Kryptographie, kryptographisches Verfahren
ist ein Überbegriff für alle Verfahren, die Informationssicherheit von Daten gewährleisten sollen, insbesonders den Schutz vor unbefugtem Lesen und nachträglicher Manipulation.

Hashfunktion, kryptografische
ist ein kryptographisches Verfahren, welches aus einem Datensatz einen Prüfwert, genannt Hashwert, errechnet.

Der Ausgangsdatensatz kann hierbei ein einzelnes Wort, aber auch ein ganzes Dokument, mit Bildern und interaktiven Grafiken sein.

Eine, momentan dem Stand der Technik entsprechende, Hashfunktion ist SHA-256 (Secure Hash Algorithm). Sie erzeugt unabhängig von der Größe der Ausgangsdaten einen eindeutig zuordbaren Hashwert mit einer fixen Länge von 64 Stellen.

Der Hashwert des Wortes „Apfel" nach SHA-256 lautet beispielsweise „2c89aa13613e60234db7359fc844738e5d372d2d50ff3ffe30e248110313f8ea". Dieser Hashwert kann nicht in den Ausgangsdatensatz „Apfel" zurückgerechnet werden, sondern ist nur ein Prüfwert.

Das „Verhashen" ist von der Verschlüsselung von Daten zu unterscheiden.

Hashwert
ist eine Art Fingerabdruck von Daten und wird mit einer Hashfunktion erzeugt. Der Hashwert kann, ähnlich einem Fingerabdruck, eindeutig einem Datensatz zugeordnet werden. Eine Änderung des Datensatzes führt zwangsläufig auch zu einer Änderung des zugehörigen Hashwertes. Somit kann durch Abgleich des Hashwerts sehr leicht bestimmt werden, ob die gegenständlichen Daten im Nachhinein verändert wurden.

Verschlüsselung
ist ein kryptographisches Verfahren, mit welchem „Klartext", durch einen geheimen wählbaren Schlüssel, in eine unverständliche Zeichenfolge umgewandelt werden kann. Eine verschlüsselte Nachricht kann nur durch den geheimen Schlüssel wieder entschlüsselt und eingesehen werden.

Die zu verschlüsselnden Daten müssen nicht zwingend Textnachrichten sein. Alle denkbaren digitalen Daten, inklusive Bilder, Videos oder Musik, können verschlüsselt werden.

Handy-Signatur
Die österreichische Handy-Signatur ist eine qualifizierte elektronische Signatur. Sie ist der eigenhändigen Unterschrift gleichgestellt.

Elektronische Signatur, qualifizierte
Eine qualifizierte elektronische Signatur wird einem Dokument zum Zweck der Authentifizierung beigefügt. Die elektronische Signatur ermöglicht die Überprüfung, ob das Dokument tatsächlich vom angegebenen Signator stammt und ob es seit der Signatur verfälscht wurde.

Eine qualifizierte elektronische Signatur erfüllt das rechtliche Erfordernis der Schriftlichkeit, weswegen grundsätzlich alle Verträge, die keine zusätzlichen Formerfordernisse verlangen, rechtsgültig elektronisch signiert werden können.

Die österreichische Handy-Signatur ist eine qualifizierte elektronische Signatur.

Datensatz
ist eine Gruppe von inhaltlich zusammengehörenden Daten, wie etwa die Artikelnummer und Artikelbezeichnung eines Produkts.

Personenbezogene Daten

sind Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (zB Name, Kontaktdaten, Rechnungsdaten). Um festzustellen, ob eine natürliche Person identifizierbar ist, sind alle Mittel zu berücksichtigen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine Person zu identifizieren. Darunter fällt etwa auch Tracking durch Cookies oder Device-Fingerprinting. Der Personenbezug wurde vom EuGH in der Vergangenheit eher weit gefasst und umfasst auch dynamische IP-Adressen.

Tracking

kommt aus dem Englischen und bedeutet „Verfolgung". Dabei wird die Spur eines Internet-Nutzers verfolgt und dieser fortlaufend identifiziert.

Das eigentliche Ziel von Trackingdiensten ist zumeist Online-Marketing bzw Direktwerbung. Hierbei wird mithilfe von gesammelten Nutzerdaten ein eindeutiges Profil zu einem bestimmten Nutzer erstellt und beispielsweise in Cookies auf dem Endgerät des Nutzers abgespeichert. Tracking kann jedoch auch ohne Cookies erfolgen, indem etwa durch Device-Fingerprinting abgefragt wird mit welchem Gerät, von wo und mit welchen spezifischen Geräteeinstellungen, der Nutzer im Web surft.

Cookies

sind kleine Textdateien, die auf dem Gerät des Benutzers abgespeichert werden. Sie dienen zumeist der Wiedererkennung des Nutzers (siehe Tracking), sowie der Speicherung temporärer Daten, wie etwa den Produkten im Warenkorb eines Online-Shops.

Blockchain
Liste von Datensätzen, die mit einem kryptographischen Verfahren (siehe auch Hashfunktion), miteinander verkettet werden.

Jeder Block (Datensatz) in der Liste enthält dabei, neben den Transaktionsdaten, den Hashwert des vorhergehenden Blocks, wodurch eine durchgehende Kette an zusammenhängenden Blöcken entsteht, die im Nachhinein grundsätzlich nicht mehr verändert werden kann.
Diese Datenstruktur wird dezentral bei jedem Teilnehmer des Blockchain-Netzwerks zur Gänze und transparent gespeichert, sowie ständig aktualisiert.

Ein Blockchain-Netzwerk kann öffentlich oder privat ausgestaltet sein. Während bei der öffentlichen Blockchain jeder teilnehmen kann, ist die private Blockchain bestimmten Teilnehmern vorbehalten und weist einen gewissen Grad an Zentralisierung auf.

Mining-Prozess

Neue Blöcke der Blockchain können nicht einfach erschaffen werden, sondern müssen durch ein vorbestimmtes Verfahren, genannt Mining, errechnet bzw geschürft werden. Hierbei wird die Authentizität von neuen Transaktionen überprüft und diese – sofern sie authentisch sind – in einem neuen Block zusammengefasst. Anschließend wird für den neuen Block ein aufwendiger Prüfwert errechnet und der gesamte neue Block, inklusive Prüfwert, mit der bisherigen Blockchain in einem Hashwert verkettet. Dieser neue Hashwert bildet wiederum die Grundlage für zukünftige Blöcke, wodurch eine fortlaufende Kette entsteht.

Miner

sind quasi die „Netzbetreiber" der Blockchain. Sie stellen dem Netzwerk ihre Rechenleistung für den Mining-Prozess zur Verfügung und halten das Netzwerk durch ständige Aktualisierung der Blockchain aufrecht. Für die dezentrale Ausrichtung der Blockchain sind Miner unerlässlich. Als wirtschaftlichen Anreiz für dieses aufwendige Rechenverfahren erhalten Miner eine Belohnung, den sogenannten Block-Reward.

Bitcoin

ist eine virtuelle Währung und basiert auf der Blockchain. Er ist ein Currency bzw Payment Krypto-Asset und hat in erster Linie Tauschmittelfunktion. Obwohl Bitcoin momentan der bekannteste und verbreitetste Anwendungsfall der Technologie ist, kann er nicht mit der Blockchain per se gleichgesetzt werden, sondern ist bloß einer von vielen möglichen Ausprägungen der Blockchain-Technologie.

Smart Contract

ist kein Vertrag im rechtlichen Sinn, sondern lediglich eine selbstausführende Abfolge von fixen Vorgängen. Diese Abfolgen können als Quellcode auf bestimmten Blockchains, wie etwa der Ethereum-Chain, gespeichert und durch vorbestimmte Ereignisse ausgelöst und ausgeführt werden.

Dadurch können sich die Nutzer ohne jegliches Vertrauen zueinander sicher sein, dass ein beabsichtigter Leistungsaustausch auch tatsächlich stattfindet. Smart Contracts können auch zivilrechtliche Verträge ausführen. -

Digitales Asset

beschreibt alle digitalen Vermögenswerte, die konsumiert oder sonst verwendet werden können. Hierzu zählen Krypto-Assets, aber auch Bilder, Musik- oder Computerprogramme. Im Gegensatz zu Krypto-Assets sind digitale Assets nicht auf die Blockchain-Technologie beschränkt, sondern technologieneutral. Trotzdem wird dieser Term häufig, gleich wie der Begriff Krypto-Asset, verwendet.

Krypto-Asset

Überbegriff für alle Vermögenswerte auf Basis der Blockchain. Diese Vermögenswerte müssen nicht zwingend eine Tauschmittelfunktion innehaben, sondern können auch Genussrechte verkörpern, oder als Grundlage für Wertpapieremissionen dienen, weswegen man verschiedene Typen von Krypto-Assets unterscheidet.

Virtuelle Währung

ist ein Ökosystem von digitalen Assets mit Tauschmittelfunktion, welches bestimmte rechtliche Bedingungen erfüllt. Es ist der einzige legaldefinierte Begriff in diesem Bereich (vgl Art 3 Z 18 Richtlinie (EU) 2018/843). Obwohl die Definition auffallend technologieneutral ist, hatte der Unionsgesetzgeber vor allem Bitcoin, als archetypische Ausprägung der Blockchain-Technologie, vor Augen.

Coins

fallen in die Übergruppe der Krypto-Assets und sind der immanente Wertträger einer Blockchain. Sie werden laufend durch Mining erzeugt und können mittels Transaktion elektronisch übertragen werden. Die Transaktion von Coins wird durch den Mining-Prozess verifiziert und in einem neuen Block transparent und unveränderlich abgespeichert.

Coins können verschiedene Funktionen haben (siehe Krypto-Assets, verschiedene Typen). Die rechtliche Einordnung eines Coin hängt daher von seiner spezifischen Ausgestaltung ab.

Token

fallen in die Übergruppe der Krypto-Assets und sind Wertträger, die auf einer fremden Blockchain aufsetzen (zb auf der Ethereum Blockchain). Im Gegensatz zu Coins werden sie nicht durch Mining geschürft, sondern idR von einem Unternehmen einmalig erzeugt.

Token können, ebenso wie Coins, verschiedene Funktionen haben (siehe Krypto-Assets, verschiedene Typen). Die rechtliche Einordnung eines Tokens hängt daher von seiner spezifischen Ausgestaltung ab.

Krypto-Assets, verschiedene Typen

In der Regel werden momentan drei verschieden Typen von Krypto-Assets unterschieden:

(i) Currency bzw Payment Krypto-Assets haben in erster Linie Tauschmittelfunktion und können gegen Waren und Dienstleistungen eingetauscht werden. Beispiele sind Bitcoin, Litecoin und Monero.

(ii) Security bzw Investment Krypto-Assets sind traditionellen Finanzinstrumenten, wie Aktien, nachempfunden und übernehmen idR ähnliche Funktionen. So können beispielsweise auch gesellschaftsrechtliche Stimmrechte auf einer Blockchain übertragen werden.

(iii) Utility Krypto-Assets sollen dem Inhaber einen Nutzen in Hinblick auf ein bestimmtes Produkt oder eine Dienstleistung zu verschaffen. Sie können zB Zugang zu einer Online-Plattform des Emittenten gewähren.

Die Grenze zwischen diesen Typen verläuft aber fließend. Es gibt auch Mischformen. Ferner dient diese Kategorisierung alleine der Strukturierung des Diskurses. Die rechtliche Einordnung hängt stets von der konkreten Ausgestaltung des Krypto-Assets ab.

ICO/ITO (Initial Coin/Token Offering)

Bei einem ICO/ITO handelt es sich um eine Form der Unternehmens- oder Projektfinanzierung via Crowdfunding auf Grundlage der Blockchain. Diese Form der Finanzierung ist durchaus mit einem klassischen Börsengang, bei welchem erstmals Aktien eines Unternehmens an einer Börse angeboten werden, vergleichbar.

Bei der Durchführung eines ICO/ITO werden Coins/Tokens, im Austausch gegen Geld oder virtuelle Währungseinheiten, angeboten. Diese angebotenen Coins/Tokens stehen in Verbindung zu dem zu finanzierenden Unternehmen oder Projekt des Organisators. Sie können beispielsweise eine Beteiligung an einem Start-up darstellen, einen Anspruch auf einen zukünftigen Gewinn versprechen oder sonstige Genussrechte verkörpern.

Stablecoin
sind Currency Krypto-Assets die primär darauf abzielen, Preisstabilität zu gewährleisten. Um dieses Ziel zu erreichen, wird der Wert des Stablecoins an Vermögenswerte, wie etwa Fiat-Währungen oder börsengehandelte Rohstoffe, angebunden. Diese Vermögenswerte werden idR von einem Dritten verwahrt, wodurch Stablecoins zumeist zentral ausgerichtet sind. Ein Beispiel ist Facebook's Stablecoin Libra.

Blockchain-Forks

beschreibt die Abspaltung eines Teils der betroffenen Blockchain. Hierbei wird der Quellcode der ursprünglichen Blockchain modifiziert und auf dessen Basis eine neue Blockchain mit idR eigenem Netzwerk gestartet. So handelt es sich, beispielsweise bei Litecoin, um eine solche Abspaltung von der Bitcoin-Blockchain.

Forks sind herausfordernde Situationen für ein Blockchain-Netzwerk, weil sich durch die Abspaltung zumeist auch die Miner bzw mit ihnen die Rechenkraft aufteilt und daraus verschiedene Komplikationen entstehen können.

Altcoins:
sind Coins, die auf einem Blockchain-Quellcode basieren, der zwar von Bitcoin mittels Fork abgespalten wurde, aber immer noch einen hohen Grad an Ähnlichkeit aufweist. Prominente Beispiele sind Dash und Litecoin. Die Unterscheidung zwischen Coins und Altcoins hat keine rechtliche Relevanz.

Dezentralität
Wenn Daten lokal an mehreren Stellen eines Netzwerks, und nicht gebündelt an einer Stelle, gespeichert bzw verarbeitet werden, spricht man von Dezentralität.

Disruptive Technologien
sind Innovationen, die etabliertere Technologien und Verfahren in oftmals relativ kurzer Zeit verdrängen. In der Vergangenheit ersetzte beispielsweise die Erfindung des Webstuhls die händische Textilproduktion. Auch die Blockchain wird immer wieder als disruptive Technologie, mit großem Innovationspotenzial, bezeichnet.

Cyber Security, Cyberstaat
bedeutet für den Staat einerseits eine Verpflichtung zum Schaffen von technischen und rechtlichen Rahmenbedingungen für die Informationssicherheit von Daten und der informationellen Selbstbestimmung der Bürger. Es bedeutet jedoch gleichzeitig und gegensätzlich zur ersten Aufgabe, die Gefahrenabwehr und Aufrechterhaltung der öffentlichen Sicherheit bzw Ordnung, womit allfällige Grundrechtseinschränkungen einhergehen können, die, verfassungsrechtlich bzw grundrechtsdogmatisch, gedeckt sein müssen. Was Staaten jedoch aufgrund der Ausrichtung unseres liberalen Grundprinzips jedenfalls verwehrt bleibt,

ist eine flächendeckende Überwachung in allen Bezügen des Alltags, die durch den Digitalisierungsprozess, auch jetzt schon, ansatzweise möglich wäre.

Internet of Things (IoT), Internet der Dinge
beschreibt die zunehmende Vernetzung von intelligenten Gegenständen miteinander und dem Internet. Hierbei werden Computerteile in Alltagsgeräte verbaut bzw integriert, die eine selbständige Kommunikation mit anderen smarten Gegenständen ermöglichen.
Im Zusammenhang mit der Blockchain ergibt sich durch Verbindung dieser Technologien eine Fülle an Anwendungsmöglichkeiten. So könnte beispielsweise in einer Blockchain abgespeichert werden, ob die Kühlkette von Produkten eingehalten wurde und die Temperaturmessungen, sowie das Abspeichern der Werte, automatisch von den smarten Produkten vorgenommen wurden.

Künstliche Intelligenz (KI), Artificial Intelligence (AI)
beschreibt einen computergestützten Algorithmus, welcher der menschlichen Entscheidungsfindung in seiner Komplexität und Problemlösungskompetenz nahekommt bzw diese sogar übertreffen kann. Ähnlich, wie die menschliche Intelligenz über Jahre heranreifen muss, ist es nötig, eine KI mit einer ausreichenden Anzahl an Datensätzen zu trainieren, damit sie ein Stadium erreicht, wo eigenständig Probleme gelöst werden können (sog „maschinelles Lernen“ bzw „machine learning“).

Maschinelles lernen, Machine learning
Siehe Künstliche Intelligenz.

Big Data
ist grundsätzlich schlicht eine große Ansammlung von Daten. Große Datenbanken gab es zwar schon immer, jedoch hat sich die Rechenkraft in den letzten Jahren so sehr verstärkt, dass diese Datenmengen heutzutage anders ausgewertet und analysiert werden können als früher. So lassen Big-Data-Analysen beispielsweise Rückschlüsse auf Information von Personen zu, welche niemals direkt angegeben wurden, sondern sich nur durch smarte Auswertungen und Verbindung von Datensätzen ergeben. Dass solche Analysen auch Grundrechte berühren können, liegt auf der Hand.

Surveillance Capitalism, Überwachungskapitalismus
beschreibt ein System, in dem sich private Konzerne, durch Bündelung von Macht und Kontrolle im digitalen Raum, eine marktbeherrschende Stellung sichern, von der aus der digitale Lebensraum des Menschen beeinflusst und bewirtschaftet werden kann. In diesem System ist es nicht mehr vorrangig der Staat, der in die Grundrechte der Bürger eingreift, sondern handelt es sich um Private, mittels der von ihnen betriebenen Plattformen. Für die Nutzer besteht oft keine andere Möglichkeit, als sich den bestimmenden Kräften, die quasi-Monopole entwickelt haben, zu unterwerfen, wenn sie am „digitalen Ökosystem“ teilnehmen wollen. Insofern sind sie auf die Plattformbetreiber, als Intermediäre, angewiesen.