community („Gemeinschaft“) und ist nur innerhalb dieser Gemeinschaft nutzbar, kann also nicht außerhalb dieser Plattform genutzt werden wie ein Coin.

Token sind mehr als nur Einheiten einer Kryptowährung. Der Grundgedanke hinter einem Token ist nicht der geldmäßige Handel, sondern eine breitere Funktionalität. Token werden häufig als Tauschinstrument bzw. Zahlmethode für Dienstleistungen (vergleichbar mit einem virtuellen Gutschein), als Stimmrecht in Communities („Gemeinschaften“) oder als digitales Asset (vergleichbar mit einem digitalen Vermögenswert) verwendet.

Es werden derzeit im Wesentlichen drei Arten von Token voneinander unterschieden - wobei viele Token Charakteristika mehrerer Kategorien aufweisen.

aa | Payment Token (Zahlungs-Token)

Als Payment- oder Zahlungs-Token (gelegentlich auch Currency-Token) werden Token bezeichnet, die neben der reinen Zahlungs-

funktion keine weiteren Funktionalitäten besitzen. Der Bitcoin wäre ein Zahlungs-Token, bei Bitcoin handelt es sich wegen der eigenen Blockchain strenggenommen aber nicht um einen Token, sondern einen Coin. Payment Token haben keinen weiteren intrinsischen Wert.

In Bezug auf Blockchain-basierte Payment Token ist manchmal die Rede davon, sie seien „general purpose". Damit ist gemeint, dass man sie universell einsetzen kann und dass sie sich nicht - wie Utility Token (siehe sogleich) - nur als Tauschmittel auf ein bestimmtes Gut beziehen.

Intrinsischer Wert

„Intrinsisch" bedeutet „von innen heraus" oder „einer Sache innewohnend". Im Zusammenhang mit Zahlungsmitteln kann der intrinsische Wert als der Materialwert betrachtet werden. Gold ist fast unmöglich zu zerstören und trübt nicht oder zerfällt, so dass es offensichtlich durch die Zeit bewahrt werden kann. Anders die heute als Zahlungsmittel verwendeten Geldscheine und Münzen: Sie haben keinen Materialwert. Geld hat daher keinen intrinsischen Wert, sondern leitet seinen Wert von seiner ausgebenden Regierung und nicht von einem physischen Gut oder einer Ware ab.

bb | Utility Token (Nutzungs-Token)

Die derzeit am häufigsten ausgegebene Art von Token sind Utility Token, was mit „Nutzungs-Token" übersetzt werden kann. Die Bezeichnung wird verwendet, weil diese Token eine bestimmte Funktion in einem Netzwerk einnehmen. Sie sind vergleichbar mit Gutscheinen oder Eintrittskarten für eine bestimmte Leistung. Damit der Utility Token innerhalb der Community langfristig als Zahlungs- oder Tauschmittel zum Erwerb einer Dienstleistung oder zum Verkauf an neue Interessenten verwendet werden kann, ist die gesamte Community an dem langfristigen Erfolg eines Utility Token-Projekts interessiert.

Bei Utility-Token finden sich regelmäßig sehr komplexe rechtliche Gestaltungen. Dennoch unterfallen sie in der Regel nicht der Finanzmarktregulierung, weil sie weder der gesetzlichen Definition für Wertpapiere, noch für Vermögensanlagen, noch für der gesetzlichen Definition für Finanzinstrumente in Gestalt von Kryptowerten unterfallen. Daher unterfallen regelmäßig weder die Ausgabe der Vertrieb solcher Utility-Token einer Erlaubnispflicht oder einer Prospektpflicht.

cc | Security Token (Anlage-Token)

Der Begriff „Security Token" wird nicht aus der deutschen Übersetzung „Sicherheit" für „Security" abgeleitet, sondern aus der deutschen Übersetzung für „Wertpapier". Security Token besitzen keine operative Funktion für die Blockchain, ihr Hauptziel ist es, Investitionsgewinne zu realisieren. Sie können als Vermögensanlage ausgestaltet sein, vergleichbar mit einer Kommanditbeteiligung an einem Unternehmen, oder als ein Wertpapier eigener Art, bei dem es sich durch Tokenisierung (hierzu unten) um am Finanzmarkt handelbar gemachte Vermögensanlagen handelt, die als Wertpapiere eingeordnet werden müssen.

Der entscheidende Unterschied zu einer traditionellen Aktie sind der Wechsel des Mediums und der Abwicklungsinfrastruktur. Eine Verbriefung in Form einer Urkunde wie bei herkömmlichen Wertpapieren ist nicht erforderlich, das elektronische Wertpapierregister und die Clearingstelle werden von einer Blockchain-Infrastruktur ersetzt.

Der klassische Security Token begründet keine Eigentumsrechte an dem zu Grunde liegenden Unternehmen wie z.B. Aktien. Anders der Equity Token, der eine Unterart des Security Token darstellt, allerdings werden beide Begriffe häufig synonym verwendet.

Für die rechtliche Einordnung als Vermögensanlage oder als Wertpapier ist die konkrete Ausgestaltung im Einzelfall entscheidend. Vor einer Investition sollten Sie sich sorgfältig über das jeweilige Projekt informieren, da die rechtliche Einordnung entscheidend ist für Ihre Rechte als Anleger, die Pflichten des Emittenten und die Chancen und Risiken der Anlage.

dd | Equity Token

Der Equity Token ist eine Unterart des Security Token und kann als eine „moderne" Version einer Aktie angesehen werden. Er repräsentiert einen Anteil am zugrunde liegenden Unternehmen. Seine Inhaber erwerben Anteilsrechte am Vermögen des Unternehmens, haben Anspruch auf einen Teil des Unternehmensgewinns und erhalten ein Stimmrecht.

3. Tokenisierung

Als Tokenisierung wird die digitalisierte Abbildung eines realen (Vermögens-)Wertes inklusive der in diesem Wert enthaltenen Rechte und Pflichten sowie dessen hierdurch ermöglichte Übertragbarkeit bezeichnet – finanztechnisch könnte man auch sagen, dass Token ein Derivat auf den abgebildeten Wert ist. Bei den Vermögenswerten kann es sich z. B. um Aktien, Anleihen, Immobilien, Gold, Lizenzrechte usw. handeln. Es kann praktisch alles tokenisiert werden. Anstatt einer Urkunde, wie bei herkömmlichen Wertpapieren, „verbrieft" ein Token die Besitzverhältnisse digital. Dabei wird der Token mit spezifischen Rechten und Pflichten versehen und in einer gewissen Anzahl gestückelt in ein Register eingetragen.

Da quasi alles tokenisiert werden kann, werden die Vermögenswerte, die bis dato an Börsen handelbar sind, um weitere Anlagegegenstände erweitert. Bislang musste z.B. eine Aktiengesellschaft gegründet werden, wenn die Unternehmensanteile an der Börse handelbar sein sollten. Werden die Unternehmensanteile in Token herausgegeben, ist dies nicht mehr erforderlich – diese können dann außerhalb der Börse gehandelt werden, in einigen Ländern inzwischen auch börslich. Hierdurch steigt die Zahl der börsenfähigen Unternehmen erheblich. Auch sog. „illiquide" Vermögenswerte wie Mehrfamilienhäuser, Kunst oder Musikrechte können durch Tokenisierung handelbar gemacht werden.

4. Einsatzmöglichkeiten und Vorteile von Token

Token werden übertragen, indem sie z. B. über eine Smartphone App direkt an die Wallet des Empfängers gesendet werden. Für den Absender und den Empfänger ist dies ein einfacher Vorgang, gegenüber herkömmlichen Überweisungen allerdings nichts Neues. Auch normale Banküberweisungen sind heute bereits in Echtzeit innerhalb weniger Sekunden möglich. Hierfür ist allerdings eine Kette von Konten erforderlich. Die Transaktion erfolgt nicht direkt vom Konto des Versenders auf das Konto des Empfängers, sondern über interne Abwicklungskonten der eigenen und der Bank des Empfängers sowie ggf. über Konten einer Verrechnungsstelle. Die Übertragung (digitaler) Token ist wesentlich einfacher. Blockchain-basierte Zahlungen werden in einer einzigen Datenbank dokumentiert, auf die alle autorisierten Teilnehmer zugreifen können. Hierdurch können Bestätigungen und Abstimmungsprozesse schneller erfolgen oder ganz entfallen. Beispielsweise ist bei der Übertragung via Token bei grenzüberschreitenden Zahlungen kein internationales Netzwerk bilateraler Kontobeziehungen erforderlich, so dass lange Laufzeiten und hohe Entgelte entfallen.

Ein weiterer erheblicher Vorteil von Token ist, dass sich Zahlungen an beliebige programmierbare Bedingungen knüpfen lassen und dadurch automatisch auslösen. Man spricht hierbei von Smart Contracts.

5. Smart Contracts

Smart Contracts enthalten grundsätzlich dieselben Informationen wie herkömmliche Verträge. Die Vertragsinformationen werden jedoch im Programmcode des Smart Contracts festgelegt und lösen automatisiert vertragliche Folgen aus. Smart Contracts enthalten Wenn-Dann-Regeln. Wenn eine im Vertrag festgelegte Bedingung erfüllt wird, dann hat das automatisch eine ebenfalls im Vertrag festgelegte Konsequenz zur Folge, z.B. wird eine Zahlung ausgeführt oder Verfügungsrechte werden übertragen. Gleichzeitig werden alle Vertragspartner in Echtzeit über Statusänderungen informiert.

a | Vorteile von Smart Contracts

Gegenüber herkömmlichen Vertragsformen verfügen Smart Contracts auf der Basis einer Blockchain über einige Vorteile.

Verlässlichkeit: Wenn ein Smart Contract korrekt programmiert wurde, sind Interpretationsschwierigkeiten der Vertragsbedingungen nahezu ausgeschlossen. Zudem können keine Dokumente verloren gehen.

Sicherheit: Kryptografische Verschlüsselungsverfahren sichern Smart Contracts vor Hackern. Die Vertragsbedingungen sind im Nachhinein unveränderbar.

Effizienz: Zwar müssen Smart Contracts programmiert werden. Dies ist jedoch weniger aufwändig als eine entsprechende bürokratische Verarbeitung von „klassischen Papierverträgen", wodurch die Vertragspartner Zeit und Geld sparen.

Unabhängigkeit: Der Einsatz von Smart Contracts macht Dritte wie z.B. Anwälte, Notare und Banker für die Vertragsdurchführung entbehrlich. Nur der Programmcode entscheidet darüber, ob die Vertragsbedingungen korrekt erfüllt wurden oder nicht. Es gilt der Grundsatz: Code is law.

b | Nachteile von Smart Contracts

Das Konzept digitaler Verträge ist noch nicht vollständig ausgereift. Zwar unwahrscheinlich aber nicht unmöglich ist, dass der Programmcode fehlerhaft ist. Da Informationen auf einer Blockchain unveränderlich sind, können derartige Fehler im Nachhinein nicht mehr korrigiert werden. Die Verlässlichkeit und Unveränderlichkeit eines digitalen Vertrages auf Basis einer Blockchain hängen von dem Programmierer und dessen Fähigkeiten ab. Wenn dieser böse Absichten verfolgt, könnte er eine „Hintertür" in den Smart Contract einbauen.

Faktisch können sich zudem die Bedingungen für die Vertragserfüllung zufällig ändern. Beispielsweise kann die gelieferte Ware beschädigt sein, was die Software grundsätzlich nicht ohne Weiteres registrieren und bei der Freigabe der Zahlung berücksichtigen kann.

Es gibt vielfältige theoretische Anwendungsmöglichkeiten von Smart Contracts, beispielsweise in Lieferketten vom Konsumenten über den Händler bis zum Produzenten; im Gesundheitswesen, wobei Patientendaten in einem digitalen Vertrag abgebildet werden könnten; sie können Mietverhältnisse und den Kauf oder Verkauf von Grundstücken regeln und erleichtern usw. Zivilrechtlich werfen Smart Contracts aufgrund der Vertragsfreiheit keine größeren Probleme auf. Allerdings können unerwartete Hindernisse durch neue Vorschriften sowohl der europäischen als auch der deutschen Finanzaufsichtsbehörden entstehen.

Die wohl bekannteste Blockchain-Plattform, die Smart Contracts anbietet, ist Ethereum. Diese Plattform bietet auch Standardvorlagen an, mit denen Nutzer ihre eigenen Tokens erstellen können.

Die Vermögensanlage mit Blockchains (Kryptowährungen und -werte)

D

In Kapitel C. wurde erläutert, dass Blockchain nicht gleichbedeutend mit Kryptowährung ist und dass die Blockchain-Technologie bzw. die Distributed-Ledger-Technologie weitaus mehr Möglichkeiten bietet als die Erstellung digitaler Währungen. Es wurde bereits die Möglichkeit der Digitalisierung von Assets durch Tokenisierung dargestellt. Im Folgenden werden verschiedene Investitionsmöglichkeiten vorgestellt, die auf der Blockchain-Technologie beruhen und sich nicht auf Kryptowährungen beschränken.

I. Die Kapitalanlage mit Kryptowährungen

Zum technologischen Fortschritt kam der Bitcoin-Boom. Etwa von Dezember 2016 bis Dezember 2017 stieg der Kurs von Bitcoin rasant. Es folgte ein dramatischer Wertverlust, bei dem viele Anleger erhebliche finanzielle Verluste erlitten . Seitdem wurde der Bitcoin für Anleger wieder interessanter und hat wieder erheblich an Wert gewonnen. Zudem machte die rekordverdächtige Wertsteigerung den Markt besonders interessant für Spekulationen und schaffte Anreize für die Entwicklung weiterer Kryptowährungen. Insgesamt zeigt sich aber eine deutlich hohe Volatilität .

1. Kryptowährungen an der Börse handeln

Für den Handel von Kryptowährungen existieren verschiedene Krypto Börsen bzw. Krypto Exchanges. Kryptowährungen werden nicht neben Wertpapieren an den klassischen Börsen gehandelt. Ähnlich dem Devisenhandel setzen Sie beim Handel mit Kryptowährungen auf Schwankungen von Wechselkursen bzw. auf eine Wertsteigerung der Kryptowährung, in die Sie investiert haben.

Krypto Börsen sind digitale Handelsplattformen, auf der sich Kryptowährungen tauschen oder mit Fiatwährungen (Euro, Dollar, etc.) kaufen lassen. Krypto Börsen sind keine tatsächlich existierenden Orte, die besucht werden können. Der Handel findet nur digital statt. Es gibt mittlerweile verschiedene Krypto Börsen mit verschiedenen Angeboten. Es bieten z. B. nicht alle Börsen den Tausch von Kryptowährung in Fiatwährung an. Bevor Sie sich für eine Börse entscheiden, sollten Sie sich daher mit dem konkreten Angebot dieser Börse vertraut machen. Es ist zudem zu beachten, dass die Kryptobörsen nicht den strengen (wenn überhaupt) Regelungen unterliegen, wie sie für herkömmliche Börsen gelten.

Sie benötigen in der Regel ein Wallet. Da beim Krypto-Handel keine Depotbank zwischen Ihnen und der Börse steht, müssen Sie sich zudem selbst bei der Krypto Börse anmelden, um am Handel teilnehmen zu können. Hierfür ist das Durchlaufen des Legitimationsprozesses zur Verhinderung von Geldwäsche erforderlich, der auch als „know your customer" bezeichnet wird. Dabei geht es vorrangig darum, Ihre Identität zutreffend zu ermitteln. Ist dies erfolgreich abgeschlossen, können Sie einen Auftrag erteilen, indem Sie die zu handelnde Kryptowährung auswählen und angeben, wie viele Coins oder Token Sie kaufen möchten. Den Gegenwert bezahlen Sie häufig durch Abbuchung von Ihrer Kreditkarte oder durch eine andere Zahlungsmethode, z.B. PayPal.

Beim Handel mit Kryptowährungen fallen Gebühren an, die je nach Börse unterschiedlich ausfallen können. Es gibt Trading Fees, die abhängig sind vom gehandelten Volumen, für die Einzahlung von Fiatgeld kann eine Einzahlungsgebühr verlangt werden – dies gilt auch für die Einzahlung per Kreditkarte -, und manchmal werden auch Gebühren bei Inaktivität des Nutzers verlangt.

Krypto Börsen weisen untereinander viele Unterschiede aus, so dass Sie sich auf jeden Fall eingehend mit den verschiedenen Anbietern beschäftigen sollten, bevor Sie sich für eine Börse entscheiden. Die unterschiedlichen Angebote und Gebühren können einen großen Einfluss auf Ihr Investment haben.

2. Kryptowährungen als Zahlungsmittel

Als Währungen sind Kryptowährungen grundsätzlich auch darauf ausgelegt, dass man mit ihnen bezahlen kann. Kryptowährungen sind jedoch kein gesetzliches Zahlungsmittel, d.h. es besteht keine allgemeine Pflicht, Kryptowährungen als Zahlungsmittel zu akzeptieren. In manchen Geschäften ist jedoch eine Bezahlung mit bestimmten Kryptowährungen möglich, weil diese dort freiwillig akzeptiert werden. Unternehmer, die eine Kryptowährung als Zahlungsmittel akzeptieren, müssen zu diesem Zwecke vorher selbst eine Wallet einrichten. Bislang sind dies in erster Linie Online-Shops, es gibt aber auch erste Restaurants, in denen mittels Krypto-

währung bezahlt werden kann.

Sie können sich derzeit nicht darauf verlassen, dass Sie mit einer Kryptowährung Waren und Dienstleistungen bezahlen können.

3. Geld verdienen mit Mining

Wie bereits oben dargestellt, lässt sich auch mit dem sog. „Kryptomining" Geld verdienen. Der Miner, der als Erster eine Lösung für das mathematische Rätsel des jeweiligen Blocks gefunden hat, erhält eine Belohnung in Form von Einheiten der entsprechenden Kryptowährung. Zusätzlich erhält er die Summe der Gebühren aller Transaktionen, welche in seinen erfolgreich gemineten Block integriert wurden. Die Chance, sich bei der Konkurrenz durchzusetzen, wird nicht nur durch Zufall, sondern primär durch Hardware entschieden, was sich auch auf die entsprechende Belohnung auswirkt. Arbeiten beispielsweise eine Vielzahl Miner an einem Block, bekommt der mit der höchsten Hash-Rate und den meisten Berechnungen auch den größten Teil der Blockprämie.

Das Auflösen der komplexen Algorithmen beansprucht immense Rechenleistungen, für die entsprechend leistungsfähige Hardware und wiederum eine große Menge Strom benötigt wird. Für einen einzelnen Nutzer ist es heute äußerst schwierig bis unmöglich, mit dem Minen erfolgreich Geld verdienen zu können. Neben den hohen Anschaffungskosten zur Sicherstellung einer hohen Rechnerleistung stellen die Stromkosten die wichtigste Größe bei der Kosten-Nutzen-Rechnung dar.

4. Derivate auf Kryptowährungen

Ein Großteil des Handelsvolumens bezüglich Kryptowährungen wird heute über Derivate abgewickelt. Als Derivate werden Finanzinstrumente bezeichnet, die die Wertentwicklung eines Basiswerts abbilden und deren Wertentwicklung somit unmittelbar oder mittelbar von der Preisentwicklung des Basiswerts abhängt. Anders als bei einer Direktinvestition in den Basiswert können Sie je nach Art des Tradings („long" oder „short") sowohl auf steigende als auch auf fallende Kurse setzen.

Long- und Short-Positionen

Mit „Long" oder „Long-Position" wird die Käufer-Position in einem Handelsgeschäft bezeichnet, und dementsprechend bezeichnet „Short" oder „Short-Position" die Verkäuferposition. Allgemein wird bei Finanzinstrumenten mit „long" jede Position bezeichnet, bei der der Inhaber von einer Wertsteigerung des Finanzinstrumentes profitiert. Entsprechend spekuliert der Inhaber einer Short-Position auf den fallenden Wert des Finanzinstruments.

Bei den derzeit angebotenen Derivaten auf Kryptowährungen handelt es sich vor allem um Zertifikate und finanzielle Differenzgeschäfte, besser bekannt als „Contracts for Difference" - CFDs. Es gibt aber auch bereits Futures und geplant ist es auch, ETFs (Exchange Traded Funds) auf Kryptowährungen aufzulegen. Diese Begriffe werden nachfolgend im Detail erklärt.

a | Zertifikate

Aus rechtlicher Sicht sind Zertifikate (ebenso wie Anleihen) Schuldverschreibungen, genauer: Inhaberschuldverschreibungen. Sie verbriefen eine Forderung gegen den Emittenten und sind als Inhaberpapiere ausgestaltet, d. h. der Besitzer der Urkunde wird in ihr nicht namentlich genannt und dem Inhaber bzw. Besitzer der Urkunde stehen die darin enthaltenen Rechte zu. Als Forderung verbrieft wird der Anspruch auf Rückzahlung eines Geldbetrags oder der Lieferung eines Basiswerts. Der Käufer erwirbt nicht wie ein Aktionär einen Anteil am Unternehmenskapital, sondern er gewährt dem Unternehmen Fremdkapital, dessen Ertrag und Rückzahlung typischerweise von anderen Werten abhängen als der Bonität der Emittenten.

Kryptowährungszertifikate bilden in der Regel den Kurs der zu Grunde liegenden Kryptowährung - des Basiswerts - 1:1 ab. Es gibt Zertifikate mit fester Laufzeit und solche mit unbegrenzter Laufzeit, sog. „Open-End-Zertifikate". Der Anleger partizipiert sowohl an den Kursgewinnen als auch an den Kursverlusten der Kryptowährung gegenüber einer anderen im Vorhinein festgelegten Währung, in der Regel Euro oder US-Dollar.

Für den Anleger hat die Investition in Kryptowährungszertifikate den Vorteil, dass er keine eigene Wallet benötigt und selbst keine Coins oder Token einer Kryptowährung erwerben muss. Demgegenüber stehen die Risiken, die der Basiswert mit sich bringt. In erster Linie sind dies die Kursentwicklungen, die durchaus auch in die falsche Richtung gehen können. Gerade bei Kryptowährungen ist eine große Schwankungsbreite der Kurse erkennbar und auch die Vergangenheit hat gezeigt, dass viele Gerüchte und Maßnahmen des Marktes, wie die Einstellung des Handels in China, auch zu einem Kursrutsch und entsprechenden erheblichen Verlusten führen können. Gerade der enorme Anstieg von Kursen lässt immer wieder Vermutungen aufkommen, dass es einmal zu größeren Kursverlust

(einem „Platzen der Krypto-Blase“) kommen könnte, was Sie als Anleger niemals aus den Augen verlieren sollten.

Eine ausführliche Darstellung zur Funktionsweise von Zertifikaten, ihren Ausstattungsmöglichkeiten und den mit einer Investition in Zertifikaten verbundenen Chancen und Risiken finden sie in der Broschüre „Grundlagenwissen Wertpapiere & Investmentfonds“, die Sie jederzeit bei Ihrem Vermögensberater oder beim Herausgeber dieser Broschüre anfragen können.

b | Exchange Traded Notes - ETNs

Die Abkürzung ETN steht für Exchange Traded Notes. ETNs sind ähnlich konstruiert wie Exchange Traded Commodities (ETCs) und dürfen auf keinen Fall verwechselt werden mit ETFs – Exchange Traded Funds. ETNs sind kein Sondervermögen und es besteht ein Emittentenrisiko. Die Vorschriften für die Streuung sind bei Fonds, die nach dem europäischen UCITS-Standard aufgelegt werden, streng. Daher ist es nicht möglich, einzelne Basiswerte wie eine Kryptowährung in einem ETF abzubilden. Möglich ist dies nur mit einer ETN.

ETNs sind börsengehandelte Wertpapiere in Form von Inhaberschuldverschreibungen einer Bank. Sie bilden die Wertentwicklung eines zu Grunde liegenden Referenzindexes bzw. der zu Grunde liegenden Kryptowährung im Verhältnis 1:1 oder mit einer Hebelwirkung ab. Durch das passive Management dieser Produkte sind die Nebenkosten relativ gering. ETNs haben oft eine sehr lange oder unbegrenzte Laufzeit und es sind keine Zinszahlungen vorgesehen. Sie werden von einer Zweckgesellschaft ausgegeben, die eigens zur Verwaltung der erworbenen Vermögenswerte gegründet wurde. Die Besicherung erfolgt entweder durch Swaps oder durch die physische Hinterlegung des Basiswerts. Häufig werden die Preise eines ETN von Market Makern gestellt, die fortlaufend für eine Quotierung des ETN in der Nähe der Entwicklung des abgebildeten Basiswertes oder der Strategie sorgen. Die Kurse von ETNs kommen durch Angebot und Nachfrage zustande. ETNs auf exotische Indizes können relativ hohe Verwaltungskosten verursachen und ein sehr geringes Handelsvolumen vorweisen, wodurch auch die Spreads deutlich höher liegen als bei ETFs.

Hebelwirkung

Wird der Kurs des Basiswerts nicht 1:1 nachvollzogen, sondern verändert sich der Wert des Derivats überproportional bei Kursveränderungen des Basiswerts, so spricht man von einer „Hebelwirkung“. Aufgrund der damit verbundenen Gewinnchancen ist dies ein gewollter Effekt. Bewegt sich der Kurs des Basiswerts allerdings in die „falsche“ Richtung, so kann die Hebelwirkung zu erheblichen Kapitalverlusten fuhren. Dabei gilt: Je größer der Hebel, desto größer das Risiko.

Die Rückzahlung des Kapitals am Ende der Laufzeit hängt zum Teil davon ab, wie sich der zu Grunde liegende Krypto-Index bzw. die zu Grunde liegend Kryptowährung entwickelt hat. Wenn der Index gesunken oder nicht ausreichend gestiegen ist, um die mit der Transaktion verbundenen Gebühren zu decken, erhält der Anleger bei Fälligkeit weniger als das, was er ursprünglich investiert hat. Als Anleger tragen Sie zudem das Bonitätsrisiko des Emittenten mit, also das Risiko, dass der Emittent zahlungsunfähig wird. Es gibt aber auch besicherte Papiere, wodurch sich das Emittentenrisiko verringert. ETNs mit ausgefalleneren Basiswerten wie Kryptowährungen schwanken oft stark im Wert.

Ein Faktor, der den Wert eines ETNs beeinflusst, ist die Bonität der emittierenden Bank. Da ETNs auf verschiedene Weise konstruiert werden können, können zusätzlich diverse weitere Faktoren einen Einfluss auf die Wertentwicklung des ETN nehmen. Manchmal finden sich auch sehr kreative Konzepte. Sie müssen als Investor diese Produkte genau verstehen, bevor Sie investieren.

c | Contracts for Difference - CFDs

CFDs sind als sog. Differenzkontrakte hochspekulative Derivate, bei denen eine Kryptowährung den Basiswert darstellt und die sich nur für sehr gut informierte Anleger eignen, die sich der erhöhten Risiken bewusst sind. Aktuell werden Krypto-CFDs insbesondere als Bitcoin-CFDs zum Handel angeboten. Als Inhaber eines CFDs sind Sie lediglich der Inhaber einer Forderung und tragen insofern das vollständige Ausfallrisiko der Gegenpartei.

Die Investition in CFDs stellt immer eine sehr spekulative Anlage dar, da sie einen Hebel beinhalten und so mit wenig Kapitaleinsatz große Handelspositionen am Markt eröffnet werden können. Die Anleger haben nicht den vollen Wert ihres Kontraktes zu leisten, sondern nur eine Sicherheitsleistung, die Margin genannt wird, zu hinterlegen

Margins

Üblicherweise werden Sicherheitsleistungen in Form von Margins bei Geschäften verlangt, deren Verpflichtungen erst in der Zukunft zu erfüllen sind. Hiermit soll die Erfüllung der schwebenden und der Höhe nach noch unsicheren Verbindlichkeiten aus diesen Geschäften abgesichert werden. Der Anleger zahlt nicht den vollen Wert des Kontraktes, sondern leistet lediglich eine Anzahlung. Man spricht insofern häufig von einem Erwerb „auf Margin".

CFDs werden nicht an Börsen notiert. Der Handel findet außerbörslich („over the counter" – OTC) statt und ist nur mit einem CFD-Broker möglich, der als Gegenpartei eines Geschäfts agiert. Das Handelsergebnis (Gewinn oder Verlust) errechnet sich aus der Differenz von Einstands- und Ausstiegskurs des CFD.

CFDs haben keine normierte Laufzeit oder standardisierte Kontraktgröße und können von den Vertragsparteien (insofern also in der Regel vom Anbieter vorgegeben) frei verhandelt werden. Daher besteht noch mehr als bei standardisierten Anlageformen wie Anleihen, Aktien oder Optionsscheinen die Gefahr, dass der Anleger die genauen Konditionen nicht versteht und deswegen für ihn unvorteilhafte Anlageentscheidungen trifft. CFDs gelten als hochrisikoreich.

d | Financial Futures

„Financial Futures" oder einfach „Futures" sind standardisierte, börsengehandelte, unbedingte Termingeschäfte auf einen Basiswert. Insofern unterscheiden sie sich von Optionen, die börsengehandelte bedingte Termingeschäfte sind.

Als Anleger können Sie bei einem Future sowohl die Position des Käufers als auch die des Verkäufers einnehmen. Das Geschäft ist für beide Vertragspartner unbedingt verpflichtend. Das bedeutet, der Käufer ist unbedingt verpflichtet, den Basiswert zu bezahlen bzw. abzunehmen, während der Verkäufer ebenso unbedingt verpflichtet ist, diesen zu verkaufen bzw. zu liefern. Allerdings sind Futures nicht grundsätzlich auf die Erfüllung des Vertrages angelegt, sondern in der Regel wird vor Ablauf des Kontraktes eine Stornierung, d. h. ein Gegengeschäft, getätigt. Es muss dann nur noch ein sich eventuell ergebender Differenzbetrag gezahlt werden. Je nachdem, ob der Wert des Basiswerts gestiegen oder gesunken ist, erzielen Sie mit dem Geschäft einen Gewinn oder einen Verlust.

Eine ausführliche Darstellung zur Funktionsweise von Futures, ihren Ausstattungsmöglichkeiten und den mit einer Investition in Termingeschäften im Allgemeinen und in Futures im Besonderen verbundenen Chancen und Risiken finden sie in der Broschüre „Grundlagenwissen Finanztermingeschäfte", die Sie jederzeit bei Ihrem Vermögensberater oder beim Herausgeber dieser Broschüre anfragen können.

II. Die Kapitalanlage mit Token

Neben der Möglichkeit, direkt oder indirekt in Kryptowährungen zu investieren, kann die Distributed-Ledger-Technologie genutzt werden, um digitalisierte Assets in Form von Token herauszugeben, die von Anlegern erworben werden können.

1. Tokenisierung

Als Tokenisierung wird im Zusammenhang mit Kapitalanlagen die digitalisierte Abbildung eines (Vermögens-)Wertes inklusive der in diesem Wert enthaltenen Rechte und Pflichten sowie dessen hierdurch ermöglichte Übertragbarkeit bezeichnet. In der Computerlinguistik bezeichnet der Begriff „Tokenisierung" die Segmentierung eines Textes in Einheiten, so kann Tokenisierung auch als „Stückelung" verstanden werden.

Der Wert eines Objektes, z.B. einer Immobilie, wird nach Belieben in mehrere Anteile aufgeteilt bzw. gestückelt. Dies erfolgt über die Blockchain und kann ggf. auch über einen Smart Contract erfolgen. Die Anteile werden dann öffentlich einem unbeschränkten Anlegerkreis oder einer bestimmten Zielgruppe zugänglich gemacht, die Anteile in Form von Token kaufen können. Hierdurch werden sie häufig Miteigentümer bzw. Teilrechtsinhaber an dem jeweiligen Objekt . Da in der Regel auch Anteile in kleineren Größen verfügbar sind, macht es die Tokenisierung vielen Menschen möglich, in den Handel einzusteigen, auch wenn sie nicht über viel Kapital verfügen.

Wichtiger Hinweis
Die häufig verwendete Formulierung, dass Immobilien "tokenisiert" werden können, ist irreführend. Eigentümer einer Immobilie ist nur, wer im Grundbuch eingetragen ist. Die Tokens repräsentieren Anteile oder Aktien an dem Unternehmen, das als Eigentümer der Immobilie im Grundbuch eingetragen ist, nicht aber Anteile an der Immobilie selbst.

2. Initital Coin Offering - ICO

Ein Initial Coin Offering (ICO) ist eine Finanzierungsform für Geschäftsmodelle, die auf der Blockchain-Technologie beruhen. Andere Bezeichnungen hierfür sind Initial Public Coin Offering (IPCO) oder Token Sale, wobei Token auch auf anderem Weg gekauft werden können. Der Begriff „Token Sale" hat sich jedoch umgangssprachlich etabliert und wird meistens gleichbedeutend mit ICOs verwendet.

Das Konzept ist einem klassischen Börsengang, der als „Initial Public Offering (IPO)" bezeichnet wird, sehr ähnlich, weshalb auch die Bezeichnung daran angelehnt ist.

Die Bezeichnung „ICO" kann im Hinblick auf die Ähnlichkeit zu „IPO" irreführend sein. Das Aktienrecht findet auf ICOs keine Anwendung. Der Anbieter kann völlig frei entscheiden, welche Rechte oder Ansprüche er den Anlegern durch die Token einräumt. Soweit der Anbieter zu seinem Projekt Unterlagen veröffentlicht, sind diese im Unterschied zu den Prospekten einer Aktienemission weder gesetzlich vorgegeben noch werden sie von einer Aufsichtsbehörde auf Vollständigkeit geprüft.

Ursprünglich waren ICOs dazu gedacht, neue Kryptowährungen auf den Markt zu bringen. Sogenannte Utility Token wurden im Austausch gegen staatlich emittierte Währungen oder gegen andere Kryptowährungen zum Verkauf angeboten, die sich später als Coins der neuen digitalen Währung handeln ließen. Stieg der Wert der Token über den Ausgangswert, wurden die Käufer über Kurssteigerungen am Erfolg beteiligt, sie erhielten aber keine Rechte an dem unterstützten Projekt.

Mittlerweile werden mit ICOs jedoch nicht mehr ausschließlich neue Kryptowährungen finanziert, sondern die Möglichkeit der Kapitalbeschaffung von Unternehmen steht zunehmend im Vordergrund. In solchen Fällen sind die verkauften Token nicht als Kryptowährung handelbar. Beispielsweise beschaffen sich Unternehmen mittels der Ausgabe von Token Kapital für die Umsetzung eines speziellen Projekts oder Business Plans. Die Token werden über Smart Contracts mit spezifischen Rechten und Pflichten versehen und in einer gewissen Anzahl gestückelt in das Register eingetragen. Dem Unternehmen fließt hierdurch Geld zu und die Käufer erhalten alle Rechte, die mit dem Token verbunden sind. In der Regel werden ICOs zur Finanzierung von Start-ups und neuen Unternehmen genutzt.

ICOs sind Methoden des Crowdfundings.

3. Crowdfunding

Crowdfunding bezeichnet eine Form der Finanzierung, zu denen meist im Internet zu einer Beteiligung in Form einer Kapitalüberlassung an einem bestimmten Projekt aufgerufen wird. Es handelt sich dabei oft um Nischen-Projekte. Wenn innerhalb einer bestimmten Zeit die angegebene Summe erreicht ist, fließt das Geld an die Initiatoren und die Idee wird umgesetzt. Bei vielen Projekten können durch die Anleger Beteiligungen an einem Unternehmen erworben werden (ohne Eigentümer des Unternehmens zu werden). Diese Beteiligungen (in Gestalt von nachrangigen Darlehen oder sog. „stillen Beteiligungen") repräsentieren einen Anspruch auf einen Anteil am Unternehmensgewinn sowie häufig auch am Verkaufserlös und können verkauft werden. Das Investitionsrisiko soll so auf zahlreiche Investoren zu kleinen Beträgen verteilt werden. Eine andere, „eingedeutschte" Bezeichnung ist „Schwarmfinanzierung".

ICOs waren zunächst gesetzlich nicht reguliert, d.h. die Initiatoren unterlagen nicht dem streng regulierten Prozess der Kapitalaufnahme. Auch weil sich das Anwendungsfeld von ICOs verändert hat, muss mittlerweile jedoch in jedem Fall individuell geprüft werden, ob es sich bei den herauszugebenden Token um eine Vermögensanlage oder um ein Wertpapier handelt. Dies richtet sich nach den mit den Token verknüpften Rechten. Je nach Ausgestaltung kann für den Initiator sogar die Pflicht bestehen, einen Wertpapierprospekt, der umfassend die wirtschaftlichen Hintergründe sowie die Chancen und Risiken enthält, zu veröffentlichen.

ICOs erfreuen sich wachsender Beliebtheit und es entstehen immer neue Formen, sodass das Angebot inzwischen schwer überschaubar geworden ist. Mit Blick auf die Rahmenbedingungen eines ICOs kann man jedoch zwischen „gedeckelten" („capped") und „ungedeckelten" („uncapped") ICOs unterscheiden. Bei einem Capped ICO erfolgt eine Deckelung der Maximalzahl emittierter Token, indem von vornherein nur eine begrenzte Menge an Token herausgegeben wird.

a | Hard Cap

Der Hard Cap ist die maximale Menge an Geld, die für ein Projekt eingesammelt werden soll. Der Hard Cap stellt das Finanzierungsziel dar, welches nicht überschritten wird, selbst wenn das Projekt noch mehr Geld einsammeln könnte. Wenn der Hard Cap erreicht wird, können keine Token für dieses Projekt mehr erworben werden.

b | Soft Cap

Der Soft Cap ist die minimale Menge an Geld, die für ein Projekt eingesammelt werden muss, damit es realisiert werden kann. Folglich wird der ICO als gescheitert erachtet, wenn der Soft Cap nicht erreicht wird. Seriöse Projekte bieten in diesem Fall den Anlegern oft die Möglichkeit an, das transferierte Geld zurückzuerhalten. Der Soft Cap ist in der Regel wesentlich niedriger als der Hard Cap.

Im Idealfall möchten die Initiatoren für ihr Projekt immer den Hard Cap erreichen.

c | Uncapped ICOs

Es gibt auch sog. „Uncapped ICOs" („ungekappte" ICOs), bei denen eine unbegrenzte Anzahl von Token über einen normalerweise langen Zeitraum ausgegeben wird. Bei solchen Projekten existieren weder ein Soft noch ein Hard Cap, weshalb sich auch der direkte Marktwert des Projekts nach dem ICO nicht beurteilen lässt. Diese Methode wird eher selten angewendet und birgt für Investoren viele Risiken. Ein Uncapped ICO hat für das Unternehmen bzw. den Herausgeber des Token den Vorteil, dass für das Projekt mehr Geld vorhanden ist als unbedingt erforderlich, und dass alle Investoren Token bekommen, die welche haben wollen. Die Token können allerdings weniger wert sein, als wenn der ICO gekappt wäre.

d | White Paper

In der Regel verfasst der Initiator eines ICOs ein „White Paper" und „Terms and Conditions". Das White Paper ist eine Art Businessplan. In den Terms and Conditions werden die rechtlichen Bedingungen für die Anleger festgelegt. Sie sind zu vergleichen mit Allgemeinen Geschäftsbedingungen.

Für das White Paper und die Terms and Conditions gibt es keine Mindestanforderungen und keine sonstigen rechtlichen Bestimmungen. Der Anbieter ist in der Ausgestaltung dieser Unterlagen völlig frei. Die Unterlagen werden keiner behördlichen Prüfung unterzogen und bedürfen - anders als ein Wertpapierprospekt - keiner Genehmigung. Vor einer Investition sollten Sie diese Unterlagen sorgfältig prüfen. Beinhalten sie nicht ausreichende oder unverständliche Informationen, so sollten Sie von einer Investition absehen.

Wie bereits ausgeführt, können Token mittlerweile auch so ausgestaltet werden, dass sie rechtlich als Vermögensanlage im Sinne des Vermögensanlagengesetzes (VermAnlG) oder als Wertpapier im Sinne des Wertpapierhandelsgesetzes (WpHG) gelten. Wenn dies der Fall ist, dann ist der Emittent u.a. verpflichtet, einen Verkaufsprospekt bzw. einen Wertpapierprospekt zu erstellen.

4. Security Token Offering – STO

Üblicherweise werden bei ICOs Utility Token ausgegeben. Ein Unterfall von ICOs sind STOs – Security Token Offerings. Hierbei werden Security Token anstelle von Utility Token herausgegeben. In der Regel stellen diese Security Token Wertpapiere eigener Art dar. Hieraus folgt in aller Regel, dass der Emittent den Regeln des Wertpapierhandelsgesetzes (WpHG) unterliegt und einen Wertpapierprospekt erstellen muss. Erst wenn dieser von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) genehmigt worden ist, darf der Emittent die Token öffentlich zum Kauf anbieten. Es erfolgt nur eine Prüfung nach formalen Gesichtspunkten, die BaFin prüft die Plausibillität des Angebots nicht.

Security Token sind vergleichbar mit Aktien oder Anleihen, dürfen jedoch nicht mit diesen verwechselt oder gleichgestellt werden. Auch wenn sie als Finanzinstrument ggf. einer behördlichen Aufsicht unterliegen, bestehen für ihre Ausgestaltung kaum gesetzlichen Regeln, weshalb sie als „Wertpapier eigener Art" bezeichnet werden.

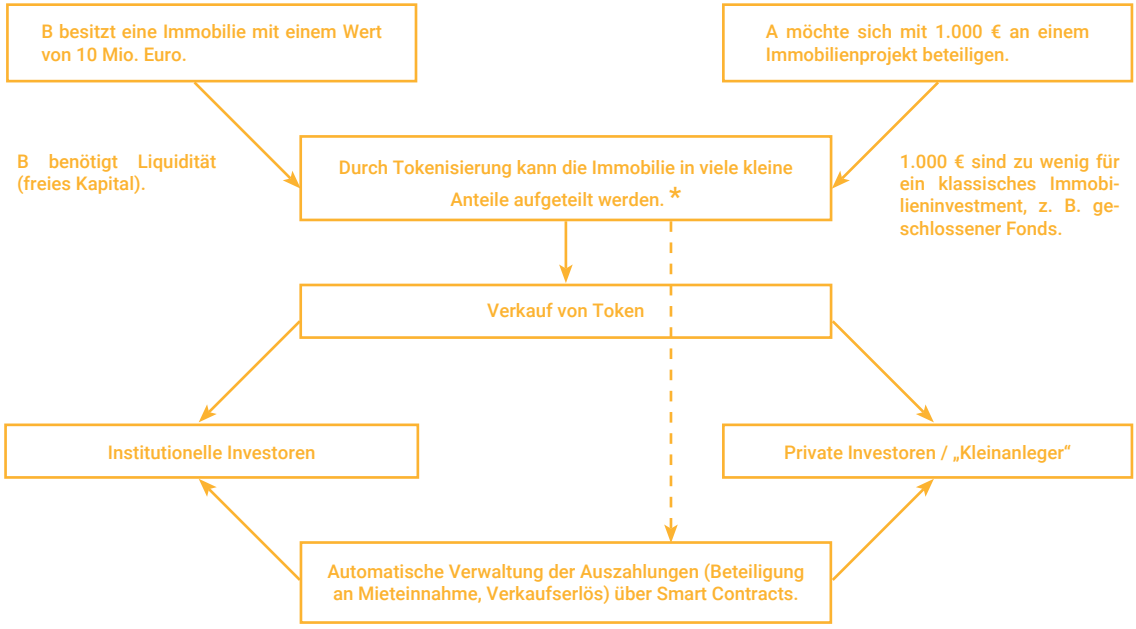
5. Equity Token Offering – ETO

Bei einem Equity Token Offering – ETO – werden Equity Token herausgegeben. Ein wesentlicher Unterschied zu Utility Token und zu Security Token besteht darin, dass den Inhabern von Equity Token Eigentumsrechte an dem Projekt zustehen sollen. Die Begriffe sind allerdings nicht geschützt und häufig wird sprachlich keine Unterscheidung gemacht zwischen Security Token und Equity Token. Je nach Ausgestaltung eines Projekts können den Token-Käufern bei einem STO daher auch Eigentumsrechte an dem Projekt zustehen.

6. In Immobilien investieren mit Token

Insbesondere im Bereich der Immobilienfinanzierung ist die Tokenisierung derzeit auf dem Vormarsch. Dabei wird ein klassisches Investment mit einer digitalen Plattform kombiniert. Wer keine Immobilie im Wert von beispielsweise 200.000 Euro kaufen oder finanzieren kann, kann so via Erwerb von Token trotzdem wirtschaftlich Beteiligter einer Immobilie werden und anteilsmäßig an den Erlösen aus Mieteinnahmen beteiligt sein. Immobilienfonds investieren häufig in Gewerbeimmobilien in den Metropolen. Durch Tokenisierung ist es auch möglich, wirtschaftlicher Anteilseigner an kleineren Wohnimmobilien, wie etwa einem Mehrfamilienhaus, zu werden, sofern ein solches Angebot besteht.

Die folgende Grafik zeigt, wie die Beteiligung an einer Immobilie durch Token erfolgen kann.



* Tatsächlich wird nicht die Immobilie aufgeteilt, sondern das Unternehmen, dem die Immobilie laut Grundbuch gehört

„Digitale“ Immobilienanteile repräsentieren Ihre Kapitalanlage und verkörpern zudem auch das Recht, Gewinnbeteiligungen, z. B. in Form von Mieteinnahmen, zu erhalten. Es ist zu beachten, dass diese Anteile jedoch kein Eigentum im rechtlichen Sinne an der Immobilie begründen. Die Blockchain dient bei Immobilienbeteiligungen als dezentrales, unveränderliches, elektronisches Register, in dem alle an der Anlage Beteiligten registriert sind. Eine wichtige Funktionalität ist die Übertragung von Token von einem auf einen anderen Teilnehmerüber die Blockchain, was den Handel des Vermögenswertes unter den Teilnehmern ermöglicht.

Wichtiger Hinweis
Hinter dem Token steckt kein digitales Krypto-Asset, sondern der Anspruch auf Zahlungen aus einem realen Investitionsobjekt. So betrachtet handelt es sich bei tokenisierten Assets „nur“ um eine neue Form der Verwahrung und Dokumentation.

Gegenüber Immobilienfonds bietet die Immobilienbeteiligung über Token eine weitaus größere Flexibilität. Für offene Immobilienfonds gilt für Neuanleger eine 24monatige Mindesthaltedauer und bei Rückgabe der Fondsanteile ist eine zwölfmonatige Kündigungsfrist einzuhalten. Beides gilt nur bei Rückgabe der Fondsanteile über die Fondsgesellschaft. Ein Verkauf der Anteile über die Börse (wenn es sich um gelistete Anteile handelt) ist zumeist jederzeit möglich, allerdings kann an der Börse nicht immer der gewünschte Preis erzielt werden; eine Großzahl der Immobilienfonds sind auch nicht an einer Börse gelistet oder in einen anderen Zweitmarkt einbezogen.

Geschlossene Immobilienfonds werden aufgrund der dahingehend strengen gesetzlichen Vorgaben meistens in der Rechtsform einer geschlossenen Investmentkommanditgesellschaft gegründet. Die Anleger werden durch die Beteiligung Kommanditisten und es gelten die Regelungen des HGB. Hieraus folgt, dass eine kurzfristige Beendigung der Beteiligung nicht möglich ist. Die Anleger sind meistens für die Laufzeit der Beteiligung, die in der Regel zwischen 10 und 30 Jahre beträgt, gebunden (daher auch die Bezeichnung

„geschlossen"). Außerordentliche Kündigungen sind selten möglich. Über den sog. Zweitmarkt können die Beteiligungen möglicherweise vorzeitig veräußert werden, in der Regel allerdings nur mit mehr oder weniger hohen Abschlägen. Der Mindestbetrag einer Beteiligung liegt zudem meistens bei 5.000 Euro, häufig noch darüber.

Anders als bei einem Immobilienfonds ist eine Immobilienbeteiligung über Token auch mit geringem Kapital möglich. Aufgrund der Tokenisierung können die Anteile einfacher übertragen werden, zudem erfolgt der Erwerb nicht über eine Wertpapierbörse, was Transaktionen einfacher und schneller macht. Das eingesetzte Kapital ist liquider als bei Immobilienfonds. In der Regel sind die Kosten geringer, auch weil der Vorgang der Tokenisierung sehr kosteneffizient ist, was sich positiv auf die Rendite der Investition auswirkt. Durch die elektronische Form der Abbildung von Besitzverhältnissen kann der Beweis für den Besitz eines Tokens ganz einfach und sicher auf elektronischen Geräten, wie z. B. einem Mobiltelefon, mitgeführt und vorgewiesen werden.

Die Einsatzmöglichkeiten der Tokenisierung sind inzwischen zahlreich und es kommen stetig neue Variationen hinzu. Da in der Regel kein Angebot dem anderen gleicht, sollten Sie sich die Angebotsbedingungen vor einer Investition in jedem Fall sorgfältig durchlesen!

Risiken bei der Vermögensanlage in Blockchain-basierte Investments und Kryptowährungen

E

Die Vermögensanlage in Blockchain-basierte Investments und Kryptowährungen bietet nicht nur die Chance auf mehr oder weniger hohe Erträge, sie birgt auch das Risiko, das eingesetzte Kapital ganz oder teilweise zu verlieren. Es gibt sog. „Basisrisiken", die für fast alle Formen der Vermögensanlage zutreffen, unabhängig von der (Rechts-)Form des Investments. Eine ausführliche Darstellung dieser Basisrisken finden Sie in der Broschüre „Grundlagenwissen Wertpapiere & Investmentfonds", die Sie jederzeit beim Herausgeber dieser Broschüre oder Ihrem persönlichen Berater anfragen können. Einige der Basisrisiken werden am Ende dieses Kapitels dargestellt, soweit sie insbesondere auch bei Blockchain-basierten Investments und Kryptowährungen bestehen. Darüber hinaus bestehen bei der Vermögensanlage in Blockchain-basierte Investments und Kryptowährungen besondere Risiken, die im Folgenden dargestellt werden.

Wichtige Hinweise

Dieses Kapitel soll Ihnen einen Überblick verschaffen, welche Risiken bei der Vermögensanlage in die Blockchain-Technologie und Kryptowährungen üblicherweise bestehen. Die Aufzählung der Risiken ist nicht abschließend und abhängig von der Ausgestaltung des jeweils konkreten Angebots. Informieren Sie sich vor einer Investition sorgfältig und nehmen Sie im Zusammenhang mit der Kapitalanlage herausgegebene Dokumente wie z. B. ein White Paper oder einen Verkaufsprospekt, sorgfältig zur Kenntnis! Eine Vermögensanlage unterliegt zudem nicht nur einem einzigen Risiko, sondern es bestehen grundsätzlich mehrere Risiken, deren Auswirkungen und Veränderungen sich gegenseitig verstärken können. Man spricht von einer „Kumulation verschiedener Risiken" bzw. einer Risikokumulation.

I. Allgemeine Risiken im Zusammenhang mit der Blockchain-Technologie

Wie jede Technologie kann auch die Blockchain-Technologie Fehler aufweisen.

1. Softwarefehler

Eine Blockchain gilt durch die Herstellung von Konsens als sicher. Enthält eine solche Anwendung einen Fehler, so stellt der Konsens aber ein Problem dar. Oftmals können Fehler in der Blockchain-Software nicht mehr rückgängig gemacht werden. Ein Fehler im Softwarecode kann dazu führen, dass Anteile an der Kryptowährung gewissermaßen „eingefroren" werden, was bedeutet, dass auf diese Anteile kein Zugriff mehr möglich ist.

Softwarefehler können auch zu anderen Störfällen führen, die sich auf die auf der Blockchain basierende Kryptowährung auswirken können.

2. Fehlende Erfahrungswerte

Ein generelles Risiko sind fehlende Erfahrungswerte bzw. daraus resultierend eine unklare langfristige Planung. Die älteste Blockchain ist die Bitcoin-Blockchain. Diese läuft seit 2009 und ist damit immer noch relativ jung. Für eine Kalkulierbarkeit von Risiken, Fehlern und anderen Störfaktoren fehlen über Jahre bzw. Jahrzehnte angesammelte Erfahrungswerte. Da Fehlerkorrekturen auf der Blockchain sehr schwierig, wenn nicht gar unmöglich sind, stellt es für sich genommen schon ein Problem dar, Erfahrungswerte mit der Behebung von Fehlern zu sammeln.

3. Hard Forks

Auch die Gabelung einer Blockchain durch eine Hard Fork muss als Risiko betrachtet werden. Die Teilnehmer müssen sich entscheiden, ob sie der neuen Blockchain folgen, oder ob sie bei der alten Blockchain bleiben. Beide Blockchains werden unabhängig voneinander weitergeführt. Bis zur Fork sind sie identisch, danach sind sie nicht mehr miteinander kompatibel. Diese „Zweiteilung" ist vom System eigentlich nicht vorgesehen. Die Mining-Kapazität verteilt sich auf zwei Systeme, wodurch sie entsprechend geschmä-

lert wird. Unter Umständen dauert es zumindest auf einer der beiden Blockchains nach einer Fork länger, bis neue Blöcke geschürft werden, wodurch die Transaktionsgeschwindigkeit sinkt.

4. Manipulationsrisiko, „51%-Attacke“

Die ganze Sicherheit und Integrität einer Blockchain hängen von dem ihr zugrundeliegenden Konzept ab. Würde die verwendete Technologie (bzw. der dahinterstehende Code) gehackt, ließe sie sich nach Belieben manipulieren.

Als 51%-Attacke wird ein potenzieller Angriff auf ein Blockchain-Netzwerk bezeichnet, bei dem eine einzelne Einheit oder Organisation in der Lage ist, den Großteil der Hash-Rate zu kontrollieren. Hierfür sind nicht zwangsläufig 51% der Hash-Power erforderlich, u. U. ist auch ein kleinerer Anteil ausreichend. Ein solcher Angriff würde es dem Angreifer ermöglichen, Transaktionen rückgängig zu machen, was zu doppelten Ausgaben führen könnte – sog. „Double-Spending“ -, oder es ermöglichen könnte, Transaktionen bewusst auszuschließen oder ihre Reihenfolge zu ändern. Der Angreifer könnte auch alle Miner am Minen hindern und sich ein sog. „Mining-Monopol“ verschaffen.

Bei großen Kryptowährungen ist eine 51%-Attacke extrem aufwändig, teuer und daher eher unwahrscheinlich. Wahrscheinlicher ist der Angriff bei Altcoins mit einer niedrigeren Hash-Rate. Mehr als die Hälfte der Rechenleistung für das Mining von Bitcoins ist mittlerweile im Besitz weniger Pools, in denen sich mehrere Miner zusammengeschlossen haben. Aus dieser Perspektive betrachtet ist aber auch bei einer großen Kryptowährung eine Manipulation durch böswillige Teilnehmer nicht unmöglich. Selbst wenn der unwahrscheinliche Fall einer 51%-Attacke eintritt, haben die Angreifer aber keinen Zugriff auf alle Blöcke der Blockchain, sondern nur auf die Transaktionen der letzten Blöcke. Zudem ist eine willkürliche Manipulation des Regelwerkes technisch prinzipiell ausgeschlossen.

5. Technische Limitierungen

Die Blockchain-Technologie unterliegt technischen Limitierungen. Je länger eine Blockchain ist, desto schwieriger ist das Finden neuer Blöcke. Die mangelnde Skalierbarkeit wird grundsätzlich als Risiko betrachtet.

Skalierbarkeit
Grundsätzlich beschreibt der Begriff eine Größenveränderung, meistens wird er für die Fähigkeit eines Systems oder Prozesses zum Wachstum verwendet.

Im Vergleich zu anderen Systemen sind die Transaktionen auf einer Blockchain extrem langsam. Sie dauern teilweise recht lang, weil die Blockchain überlastet ist. In der Zeit, in der Sie auf den Transfer warten, können die Kurse fallen und Sie verlieren Geld.

6. Kriminelles Ausnutzen der Unwissenheit von Anlegern

Das allgemeine bzw. allgemein verbreitete Wissen über Blockchains ist relativ gering. Es besteht ein erhebliches Risiko, dass Betrüger die Unwissenheit zu ihren Gunsten ausnutzen. Unwissenheit birgt grundsätzlich das Risiko fehlerhaften eigenen Anlegerverhaltens und erhöht zudem die Gefahr betrügerischem Verhalten oder dahingehenden Versuchen.

7. Datensicherheit

Faktisch sind öffentliche Blockchain-Systeme nicht anonym zu nutzen. Dem Transparenzprinzip der Blockchain-Technologie steht der Aspekt der Vertraulichkeit von Daten grundsätzlich diametral gegenüber, Public Keys sind für jeden Teilnehmer des Systems öffentlich und uneingeschränkt einsehbar. Die Teilnehmer eines Systems können sich, trotz der grundsätzlich vorhandenen Pseudonymität, nicht gänzlich anonym in diesem System bewegen.

8. Stromverbrauch

Wie bereits ausgeführt, wird für das Proof-of-Work Verfahren enorm viel Strom benötigt, mit wachsender Anzahl der Blöcke in der Blockchain steigt auch der Stromverbrauch. Je nach Studie und Methodik wird der jährliche Verbrauch von Bitcoin mit 30 bis 75 Terawattstunden (TWh) angegeben. Zum Vergleich: In Deutschland beträgt der Stromverbrauch rund 537 Terawattstunden pro Jahr, in Irland etwa 26 TWh und in der Schweiz etwa 58 TWh. Bitcoin verbraucht also bereits jetzt mehr Strom pro Jahr als viele Länder. Und diese Angabe bezieht sich nur auf Bitcoin, dazu kommen noch die vielen weiteren Kryptowährungen, die (bzw. deren Mining und Nutzung) ebenfalls Strom verbrauchen.

Zwar resultiert aus dem immensen Stromverbrauch nicht unmittelbar das Risiko von Vermögenseinbußen auf Seiten der Investoren, es darf jedoch insofern nicht außer Acht gelassen werden, dass die klimapolitische Tragfähigkeit von Blockchains, die das Proof-of-Work Verfahren nutzen, zunehmend in Frage gestellt und kritisiert wird. Weitere Ausführungen hierzu finden Sie in Kapitel F. dieser Broschüre.

II. Im Zusammenhang mit Wallets bestehende Risiken

Es besteht das Risiko, dass der Zugriff auf Ihre Wallet endet oder eingeschränkt wird oder dass jemand unbefugt Zugriff auf Ihre Wallet erhält und über die Coins, die dieser Wallet zugewiesen sind, verfügen kann.

1. Verlust des Private Keys

Wenn Sie Ihren Private Key verlieren, verlieren Sie die Möglichkeit, Zugriff auf Ihre dort vorhandenen Coins zu nehmen. Ohne den Zugriff auf die Coins können Sie nicht über diese verfügen und Ihr Kapital ist, obwohl noch theoretisch vorhanden, unbrauchbar.

Ihr in eine Kryptowährung investiertes Geld ist demnach nur so sicher wie Ihr Umgang mit dem Private Key!

Es ist bei manchen Wallets mittels einer Wiederherstellungsoption möglich, durch die Verwendung bestimmter Authentifizierungsmerkmale den Private Key wiederzuerlangen. Sie sollten sich hierauf aber nicht uneingeschränkt verlassen.

2. Aus der Art des Wallets resultierende Risiken

Einen Überblick über die verschiedenen Arten von Wallets finden Sie in Kapitel C. unter Ziff. III.

Bei Soft Wallets bzw. Software Wallets besteht durch die Verbindung zum Internet die Gefahr, dass sie gehackt werden. Für diese Wallets sollte stets und unbedingt ein extrem sicheres Passwort gewählt werden. Ähnlich verhält es sich bei Paper Wallets, bei denen für das Eingeben des Schlüssels eine Verbindung zum Internet hergestellt werden muss. Dieser – wenn auch nur kurze – Moment stellt ggf. ebenfalls eine Sicherheitslücke dar.

Bei Mobile und Desktop Wallets besteht die Gefahr, dass Sie das Gerät, auf dem die jeweilige Wallet gespeichert ist, z. B. Smartphone oder Laptop, verlieren können. Dieses Risiko lässt sich absichern, indem Sie den Private Key parallel in einer Paper Wallet (mit den vorgenannten Risiken) verwahren. Dann können Sie ggf. auf deren Grundlage eine neue Wallet einrichten und die Coins trotz des Verlustes der eigentlichen Wallet in die neue Wallet transferieren.

Bei Exchange Wallets besteht die Gefahr, dass die anbietende Exchange bzw. Börse Opfer eines Hacker-Angriffs wird, wodurch diese Zugriff auf die dort verwalteten und verwahrten Coins nehmen können.

3. Tipps zum Umgang mit Private Keys und Wallets

Das wesentliche Element zur Verfügung über Coins ist der Private Key. Es empfiehlt sich, den oder die Private Keys immer parallel auf Papier zu sichern und diese Dokumente im Safe und für niemanden zugänglich aufzubewahren. Sie sollten die Verantwortung für Ihre Wallet und den Private Key nicht in Gänze an andere Personen oder an Geräte abgeben.

Damit im Falle eines Verlusts des Private Keys oder eines Zugriffs durch einen Unbefugten nicht Ihr ganzes in Coins bestehendes Vermögen verloren ist, ist es sinnvoll, verschiedene Wallets zu besitzen und diese für jeweils unterschiedliche Zwecke zu nutzen. Eine Wallet kann z. B. wie eine Art Sparbuch verwendet werden, während mit einer anderen alltägliche Ausgaben getätigt werden.

III. Risiken bei der Vermögensanlage in Kryptowährungen

Der Markt für Kryptowährungen ist noch jung und in vielen Teilen unreguliert. Investitionen in diesen Markt bergen daher ein erhebliches Risiko. Bisher kann niemand sicher prognostizieren, wie sich der Markt und die „virtuellen Devisen" entwickeln werden.

Beim Handel mit Kryptowährungen besteht grundsätzlich ein Totalverlustrisiko, da der Kurswert einer Kryptowährung allein auf der Nachfrage basiert und jederzeit auf Null fallen kann. Sie sollten daher nur investieren und nur solche Beträge investieren, wenn Sie auf das investierte Kapital auch vollständig verzichten können.

1. Keine rechtliche Regulierung

Es handelt sich bei Kryptowährungen in der Regel um Finanzinstrumente (und jedenfalls nach Auffassung der Behörden zumindest auch um sog. „Rechnungseinheiten"). Sie sind damit bereits teilweise gesetzlich reguliert. Insbesondere die Anbieter von dahingehenden Verwahrdienstleistungen, wie z.B. Krypto-Börsen unterfallen regelmäßig einer Erlaubnispflicht und stehen unter der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht. Es gibt jedoch derzeit kaum oder keine verbindlichen Vorgaben für den Handel mit Kryptowährungen und dessen Abwicklung. Informieren Sie sich daher sorgfältig, wenn Sie in den Markt für Kryptowährungen investieren wollen!

2. Hohe Volatilität

Prinzipiell basiert der Wert einer Kryptowährung auf Vertrauen und Akzeptanz. Im Gegensatz zu etablierten Währungen wie Euro oder Dollar, die von Zentralbanken und Staaten überwacht und abgesichert werden, steht hinter einer Kryptowährung lediglich ein dezentrales, technisches System, an dem grundsätzlich jeder ohne Zugangsbeschränkung teilnehmen kann und für das die Stabilität der Währung keine Rolle spielt. Umgekehrt spielt auch das System für die Stabilität der Währung ebenfalls keine Rolle. So gibt es bei Kryptowährungen keine zentrale Stelle, wie etwa eine Zentralbank, die für die Werthaltigkeit der ausgegebenen Währung (wenigstens repräsentativ) einsteht. Der Wert einer Kryptowährung hängt also entscheidend und alleinig von dem ihm durch die Nutzer des Netzwerks zum Zeitpunkt der jeweiligen, individuellen Wertbeurteilung zugedachten Wert ab.

Kryptowährungen sind extrem volatil und die Kurse können sich mit radikaler Geschwindigkeit verändern. Über lange Zeiträume erzielte Kursgewinne können bei Kursrückgängen innerhalb kürzester Zeit verloren gehen . Kursschwankungen sind in ihrem Auftreten und in ihrem Umfang nicht vorhersehbar und unkalkulierbar. Wer mit Kryptowährungen handeln möchte, sollte daher in der Lage sein, sehr viel Zeit und Aufmerksamkeit für derartige Geldanlage aufzubringen.

3. Kein gesetzliches Zahlungsmittel

Kryptowährungen sind keine gesetzlichen Zahlungsmittel, auch wenn der Begriff „Währung" vielleicht hierauf schließen lässt. Kryptowährungen sind auch von keiner staatlichen Stelle ausgegeben, sondern basieren alleine auf der Akzeptanz von Privatpersonen. Dabei kann jeder Gewerbetreibende und jede Privatperson frei entscheiden, ob sie eine Kryptowährung als Zahlungs- oder Tauschmittel verwenden akzeptieren möchte oder nicht. Die Einsatzmöglichkeiten von Kryptowährungen als häufiges Zahlungs- oder Tauschmittel im Alltag bestehen daher nur stark eingeschränkt.

4. Fehlende Umtauschmöglichkeiten

Kryptowährungen können nicht ohne weiteres in Fiatgeld, z. B. in Euro oder Dollar, umgetauscht werden. Viele Kryptowährungen müssen zunächst in eine der größeren Kryptowährungen wie Bitcoin umgetauscht werden, um sie dann für Euro zu verkaufen. Mangels der Eigenschaft als gesetzliches Zahlungsmittel besteht zudem das Risiko, dass Kryptowährungen allgemein als wertlos erachtet werden und keinerlei Umtausch in Fiatgeld mehr möglich ist. Es gibt zudem keine stabilen Wechselkurse. Sie müssen sich auf die Wechselkursangaben und -angebote der Händler verlassen, die insofern keiner Kontrolle unterliegen.

5. Die Limitierung von Kryptowährungen

Es existieren Kryoptowährungen, bei denen quasi unendlich viele Coins geschürft werden können. Bei der weitaus größeren Zahl von Kryptowährungen ist die Anzahl der Coins, die geschürft werden können, allerdings begrenzt. Eine solche Begrenzung der Anzahl der Coins bedeutet, dass aufgrund des jeweiligen Konsens und des gewählten Rechenalgorithmus maximal eine bestimmte, im Vorhinein festgelegte Anzahl an Coins geschürft werden kann.

Die Limitierung von Kryptowährungen wird in der Regel eher als Vorteil denn als Risiko betrachtet, da hieraus eine gewisse Wertstabilität resultieren soll. So wie ein Überschuss an von einer Zentralbank ausgegebenem (Fiat-)Geld regelmäßig zu einer Inflation der entsprechenden Währung führt, kann auch die unbegrenzte Ausgabe von Coins einer Kryptowährung zu einem vergleichbaren Wertverlust der jeweiligen Kryptowährung führen. Kryptowährungen mit einer im Vorhinein festgelegten, maximalen Anzahl von Coins sind daher im Gegensatz dazu systemisch deflationär statt inflationär.

Das ist beispielsweise bei Bitcoin der Fall. Es wird angenommen, dass die maximale Menge an Bitcoins im Jahr 2140 erreicht werden wird, vorausgesetzt, das aktuelle Bitcoin-Protokoll bleibt unverändert.

Weitere Ausführungen zur Limitierung von Kryptowährungen finden Sie im letzten Kapitel dieser Broschüre.

6. Kursmanipulation

Personen, die einen großen Anteil an einer Kryptowährung besitzen, könnten diesen - ähnlich wie es z.B. auch bei Aktien oder anderen Finanzinstrumenten möglich ist - , nutzen, um die Kurse zu ihrem Vorteil zu manipulieren.

Der Kurs einer Kryptowährung kann auch auf vielen anderen Wegen manipuliert werden. Aufgrund der Abhängigkeit von Entscheidungen des Emittenten bei Stablecoins können z.B. künstliche Kursschwankungen produziert werden

7. Kriminalität und Diebstahl

Bei Kryptowährungen ist nicht unbedingt nachvollziehbar, wer über sie verfügt bzw. verfügen kann. Dadurch sind sie dem Risiko von Cyberangriffen ausgesetzt. Es sind berühmte Fälle bekannt, in denen Kryptowährungen aus Wallets abgebucht und damit letztlich den eigentlichen Inhabern „entwendet" worden sind.

Allerdings sind über eine Blockchain ausgeführte Transaktionen nicht „anonym", sondern nur „pseudonym", da alle auf der Blockchain gespeicherten Transaktionen grundsätzlich ewig nachvollziehbar bleiben. Es gibt also Muster, Schnittstellen zu Börsen und Spuren auf anderen Plattformen, die sich zurückverfolgen lassen. Behörden und andere Akteure haben auf diese Weise bereits mehrfach die natürlichen Personen hinter Krypto-Transaktionen ausfindig gemacht. Spätestens beim Umtausch einer Kryptowährung in Bargeld bzw. Fiatgeld muss sich der Inhaber einer Kryptowährung zu erkennen geben.

8. Kein umfassender Anlegerschutz

Kryptowährungen unterliegen einer grundlegenden staatlichen Regulierung, die auf die Anbieter von Verwahr- und Verwaltungsdienstleistungen bezüglich Kryptowerten abstellt. Mittelbar durch die Regulierung dieser Anbieter (sog. Intermediäre) ist es der Bundesanstalt für Finanzdienstleistungsaufsicht entsprechend möglich, Maßnahmen des Verbraucherschutzes zu ergreifen und zu erlassen. So kann die Bundesanstalt etwa einen Anbieter (z. B. eine Krypto-Börse) intensiv überprüfen, Auflagen erteilen, die Erteilung einer Erlaubnis versagen oder sogar eine erteilte Erlaubnis entziehen. Gemeinsam mit anderen Aufsichtsbehörden innerhalb der Europäischen Union warnt die Bundesanstalt außerdem regelmäßig Verbraucher vor den mit Kryptowerten verbundenen Risiken, insbesondere der großen Volatilität. Konsultieren Sie vor einer Anlage in Kryptowerte ggf. die entsprechenden Angebote und informieren Sie sich ausführlich!

9. Keine Einlagensicherung oder Anlegerentschädigung

Für Kryptowährungen gibt es keine Einlagensicherung wie etwa für bei Banken bestehende Einlagen, d.h. auf Konten bestehende Guthaben der Kunden, oder eine anderweitige Einrichtung der Anlegerentschädigung. Außerdem besteht durchaus ein Risiko, dass die Gegenpartei (z.B. eine Krypto-Börse) behauptete Guthaben einer Kryptowährung gar nicht erworben oder gutgeschrieben hat. Kommt es zu einer starken Entwertung von Kryptowährungen, besteht hier somit keine Möglichkeit einen Ausgleich oder eine Entschädigung zu erhalten und es kann zum unumkehrbaren Totalverlust des angelegten Vermögens führen.

IV. Besondere Risiken bei Stable Coins

Stable Coins sollen durch ein festes Verhältnis zu einem Basiswert wertstabiler und – vermeintlich – sicherer als sonstige Kryptowährungen sein. Die Wertstabilität und die Sicherheit eines Stable Coins sind jedoch wesentlich abhängig von der Ausgestaltung des Stable Coins. Es gibt keine verbindlichen Vorgaben zu Stable Coins und die Emittenten sind im Wesentlichen frei in der Ausgestaltung und Namensgebung.

1. Absicherung mit klassischen Assets

Ein Stable Coin, der mit einem klassischen Asset als Basiswert hinterlegt ist, unterliegt gleichzeitig den Risiken des Basiswerts. Im Falle der Hinterlegung mit Gold besteht z. B. das Risiko, dass der Goldpreis sinkt. Bei der Hinterlegung mit einer Fiatwährung besteht ein Währungsrisiko, dass die Währung an Wert verliert.

Stable Coins haben zudem einen Emittenten, d.h. sie werden von einem Unternehmen herausgegeben. Der Emittent legt das Umtauschverhältnis fest und sorgt dafür, dass die Sicherheiten hinterlegt werden. Allerdings garantiert der Emittent in der Regel das feste Umtauschverhältnis des Stable Coins zu dem Basiswert nicht. Die Anleger müssen sich zudem auf die Aussage des Emittenten verlassen, dass der Basiswert tatsächlich existent und hinterlegt ist. Eine Kontrolle durch eine unabhängige Instanz findet in der Regel nicht statt. Es besteht daher ebenso ein Emittentenrisiko. Wird der Emittent zahlungsunfähig oder existieren die behaupteten Stable Coins gar nicht oder hinterlegt er die Sicherheiten nicht, sind die Stable Coins letztlich wertlos.

2. Absicherung durch Kryptowährungen

Stable Coins können auch durch eine Kryptowährung besichert werden. In diesem Fall setzen die Anbieter häufig nicht nur auf „Absicherung", sondern auf „Übersicherung". Das kann z. B. bedeuten, dass für jeden ausgegebenen Stable Coin nicht 1 US-Dollar in Fiatgeld, sondern der Gegenwert von 2 US-Dollar in Gestalt von anderen Kryptowährungen pro Stable Coin hinterlegt werden. Preisschwankungen sollen laut Angaben der Anbieter so besser aufgefangen werden können. Allerdings ist die Volatilität dieser Stable Coins weitaus höher als die Volatilität von Stable Coins, die mit klassischen Assets, wie z. B. Gold oder einer Fiatwährung, hinterlegt sind. Im schlimmsten Fall fällt der Wert der als Underlying verwendeten Kryptowährung so enorm, dass auch der Stable Coin selbst keinen Wert mehr hat.

3. Arithmetische Absicherung

Bei einer arithmetischen Absicherung wird kein Basiswert hinterlegt. Automatisierte An- und Verkauf-Algorithmen sollen für Kursstabilität sorgen. Diese Stable Coins werden „Seignorage Shares" genannt. Sie haben den Vorteil, dass durch die Automatisierung keine Abhängigkeit von den Entscheidungen eines Emittenten besteht. Das dahinterliegende automatisierte System basiert stattdessen auf dem Prinzip des Ausgleichs von Angebot und Nachfrage. Wenn der Stable Coin im Verhältnis zum Basiswert zu hoch gehandelt wird, sorgt ein Smart Contract dafür, dass mehr Einheiten dieses Stable Coins emittiert werden (bzw. entstehen), um das Angebot zu erhöhen und so den Wert des Stable Coins zu mindern. Dies entspricht etwa dem (jedoch nicht automatisierten) Mechanismus, den Zentralbanken anwenden, um mittels Geldmengensteuerung Schwankungen von Angebot oder Nachfrage (bzw. Inflation und Deflation) zu beeinflussen. Auch hier besteht jedoch das immanente Risiko, dass wenn die Investoren das Vertrauen in den Stable Coin verlieren, erhebliche Wertverluste bis hin zum Totalverlust eintreten können. Zudem können die angelegten Algorithmen grundsätzlich nachteilig zum Anlegerinteresse ausgestaltet oder fehlerhaft sein. Derzeit sind die Kurse am Markt verfügbarer Stable Coins mit arithmetischer Absicherung volatiler als die Kurse durch Hinterlegung besicherter Stable Coins.

V. Besondere Risiken bei Derivaten auf Kryptowährungen

Das wesentliche Merkmal von Derivaten ist die unmittelbare oder mittelbare Abhängigkeit von einem Basiswert. Ihr Preis bzw. Kurs wird von einem ihnen zugrundeliegenden Marktgegenstand als Basiswert abgeleitet (lat. derivare = ableiten). Alle Faktoren, die sich auf den Basiswert auswirken, wirken sich daher mittelbar auch auf den Kurs des Derivats aus. Je nach Art des Derivats kommen noch spezielle Risiken hinzu.

1. Das Emittentenrisiko

Das Emittentenrisiko ist das zentrale Risiko, das bei der Investition in die hier dargestellten Derivate besteht. Der Anleger trägt das Risiko, bei Zahlungsschwierigkeiten bzw. Zahlungsunfähigkeit des Emittenten einen Teil- oder sogar Totalverlust des eingesetzten Kapitals zu erleiden. Sind ausnahmsweise Bonus- oder Dividendenzahlungen vorgesehen, so können diese ebenfalls ausfallen.

Auch wenn ein Produkt durch die Garantie eines Dritten abgesichert ist, kann hierdurch das Insolvenzrisiko nicht gänzlich ausgeschaltet werden. Auch der Garantiegeber kann zahlungsunfähig werden.

Derivate, Zertifikate, Exchange Trades Notes und Contracts for Difference unterliegen keiner Einlagensicherung! Ggf. werden teilweise Forderungen durch die Mechanismen des Anlegerentschädigungsschutzes gesichert, jedoch greift diese ausdrücklich nicht bei Gewinnen oder Verlusten, die aufgrund falscher oder nicht erfolgreicher Anlagestrategie entstanden sind!

2. Besondere Risiken bei Zertifikaten auf Kryptowährungen

Die Risiken von Zertifikaten ähneln denen von Anleihen. Wenn Sie erwägen, in Zertifikate zu investieren, sollten Sie sich zum besseren Verständnis auch mit der Funktionsweise und den Risiken von Anleihen beschäftigen. Wir empfehlen die Broschüre „Grundlagenwissen Wertpapiere & Investmentfonds", die Sie jederzeit beim Herausgeber dieser Broschüre oder bei Ihrem persönlichen Berater anfragen können.

a | Besondere Risiken bei Zertifikaten aufgrund ihres Charakters als Schuldverschreibungen

Der Anleger sollte eine Vorstellung davon haben, wie sich der dem gewünschten Zertifikat zugrunde liegende Basiswert entwickeln und wie sich diese Entwicklung auf das Zertifikat selbst auswirken wird und hierauf seine Anlageentscheidung stützen, da die Entwicklung des Basiswerts maßgeblich für den Erfolg oder Misserfolg der Anlage ist. Die im Folgenden dargestellten Risiken resultieren im Wesentlichen auch aus der Abhängigkeit von dem Basiswert.

b | Das Kursänderungsrisiko

Alle Faktoren, die sich auf den Preis des zugrundeliegenden Basiswerts auswirken, wirken sich durch Preisveränderungen des Basiswerts auch auf den Preis des Zertifikats aus. Grundsätzlich unterliegt das Zertifikat umso höheren Preisschwankungen, je volatiler der Preis des Basiswerts ist. Wenn das Zertifikat nicht ausnahmsweise mit einer Partizipationsmöglichkeit an Erträgen, z. B. Dividenden, ausgestattet ist, besteht keine Möglichkeit, Kursverluste auszugleichen. Der Anleger kann dann nur noch auf (wieder) steigende Kurse hoffen.

c | Der Einfluss von Hedge-Geschäften

Der Kurs des Basiswerts und damit mittelbar des Zertifikats selbst ist von diversen Faktoren abhängig. Er kann beeinflusst werden durch die Geschäfte, die der Emittent zur Sicherung seiner finanziellen Risiken aus dem Zertifikat schließt. Hierbei handelt es sich z.B. um Termingeschäfte, die an den Basiswert gekoppelt sind, weshalb je nach Ausgestaltung ggf. auch das Eingehen oder Auflösen dieser Geschäfte seinerseits bereits Einfluss auf den Kurs des Basiswerts haben kann. Der negative Einfluss auf die Höhe des Rückzahlungsbetrages ist häufig besonders hoch, wenn die Sicherungs-Positionen am Ende der Laufzeit des Zertifikats oder bei Zertifikaten mit sog. Stop-loss-Barriere nach Auslösen einer Knock-out-Schwelle aufgelöst werden. Diese Absicherungsgeschäfte werden Hedge-Geschäfte genannt. Man spricht daher auch vom „Hedging".

d | Das Risiko des Wertverfalls

Das Risiko des Wertverfalls des Zertifikats ähnelt dem Kursänderungsrisiko, da der Wert des Zertifikats sich ausschließlich am Wert seines Basiswerts orientiert und mit dem Erwerb eines Zertifikats kein fester Auszahlungsbetrag am Ende der Laufzeit garantiert wird. Der Auszahlungsbetrag richtet sich ausschließlich nach den Zertifikatsbedingungen und ist abhängig von dem Wert des Basiswerts zum Laufzeitende eines Zertifikats, so dass das Zertifikat sogar vollständig wertlos sein kann.

e | Das Korrelationsrisiko

Das Korrelationsrisiko beschreibt den Effekt, dass Kursveränderungen des Basiswerts sich nicht 1:1 in der Kursveränderung des Zertifikats wiederspiegeln. Der Grund hierfür liegt darin, dass noch weitere Faktoren von außen auf die Wertentwicklung des Zertifikats einwirken oder hier ausdrücklich andere Faktoren zwischen den Parteien in den Zertifikatsbedingungen vereinbart wurden. Üblicherweise zu berücksichtigende Faktoren sind im Wesentlichen das Marktzinsniveau, die Markterwartung und ggf. die Wechselkurse.

f | Die Lieferung des Basiswerts als Risiko

Bei Zertifikaten, die auf einen einzigen Basiswert – z. B. eine Kryptowährung – aufgelegt worden sind, kann die Lieferung des Basiswerts vorgesehen sein. Dies ist meistens dann der Fall, wenn sich der Basiswert nicht so positiv entwickelt hat wie erhofft. Der aktuelle Marktwert des Basiswerts kann daher weit unter dem für das Zertifikat gezahlten Kaufpreis liegen. Im Extremfall können Sie einen quasi wertlosen Basiswert erhalten, was einem Totalverlust des eingesetzten Kapitals entspricht. Sie sind bei vorgesehener Lieferung nicht dazu verpflichtet, den empfangenen Basiswert wieder zu verkaufen, wodurch Sie Ihren finanziellen Verlust realisieren. Alternativ können Sie den Basiswert auch behalten und auf eine Wertsteigerung hoffen. Mit der Lieferung des Basiswerts bestehen für Sie in jedem Fall die finanziellen Risiken, die für diesen Basiswert bestehen.

g | Währungsrisiko

Sofern die Währung des Landes, in dem Sie ein Zertifikat erwerben, oder des Kontos, dem auf dieses Produkt gezahlte Geldbeträge gutgeschrieben werden, sich von der Währung des Produkts unterscheidet, besteht ein Währungsrisiko. Sie erhalten Zahlungen in einer anderen Währung, sodass Ihre endgültige Rendite vom Wechselkurs abhängt. Selbst wenn sich der Kurs des Basiswerts positiv entwickelt, kann es dennoch zu Verlusten kommen, wenn die ausländische Währung gegenüber dem Euro an Wert verliert.

h | Das Liquiditätsrisiko

Die Kapitalanlage in einem Zertifikat ist in der Regel auf eine gewisse Dauer ausgerichtet. Es gibt keine Garantie dafür, dass das Zertifikat während seiner Laufzeit regelmäßig gehandelt werden kann. Wenn Sie auf das eingesetzte Kapital angewiesen sind, kann es sein, dass Sie das Zertifikat gar nicht oder nur mit hohen Abschlägen verkaufen können. Bei einem vorzeitigen Verkauf verzichten Sie in der Regel zudem auf Bonuszahlungen, die ggf. am Ende der Laufzeit fällig werden.

i | Die Komplexität der Produkte

Ein besonderes Risiko kann sich aus der Komplexität eines Produkts ergeben. Je komplizierter ein Produkt ist, desto schwieriger ist in der Regel zu erkennen, welche Risiken bestehen. Bei Zertifikaten kann die Verknüpfung mit der Kursentwicklung des Basiswerts, aber ebenso die Auszahlung am Laufzeitende an diverse Kriterien gekoppelt sein. Lassen Sie sich diese Kriterien vor Ihrer Anlageentscheidung ausführlich erläutern!

j | Kostenrisiko

Die Investition über ein Zertifikat ist meistens teurer als die Direktinvestition in die Kryptowährung. Die Kosten sollten in einem angemessenen Verhältnis zu den Vorteilen und der möglichen Rendite, die Sie mit dem Zertifikat erzielen können, stehen.

k | Besondere Risiken bei speziellen Zertifikaten

Je nach Ausgestaltung des Zertifikats, z. B. als Bonus-Zertifikat oder als Express-Zertifikat, bestehen die Risiken in verschiedener Ausprägung und es können noch weitere Risiken hinzukommen. Eine ausführliche Darstellung verschiedener „Grundtypen" von Zertifikaten und ihren besonderen Risiken finden Sie in der Broschüre „Grundlagenwissen Wertpapiere & Investmentfonds", die Sie jederzeit beim Herausgeber dieser Broschüre oder Ihrem persönlichen Berater anfragen können.

3. Besondere Risiken bei Exchange Traded Notes (ETNs)

Die Risiken von ETNs ähneln denen von ETCs. Es besteht ein Emittentenrisiko. Bei den Emittenten handelt es sich um eigens gegründete Zweckgesellschaften, die in der Regel über kein nennenswertes Vermögen verfügen bis auf die Basiswerte, in die investiert wird. Eine gute Bonität sichert die Erfüllung der vertraglichen Pflichten des Emittenten. Die Bonität des Emittenten kann sich während der Laufzeit der ETN verändern. Bonitätsveränderungen können ihre Ursache direkt im unternehmensspezifischen Umfeld haben oder auf gesamtwirtschaftlichen Veränderungen beruhen. Politische Entwicklungen oder konjunkturelle Veränderungen innerhalb eines Staates wirken sich ebenso auf die Gesamtwirtschaft des betroffenen Staates aus. Je länger ein Abschwung anhält, desto stärker kann sich dies auf die Gewinnsituation und die Zahlungsfähigkeit von Emittenten auswirken. Hohe Staatsdefizite und wirtschaftliche Krisen haben Auswirkungen auf gesamtwirtschaftlicher Ebene. Von einer wirtschaftlichen Krise können aber auch (nur) einzelne Branchen betroffen sein.

Verschlechtert sich die Bonität eines Emittenten - gleich ob aus (unternehmens-)internen oder aus gesamtwirtschaftlichen Gründen -, so wirkt sich dies negativ auf die Kursentwicklung der betroffenen Wertpapiere aus. Von dem eigentlichen Wert des Wertpapiers wird ein Risikoabschlag vorgenommen, der sich an den möglichen Wertschwankungen des Wertpapiers unter Berücksichtigung der Bonität orientiert. Je länger die Restlaufzeit einer ETN ist, desto höher ist in der Regel das Bonitätsrisiko.

Im Insolvenzfall werden die Forderungen der Gläubiger der ETNs je nach Ausgestaltung ggf. nachrangig befriedigt. Das Emittentenrisiko kann durch eine werthaltige Besicherung verringert werden. Bei einer Besicherung mit garantierten Kontrakten eines Partners besteht jedoch das Kreditrisiko des Partners. Werden bei einem Ausfall des Emittenten physisch hinterlegte Sicherheiten verwertet, besteht das Risiko, dass der Verwertungserlös niedriger ist als das eingesetzte Kapital. ETNs haben keine Kapitalgarantie. Ein Verlust des eingesetzten Kapitals bis zum Totalverlust ist möglich.

Grundsätzlich sind ETNs während ihrer Laufzeit jederzeit handelbar. Es kann aber passieren, dass keine Nachfrage nach einer bestimmten ETN besteht. Dann kann eine Veräußerung aufgrund des fehlenden Handelsvolumens schwierig oder sogar unmöglich sein. ETNs sind zudem häufig vielfach gehebelt, was ein hohes Gewinnpotential, aber auch ein enormes Verlustrisiko mit sich bringt.

4. Besondere Risiken bei Exchange Traded Commodities (ETCs)

Häufig handelt es sich bei den Emittenten um eigens gegründete Zweckgesellschaften, die über kein nennenswertes Vermögen bis auf die die Basiswerte, in die investiert wird, verfügen. Das Emittentenrisiko kann durch eine Besicherung verringert werden. Bei einer Besicherung mit garantierten Kontrakten eines Partners besteht jedoch das Kreditrisiko des Partners. Werden bei einem Ausfall des Emittenten physisch hinterlegte Sicherheiten wie z. B. Edelmetalle verwertet, besteht das Risiko, dass der Verwertungserlös niedriger ist als das eingesetzte Kapital. ETCs haben keine Kapitalgarantie. Grundsätzlich ist ein Verlust des eingesetzten Kapitals bis zum Totalverlust möglich.

Bei swapbasierten ETCs besteht zudem ein Kontrahentenrisiko. Hierunter wird das Risiko verstanden, dass einer der Vertragspartner – in diesem Fall der Swapkontrahent - seinen Verpflichtungen aus dem Vertrag nicht mehr nachkommt.

Es kann zu einer vorzeitigen Kündigung und Tilgung kommen, wenn der Emittent oder der Swap-Kontrahent von seinem einseitigen Kündigungsrecht Gebrauch macht. Der Rückzahlungsbetrag kann dabei unter dem Kaufpreis für das ETC liegen.

Da ETCs so konzipiert sind, dass sie die Marktrenditen nachbilden, sind Anleger von ETCs dem Marktrisiko ausgesetzt. Wenn also der Preis der zugrunde liegenden Kryptowährung fällt, erleidet das ETC einen Verlust. Steigt der Preis der zugrunde liegenden Kryptowährung, erzielt das ETC einen Gewinn. Die Kurse von Kryptowährungen reagieren unter anderem auf verschiedene ökonomische Faktoren wie beispielsweise ein verändertes Verhältnis zwischen Angebot und Nachfrage, die Agrar-, Handels-, Steuer-, Geld- und sonstige Politik, was den Wert des ETC beeinflussen kann.

5. Besondere Risiken bei Contracts for Difference (CFDs)

Der Handel mit CFDs birgt einige besondere Risiken, die über jene im Handel mit anderen Wertpapieren hinausgehen. Im Extremfall kann der Verlust den Einsatz um ein Vielfaches übersteigen – selbst wenn jede Position mit einem Stop Loss abgesichert wird.

Stop-loss-Order

Eine Stop-Loss-Order ist ein Verkaufsauftrag, der erst aktiviert wird, wenn der Kurs des Wertpapiers die von Ihnen angegebene Schwelle erreicht oder unterschreitet. Die Stop-Loss-Order soll bei Kurseinbrüchen vor hohen Verlusten schützen. Sie erhalten allerdings keine Garantie dafür, dass die Wertpapiere zu dem von Ihnen angegebenen Preis verkauft werden. Der Verkaufspreis kann auch unter der angegebenen Schwelle liegen, da Ihr Verkaufsauftrag zu dem nächsten verfügbaren Kurs „bestens" ausgeführt wird. Weitere Informationen hierzu finden Sie in der Broschüre „Grundlagenwissen Wertpapiere & Investmentfonds", die Sie jederzeit beim Herausgeber dieser Broschüre oder bei Ihrem persönlichen Berater anfragen können.

a | Komplexität der Produkte

CFDs haben keine normierte Laufzeit oder Kontraktgröße und können von den Vertragsparteien frei verhandelt werden. Daher besteht noch mehr als bei standardisierten Anlageformen wie Anleihen, Aktien oder Optionsscheinen die Gefahr, dass der Anleger die genauen Konditionen nicht versteht und deswegen für ihn unvorteilhafte Anlageentscheidungen trifft. CFDs gelten auch deshalb als hochrisikoreich.

b | Risiko der Hebelwirkung

Für Geschäfte in Derivate oder CFDs muss nur ein Bruchteil des Kapitals eingesetzt werden, das für den Erwerb des zugrundeliegenden Basiswerts erforderlich wäre. Diese sogenannte Hebelwirkung ist typisch für Derivate. Dieser Effekt entsteht dadurch, dass die Preise von Derivaten überproportional auf Preisveränderungen des Basiswerts reagieren. Dies birgt ein erhebliches Gewinn- aber auch ein ebenso großes Verlustpotential, da der Hebel grundsätzlich in beide Richtungen wirkt.

Der Hebel gibt wieder, in welchem Verhältnis sich der Kurs des Derivats in Bezug auf den Basiswert verändert. Wenn der Hebel z. B. 20 beträgt, dann hat eine 1%ige Preisveränderung des Basiswerts eine 20%ige Preisveränderung des Derivats zur Folge, vorausgesetzt, alle anderen Faktoren bleiben unverändert.

Beispiel:

Der Anleger kauft 100 Future-Kontrakte zu je 1,50 Euro mit einem Hebel von 10 bei einem Kurs des Basiswerts von 200 €. Insgesamt investiert er also 150 €. Steigt der Basiswert um 10%, also von 200 € auf 220 €, so profitiert der Anleger hiervon im Verhältnis von 1:10. Die Future-Kontrakte steigen im Wert um 100%, und zwar von 1,50 € auf 3 €. Mit 100 Future-Kontrakten hat der Anleger 150 € Gewinn gemacht.

Sinkt der Kurs des Basiswerts allerdings um 5%, also von 200 € auf 190 €, so sinkt der Wert der Future-Kontrakte um 50% (Kursveränderung 5% x Hebel 10). Die Future-Kontrakte sinken im Wert von 1,50 € auf 0,75 €. Der Verlust des Anlegers beträgt 75 € bzw. die Hälfte des ursprünglich eingesetzten Kapitals.

Da in der Regel weitaus höhere Beträge als in dem Beispiel angelegt werden, wird deutlich, wie schnell es zu hohen Verlusten kommen kann. Je größer der Hebel, desto risikoreicher ist das Geschäft. Da der Hebel nie kleiner ist als 1, ist der absolute Gewinn oder Verlust aus einem Derivategeschäft immer größer als der bei dem zugrundeliegenden Kassageschäft, also der Direktinvestition in

den Basiswert.

c | Risiko von Marginzahlungen

Wie in Kapitel D. beschrieben, sind für CFDs Sicherheitsleistungen in Form von Margins zu erbringen. Margins sind in der Regel täglich zu bezahlen. Ihre Höhe im Sinne eines konkreten und fixen Geldbetrages ist im Vorhinein nicht bestimmbar, da sie von der Kursentwicklung der eingegangenen Geschäfte abhängig sind.

Es gibt verschiedene Arten von Margins. Die Initial Margin gibt an, welcher Prozentsatz des Kontraktwertes für die Eröffnung einer Position (mindestens) erforderlich ist. Die Maintenance Margin gibt an, welcher Prozentsatz der Initial Margin – manchmal auch des Kontraktwertes - nicht unterschritten werden darf, damit eine Position aufrechterhalten bleibt. Üblich sind Prozentsätze von 20-60 %. Reicht die hinterlegte Sicherheit im Falle eines Kursverlusts nicht aus, um die Mindestdeckungshöhe zu erreichen, so fordert der Broker einen Nachschuss, was „Margin Call" bezeichnet wird. Wird dieser Aufforderung nicht umgehend gefolgt, so kann der Broker die Position schließen oder in angemessenem Umfang reduzieren. Der Anleger muss also über genügend finanzielle Sicherheiten verfügen, um der Aufforderung zum Nachschuss nachkommen zu können.

Wichtiger Hinweis
Sie haben immer Ihr gesamtes auf dem CFD-Konto eingesetztes Kapital im Risiko und nicht nur die hinterlegte Margin.

Wichtiger Hinweis
Aufgrund des dargestellten hohen Risikos ist es in Deutschland (und vielen anderen Ländern der Europäischen Union) verboten, Privatkunden CFD-Produkte mit einer Nachschusspflicht anzubieten.

6. Besondere Risiken bei Financial Futures

Financial Futures – umgangssprachlich oft auch nur als „Futures" bezeichnet – sind Termingeschäfte. Termingeschäfte bergen erhebliche Verlustrisiken.

Wesentlich für Futures sind das Risiko der Hebelwirkung und das Risiko von Marginzahlungen, wie oben zu CFDs beschrieben.

Je nach Art des Geschäfts kann es zu einem Totalverlust des eingesetzten Kapitals kommen. Bei Futures können die für Sie entstehenden finanziellen Verpflichtungen je nach Kursverlust zu unbegrenzten Verlusten führen, die Ihre finanzielle Leistungsfähigkeit übersteigen können. Termingeschäfte zählen daher zu den risikoreichsten Kapitalanlagen, die sich nur für erfahrene Anleger eignen, die auch die sich aus ihnen ggf. resultierenden Verluste finanziell tragen können.

Bei Verbindlichkeiten aus Finanztermingeschäften kann Ihr Verlustrisiko unbestimmbar sein und auch über die von Ihnen geleisteten Sicherheiten hinaus Ihr sonstiges Vermögen erfassen.

a | Marktpreisrisiko

Da die Future-Preise im Wesentlichen abhängig sind von der Entwicklung des Basiswerts, den Finanzierungskosten und sonstigen Einflüssen, besteht ein Marktpreisrisiko.

b | „Basisrisiko"

Eine wichtige Größe ist die sog. „Basis", die Differenz zwischen dem Kassapreis und dem Terminpreis, die sich aus der Entwicklung des Basiswerts, den Finanzierungskosten und den sonstigen Einflüssen ergibt. Das sich aus den Änderungen dieser Faktoren erge-

bende Risiko wird „Basisrisiko“ genannt. Diese Faktoren können den Future-Kurs beeinflussen und den Wert einer Position verändern, obwohl sich die Bonität des Kontraktpartners nicht verändert hat. Aufgrund der sich im Zeitablauf verändernden Kosten und unterschiedlicher Erwartungen im Kassa- und im Futuremarkt verändert sich die Basis während der Laufzeit des Futures. Ihr genauer Wert zu einem bestimmten in der Zukunft liegenden Zeitpunkt kann nicht mit Sicherheit vorhergesagt werden. Daher kann auch ein sog. „Hedge“ - eine Future-Position, die zur Absicherung einer Kassaposition eingegangen worden ist - nicht völlig sicher kalkuliert werden. Aus Sicht des Anlegers, der seine Position mit einem Hedge absichern möchte, besteht das Basisrisiko darin, dass sich der Kurs des Futures nicht völlig parallel zum Kurs des Kassageschäfts entwickelt. Aus dem ursprünglich zur Absicherung abgeschlossenen Hedge kann daher auch ein unvorhergesehener Verlust entstehen.

c | Fehlende Absicherungsmöglichkeit

Da Futures standardisiert sind, ist in der Regel eine 100%ige Absicherung des Kassageschäfts nicht möglich. Der Fall, dass das Kassa- und das Futuregeschäft nicht deckungsgleich sind, kann sich daraus ergeben, dass

- kein zu 100% passender Future auf die abzusichernde Kassaposition gefunden wird (Verfügbarkeitsproblem);
- der Betrag der abzusichernden Position nicht mit der Kontraktgröße oder einem Vielfachen davon übereinstimmt (Ganzzahligkeitsproblem); oder
- die Fälligkeitstermine der Future-Position und des Kassageschäfts nicht deckungsgleich sind (Fristeninkongruenz).

d | Lieferrisiko

Am Ende der Laufzeit – am sog. Verfalltag – besteht ein Lieferrisiko, sofern die Position nicht vorher glattgestellt worden ist. Als Käufer müssen Sie die vereinbarte Kaufsumme bereitstellen, um den gelieferten Basiswert zu bezahlen. Sie benötigen umfangreiche Barmittel, die die gezahlten Margin-Beträge in der Regel weit übersteigen. Auf Seiten des Verkäufers besteht das Risiko, dass er den Basiswert liefern muss. Befindet sich dieser nicht in seinem Besitz, so muss er diesen zu dem aktuellen Marktwert kaufen, der erheblich über dem vereinbarten Future-Preis liegen kann. Da der Preis theoretisch unbegrenzt steigen kann, besteht ein theoretisch unbegrenztes Verlustrisiko. Der eintretende Verlust kann die geleisteten Margin-Zahlungen weit übersteigen.

Wenn Sie in Futures investieren wollen, sollten Sie sich vorab ausführlich mit ihrer Funktionsweise und auch mit den allgemeinen Risiken bei der Vermögensanlage in Termingeschäften befassen, die grundsätzlich zusätzlich zu den oben aufgeführten besonderen Risiken bestehen. Eine Darstellung hierzu finden Sie in der Broschüre „Grundlagenwissen Termingeschäfte“, die Sie jederzeit beim Herausgeber dieser Broschüre oder bei Ihrem persönlichen Berater anfragen können.

VI. Risiken bei der Vermögensanlage in tokenisierte Assets

So wie die Rendite einer Vermögensanlage in Token bzw. tokenisierte Assets sehr hoch sein kann, können auch die Risiken und ggf. der Kapitalverlust sehr hoch sein. Es droht der Totalverlust des eingesetzten Kapitals.

1. Keine gesetzliche Regulierung

Ein wesentliches Risiko bei der Investition in Token ergibt sich daraus, dass für Token und tokenisierte Assets derzeit nur die bestehende gesetzliche Regulierung, nicht aber eine eigene, spezifische Regulierung existiert. Zwar werden Token anders als Kryptowährungen an einem regulierten Markt gehandelt und die bestehenden Gesetze (wie etwa das Vermögensanlagengesetz, das Wertpapierprospektgesetz oder das Wertpapierhandelsgesetz) werden je nach deren individueller Ausgestaltung im Einzelfall bereits auf Token angewendet. Es gibt aber derzeit noch keine eigens für Token erstellten, gesetzlichen Spezial-Regularien. Token müssen keine bestimmten gesetzlichen Bedingungen erfüllen, um ausgegeben werden zu dürfen. Anders ist dies bei den meisten herkömmlichen Wertpapieren. So darf ein Wertpapier etwa nur dann als Aktie bezeichnet werden, wenn gewisse rechtliche Voraussetzungen erfüllt sind, z. B. muss es sich bei dem Emittenten um eine Aktiengesellschaft mit einem gesetzlich vorgeschriebenen Mindesteigenkapital handeln.

Aus der eingeschränkten rechtlichen Regulierung resultieren verschiedene Risiken.

a | Mangelnde Informationsmöglichkeiten

Für das White Paper und die Terms and Conditions gibt es (sofern nicht die oben erwähnten gesetzlichen Vorgaben bereits eingreifen) keine Mindestanforderungen und keine sonstigen rechtlichen Bestimmungen. Der Anbieter ist dann in der Ausgestaltung dieser Unterlagen völlig frei. Die Unterlagen werden keiner behördlichen Prüfung unterzogen und bedürfen - anders als etwa ein Wertpapierprospekt - keiner Billigung bzw. Genehmigung. Sie enthalten oftmals objektiv unzureichende, unverständliche oder irreführende Informationen zum Projekt, zu den Risiken, zu den mit den Token verbundenen Rechten und zu potenziellen Interessenkonflikten. Eine informierte Investitionsentscheidung ist mit diesen Dokumenten regelmäßig nicht möglich.

Der Anbieter kann das White Paper zudem jederzeit ändern - sowohl vor als auch während des ICOs -, so dass dieses keine verlässliche Grundlage für Investitionsentscheidungen darstellen kann.

b | Fehlender Schutz

Oftmals existieren kein Verbraucherschutz, keine kapitalmarktspezifischen Anlegerschutzinstrumente und kein Schutz personenbezogener Daten. Das White Paper und die Terms and Conditions stellen zudem kein mit einem Wertpapierprospekt vergleichbares Haftungsdokument mit einer speziellen Haftungsgrundlage dar.

c | Keine Einlagensicherung

Für tokenisierte Assets besteht keine Einlagensicherung und kein Anlegerschutz.

d | Verstoß gegen Prospekt- oder Erlaubnispflichten

Da die rechtliche Einordnung von Token je nach Ausgestaltung des Angebots unterschiedlich ist, ist Emittenten häufig nicht bewusst, dass im Falle eines Angebotsbeginns vor einer abschließenden Entscheidung der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) hinsichtlich der Einordnung der Token, die Möglichkeit der Untersagung des öffentlichen Angebotes und der Einleitung eines Ordnungswidrigkeitsverfahrens durch die BaFin besteht, sollte sich herausstellen, dass ein Prospekt – im Rahmen der bereits bestehenden gesetzlichen Vorschriften, die auch auf Token Anwendung finden - erforderlich gewesen wäre.

Für das öffentliche Angebot der Token kann zudem eine behördliche Erlaubnis erforderlich sein. Dies hängt ebenfalls von der Ausgestaltung des Angebots ab. Wird das Geschäft ohne die erforderliche Erlaubnis betrieben, kann die BaFin das öffentliche Angebot untersagen, die Abwicklung des Geschäfts anordnen und weitere Strafen verhängen. Unter Umständen kann der Anbieter in diesem Fall bereits von Anlegern eingesammeltes Kapital nicht zurückzahlen, so dass die Anleger einen Totalverlust erleiden.

e | Steuerliche Risiken

Je nach Art des Angebots und der ausgegebenen Token fallen für das Unternehmen, das die Token ausgibt, und auf das eingesammelte Kapital unterschiedliche Steuern an. In Betracht kommen regelmäßig Umsatz-, Körperschafts- und Gewerbesteuer. Je nachdem kann die Steuerlast erheblich sein.

Es besteht das Risiko, dass der Emittent die steuerliche Einordnung falsch beurteilt und es zu erheblichen (Nach-)Forderungen durch das Finanzamt kommt, was bei der Ermittlung der prognostizierten Renditen nicht berücksichtigt worden ist. Hierdurch kann sich die Rendite für die Anleger erheblich schmälern und es kann zu Kapitalverlusten kommen.

Ungeachtet dessen hat der Anleger seinerseits ggf. steuerliche Abgaben zu erfüllen, die individuell berücksichtigt werden müssen. Insofern ist potentiellen Anlegern dringend empfohlen, auf entsprechende, fachkundige Beratung zurückzugreifen.

f | Risiko fehlender Umtauschmöglichkeiten

Es gibt keine Garantie dafür, dass Sie die von Ihnen erworbenen Token jederzeit oder überhaupt jemals wieder in eine Kryptowährung oder in Fiatgeld umtauschen können. Sie sind bei Anlagen in Token regelmäßig davon abhängig, dass der Emittent den Zusagen, die er bei der Emission gemacht hat, nachkommt.

2. Besondere Risiken von Intitial Coin Offerings - ICOs

Zusätzlich zu den oben dargestellten Risiken bei der Vermögensanlage in tokenisierte Assets bestehen bei ICOs besondere Risiken. Typischerweise befinden sich über ICOs zu finanzierende Projekte in einem sehr frühen Stadium. Zudem handelt es sich bei dieser

Finanzierungsart um eine junge, neuartige Form der Finanzierung. Entwicklungsstand und Geschäftsmodelle sind entsprechend unerprobt. Allein diese Umstände machen ICOs für Anleger zu einem risikoreichen, hochspekulativen Investment. Ein Totalverlust der Investition ist möglich.

Als Investor sollte man sich der Unterschiede zwischen den verschiedenen Arten von Token bewusst sein, da sich die aus den Token für den Inhaber ergebenden Rechte erheblich voneinander unterscheiden. Mit einem Utility-Token hat der Inhaber Zugang auf ein Produkt oder einen Service des Unternehmens, es ist aber kein darüber hinausgehender, langlebiger Vermögenswert damit verknüpft. Demnach hat er keine Rechte oder Beteiligung am Vermögen oder erzielten Gewinn eines Unternehmens. Demgegenüber hat der Inhaber eines Security Token Inhaberrechte und somit einen extern handelbaren Vermögenswert.

---

a | Hohe Volatilität

Es sind große Preisschwankungen möglich.

b | Betrugsrisiko

ICO-Strukturen bieten großes Potenzial für Missbrauch und Betrug. Nur Experten können anhand des zugrundeliegenden Programmiercodes (etwa des Smart Contracts) überprüfen, ob die im White Paper oder den Terms and Conditions angegebene Funktionsweise der Token zutrifft. Der Anleger trägt das Risiko, dass der Anbieter hier falsche Angaben macht.

Die Anbieter eines ICOs erhalten das von den Anlegern eingesammelte Geld sofort. Die Auszahlung oder Freigabe der Gelder ist in der Regel an keine Bedingungen wie z. B. Projektfortschritte geknüpft. Anleger sind einem erhöhten Betrugsrisiko ausgesetzt, wenn der Anbieter des ICOs nicht eindeutig identifizierbar ist oder wenn sie in Systeme investieren, die außerhalb von Deutschland betrieben werden. Ansprüche gegen Token-Anbieter mit Sitz im Ausland können im Streitfall – wenn überhaupt – nur unter großem Aufwand und mit Schwierigkeiten durchgesetzt werden. Die systembedingte Anfälligkeit von ICOs für Betrug, Geldwäsche und Terrorismusfinanzierung erhöht zusätzlich das Risiko, dass Anleger ihr eingesetztes Kapital verlieren. Vor einer Investition sollten Sie sorgfältig prüfen, welche Personen hinter dem Angebot stehen.

c | Risiko fehlerhafter Software

Der hinter den Token stehende Programmiercode kann Programmierfehler enthalten oder manipulierbar sein, was Dritte nachteilig ausnutzen können und bis zum Totalverlust des angelegten Betrags führen kann.

d | Komplexitätsrisiko

Oftmals ist tiefes, insbesondere technisches Verständnis notwendig, um ICO-Projekte umfassend beurteilen zu können. Ohne eine umfassende Beurteilung ist eine realistische Einschätzung der mit einem Projekt verbundenen Chancen und Risiken nicht möglich. Enthält ein White Paper abgesehen von einer attraktiven Geschäftsidee keine weiteren konzeptionellen Elemente, insbesondere bereits eine eigene Infrastruktur, sollte dem Risiko hinreichend Rechnung getragen werden, dass das Entwicklerteam möglicherweise an der Umsetzung scheitert.

e | Besondere Risiken von Uncapped ICOs

Bei ungedeckelten („uncapped") ICOs lässt sich der direkte Marktwert des Projekts nach dem ICO nicht beurteilen. Der Anleger weiß im Vorhinein nicht, wie viele Token er für seinen Kapitaleinsatz erwerben kann. Die Token können daher weniger wert sein, als wenn der ICO gekappt wäre.

3. Besondere Risiken von Security Token Offerings – STOs

Ein STO ist ein öffentliches Angebot eines tokenbasierten Wertpapiers. Ein Security Token hat grundsätzlich die Charakteristika eines Wertpapiers. Security Token sind häufig durch reelle Assets abgesichert und werden strikten Richtlinien zu Compliance, Emission und Handel unterworfen. Sie sind in der Regel vergleichbar mit (Unternehmens-)Anleihen. Je nach Ausgestaltung des STOs bestehen verschiedene Risiken, die im Wesentlichen identisch sind mit denen von Anleihen.

Wichtiger Hinweis

Security Token ähneln Unternehmensanleihen, sie können aber ebenso gut aktienähnlich ausgestaltet sein. Welche Rechte ein Security Token gewährt, ist dem dem jeweiligen STO zugrundeliegenden Wertpapierprospekt zu entnehmen. Da sprachlich häufig nicht unterschieden wird zwischen STOs und ETOs, können grundsätzlich zusätzlich zu den hier aufgeführten Risiken auch die unter der folgenden Ziff. 4. aufgeführten Risiken bestehen.

a | Das Emittentenrisiko

Es besteht das Risiko, dass der Emittent der Security Token in Zahlungsverzug kommt oder sogar zahlungsunfähig wird. Für den Anleger bedeutet dies einen teilweisen oder völligen Verlust des eingesetzten Kapitals. Da der Käufer der Token Gläubiger des Emittenten wird, ist die Bonität des Emittenten ein wichtiges Kriterium bei der Anlageentscheidung. Eine gute Schuldnerbonität ist allerdings keine Garantie für vollständige Zins- und Tilgungszahlungen, da sich die Bonität des Emittenten während der Laufzeit der Investition verändern kann.

b | Das Ausschüttungsrisiko

Ausschüttungen sind in der Regel nicht garantiert. Erleidet der Emittent einen Verlust, so können Ausschüttungen, z. B. in Form von Zinsen, entfallen. Ob eine garantierte Verzinsung oder ggf. ein Anspruch auf Nachzahlung vorgesehen ist, ist den Emissionsbedingungen zu entnehmen.

c | Das Rückzahlungsrisiko

Der Rückzahlungsbetrag am Laufzeitende ist nicht garantiert. Im Falle von Unternehmensverlusten kann sich der Auszahlungsbetrag am Laufzeitende – ggf. bis auf Null, also zu einem Totalverlust - reduzieren.

4. Besondere Risiken von Equity Token Offerings - ETOs

Ein wesentlicher Unterschied zu Equity Token und zu Security Token besteht darin, dass den Inhabern von Equity Token „Eigentums"-Rechte an einem Projekt zustehen. Equity Token sind aktienähnlich und es bestehen neben den allgemeinen mit tokenisierten Assets verbundenen Risiken im Wesentlichen mit einer Investition in Aktien vergleichbare Risiken.

a | Das unternehmerische Risiko

Als Besitzer von Equity Token sind Sie nicht Gläubiger eines Unternehmens, sondern werden wirtschaftlich betrachtet wie ein Mitinhaber und beteiligen sich damit (positiv wie negativ) an der wirtschaftlichen Entwicklung des Unternehmens. Entwickelt sich das Unternehmen nicht wie von Ihnen erhofft, müssen Sie mit Verlusten rechnen. Im Extremfall, d. h. im Falle der Insolvenz des Unternehmens, kann die Investition den vollständigen Verlust des investierten Kapitals bedeuten. In der Regel werden die Besitzer von Equity Token wie Mitinhaber, die eigenes Kapital in ein Projekt oder Unternehmen investiert haben, erst nach Befriedigung aller Gläubigeransprüche Dritter am Liquidationserlös – sofern einer vorhanden ist – beteiligt.

b | Das Dividenden- bzw. Gewinnausschüttungsrisiko

Das Dividendenrisiko bezeichnet das Risiko, dass Dividendenzahlungen oder sonstige Gewinnbeteiligungen geringer ausfallen als erwartet oder dass sie sogar gänzlich entfallen. Da die Dividende sich maßgeblich nach dem erzielten Gewinn des Unternehmens richtet, kann sie bei niedrigen Gewinnen oder in Verlustsituationen gekürzt werden oder ausfallen. Selbst eine jahrelange ununterbrochene Dividendenzahlung ist keine Garantie für Dividendenzahlungen in der Zukunft.

Das Dividendenrisiko stellt kein Verlustrisiko im eigentlichen Sinn dar, da ausbleibende Dividendenzahlungen Ihr bestehendes Vermögen nicht schmälern. Wenn Sie auf laufende Dividendenzahlungen oder Gewinnausschüttungen angewiesen sind oder diese voraussetzen, kann ihr Ausbleiben für Sie dennoch negative finanzielle Folgen haben.

5. Besondere Risiken bei der Investition in Immobilien über Token

Die besonderen Risiken bei der Investition in Immobilien über Token ergeben sich im Wesentlichen nicht aus dem Investitionsobjekt.

a | Marktrisiko

Veränderungen an den Immobilienmärkten wirken sich auf den Ertrag und damit auf den Wert der Token aus. Preisschwankungen können zu Wertverlusten führen. Durch mögliche Leerstände der Objekte, Probleme der Erstvermietung oder gesunkene Mietpreise bei Neuvermietung besteht ein Ertragsrisiko. Dies kann zu Ausschüttungskürzungen führen.

b | Illiquiditätsrisiko

Das Investitionsobjekt hinter dem Token bleibt illiquide – auch wenn die Anteile selbst dank Tokenisierung schnell und kostengünstig den Besitzer wechseln können. Im Falle von wirtschaftlichen Problemen auf Ebene eines Immobilienprojekts besteht das Risiko, dass der Kurs eines das Projekt abbildenden Tokens stark fällt. Dies kann – z.B. wenn das Projekt vollständig scheitert – zum Totalverlust führen.

c | Fehlender Zweitmarkt

Bislang gibt es in der Regel keinen geregelten Zweitmarkt, d.h. geregelte Handelsmöglichkeiten für die Token nach der Emission.

6. Basisrisiken

Die sog. „Basisrisiken" treffen für fast alle Formen der Vermögensanlage zu, unabhängig von der (Rechts-)Form des Investments. Eine ausführliche Darstellung dieser Basisrisken finden Sie in der Broschüre „Grundlagenwissen Wertpapiere & Investmentfonds", die Sie jederzeit beim Herausgeber dieser Broschüre oder Ihrem persönlichen Berater anfragen können.

Die im Folgenden aufgeführten Basisrisiken bestehen insbesondere auch bei Blockchain-basierten Investments und Kryptowährungen. Die Aufzählung ist nicht abschließend, bei Ihrem Investment können zusätzlich weitere (Basis-)Risiken bestehen.

a | Das allgemeine Börsenrisiko

Das allgemeine Börsenrisiko besteht in grundsätzlich schwankenden, weil Markt-abhängigen Preisentwicklungen. Eine vollständige Absicherung des Börsenrisikos ist nicht möglich, da dieses der Teilnahme an einem Börsenmarkt inhärent ist. Zudem bestehen damit zusammenhängende Wechselwirkungen: Ein Crash an den Börsen wirkt sich zumindest mittelbar auch auf nicht börsennotierte Kapitalanlagen aus, z.B. weil Anleger ihre Gelder aus Kapitalanlagen abziehen, die Nachfrage nach bestimmten Waren sinkt, Unternehmen durch Kursstürze Verluste erleiden etc. Ebenfalls die politische Lage in einem Land, z.B. anstehende Wahlen oder Krisen, hat in der Regel weitere unmittelbare Auswirkungen auf die Märkte dieses Landes.

b | Das psychologische Marktrisiko

Das psychologische Marktrisiko kann als Unterfall des allgemeinen Börsenrisikos betrachtet werden. Auf die allgemeine Kursentwicklung an der Börse wirken diverse Faktoren ein, die nicht ausschließlich rationale Gründe oder Hintergründe haben. Individuelle und öffentliche Meinungen, Gerüchte und Einstellungen zu einem Unternehmen können unabhängig von der tatsächlichen Ertragslage des betroffenen Unternehmens erhebliche Kursveränderungen (positiv und negativ) bewirken. Möglich ist auch, dass individuell rationales Verhalten in ein im Kollektiv irrationales „Herdenverhalten" mündet, das seinerseits alleine aufgrund der hohen Anzahl an betroffenen Marktteilnehmern die Finanzstabilität beeinträchtigen kann. Der Wert von Kryptowährungen hängt entscheidend von dem ihm durch die Nutzer des Netzwerks zum Zeitpunkt der Wertbeurteilung zugewiesenen Wert ab. Verlieren diese Nutzer „den Glauben" an eine Kryptowährung, erachten sie diese also z.B. als im Wert sinkend oder sogar wertlos, so kann dies zu erheblichen Verlusten bis hin zum Totalverlust führen.

c | Steuerliche Risiken

Die steuerliche Situation innerhalb eines Landes kann sich jederzeit ändern. Änderungen im Steuerrecht (z.B. bei der Definition oder der Absetzbarkeit von Werbungskosten), in der steuerlichen Rechtsprechung oder in der Verwaltungspraxis können Auswirkungen nicht nur unmittelbar auf die konkrete steuerliche Behandlung von Einkünften aus Kapitalvermögen haben, sondern mittelbar auch auf die Kursentwicklung am Kapitalmarkt generell.

Die (einkommens-)steuerliche Behandlung von neuen Anlageformen ist bei deren Emission nicht immer abschließend geklärt. Der Kauf innovativer Finanzprodukte – wozu sämtliche in dieser Broschüre dargestellten Anlageformen zählen - birgt das Risiko, im Falle einer ungünstigen steuerrechtlichen Entwicklung oder unerwarteter Entscheidungen der Finanzverwaltung während der Laufzeit der

Anlage nicht die erwartete Rendite erzielen zu können.

d | Risiko der Kreditfinanzierung

Kapitalanlagen können ganz oder teilweise durch Kreditaufnahme finanziert werden. Hierbei besteht das Risiko, dass Sie im Falle von Kursverlusten nicht nur das eingesetzte Kapital (ggf. vollständig) verlieren, sondern darüber hinaus den aufgenommenen Kredit zzgl. Zinsen zurückzahlen müssen.

e | Rechtliche Risiken

Für Kryptowährungen und jegliche Form von Token bzw. tokenisierten Assets besteht derzeit noch keine eigene gesetzliche Regelung, sondern es werden grundsätzlich die bestehenden Regeln (entsprechend) angewendet. Es besteht das Risiko, aufgrund einer Änderung der Rechtslage (geänderte Rechtsprechung oder Gesetzesänderung) für in der Vergangenheit abgeschlossene Geschäfte Verluste zu erleiden. Außerdem besteht mittelbar durchaus das Risiko, dass Unternehmen, in die Sie unmittelbar oder mittelbar investiert haben, aufgrund einer geänderten Rechtslage gezwungen sind, ihre zukünftige Geschäftstätigkeit umstellen zu müssen, was sich erheblich auf Ihre Investition auswirken kann.

Weiterführende Informationen

F

In diesem Kapitel finden Sie nach einem Überblick über die steuerliche Behandlung von Kryptowährungen und auf der Blockchain-Technologie basierenden Kapitalanlagen auf Anlegerseite jeweils eine ergänzende Ausführung zum Thema „Blockchains und das Klima" und zur Limitierung von Bitcoin sowie eine Übersicht über die nach Marktkapitalisierung zehn größten Kryptowährungen.

I. Die steuerliche Behandlung

Die Besteuerung von Kryptowährungen und Blockchain-basierten Investments ist von Land zu Land anders. Sie sollten sich bereits vor einer Investition mit der steuerlichen Behandlung des gewünschten Investments vertraut machen und erforderlichenfalls einen fachkundigen steuerlichen Berater zu Rate ziehen.

Die folgende Darstellung stellt **keine steuerliche Beratung** dar und gibt die steuerliche Behandlung von Kryptowährungen und auf der Blockchain-Technologie basierenden Investments nicht abschließend wieder. Sie soll Ihnen lediglich einen ersten Eindruck über die steuerliche Behandlung solcher Kapitalanlagen verschaffen.

---

1. Der Handel mit Kryptowährungen

Der Handel mit Kryptowährungen unterliegt der Besteuerung. Sie sollten Gewinne hieraus bei Ihrer Steuererklärung keinesfalls verschweigen bzw. nachlässig „unter den Tisch fallen lassen".

Die Veräußerung von Kryptowährungen stellt in der Regel ein privates Veräußerungsgeschäft i.S.d. § 23 Abs. 1 des Einkommensteuergesetzes (EstG) dar, auch als „Spekulationsgeschäft" bezeichnet. Gewinne aus Verkäufen im privaten Umfeld sind nach einer einjährigen Haltefrist steuerfrei. Diese Frist wird „Spekulationsfrist" genannt. Werden Anteile der Kryptowährung vor Ablauf der Spekulationsfrist veräußert, so ist der Veräußerungsgewinn steuerpflichtig. Es gilt der persönliche Steuersatz des Anlegers.

In der Regel wird bei der Berechnung der Haltefrist und für die Gewinnermittlung die „First In – First Out" -Regelung (Kurz: „FIFO"-Regelung) angewendet, bei der Verkäufe so behandelt werden, als würden immer die ältesten Coins aus dem Bestand veräußert werden. Aber Achtung: Die steuerliche Behandlung von Kryptowährungen ist noch nicht abschließend geklärt. So muss die FIFO-Regelung nicht zwingend von den Finanzämtern angewendet und akzeptiert werden. Theoretisch können auch andere Methoden für die Gewinnermittlung zum Tragen kommen.

Für private Veräußerungsgeschäfte gilt eine Freigrenze von 600 Euro pro Jahr. Liegt der erzielte Gewinn darunter, so fallen darauf keine Steuern an. Die Freigrenze gilt allerdings für alle privaten Veräußerungsgewinne zusammen, z. B. auch aus der Veräußerung von Gold, Devisen oder Antiquitäten, und nicht nur für die mit Kryptowährungen erzielten Gewinne. Wird die Freigrenze überschritten, muss der komplette Veräußerungsgewinn versteuert werden und nicht nur der die Freigrenze übersteigende Betrag.

Auch das Bezahlen von Waren oder Dienstleistungen mit Coins einer Kryptowährung stellt steuerlich ein privates Veräußerungsgeschäft dar, ebenso der Umtausch von einer Kryptowährung in eine andere Kryptowährung.

Ergibt sich aus den Geschäften mit Kryptowährungen ein Verlust, so fällt keine Steuer an. Ein Verlust kann mit Gewinnen anderer Jahre verrechnet werden, indem er entweder mit Gewinnen aus zurückliegenden Jahren verrechnet oder in die Folgejahre vorgetragen wird.

Erzielen Sie mit einer Kryptowährung Zinsen, so fällt hierauf die Abgeltungssteuer an. Der Abgeltungssteuersatz beträgt 25%, ggf. zzgl. Solidaritätszuschlag und Kirchensteuer. Für Einkünfte aus Kapitalvermögen, die der Abgeltungssteuer unterliegen, gilt ein Freibetrag von 801 Euro pro Person. Bis zu diesem sog. „Sparer-Pauschbetrag" werden Einkünfte aus Kapitalvermögen nicht versteuert. Wenn Sie bei Ihrer Bank oder Depotstelle einen Freistellungsauftrag erteilt haben, wird dieser Freibetrag bei der Abführung der Abgeltungssteuer berücksichtigt. Ohne einen Freistellungsauftrag können Sie sich ggf. zu viel gezahlte Steuern über Ihre Steuererklärung zurückholen.

Wichtiger Hinweis

Nach § 23 Abs. 1 Nr. 2 Satz 4 EstG erhöht sich die Spekulationsfrist von einem auf zehn Jahre, wenn aus der Nutzung eines Wirtschaftsguts als Einkunftsquelle zumindest in einem Kalenderjahr Einkünfte erzielt werden. Für Kryptowährungen bedeutet das, falls Sie für das erste Jahr Zinsen auf die gehaltene Kryptowährung bekommen, verlängert sich die Spekulationsfrist auf 10 Jahre. Diese Auffassung ist jedoch umstritten und einige Finanzämter vertreten durchaus eine andere Meinung. Bei signifikanten Investitionsbeträgen ist es aus Risikogesichtspunkten ratsam, eine rechtsverbindliche Auskunft gemäß § 89 der Abgabenordnung (AO) vor der Investition einzuholen.

2. Derivate auf Kryptowährungen

Gewinne aus Derivaten auf Kryptowährungen werden – wie Zinsen auf Kryptowährungen - nicht mit dem persönlichen Steuersatz, sondern mit der Abgeltungssteuer in Höhe von 25% - ggf. zzgl. Solidaritätszuschlag und Kirchensteuer - versteuert. Da es keine Spekulationsfrist gibt, Gewinne aus der Veräußerung von Derivaten also unabhängig von der Haltedauer immer steuerpflichtig sind, können kurze Trades mit Derivaten sinnvoller sein als der kurzfristige Kauf und Verkauf einer Kryptowährung. Die steuerliche Behandlung sollte jedoch niemals die alleine Grundlage für eine Investitionsentscheidung sein!

Auch der bei Fälligkeit eines Future-Kontrakts ggf. gezahlte Differenzausgleich unterfällt der Abgeltungssteuer.

3. Mining

Beim Mining können gewerbliche Einkünfte entstehen, die als solche zu versteuern sind. Falls Sie nicht gewerblich tätig sind und nur gelegentliches Mining betreiben, können Sie von der Freigrenze von 256 Euro im Kalenderjahr für Einkünfte aus Leistungen (§ 22 Nr. 3 EStG) profitieren. Liegen Ihre Einnahmen unter dieser Freigrenze, müssen Sie darauf keine Steuern zahlen. Wenn Sie sich einem Mining-Pool anschließen oder sog. „Cloud-Mining" betreiben, sollten Sie sich den Vertrag mit dem Anbieter sorgfältig durchlesen, da sich aus der vertraglichen Ausgestaltung Abweichungen von der hier dargestellten Form der Besteuerung ergeben können.

4. Tokenisierte Assets

Die steuerliche Betrachtung von ICOs, STOs und ETOs ist komplizierter. Bisher gibt es von Seiten der Finanzverwaltung noch keine offizielle Stellungnahme zur Besteuerung dieser Investitionen. Das Finanzamt wird dementsprechend aktuell jeden Fall individuell prüfen.

Bei der steuerlichen Behandlung bestehen für den Privatanleger zwischen Security und Equity Token einerseits und Utility Token andererseits deutliche Unterschiede. Token, die nur als alternatives Zahlungsmittel dienen und mit keinen Rechten verbunden sind, und Token, die wie ein Gutschein betrachtet werden können (Utility Token), sind nicht mit Wertpapieren vergleichbar. Steuerlich unterfallen sie § 23 EStG, Gewinne sind nach Ablauf der einjährigen Spekulationsfrist steuerfrei.

Security Token hingegen stellen im deutschen Steuerrecht keine privaten Wirtschaftsgüter im Sinne des § 23 EStG dar, sondern unterliegen je nach Ausgestaltung als eigenkapital- oder fremdkapitalähnliche Wertpapiere der Besteuerung als Einkünfte aus Kapitalvermögen i.S.d. § 20 EStG. Steuerlich werden Security Token also ähnlich wie Aktien behandelt. Damit besteht z.B. auch keine Spekulationsfrist, nach welcher einer etwaiger Veräußerungsgewinn bzw. -verlust steuerfrei wäre. Ausschüttungen und Veräußerungsgewinne unterliegen der Abgeltungssteuer mit einem Steuersatz i.H.v. 25%, ggf. zzgl. Solidaritätszuschlag und Kirchensteuer.

Wichtiger Hinweis

Die Ausführungen in diesem Kapitel beziehen sich auf die steuerliche Behandlung von Investitionen im privaten Umfeld. Tätigen Sie Investitionen als Unternehmer, kann die steuerliche Behandlung von der Darstellung in dieser Broschüre abweichen. Kontaktieren Sie vor der Investition in jedem Fall einen steuerlichen Berater!

II. Blockchains und das Klima

Der hohe Stromverbrauch vieler Blockchains entsteht vor allem durch den Proof-of -Work- Mechanismus (PoW). Bereits heute übersteigt der jährliche Energieverbrauch der auf dieser Methode basierenden Bitcoin-Blockchain den mehrerer Nationen. Dies wird von Seiten der Klimapolitik regelmäßig kritisiert. Allerdings kann zukünftig davon ausgegangen werden, dass für die Blockchain-Tech-

nologie grundsätzlich ein derart hoher Energieaufwand technologisch nicht erforderlich ist. Es gibt Mechanismen zur Erzeugung von Konsens – z.B. Proof of Stake -, die nur einen Bruchteil der Energie benötigen, die der PoW-Mechanismus erfordert. Es könnten sogar bereits bestehende Blockchains, die den PoW-Mechanismus nutzen, auf ein anderes Verfahren umgestellt werden.

Der hohe Stromverbrauch sollte daher kein Argument gegen die Blockchain an sich, sondern lediglich gegen energieaufwändige Verfahren zur Herstellung von Konsens sein. Die technologische Entwicklung der Blockchain ist außerdem unvorhersehbar und jung. Es ist nicht auszuschließen, dass in Zukunft weitere Wege gefunden werden, wie die Blockchain-Technologie energiesparend und umweltschonend eingesetzt werden kann.

III. Die Limitierung von Bitcoin

Wie in Kapitel E. ausgeführt, ist bei den meisten Kryptowährungen die Anzahl der Coins, die geschürft werden können, begrenzt. Angenommen, das aktuelle Bitcoin-Protokoll bleibt unverändert, wird Bitcoins vollständiger Umfang aktuellen Schätzungen zufolge im Jahr 2140 erreicht werden, also in 120 Jahren. Dies wirft einige Fragen auf. Da durch das Mining spätestens ab diesem Zeitpunkt keine neuen Coins geschürft werden können, verbleiben die ihnen zufließenden Transaktionsgebühren als einziger Anreiz für Miner das Mining zu betreiben.

Bereits heute gibt es verschiedene Lösungsansätze für das darin zum Ausdruck kommende Skalierungsproblem von Bitcoin mit Auswirkungen auf die maximale Blockgröße, die Transaktionsgeschwindigkeit und letztlich auch auf die Höhe der Transaktionsgebühren.

Glossar

51%-Angriff

Potenzieller Angriff auf ein Blockchain-Netzwerk, bei dem eine einzelne Einheit oder Organisation in der Lage ist, den Großteil der Hash-Rate zu kontrollieren, wobei nicht zwangsläufig 51% der Hash-Power erforderlich sind.

Algorithmus

Allgemein: Systematische Vorgehensweise, um ein Problem zu lösen. Der Begriff wird in der Regel im Bereich der Informatik und der Mathematik für Computerprogramme bzw. Teile von Computerprogrammen verwendet.

Altcoin

Coin, der eine direkte Alternative zum Bitcoin darstellt, da er seinem Wesen nach dem Bitcoin mit eigener Blockchain, Minern und Nodes entspricht.

Anleihe

Wertpapier, das das Recht auf Rückzahlung des Nennwerts zzgl. einer Verzinsung verbrieft. Emittenten sind hauptsächlich Länder, Banken und Unternehmen.

Asset

engl. für „Vermögen“ oder „Vermögenswert“

Basis

Bei Termingeschäften die Differenz zwischen dem Kassapreis und dem Terminpreis.

Basiswert

Der einem Termin- oder Kassageschäft zugrundeliegende Vermögenswert.

Bestens

Bezeichnung für eine unlimitierte Verkaufsorder, was bedeutet, dass die Order zum aktuell bestmöglichen Kurs ausgeführt wird, faktisch zu jedem beliebigen Kurs, zu dem eine entsprechende Nachfrage besteht.

Binnenwährung

Eine nur innerhalb der Grenzen eines Staates oder eines Staatenbündnisses gültige Währung.

Bit

Abk. für: „binary digit“, die kleinste elektronische Speichereinheit

Bitcoin **d**

ie weltweit führende Kryptowährung

Blase

Auch: Spekulationsblase. Marktsituation, in der die Preise eines oder mehrerer Handelsgüter oder Vermögensgegenstände bei hohen Umsätzen über ihrem inneren Wert liegen.

Blockchain

Engl. für „Blockkette“, eine kontinuierlich erweiterbare Liste von Datensätzen, die mittels kryptografischer Verfahren miteinander verkettet sind.

Blockprämie

Belohnung in Form einer digitalen Währung für das Finden eines neuen Blocks in der Blockchain.

Body

Teil des Blocks einer Blockchain, in dem sich die Transaktionen, die mit dem Block ausgeführt werden sollen, befinden.

Bonität

Fähigkeit und Bereitschaft einer Person oder eines Unternehmens, ihre/seine zukünftigen Zahlungsverpflichtungen vollständig und fristgerecht zu erfüllen, die Kreditwürdigkeit.

Broker

Börsenmakler; ist für die Durchführung von Aufträgen von Anlegern an der Börse zuständig.

Bug

Umgangssprachliche Bezeichnung für einen Software-Fehler oder eine Software-Anomalie.

Cap

Bezeichnung für eine Kappungs- oder Obergrenze.

Cloud-Mining

Anmieten von Hardware in einem Rechenzentrum, um ohne eigene Ausrüstung das Mining zu betreiben. Allgemein bezeichnet Cloud Computing das Zusammenspiel von mehreren Servern, die gemeinsam einen Zusammenschluss („Wolke") bilden.

Coin

Digitale Münze, mit der Waren oder Dienstleistungen bezahlt werden können; eine Einheit einer Kryptowährung, die eine eigene Blockchain besitzt.

Cold Wallet

Wallet, die vollständig offline ist, z. B. Paper Wallet.

Contract for Difference (CFD)

Differenzkontrakt, bei dem zwei Vertragsparteien den Austausch von Wertentwicklung und Erträgen eines Basiswerts gegen Zinszahlungen während der Laufzeit vereinbaren.

Crowdfunding

Form der Finanzierung mit Eigenkapital oder Eigenkapital ähnlichen Mitteln, zu der meist im Internet zu einer Beteiligung in Form einer Finanzierung an einem bestimmten Projekt aufgerufen wird, auch: „Schwarmfinanzierung".

Derivat

Finanzinstrument, das die Wertentwicklung eines Basiswerts abbildet und dessen Wertentwicklung somit unmittelbar oder mittelbar von der Preisentwicklung des Basiswerts abhängt.

Dezentralisierung

Organisatorische Verteilung von Aufgaben und Zuständigkeiten auf verschiedene Stellen.

Dezimalsystem

Auf der Grundzahl 10 aufbauendes Zahlensystem.

Differenzausgleich

Auch: Barausgleich oder Cash Settlement. Dabei findet mit der Ausübung einer Option kein Erwerb bzw. keine Veräußerung des Basiswertes statt, sondern es wird der Differenzbetrag zwischen Basispreis und aktuellem Marktwert des Basiswertes an den Optionsscheininhaber ausgezahlt.

Differenzgeschäft

Termingeschäft, bei dem die Vertragsparteien nicht an dem Erwerb des Basiswerts interessiert sind, sondern am Kurs- oder Preisunterschied zwischen dem Wert am Tag des Geschäftsabschlusses und dem aktuellen Marktwert am Erfüllungstag.

Difficulty

Schwierigkeitsgrad für das Finden neuer Blocks einer Kryptowährung.

Distributed-Ledger-Technologie

„Technik verteilter Kassenbücher"; Technik, bei der Informationen auf verschiedenen Systemen gehalten, verifiziert und erforderlichenfalls durch das Schaffen von Konsens angepasst werden.

Dividende

Anteil des Gewinns, den eine Aktiengesellschaft jährlich an ihre Aktionäre ausschüttet.

Double-Spending

Doppeltes Ausgeben der gleichen Einheiten einer digitalen Währung.

E-Geld

Elektronisches Geld; jeder elektronisch – auch magnetisch – gespeicherte monetäre Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge durchzuführen, und der auch von anderen Personen als dem Emittenten angenommen wird (gesetzliche Definition).

Einlagensicherung

Gesetzliche und freiwillige Maßnahmen, die in einer Bankenkrise die Gläubiger von Kreditinstituten vor dem Verlust ihrer Bankguthaben bewahren sollen.

Emittent

Herausgeber von Wertpapieren

Emittentenrisiko

Risiko, dass der Herausgeber von Wertpapieren nicht mehr in der Lage ist, seinen Zahlungsverpflichtungen nachzukommen.

Equity Token

Unterart des Security Token; repräsentiert einen Anteil am zugrunde liegenden Unternehmen, wobei die Inhaber Anteilsrechte am Vermögen des Unternehmens und des Unternehmensgewinns erwerben und ein Stimmrecht erhalten.

Equity Token Offering - ETO

Herausgabe von Equity Token zur Unternehmensfinanzierung.

Exchange

engl. für „Börse"

Exchange Traded Fund - ETF

Passiv verwalteter Indexfonds, der die Wertentwicklung eines Indexes abbildet.

Exchange Traded Note - ETN

Börsengehandeltes Wertpapier in Form von Inhaberschuldverschreibungen einer Bank, bei dem die Wertentwicklung eines zu Grunde liegenden Referenzindexes bzw. der zu Grunde liegenden Kryptowährung im Verhältnis 1:1 oder mit einer Hebelwirkung abgebildet wird.

Exchange Wallet

Wallet, bei der der Nutzer seinen Private Key von der jeweiligen Börse („Exchange") verwalten lässt.

Fiatgeld

Geld, das zum gesetzlichen Zahlungsmittel erklärt und von einer Zentralbank ausgegeben wird. Sein Wert basiert größtenteils auf dem Vertrauen der Öffentlichkeit in seinen Herausgeber und nicht auf dem Geldzeichen an sich.

FIFO-Regelung

First In First Out-Regelung; jegliche Verfahren der Speicherung, bei denen diejenigen Elemente, die zuerst gespeichert wurden, auch zuerst wieder aus dem Speicher entnommen werden. Standardmäßiges Verfahren zur Besteuerung beim Verkauf von Wertpapieren, bei Teilverkäufen identischer Wertpapiere aus einem Depot werden die zuerst gekauften Wertpapiere auch zuerst wiederverkauft.

Fork

Deutsch: „Gabelung"; bezeichnet die Weiterentwicklung einer Open Source Software und die hierdurch herbeigeführte Abspaltung von der Original- Software.

Future

Standardisiertes, börsengehandeltes, unbedingtes Termingeschäft auf einen Basiswert.

Geld

Allgemein anerkanntes Tausch- und Zahlungsmittel, auf das sich eine Gesellschaft verständigt hat und das als gesetzliches Zahlungsmittel zur Tilgung von Schulden mit rechtlicher Wirkung dient.

General Purpose

Bezeichnung für blockchainbasierte Payment Token dafür, dass man sie universell einsetzen kann und dass sie sich nicht nur als Tauschmittel auf ein bestimmtes Gut beziehen.

Glattstellung

Abschluss eines zu einem bestehenden Geschäft gegenläufigen Geschäfts, wodurch das ursprüngliche Geschäft neutralisiert wird, so dass faktisch keinerlei Verpflichtung aus den Kontrakten mehr besteht.

Hard Fork

Änderungen an der Blockchain, die nicht rückwärtskompatibel sind und dazu führen, dass die Blockchain in zwei Ketten weitergeführt sind.

Hard Wallet

Elektronisches Gerät zur Sicherung des Private Keys und zur Verwaltung von Kryptowährung.

Hash

Engl. für „Streuwert"; digitaler Code, der nach Anwendung einer Hashfunktion als Ergebnis herauskommt.

Hash Baum

Baumförmige Struktur aus Hashwerten von Datensätzen, auch „Merkle Tree" genannt.

Hashfunktion

Funktion, die eine große Eingabemenge auf eine kleinere, festgelegte Ausgabemenge abbildet.

Hashing

Prozess, bei dem eine große Eingabemenge auf eine kleinere, festgelegte Ausgabemenge abgebildet wird, abgeleitet von der engl. Bedeutung für „zerhacken".

Hash Power

Geschwindigkeit, mit der die Rechenoperationen bei der Erschließung eines neuen Blocks durchgeführt werden. Der Begriff wird sowohl zur Bezifferung der Leistungsfähigkeit eines Computers, als auch zur Geschwindigkeitsangabe der Datenverarbeitung im Blockchain-Netzwerk verwendet und daher als Maßeinheit für die Rechenleistung des Bitcoin-Netzwerks angesehen.

Hash Rate

Synonym für „Hash Power".

Header

Teil des Blocks einer Blockchain, in dem u. a. der Hash des vorigen Blocks und die sog. Nonce enthalten sind.

Hebelwirkung

Bezeichnet bei Derivaten den Effekt, dass die prozentuale Wertveränderung des Derivats größer ist als die verursachende prozentuale Wertveränderung des Basiswertes. Auch: Die Erhöhung der Rendite durch den Einsatz von Fremdkapital.

Hedge-Geschäft

Absicherungsgeschäft

Hedging

Absicherung von Wertpapierpositionen gegen eine negative Kursentwicklung durch den Kauf bzw. Verkauf von Derivaten, die geeignet sind, von derselben Kursentwicklung zu profitieren.

Hot Wallet

Wallet, die auf einem Endgerät läuft, das mit dem Internet verbunden ist.

Index

Kennziffer zur Darstellung von Veränderungen bestimmter Größen im Zeitablauf. Börsenindizes geben die Veränderung der Entwicklung einer bestimmten Zahl ausgewählter Finanzinstrumente über einen bestimmten Zeitraum an.

Initial Coin Offering - ICO

Finanzierungsform für Geschäftsmodelle, die auf der Blockchain-Technologie beruhen, auch Initial Public Coin Offering (IPCO) oder Token Sale genannt.

Initial Public Offering - IPO

Börsengang, bei dem erstmalig Aktien eines Unternehmens öffentlich zum Kauf angeboten werden.

intrinsisch

„Von innen heraus" oder „einer Sache innewohnend"; im Zusammenhang mit Zahlungsmitteln kann der intrinsische Wert als der Materialwert betrachtet werden.

Kassageschäft

Börsengeschäft, das sofort, spätestens aber am zweiten Börsentag nach Geschäftsabschluss, zu erfüllen ist.

Kollision

Bezeichnung dafür, dass beim Hashing unterschiedlichen Eingabedaten derselbe Hashwert zugeordnet wird.

Kommanditist

Gesellschafter einer Kommanditgesellschaft, dessen Haftung auf seine Einlage beschränkt ist.

Komplementärwährung

Ein Zahlungsmittel, das durch die Vereinbarung innerhalb einer Gemeinschaft, etwas zusätzlich neben dem offiziellen Geld als Tauschmittel zu akzeptieren, ergänzenden Charakter hat, aber kein gesetzliches Zahlungsmittel ist.

Konsens

Übereinstimmung; in Bezug auf Kryptowährungen die gemeinsame Einigung auf eine identische Version der verteilten Datenbank in Form der Blockchain.

Konsensmechanismus

Algorithmus, der eine Einigung über den Status eines Netzwerkes zwischen seinen Teilnehmern erzielt.

Kontrahent

Vertragspartner, Gegenpart

Kontrakt

Vertrag

Konvertibilität

Die Eigenschaft einer Währung, unbegrenzt in andere Währungen getauscht zu werden.

Korrelation

Wechselbeziehung; beschreibt den Zusammenhang zwischen verschiedenen Messgrößen.

Kryptoasset

Vermögenswert, der per dezentral organisierter Distributed-Ledger-Technologie abgebildet wird.

Kryptogeld

Digitale Zahlungsmittel, die auf kryptographischen Werkzeugen wie Blockchains und digitalen Signaturen basieren.

Kryptografie

Teilgebiet der Kryptologie, das sich mit dem Verschlüsseln von Informationen befasst.

Kryptowährung

Währung, die auf kryptografischen Algorithmen basiert.

Kryptowert

Digitale Darstellung eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann (gesetzliche Definition).

Leitwährung

Eine Währung innerhalb eines internationalen Währungssystems, die als internationales Zahlungs- und Reservemittel sowie als internationale Anlagewährung sowie als Recheneinheit zur Bestimmung des Wertes aller Währungen verwendet wird.

long

Als „Long-Position" wird die Käufer-Position in einem Handelsgeschäft bezeichnet, allgemein wird bei Finanzinstrumenten mit „long" jede Position bezeichnet, bei der der Inhaber von einer Wertsteigerung des Finanzinstruments profitiert.

Margin

Sicherheitsleistung für Börsentermingeschäfte

Margin Call

Aufforderung zur Leistung eines Nachschusses auf das Marginkonto.

Marktkapitalisierung

Bezeichnung für den rechnerischen Gesamtwert der Anteile eines börsennotierten Unternehmens am Kapitalmarkt. Zu seiner Ermittlung werden die im Umlauf befindlichen Anteile mit dem Kurs der Anteile multipliziert.

Marktportfolio

Theoretisches Konstrukt, das alle am Markt existenten, risikobehafteten Vermögensgegenstände beinhaltet.

Marktrendite

Die Rendite des Marktportfolios, des Gesamtmarkts oder eines relevanten Teilmarkts, z.B. des deutschen Aktienmarktes.

Marktrisiko

Risiko finanzieller Verluste aufgrund der Veränderung von Marktpreisen.

Merkle Root

Wurzel des Hash Baumes bzw. Merkle Trees, die alle Informationen über jeden einzelnen Transaktionshash, der auf dem Block existiert, enthält.

Mobile Wallet

Auf einem mobilen Endgerät (z.B. Smartphone, Notebook) gespeicherte Softwareapplikation zur Sicherung des Private Keys.

Mind Wallet

Wenn jemand den Private Key auswendig lernt und ihn dann ausschließlich in seinem Gedächtnis abspeichert, spricht man von einer „Mind Wallet".

Mining

Das Schaffen neuer Blöcke in der Blockchain durch Lösen eines komplexen mathematischen Problems.

Mining-Pool

Zusammenschluss mehrerer (professioneller) Miner oder Institutionen zur Erhöhung der Hash-Rate.

Nichtabstreitbarkeit

Verbindlichkeit; sie erfordert, dass im Nachhinein kein unzulässiges Abstreiten durchgeführter Handlungen möglich ist.

Node

Knotenpunkt, der die gesamte Blockchain speichert.

Nonce

Abk. für „used only once" oder „number used once". Eine zufällig generierte Zahlen- oder Buchstabenkombination, die nur ein einziges Mal in dem jeweiligen Kontext verwendet wird.

Open Source

Bezeichnung für eine Software, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann.

Orphan Block

„Verwaister" Block, der letzte Block der Kette, die bei einer Fork nicht weitergeführt wird.

over the counter – OTC

Direkt-Handel ohne Einschaltung einer Börse.

Paper Wallet

Stück Papier, auf das der Nutzer sich den Private Key notiert hat.

Payment-Token

Auch: Zahlungs-Token; Token, die neben der reinen Zahlungsfunktion keine weiteren Funktionalitäten besitzen.

Private Key

Privater Schlüssel, ein geheimer Datenblock, der über eine kryptografische Signatur das Recht beweist, Coins einer bestimmten Wallet ausgeben zu dürfen; vergleichbar mit einer PIN.

Proof-of-Stake (PoS)

Verfahren zur Herstellung von Konsens, ohne dass neue Einheiten geschaffen werden, bei dem der Anteil (engl.: „stake") eines Nutzers an der gesamten Menge an Tokens ausschlaggebend ist.

Proof of Work (PoW)

Verfahren zur Herstellung von Konsens durch Erbringung eines Arbeitsnachweises, indem ein mathematisches Rätsel durch einen Computer gelöst werden muss.

Pseudonymisierung

Das Ersetzen des Namens und anderer Identifikationsmerkmale einer Person durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren, wobei die Daten so zusammengeführt werden können, dass der Name im Nachhinein wieder zugeordnet werden kann.

Public Key

Empfangsadresse der Wallet, an die Zahlungen gesendet werden können.

Rechnungseinheit

Dem internationalen Geldverkehr zugrunde gelegte, künstlich konstruierte Einheit, in der Werte und Preise ausgedrückt werden.

Repräsentativgeld

Geld, bei dem es sich nicht um den Gegenstand selbst handelt, sondern um eine verbriefte Form, d.h. das staatliche und gesetzlich garantierte Versprechen, den „Brief" jederzeit eintauschen zu können.

Schuldverschreibung

Anleihe

Security Token (Anlage-Token)

Wird von dem englischen Begriff „Security" für Wertpapier abgeleitet. Token ohne operative Funktion für die Blockchain, ihr Hauptziel ist es, Investitionsgewinne zu realisieren.

Security Token Offering - STO

Unterfall eines ICOs, bei dem Security Token herausgegeben werden.

Seignorage Share

Stable Coin mit einer arithmetischen Absicherung ohne Hinterlegung eines Basiswerts, bei dem automatisierte An- und Verkauf-Algorithmen für Kursstabilität sorgen sollen.

short

Als „Short-Position" wird die Verkäuferposition in einem Handelsgeschäft bezeichnet. Allgemein wird bei Finanzinstrumenten mit „short" jede Position bezeichnet, bei der der Inhaber von einem Wertverlust des Finanzinstruments profitiert.

Skalierbarkeit

Fähigkeit eines Systems oder Prozesses zum Wachstum.

Smart Contract

„Intelligente" Verträge mit Transaktionsbedingungen in Form von Wenn-Dann-Regeln, die auf Computerprotokollen basieren und selbstausführend sind.

Soft Fork

Kleinere Änderungen an der Blockchain, die rückwärtskompatibel sind und nicht zu einer Fork führen.

Soft Wallet

Wallet in Form einer Software, dabei wird der Private Key mit einem Passwort auf einem Computer oder einer App gesichert.

Sparer-Pauschbetrag

Freibetrag, der Kapitaleinkünfte bis zur Höhe von derzeit 801 Euro im Rahmen der Einzelveranlagung bzw. 1.602 Euro bei zusammenveranlagten Personen pro Jahr steuerfrei stellt.

Spekulationsfrist

Frist, die darüber entscheidet, ob ein bei einem privaten Veräußerungsgeschäft erzielter Gewinn versteuert werden muss oder nicht.

Spekulationsgeschäft

Bezeichnet im Steuerrecht die Veräußerung von privaten Vermögensgegenständen.

Stable Coin

(Vermeintlich) Stabiler Wert in digitaler Form, der sich durch ein festes Verhältnis zu einem Basiswert auszeichnet und dessen Wertentwicklung im Idealfall exakt nachbilden soll.

Staking

Der Prozess des Haltens und Sperrens bzw. Entsperrens von Anteilen in einer Wallet, um Transaktionen auf der Blockchain zu validieren und hierfür eine Belohnung zu erhalten.

Stop-Loss-Order

Verkaufsauftrag, der erst aktiviert wird, wenn der Kurs des Wertpapiers die vom Anleger angegebene Schwelle erreicht oder unterschreitet.

Swap

In der Regel außerbörslich gehandeltes Finanzderivat, dessen Grundlage die vertragliche Vereinbarung zum Austausch von Zahlungsströmen ist.

Termingeschäft

Geschäft, bei dem die Bedingungen, die beim Abschluss des Vertrages festgelegt wurden, erst zu einem späteren Termin erfüllt werden müssen

Terrawattstunde

Abk.: ThW; physikalische Maßeinheit für große Strommengen; 1 TWh = 1 Billion Wattstunden (Wh) = 1 Milliarde Kilowattstunden (kWh)

Token

Digitaler Vermögenswert mit einer breiteren Funktionalität als Coins, der keine eigene Blockchain besitzt, sondern eine bereits vorhandene nutzt. Er kann als eine Art Gutschein betrachtet werden, der wiederum ein bestimmtes Wirtschaftsgut oder auch einen Vermögenswert repräsentiert. Der Begriff wird fälschlicherweise oft synonym für „Coin" verwendet.

Token Sale

siehe Initial Coin Offering

Tokenisierung

Digitalisierte Abbildung eines realen (Vermögens-)Wertes inklusive der in diesem Wert enthaltenen Rechte und Pflichten sowie dessen hierdurch ermöglichte Übertragbarkeit. In der Computerlinguistik bezeichnet der Begriff die Segmentierung eines Textes in Einheiten, so kann Tokenisierung auch als „Stückelung" verstanden werden.

Utility Token

„Nutzungs-Token"; Token, die eine bestimmte Funktion in einem Netzwerk einnehmen und vergleichbar mit Gutscheinen für eine bestimmte Leistung sind.

volatil

schwankend

Währung

Im weiteren Sinne die Verfassung und Ordnung des gesamten Geldwesens eines Staates. Allgemein wird mit dem Begriff auch das gesetzliche Zahlungsmittel eines Landes oder der Länder einer Währungsunion bezeichnet.

Wallet

Digitale Geldbörse für Kryptowährungen, die mit einem Passwort-Manager verglichen werden kann.

Wertpapierprospekt

Ein vor jedem öffentlichen Angebot von Wertpapieren und vor jeder Börsenzulassung an einem geregelten Markt innerhalb des Europäischen Wirtschaftsraums (EWR) zu veröffentlichender Prospekt, der bestimmte, gesetzlich vorgeschriebene Informationen für Anleger enthalten muss.

White Paper

Bei ICOs regelmäßig bereitgestelltes Informationsblatt, das nicht gesetzlich reguliert und in Form und Inhalt beliebig gestaltbar ist, vergleichbar mit einer Art Businessplan.

Zentralbankgeld

Das von der Zentralbank geschaffene Geld, das in Form von Sichtguthaben bei der Zentralbank oder als Bargeld in Form von Banknoten und Münzen existiert.

Zertifikat

Schuldverschreibung, deren Wert von der Wertentwicklung eines oder mehrerer anderer Basiswerte abhängt.

Zweckgesellschaft

Synonym: Special Purpose Vehicle (SPV); eine Gesellschaft, die zur Abwicklung besonderer Geschäfte, zum Beispiel der Wertpapieremission, gegründet und nach Erreichen des Geschäftszieles wieder aufgelöst wird.

Zweitmarkt

Keiner staatlichen Kontrolle unterliegender Sekundärmarkt zum Handel von Anteilen an geschlossenen Fonds oder anderen Vermögensgegenständen während der Laufzeit der Anlage.

Impressum

Texte: Sarah Lemke und Christian Hammer

Stand: August 2022