Teil I
Grundlagen

1. Kapitel
Grundlagen der Blockchain-Technologie und verwendete Begriffe

Literatur: *Bernt,* Kryptostrafrecht 101: zur strafrechtlichen Relevanz von Krypto-Assets, ÖJZ 2021, 924; *Bertel* in *Bergmann/Kalss* (Hrsg), Rechtsformwahl (2020) Kapitel 9: Verfassungsrechtlicher Vertrauensschutz und Rechtsformwahl; *Ebner/Kalss,* Die digitale Sammelurkunde – ein erster Schritt zur vollständigen Digitalisierung des österreichischen Wertpapierrechts, GesRZ 2020, 369; *Enzinger,* Mining von Kryptowährungen, SWK 2017, 1013; *Hanzl/Pelzmann/Schrag* (Hrsg), Handbuch Digitalisierung (2021); *Hanzl/Rubey,* Blockchain – frischer Wind im Gesellschaftsrecht? GesRZ 2018, 102; *Kreuzer,* Was ist eine Blockchain? CFOaktuell 2017, 109; *Kreuzer,* NFT – Non-Fungible Token, CFOaktuell 2021, 127; *Kucsko/Pabst/Tipotsch/Tyrybon,* NFT – Ein Selbstversuch, ecolex 2021, 495; *Miernicki,* Central Bank Digital Currencies als eine neue Form gesetzlicher Zahlungsmittel? ZFR 2021, 109; *Stadler/Chochola,* Erst Pläne für digitalen Euro, Der Standard 2020/42/01; *Varro,* Bitcoin-Mining: nicht steuerbares Glücksspiel? taxlex 2017, 399; *Völkel,* Initial Coin Offerings aus kapitalmarktrechtlicher Sicht, ZTR 2017, 97; *Völkel,* Privatrechtliche Einordnung der Erzeugung virtueller Währungen, ecolex 2017, 639; *Völkel,* Privatrechtliche Einordnung virtueller Währungen, ÖBA 2017, 385; *Völkel,* Vertrauen in die Blockchain und das Sachenrecht, ZFR 2020, 492.

Übersicht

I. Einheitliche Taxonomie

1.1 Seit dem Erscheinen der ersten Auflage dieses Handbuchs haben sich in der Praxis neue Begriffe etabliert. Neben digitalen Assets ist vermehrt von Kryptoassets die Rede. Im österreichischen Steuerrecht hat der Begriff der Kryptowährung[1] Niederschlag gefunden. Auf europäischer Ebene wurden die Begriffe des Kryptowerts[2], des vermögenswertereferenzierten Tokens[3], des E-Geld-Tokens[4] und des Utility Tokens[5] legaldefiniert. Weiters haben sich als neue Kategorie die Non-Fungible-Tokens (NFTs) entwickelt.[6] Zentralbanken denken über die Einführung von Central Bank Digital Currencies (CBDCs) nach. Asset Token, Fund Token, Pointer Token oder Security Token sind weitere Kategorien, die sich seit der ersten Auflage dieses Handbuchs am Markt etabliert haben. Wem es nicht aufgefallen ist: Der Begriff der virtuellen Währung[7] war in der Aufzählung noch gar nicht enthalten.

1.2 Um angesichts dieses Begriffsdschungels nicht den Überblick zu verlieren, wird in diesem Handbuch die nachfolgende Taxonomie vorgeschlagen:

1. **Digitales Asset** wird als Überbegriff verwendet für
   a) Kryptowert bzw Kryptoasset,
   b) Kryptowährung,
   c) sonstige fungible Token und
   d) Nicht-Fungible bzw Non-Fungible Token (NFT).
2. **Kryptowert** oder **Kryptoasset** bezieht sich auf die Legaldefinition unter MiCAR und umfasst damit
   a) vermögenswertereferenzierte Token,
   b) E-Geld-Token,
   c) Utility Token und
   d) andere Kryptowerte, wie etwa auch virtuelle Währungen.
3. **Virtuelle Währung** wird nur im definierten Sinn des FM-GwG verwendet.
4. **Kryptowährung** wird nur im definierten Sinn des EStG verwendet.
5. Sonstige **Fungible Token** bezieht sich auf sämtliche austauschbare, also fungible, Token, die nicht bereits als Kryptowert/Kryptoasset oder Kryptowährung erfasst sind, also bspw Asset Token, Fund Token, Pointer Token oder Security Token; allerdings

1 § 27b EStG.
2 Art 3 Abs 1 Z 5 MiCAR.
3 Art 3 Abs 1 Z 6 MiCAR.
4 Art 3 Abs 1 Z 7 MiCAR.
5 Art 3 Abs 1 Z 9 MiCAR.
6 Vgl Rz 17.1 ff.
7 Vgl Rz 8.1 ff.

ausschließlich im Hinblick auf das technische Trägermedium, also den von einem bestimmten Smart Contract verwalteten Token, nicht hingegen im Hinblick auf die schuldrechtliche Beziehung, die zwischen einem Halter solcher Token und einem Emittenten ggf existiert.

6. **Nicht-Fungible Token** oder **Non Fungible Token** oder **NFT** bezieht sich auf Token eines bestimmten technischen Standards, bei dem einzelne von einem Smart Contract verwaltete Token individualisierbar und dadurch von anderen Tokens unterscheidbar gemacht werden, die von demselben Smart Contract verwaltet werden; auch hier gilt, dass die schuldrechtliche Beziehung, die zwischen einem Halter von NFTs und einem Emittenten ggf existiert, nicht Gegenstand der Einstufung ist.
7. **CBDCs** werden in diesem Handbuch völlig ausgeklammert, weil die genaue Ausgestaltung derselben derzeit noch nicht absehbar ist. Aus primärrechtlicher Perspektive bestehen grds keine Bedenken gegen die Einführung eines digitalen Euros als neues gesetzliches Zahlungsmittel. Die mit der Ausgabe von Digitalwährung durch Zentralbanken einhergehende Entmaterialisierung des Geldes ist dabei das Zentrum der (mehr ökonomisch-politischen als rechtlichen) Diskussion.[8]

II. Grundlegende technische Begriffe

1.3 Wer sich mit der Blockchain-Technologie und seinen Anwendungsformen auseinandersetzt, der muss die Sprache der Branche sprechen. Diese Sprache hat sich im Lauf der letzten Jahre weiterentwickelt. Die nachfolgende Darstellung soll einen ersten Einstieg erleichtern und ggf auch als Nachschlagehilfe dienen.

1.4 **Adresse** bezeichnet eine alphanumerische Zeichenfolge, die verwendet wird, um die Quelle oder das Ziel einer → Transaktion auf einer → Blockchain oder einen → Smart Contract eindeutig zu identifizieren. Adressen werden erzeugt, indem bestimmte vorab festgelegte mathematische Schritte befolgt werden. Dies geschieht ohne Interaktion mit der → Blockchain und ohne Anschluss an das Internet. Bei der Erzeugung neuer Adressen wird durch Einhaltung der jeweiligen mathematischen Schritte ein passender → privater Schlüssel erzeugt.

1.5 **Block** bezeichnet eine Zusammenstellung von → Transaktionen. Durch die Aufnahme eines → Transaktionswunsches in einen Block in der → Blockchain wird dieser zur bestätigten → Transaktion.

1.6 **Block Reward** bezeichnet die im jeweiligen → Konsensmechanismus einer → Blockchain vorgesehene Menge des jeweils nativen → Coins, den eine Person durch eine → Transaktion auf eine eigene → Adresse für sich selbst neu schöpft, nachdem diese Person unter Beachtung des → Konsensmechanismus eine für das Bestehen der → Blockchain relevante Funktion erfüllt hat, etwa wenn die Personen im → Proof of Work einen neuen → Block erzeugt, oder im → Proof of Stake einen neuen → Block vorschlägt *(proposing)* oder die Gültigkeit eines vorgeschlagenen → Blocks belegt *(attesting)*.

1.7 **Blockchain** bezeichnet eine Datenbankstruktur zur Speicherung von → Transaktionen, die sich dadurch auszeichnet, dass sie nur (blockweise) um neue Einträge ergänzt werden

8 Vgl *Miernicki,* ZFR 2021, 109; *Stadler/Chochola,* Der Standard 2020/42/01.

kann. Bereits bestehende Einträge bzw → Blöcke in der Struktur sind unveränderlich in dem Sinne, dass jede Änderung die Datenintegrität zerstört und ein Manipulationsversuch sofort auffallen würde. Die Blockchain kann technisch als ‚append-only'-Datenbank beschrieben werden, also eine Datenbank, deren Datenstruktur nur durch das Anfügen neuer Transaktionsdaten veränderlich ist.

1.8 **Builder** bezeichnet eine Person, die aus dem → Mempool, also dem öffentlichen Pool unbestätigter → Transaktionswünsche, sowie anderen (über nicht-öffentliche Kanäle empfangene) → Transaktionswünschen einen → Block zusammenstellt. Im Rahmen der → Builder/Proposer Separation übermittelt der Builder den → Block mittels → Gateway an den → Proposer. Außerhalb der → Builder/Proposer Separation fällt die Funktion des Builders und jene des → Proposers beim → Miner (→ Proof of Work) bzw beim → Validator (→ Proof of Stake) zusammen.

1.9 **Coin** bezeichnet eine Einheit, die einer bestimmten → Blockchain immanent ist, die also im Gegensatz zum → Token konzeptuell und technisch im jeweiligen System verankert ist und die idR von Teilnehmern des jeweiligen → Konsensmechanismus selbst neu geschöpft wird. Für Details siehe Rz 1.113 ff.

1.10 **Cold Wallet** bezeichnet ein physisches Trägermedium wie bspw Papier, Plastik oder Metall auf dem eine → Adresse und der dazugehörige → private Schlüssel festgehalten sind.

1.11 **Decentralized Finance** *oder* **DeFi** bezeichnet die Nachbildung finanzieller Dienstleistungen, die mittels → Smart Contracts auf einer → Blockchain abgebildet werden, wobei nach Ansicht des Autors das entscheidende Merkmal darin besteht, dass die beteiligten Akteure nicht miteinander in vertragliche Schuldverhältnisse eintreten. Erfüllt eine DeFi-Anwendung diese Anforderung nicht, so handelt es sich bei den jeweiligen → Smart Contracts schlicht um Software, die ein Anbieter einsetzt, um seine Dienstleistung zu erbringen.

1.12 **Distributed Ledger Technology** *oder* **DLT** bezeichnet im Allgemeinen – beachte aber die Legaldefinition unter MiCAR[9] – eine Technologie, bei der die Aufzeichnung eines Datenbestandes nicht durch eine zentrale Instanz erfolgt, sondern unter mehreren → Nodes synchron gehalten wird. Beachte, dass es unter MiCAR nicht erforderlich ist, dass die DLT-Netzwerkknoten[10] von unterschiedlichen Personen betrieben werden, das heißt, unter MiCAR kann ein zentral verwaltetes System ebenso den Begriff der DLT erfüllen.

1.13 **DLT-Netzwerk** bezeichnet im Allgemeinen – beachte aber die Legaldefinitionen unter der MiCAR[11] – die Gruppe an → Nodes, die am jeweiligen → Konsensmechanismus einer → Blockchain teilnehmen.

1.14 **Fork** bezeichnet eine Änderung am → Konsensmechanismus der jeweiligen → Blockchain, wobei zwischen solchen Änderungen unterschieden wird, die dazu führen, dass die → Konsensmechanismen vor und nach der Änderung inkompatibel sind *(hard fork)* und solchen Änderungen, die nicht dazu führen *(soft fork)*. Beispiele für *hard forks* sind die

9 Art 3 Abs 1 Z 1 MiCAR.
10 Art 3 Abs 1 Z 4 MiCAR.
11 Art 3 Abs 1 Z 1 bis Z 4 MiCAR.

Abspaltung von Ethereum Classic von Ethereum oder Bitcoin Gold von → Bitcoin. Beispiele für *soft forks* sind einfache Softwareupdates.

Gateway bezeichnet eine Person, die von einer Mehrzahl an → Buildern → Blöcke entgegennimmt, um sie nach inhaltlicher Prüfung an → Proposer weiterzuleiten. Ein Gateway ist somit ein Intermediär zwischen → Builder und → Proposer. Diese Tätigkeit ist den vorzufindenden → Konsensmechanismen nicht immanent. **1.15**

Hot Wallet bezeichnet eine Software, die mit dem Internet verbunden ist, und die zur Verwaltung von → Adressen und → privaten Schlüsseln verwendet wird, um → Transaktionswünsche an das jeweilige → DLT-Netzwerk zu übermitteln, das eine bestimmte → Blockchain verwaltet. **1.16**

Knoten ist eine andere Bezeichnung für → Nodes in einem → DLT-Netzwerk. **1.17**

Konsensmechanismus bezeichnet die Vereinbarung zwischen den im → DLT-Netzwerk als → Nodes teilnehmenden Personen, wie sie untereinander Einigkeit darüber herstellen, wer als nächstes eine für das Fortbestehen der → Blockchain wesentliche Aufgabe wahrnimmt, etwa wer als nächstes bestimmt, ob und in welcher Reihenfolge → Transaktionswünsche aus dem → Mempool als bestätigte → Transaktionen in einem → Block aufgenommen werden. **1.18**

Maximal Extractable Value *oder* **MEV** (manchmal auch **Miner Extractable Value**) bezeichnet den Vorgang, bei dem → Builder oder → Proposer versuchen, zusätzlich zu → Transaktionsgebühren weitere Erträge zu erwirtschaften, etwa durch das Ausnutzen von Arbitragemöglichkeiten bei Interaktionen mit → DeFi-Anwendungen. **1.19**

Mempool bezeichnet den öffentlichen Pool an unbestätigten → Transaktionswünschen. Wird ein → Transaktionswunsch mittels → Wallet-Software an einen → Node öffentlich übermittelt, also nicht über private Kanäle direkt an → Builder, so wird dieser → Transaktionswunsch Teil des Mempools. **1.20**

Miner bezeichnet beim → Konsensmechanismus des → Proof of Work eine Person, welche die Bestimmungen des jeweiligen → Konsensmechanismus beachtet, um einen neuen → Block zu erzeugen und den damit einhergehenden → Block Reward sowie → Transaktionsgebühren zu vereinnahmen. **1.21**

Mining bezeichnet bei → Proof of Work den Prozess des Erstellens eines → Blocks an → Transaktionen unter Beachtung des jeweiligen → Konsensmechanismus der jeweiligen → Blockchain. Das Festhalten eines → Transaktionswunsches in einem → Block wird deshalb auch als Mining des jeweiligen → Transaktionswunsches bezeichnet. **1.22**

Mining Pool bezeichnet den Zusammenschluss mehrerer Personen, die ihre Rechenleistung bündeln wollen, um beim → Konsensmechanismus des → Proof of Work als Gruppe bessere Chancen zur Lösung des jeweiligen mathematischen Problems zu haben als jede Person für sich alleine, wobei die Abrede besteht, den → Block Reward und die → Transaktionsgebühren entsprechend der beigestellten Rechenleistung unter den Teilnehmern des Mining Pools aufzuteilen. **1.23**

Mnemonic Phrase bezeichnet eine zwölfstellige Wortfolge aus einem vordefinierten Wörterbuch an 2048 Wörtern, aus der durch bestimmte mathematische Verfahren eine **1.24**

Vielzahl an → Adressen für → Transaktionen auf einer → Blockchain errechnet werden können.

1.25 **Multi Signature Wallet** *oder* **Multi-Sig Wallet** bezeichnet eine → Wallet bei der zwei oder mehr → private Schlüssel zum → Signieren einer → Transaktion erforderlich sind bzw der → private Schlüssel in zwei oder mehr Teile aufgeteilt wird.

1.26 **Node** bezeichnet eine Person, die im Rahmen eines → DLT-Netzwerkes ein Computersystem betreibt, um unter Beachtung des → Konsensmechanismus gewisse für das Fortbestehen der → Blockchain erforderliche Aufgaben wahrzunehmen wie etwa das Speichern der Datenstruktur, das → Mining eines → Blocks beim → Proof of Work, das Vorschlagen eines neuen → Blocks *(proposing)* oder Belegen der Gültigkeit eines vorgeschlagenen → Blocks *(attesting)* beim → Proof of Stake.

1.27 **Non-Fungible Token** *oder* **NFT** bezeichnet einen technischen Standard, bei dem einzelne von einem → Smart Contract verwaltete → Token individualisierbar und dadurch von anderen → Token unterscheidbar gemacht werden, die von demselben → Smart Contract verwaltet werden.

1.28 **Oracle** bezeichnet eine natürliche oder juristische Person, die über das Internet Daten zur Verfügung stellt, die von → Smart Contracts für Berechnungen verarbeitet werden können.

1.29 **Paper Wallet** ist ein Unterfall der → Cold Wallet, bei dem Papier als Trägermedium dient.

1.30 **Peer-to-Peer** bedeutet, dass die Kommunikation in einem Computernetzwerk nicht über einen oder mehrere zentrale Knotenpunkte organisiert ist, sondern dass jeder → Node mit jedem anderen → Node unmittelbar und direkt Informationen austauschen kann. Auf diese Weise wird etwa ein → Transaktionswunsch, der bei einem → Node einlangt, an andere → Nodes im → DLT-Netzwerk weitergeleitet.

1.31 **Penalty** bezeichnet beim → Konsensmechanismus des → Proof of Stake eine Reduktion der als → Stake hinterlegten → Coins wegen der Missachtung des jeweiligen → Konsensmechanismus (Handlung oder Unterlassung).

1.32 **Pool unbestätigter Transaktionswünsche** ist eine andere Bezeichnung für → Mempool.

1.33 **Privater Schlüssel** bezeichnet eine alphanumerische Zeichenfolge, die benötigt wird, um einen → Transaktionswunsch mittels mathematischer Verfahren so zu → signieren, dass die darin beschriebene Verfügung über eine → Adresse auf der → Blockchain von → Nodes des jeweiligen → DLT-Netzwerk als authentisch akzeptiert wird, um schließlich als → Transaktion in einem → Block aufgenommen zu werden. Für Details siehe Rz 1.132 ff.

1.34 **Proof of Stake** *oder* **PoS** bezeichnet einen → Konsensmechanismus, an dem nur teilnehmen kann, wer bereit ist, seine Regeltreue durch das Einsetzen eines → Stakes zu bekräftigen, wobei zur Entscheidung über die Frage, wer als nächstes eine für das Fortbestehen der → Blockchain wesentliche Aufgabe wahrnehmen darf – um → Block Reward und → Transaktionsgebühren zu vereinnahmen – zunächst eine Mehrzahl an → Nodes eine gemeinsame Zufallszahl generieren, auf deren Basis aus der Liste an → Validatoren die nächste Person bestimmt wird. Für Details siehe Rz 1.108.

Proof of Work *oder* **PoW** bezeichnet einen → Konsensmechanismus, bei dem diejenige Person, der es als erstes gelingt, ein bestimmtes komplexes mathematisches Problem zu lösen, als nächstes eine für die → Blockchain wesentliche Aufgabe wahrnehmen darf – um letztlich → Block Reward und → Transaktionsgebühren zu vereinnahmen; für Details siehe Rz 1.105. **1.35**

Proposer bezeichnet eine Person, die durch Befolgung des jeweiligen → Konsensmechanismus versucht, die jeweilige → Blockchain um einen neuen → Block an Transaktionsdaten zu erweitern. Bei → Proof of Work wird der Proposer auch → Miner genannt, bei → Proof of Stake wird der Proposer auch → Validator genannt. Siehe auch Rz 1.100. **1.36**

Security Token bezeichnet → tokenisierte übertragbare Wertpapiere iSd MiFID II oder sonstige → tokenisierte Finanzinstrumente, bei denen nicht Papier, sondern → Blockchain-basierte → Token als Publizitätsmedium zum Einsatz gelangen. **1.37**

Security Token Offering *oder* **STO** bezeichnet die erstmalige Ausgabe von tokenisierten übertragbaren Wertpapieren oder tokenisierten Finanzinstrumenten nach MiFID II. **1.38**

Signatur bezeichnet das Ergebnis des → Signierens. **1.39**

Signieren bezeichnet den Vorgang, bei dem eine Person einen → Transaktionswunsch zur Verfügung über eine → Adresse dergestalt vervollständigt, dass ohne Preisgabe des → privaten Schlüssels Dritte in die Lage versetzt werden, zu erkennen, dass der → Transaktionswunsch von einer Person stammt, die tatsächlich Kenntnis vom → privaten Schlüssels hat. Für Details siehe Rz 1.132. **1.40**

Slashing bezeichnet bei der Implementierung des → Proof of Stake → Konsensmechanismus bei Ethereum eine bestimmte Form von → Penalty. **1.41**

Smart Contract bezeichnet ein Computerprogramm, dessen Programmcode in kompilierter Form in einem → Block auf einer → Blockchain gespeichert wird und mit dem im Rahmen von → Transaktionen über die dem jeweiligen Smart Contract zugeordnete → Adresse interagiert werden kann, um etwa Funktionen aufzurufen, mit denen Berechnungen durchgeführt oder der Inhalt von ebenfalls auf der Blockchain gespeicherten Variablen dauerhaft verändert werden kann. Der Einsatzzweck von Smart Contracts ist sehr vielfältig und reicht von der Verwaltung einfacher → Token, also der Neuschöpfung und Zuordnung zu → Adressen, bishin zu komplexen → DeFi-Anwendungen. Durch die Einbindung von → Oracles kann ein Smart Contract Vorgänge verarbeiten, die außerhalb der → Blockchain stattfinden. Zur rechtsgeschäftlichen Zurechnung von Smart Contracts siehe Rz 3.65. **1.42**

Stake bezeichnet beim → Konsensmechanismus des → Proof of Stake eine bestimmte Menge → Coins, die von einer Person, die am → Konsensmechanismus teilnehmen möchte zur Sicherstellung dafür hinterlegt werden, dass diese Person sich an die Regeln des → Konsensmechanismus hält. Missachtet die Person diese Regeln, so sieht der → Konsensmechanismus ökonomische Nachteile für diese Person vor, nämlich den Verlust eines Teils oder des gesamten Stakes. **1.43**

Staking bezeichnet die Teilnahme am → Konsensmechanismus des → Proof of Stake, bei dem eine gewisse Anzahl an → Coins als → Stake eingesetzt werden. Von diesem Verständnis des Staking ieS ist Staking im weiteren Sinn zu unterscheiden, bei dem es zur **1.44**

Überlassung oder Hinterlegung von → Coins oder → Tokens kommt, mit dem Verständnis, dass die überlassende oder hinterlegende Person daraus einen Vorteil zieht, etwa in Form weiterer → Coins oder → Token. Diese Verwendung des Begriffs, also Staking im weiteren Sinn, lässt für sich allein noch keinen Rückschluss auf die rechtliche Qualität eines allenfalls zugrundeliegenden Rechtsgeschäfts oder technischen Mechanismus zu.

1.45 **Staking Pool** bezeichnet eine Gruppe an Personen, die gemeinsam jene Menge an → Coins aufbringen, die zum Betrieb eines → Validators bei → Proof of Stake → Blockchains benötigt werden.

1.46 **Token** bezeichnet digitale Einheiten, die der jeweiligen → Blockchain nicht immanent sind. Das bedeutet, dass Tokens im Gegensatz zu → Coins im → Konsensmechanismus der jeweiligen → Blockchain nicht vorgesehen sind, sondern erst später, etwa durch → Smart Contracts konzeptuell neu geschaffen werden. Nicht jede → Blockchain unterstützt Tokens. Ein Beispiel für eine → Blockchain, die Tokens unterstützt, ist Ethereum. Die Programmierung des → Smart Contract, der den Token verwaltet, bestimmt seine Ausgestaltung. Tokens können daher äußerst unterschiedlich ausfallen. Sie können bspw übertragbar sein oder auch nicht; oder sie können so ausgestaltet sein, dass Verfügungen Dritter ausgeschlossen sind oder zugelassen werden. Für bestimmte Funktionen von Tokens auf der Ethereum → Blockchain haben sich sogenannte ERC-Standards entwickelt (kurz für *E*thereum *R*equest for *C*omments), etwa ERC20 für einfache austauschbare Tokens, oder ERC721 für → NFTs. Für Details zum Tokenbegriff siehe auch Rz 1.116.

1.47 **Tokenisierung** bezeichnet die Verknüpfung → Blockchain-basierter → Tokens mit Vermögenswerten aller Art wie beispielweise Forderungsrechten oder körperlichen Sachen dergestalt, dass zur Ausübung des Rechts am jeweiligen Vermögenswert die Innehabung des dazugehörigen → Tokens notwendig ist. Für Details siehe Rz 19.1 ff.

1.48 **Transaktion** bezeichnet einen → Transaktionswunsch, der in einem → Block aufgenommen und damit Teil der → Blockchain wurde. Für Details siehe Rz 1.124 ff.

1.49 **Transaktionsgebühr** bezeichnet eine bestimmte Menge des der jeweiligen → Blockchain nativen → Coins, der von einer Person, die einen → Transaktionswunsch in einem → Block bestätigt sehen möchte, demjenigen → Miner (bei → Proof of Work) oder demjenigen → Validator (bei → Proof of Stake) versprochen wird, der den → Transaktionswunsch in einem → Block festhält.

1.50 **Transaktionswunsch** bezeichnet die gültig signierte und korrekt aufgebaute technische Instruktion zur Übertragung von → Coins von bestimmten → Adressen (Absender-Adressen) auf eine oder mehrere andere → Adressen (Empfänger-Adresse), oder zur Interaktion mit einem → Smart Contract, etwa das Aufrufen bestimmter Funktionen. Teil des Transaktionswunsches ist neben der technischen Instruktion und der → Signatur auch die versprochene → Transaktionsgebühr.

1.51 **Validator** bezeichnet bei → Proof of Stake eine Person, die nach Leisten des → Stakes in die Liste der Validatoren aufgenommen wird, um unter Beachtung des → Konsensmechanismus einen neuen → Block vorzuschlagen *(proposing)* oder die Gültigkeit eines vorgeschlagenen → Blocks zu belegen *(attesting),* um → Block Rewards und → Transaktionsgebühren zu vereinnahmen.

Wallet bezeichnet die Kombination aus → Adresse und → privatem Schlüssel. **1.52**

Wallet-Software bezeichnet eine Software zur Verwaltung von → Wallets und zum Erstellen, → Signieren und Übermitteln von → Transaktionswünschen an das jeweilige → DLT-Netzwerk. **1.53**

III. Die öffentliche Blockchain

A. Zweck der öffentlichen Blockchain

Wer von Distributed Ledger oder Blockchain[12] spricht, meint damit zu allermeist die Technologie, die den bekannten virtuellen Währungen wie Bitcoin oder Ether zugrunde liegt. Doch hinter dem Schlagwort Blockchain verbergen sich idR viele verschiedene Technologien, und neue Technologien werden laufend entwickelt. **1.54**

Gemein ist den öffentlichen Blockchains ihr Zweck: Unter einer Gruppe an Personen soll Einigkeit darüber hergestellt werden, (a) ob Ereignisse stattgefunden haben (etwa Transaktionen oder Berechnungen) und (b) in welcher Reihenfolge. Diese Ereignisse sollen (c) auf eine Weise aufgezeichnet werden, die unveränderlich ist, oder zumindest auf eine Weise, die es jedem ermöglicht, sofort zu erkennen, dass nachträglich Veränderungen vorgenommen wurden. Zuletzt – und das ist das Alleinstellungsmerkmal der Technologie – soll (d) der gesamte Prozess ohne eine vertrauenswürdige zentrale Stelle auskommen. **1.55**

Gerade der letzte Punkt – das Fehlen einer vertrauenswürdigen zentralen Stelle – bereitet idR das größte Kopfzerbrechen für jene, die sich zum ersten Mal mit der Technologie beschäftigen. Als erster Einstieg bietet sich zum Verständnis der Technologie als Gedankenexperiment die Vorstellung einer Blockchain in der analogen Welt an. **1.56**

Man stelle sich eine Gruppe von 20 Personen in einem Raum vor. Die Gruppe entscheidet, dass sie untereinander nicht mehr mit Geld handeln möchte, sondern stattdessen mit einer eigenen Währung. Diese Währung soll aber nicht physisch existieren, sondern nur auf dem Papier. Um die Wirtschaft rund um diese virtuelle Währung in Gang zu bringen, wird entschieden, dass alle Personen mit einem Betrag von 100 starten. Zu diesem Zweck notiert jede Person für sich selbst ein Startguthaben von 100 Punkten auf einem eigenen Stück Papier. Wird Handel betrieben, so wird in der Gruppe vereinbart, dass sich jede Person notiert, welche Anzahl an Punkten sie von einer anderen Person erworben oder an eine andere Person abgegeben hat. Jeder notiert also seinen eigenen Punktestand. **1.57**

Leider hat sich in die Gruppe ein unredlicher Teilnehmer eingeschlichen, der nicht notiert, wenn er Punkte abgeben sollte. Die Gruppe erkennt schnell, dass ihre virtuelle Währung auf diese Weise nicht funktionieren kann. Schließlich kann im Nachhinein nicht mehr mit Sicherheit bestimmt werden, welche der beteiligten Personen die Übertragungen korrekt aufgezeichnet hat. Eine einzelne Person zu bestimmen, die für alle anderen die Aufzeichnungen führt, kommt aber aus genau demselben Grund nicht in Betracht. Was wenn diese zentrale Stelle Fehler macht oder unredlich handelt? **1.58**

12 Vgl zB *Varro,* taxlex 2017, 399; *Enzinger,* SWK 2017, 1013; *Kreuzer,* CFOaktuell 2017, 109; *Hanzl/Rubey,* GesRZ 2018, 102; *Völkel,* ÖBA 2017, 385; *Völkel,* ecolex 2017, 639.

1.59 Die Gruppe entscheidet daher, dass alle Teilnehmer auf ihrem eigenen Stück Papier nicht nur die eigene Anzahl an Punkten notieren, sondern auch das Startguthaben aller anderen neunzehn Teilnehmer und die Transaktionen aller anderen. Möchte eine Person Punkte übertragen, solle sie das so laut in den Raum rufen, dass alle anderen in der Gruppe es hören. Jeder notiert auf dem eigenen Stück Papier die Übertragung. Auf diese Weise sollte immer jeder in der Gruppe genau wissen, wem wie viele Punkte zustehen.

1.60 Diese Idee scheint gut zu funktionieren. Als A dem B fünf Punkte übertragen möchte, ruft er dies laut in den Raum und alle notieren die Übertragung. Das Problem scheint gelöst und die Teilnehmer im Raum beginnen die neue virtuelle Währung immer eifriger zu nutzen. Irgendwann jedoch wird genau dies zum Problem. Es wird laut durcheinandergerufen. Nicht jeder Teilnehmer hört alle Rufe, manche missverstehen sie, und manche Teilnehmer sind schlicht nicht schnell genug beim Notieren. Schon nach kurzer Zeit unterscheiden sich die Aufzeichnungen der Teilnehmer erheblich. Es besteht in der Gruppe keine Einigkeit mehr darüber, welche Übertragungen tatsächlich stattgefunden haben und in welcher Reihenfolge. Ein neues System muss gefunden werden.

1.61 Das Notieren jeder Transaktion durch alle Teilnehmer war eine gute Idee, in der Praxis aber zu fehleranfällig. Die Gruppe entscheidet daher, doch eine einzelne Person als „Aufzeichner" zu bestimmen. Der Aufzeichner soll jedoch laufend abgelöst werden und am Ende seiner Funktionsperiode alle von ihm aufgezeichneten Übertragungen vorlesen. Alle anderen in der Gruppe schreiben diesen Block an Transaktionen mit und kontrollieren, ob die eigenen Transaktionen richtig aufgezeichnet sind. Bemängelt kein Teilnehmer den Block, so darf der Aufzeichner als Belohnung seinen eigenen Punktestand um eine vorab vereinbarte Menge erhöhen, was ebenfalls von allen in der Gruppe notiert wird. Macht der Aufzeichner hingegen einen Fehler, so wird der gesamte Block von allen Teilnehmern ignoriert. Neue Punkte erhält der Aufzeichner dann nicht. In einem solchen Fall müssen alle gewünschten Transaktionen eben dem nächsten Aufzeichner nochmals gesagt werden.

1.62 Dieses System löst gleich mehrere Probleme auf einmal. Zunächst besteht auf diese Weise immer Einigkeit in der Gruppe, welche Übertragungen in welcher Reihenfolge stattgefunden haben. Gleichzeitig besteht aber auch ein Anreiz für den Aufzeichner, sich an die Regeln des Systems zu halten. Wer den mühsamen Prozess des richtigen Aufzeichnens fehlerfrei erledigt, der darf sich selbst belohnen. Wer hingegen als Aufzeichner unredlich handelt, wird entlarvt und hat diese Aufgabe umsonst erledigt.

1.63 Das System ist freilich kompliziert. Denn um festzustellen, welchen Punktestand eine Person hat, genügt es nicht, einen einzelnen Zahlenwert zu kontrollieren. Stattdessen müssen die Teilnehmer, ausgehend von den ursprünglichen 100 Punkten alle Übertragungen nachvollziehen, um den Punktestand der einzelnen Personen zu ermitteln. Dabei fällt den Teilnehmern aber noch ein Problem auf: Nicht nur der Aufzeichner kann Fehler machen, sondern auch die Gruppenmitglieder, wenn sie den vom Aufzeichner am Ende seiner Funktionsperiode vorgelesenen Block mitschreiben. Außerdem könnten die Teilnehmer der Versuchung unterliegen, vergangene Übertragungen zu verändern oder unter den Tisch fallen zu lassen. Nicht nur der Aufzeichner, sondern auch die anderen Teilnehmer könnten unredlich agieren. Wer entscheidet in so einem Fall, welcher Aufzeichnungsstand die wahren Geschehnisse wiedergibt?