HEUKING KÜHN LÜER WOJTEK

Grundbegriffe von Distributed Ledger-Technologie und Blockchain-Technologie

Grundbegriffe von Distributed Ledger-Technologie und Blockchain-Technologie

Inhaltsverzeichnis

A. Distributed Ledger-Technologie (DLT)

Die Distributed Ledger-Technologie (DLT) zeichnet sich durch die dezentrale Speicherung von Daten aus. Anstatt alle Informationen auf einem zentralen Rechner zu speichern und zu verwalten, werden die Daten von verschiedenen Rechnern gespeichert, die alle ein Netzwerk bilden (Peer-to-Peer-System). Auf jedem der teilnehmenden Rechner befindet sich eine Kopie des gesamten Registers. Daher spricht man von einem verteilten oder dezentralen Kontobuch (Distributed Ledger).

Jede Änderung des Registers, die ein Rechner vornimmt, kann mit den auf den übrigen Rechnern gespeicherten Registerinhalten verglichen werden. Nur wenn zwischen den einzelnen Registerspeicherpunkten ein Konsens bzgl. einer Änderung des Registers hergestellt wird, kann diese mit Wirkung für das gesamte Register erfolgen. Der Abgleich untereinander erlaubt es, Fälschungen des Registers aufzuspüren. Denn ein Berechtigter kann nur so viele Transaktionen vornehmen, wie er aufgrund seines Kontostands befugt ist. Die doppelte Ausführung einer Transaktion gegenüber zwei verschiedenen Parteien und betrügerische Handlungen werden damit verhindert (Problem des Double Spending). Auf diese Weise entfällt das Bedürfnis nach einer zentralen Stelle oder Gegenpartei, die die sichere Ausführung garantiert. Zudem hat grundsätzlich jeder Teilnehmer Zugriff auf den gesamten Inhalt des Registers. Daher bedarf es keiner Intermediäre mehr, welche bestätigen, ob jemand noch Berechtigter ist.

Zusammengefasst kann DLT zwei Funktionen haben: Einerseits speichert sie Informationen fälschungssicher ab und dokumentiert sie (Dokumentationsfunktion). Andererseits ermöglicht sie die Ausführung von Transaktionen über digitale Vermögensgegenstände (Transaktionsfunktion).

B. Blockchain-Technologie

Die Blockchain-Technologie ist eine besondere Variante der Distributed Ledger-Technologie. Im dezentralen Register werden Informationen in Blöcken mit Zeitstempeln gespeichert. Sobald eine oder mehrere neue Transaktionen stattfinden, werden alle bisherigen Informationen sowie die Informationen über die neuen Transaktionen in einem neuen Block gespeichert. Auf diese Weise gibt jeder neue Block die gesamte bisherige Transaktionshistorie wider. Dabei kommen zwei Sicherungsmechanismen zum Einsatz:

- Bereits vorhandene Blöcke werden durch die Verwendung eines Hash-Werts verschlüsselt. Dadurch können sie nicht mehr rückwirkend verändert oder gelöscht werden (Immutability).
- Neue Blöcke können nur geschaffen werden, wenn innerhalb des Blockchain-Systems hinreichend viele Teilnehmer die Ausführung der Transaktion bestätigen (Validierung).

Steht ein Transaktionsauftrag im Widerspruch zur bisherigen, dezentral gespeicherten Transaktionshistorie, wird die Transaktion nicht ausgeführt. Eine Fälschung ist nur dann möglich, wenn jemand mehr als 50% der Rechnerleistung des gesamten Netzwerks kontrollieren und damit den Validierungsprozess beherrschen würde. Dies ist technisch kaum realisierbar, aber möglich.

Darüber hinaus kann eine Blockchain derart programmiert werden, dass Transaktionen nur durch die Zustimmung mehrerer Personen durchgeführt werden können (ähnlich einer Vinkulierung im Gesellschaftsrecht).

Die Blockchain dient der Speicherung von Daten. Sie prüft aber selbst nicht, ob und inwieweit diese Daten valide sind, d. h. mit der realen Welt übereinstimmen. Will man die inhaltliche Richtigkeit der Daten sicherstellen, bedarf es wahrscheinlich eines kontrollierenden Intermediärs.

C. Zugriff auf die Blockchain (Netzwerkarten)

Eine Blockchain zeichnet sich insbesondere dadurch aus, dass alle Teilnehmer das gesamte Register einsehen können. Allerdings handeln alle Teilnehmer unter einem Pseudonym, sodass sich ihre wahre Identität nicht erkennen lässt. Je nach Ausgestaltung des Netzwerks kann nicht jeder Teilnehmer Veränderungen des Registers initiieren. Folgende Arten der Blockchain sind zu unterscheiden.

I. Offene Blockchain (Permissionless Public Blockchain)

Zu einer offenen Blockchain (Permissionless Public Blockchain) hat ausnahmslos jeder Teilnehmer Zugang und kann Transaktionen ausführen lassen, wenn er über einen öffentlichen Schlüssel verfügt (volle Transparenz). Hier kann die Blockchain nur sicherstellen, dass die Daten nach dem Konsensmechanismus validiert werden. Sie kann aber keine Aussage darüber treffen, ob diese Daten inhaltlich richtig sind.

II. Halboffene Blockchain (Permissioned Public Blockchain)

In einer halboffenen Blockchain (Permissioned Public Blockchain) können alle Teilnehmer das Register einsehen und nachvollziehen, wer Einträge vorgenommen hat. Allerdings können nicht alle Teilnehmer selbst Transaktionen initiieren.

III. Geschlossene Blockchain (Permissioned Private Blockchain)

In einer geschlossenen Blockchain (Permissioned Private Blockchain) entscheidet ein Marktbetreiber über die Zulassung zum Netzwerk und definiert dafür i. d. R. bestimmte Parameter. Den Zugang erhalten meist um Personen, deren Identität bekannt ist. Über diese Beschränkung kann sichergestellt werden, dass die gespeicherten Daten auch inhaltlich auf ihre Richtigkeit geprüft werden.

D. Hash-Wert

Dass die Transaktionshistorie nicht nachträglich geändert werden kann, wird durch einen Hash-Wert (Prüfsumme) sichergestellt. Dabei handelt es sich um eine einzigartige Buchstaben-Zahlenfolge, mit dem jeder blockweise gespeicherte Datensatz verschlüsselt wird. Der Hash-Wert wirkt wie ein Fingerabdruck. Wird ein neuer Block erstellt, beinhaltet er stets den Hash-Wert des vorherigen Blocks. Aus dem Hash-Wert lassen sich die abgespeicherten Informationen eines Blocks nicht rekonstruieren. Wenn jemand den Hash-Wert eines gespeicherten Blocks kennt, kann er also nicht den Inhalt des Blocks ermitteln. Zugleich können grundsätzlich alle Teilnehmer der Blockchain den Hash-Wert nachberechnen. Dadurch können sie überprüfen, ob der abgespeicherte Datensatz richtig ist oder verändert wurde.

Wenn jemand einen Blockinhalt fälscht, etwa indem er sich selbst als Berechtigten einträgt, ändert sich der Hash-Wert. Infolgedessen passen der neue Hash-Wert und der Inhalt des Blocks nicht mehr zueinander. Da der Hash-Wert des richtigen Blocks im folgenden Block gespeichert wird, fällt die Fälschung auch in den nachfolgenden Blöcken auf. Dadurch werden Transaktionen zugunsten des Fälschers ungültig.

E. Knoten (Nodes)

Als Knoten (Nodes) bezeichnet man einzelne Rechner, auf denen das gesamte Register jeweils abgespeichert ist.

F. Schürfen (Mining)

Der Begriff Schürfen (Mining) beschreibt eine spezifische Tätigkeit von Betreibern eines Knoten: Sie stellen Rechenkapazität zur Verfügung, um zu prüfen, ob eine Änderung des Registers akzeptiert werden soll. Die Überprüfung findet typischerweise in einem Proof-of-Work-Verfahren oder in einem Proof-of-Stake-Verfahren statt.

G. Proof-of-Work

Das Proof-of-Work-Verfahren ist eine gängige Variante, um die Überprüfung durch und den Konsens zwischen den Teilnehmern des dezentralen Registers herzustellen: Ein neuer Block kann nur gebildet werden, wenn eine anspruchsvolle mathematische Aufgabe richtig gelöst wird, etwa die Errechnung einer bestimmten Zahlen- und Buchstabenkombination (nonce). Diese Zahlenkombination muss zusammen mit dem neuen Datensatz über Transaktionen einen bestimmten (neuen) Hash-Wert ergeben (Hashpuzzle). Die Person, welche das Rätsel als erste richtig gelöst hat, sendet ihre Lösung an die weiteren Mitglieder des Netzwerks. Wenn hinreichend viele Knoten die gefundene Lösung bestätigt haben, wird der neue Block auf der Blockchain gespeichert. Wer die Aufgabe als erster löst, kann eine Belohnung dafür (meist in Form von neuen Token) erhalten. Dementsprechend konkurrieren viele Person darum, mittels ihrer eigener Rechenleistung das Rätsel als erstes zu lösen. Nachteil dieses Verfahrens ist der hohe Energieaufwand

H. Proof-of-Stake

Das Proof-of-Stake-Verfahren ist das Alternativmodell zum Proof-of-Work-Verfahren. Es soll den hohen Energieverbrauch vermeiden. Jeder Netzwerkteilnehmer kann entscheiden, ob er für eine bestimmte Zeit darauf verzichtet, vorhandene Token zu übertragen. Für diesen Einsatz bekommt der jeweilige Teilnehmer die Chance, für die Bestätigung einer Transaktion ausgewählt zu werden und dafür eine Belohnung in Form neuer Token zu erhalten.

I. Minting

Der Begriff Minting beschreibt eine spezifische Verfahrensweise, mit der Token neu entstehen und verteilt werden. Zunächst werden neue Token auf einer bestehenden Blockchain manuell erschaffen. Anschließend kann ein erwerbswilliger Teilnehmer einen Betrag einer Kryptowährung an die eingerichtete Adresse des Token-Emittenten überweisen. Im Gegenzug erhält der Erwerber neu geschaffene Token überwiesen.

J. Gabel (Fork)

Es kann vorkommen, dass zeitgleich zwei oder mehr Personen die richtige Lösung des Rätsels finden und beide Lösungen jeweils von einer hinreichend großen Zahl von Teilnehmern bestätigt werden. Infolgedessen wird nicht ein neuer Block, sondern es werden zwei neue Blöcke gespeichert. Daraus ergeben sich zwei Stränge. Dieses Phänomen bezeichnet man als Gabel (Fork). Die Gabel wird aufgelöst, wenn für einen der beiden Stränge weitere Blöcke bestätigt werden. Nur der längere Strang kann Bestand haben.

K. Token

Ein Token ist vereinfacht gesprochen ein digitaler Eintrag auf einer Datenbank. Er repräsentiert einen bestimmten Vorteil, der einer konkreten Person zugeordnet ist. Jeder Token ist einzigartig und kann nicht vervielfältigt werden. Für die Übertragung eines Token muss die Berechtigung über den Datenbankeintrag wechseln, d. h. nicht mehr Teilnehmer A, sondern Teilnehmer B muss in der Lage sein, den Datenbankeintrag verändern zu können.

Im Grundsatz kann ein Token jede Art von Vermögensvorteil repräsentieren, z. B. eine Einheit eines Rohstoffs, ein Gemälde oder einen Gesellschaftsanteil („Digitale Wertmarke“). Es hat sich folgende Differenzierung zwischen drei Idealtypen von Token anhand der ökonomischen Funktion herausgebildet. Dazwischen gibt es Hybridformen.

I. Zahlungsmittel-Token (Payment/Currency Token)

Zahlungsmittel-Token (Payment/Currency Token) ähneln Geld in dem Sinne, dass sie als universelles Tauschmittel eingesetzt werden können. Da sie nicht von einer staatlichen Stelle ausgegeben werden und keine Forderung gegen eine Bank oder einen Emittenten begründen, stellen sie keine Währung und kein Fiat-Geld dar. Das bekannteste Beispiel eines Zahlungstoken ist der Bitcoin. Dieser erhält seinen Wert aus sich heraus, weil ihm seine Nutzer einen bestimmten Wert beimessen (sog. intrinischer Token).

II. Kapitalanlage-Token (Investment/Security Token)

Kapitalanlage-Token (Investment/Security Token) ähneln einem Finanzinstrument in dem Sinne, dass sie bestimmte Rechte und Ansprüche darstellen, insbesondere Dividenden- und Stimmrechte. Sie lassen sich ihrerseits aufteilen in Equity Token und Debt Token. Equity Token vermitteln aktienähnliche Rechte (Auszahlung einer Dividende, Stimmrechte). Debt Token vermitteln dagegen einen schuldrechtlichen Rückzahlungsanspruch und Zinsanspruch.

Der Security Token bildet nur den Mantel für ein Recht, das in der analogen Welt besteht („Tokenisierung“). Der Token selbst hat keinen Wert aus sich selbst heraus (sog. extrinsischer Token). Ähnlich wie bei einer Aktie ist also zwischen dem verbrieften Recht und der Urkunde zu unterscheiden. Wird das ummantelte Recht auf einen Erwerber übertragen, sollte ihm der Token folgen. Sobald der Token von einer Rechtsordnung als eigenständiges Vermögen*recht* anerkannt wird, sollte das Gegenteil gelten: Sobald der Token übertragen wird, sollten ihm das ummantelte Recht folgen („Das Recht aus dem Token folgt dem Recht an dem Token.“)

III. Nutzwert-Token (Utility Token)

Nutzwert-Token (Utility Token) ähneln einem Gutschein, weil sie oftmals zum Bezug von Waren oder Dienstleistungen genutzt werden können. Anders als Zahlungsmittel Token können sie nicht universell, sondern nur auf bestimmten Plattformen eingesetzt werden. Auch sie beziehen ihren Wert aus dem Bezug auf einen externen Gegenstand, sind also extrinsische Token.

L. Digitale Brieftasche (Wallet)

Die Blockchain speichert nur die Transaktionshistorie ab und stellt den aktuellen Kontostand dar. Um Token übertragen zu können, bedarf es eines besonderen Autorisierungsverfahrens. Typischerweise werden Token in einer digitalen Brieftasche (Wallet) gespeichert. Zugang zur Brieftasche und zur Vornahme von Transaktionen hat nur derjenige, der über einen öffentlich verfügbaren Schlüssel (Public Key) und einen privaten Schlüssel (Private Key) zur Blockchain verfügt.

M. Öffentlicher Schlüssel (Public Key)

Der öffentlich verfügbare Schlüssel (Public Key) lässt sich mit einer Adresse oder IBAN vergleichen. Er dient dazu, die Transaktionsbeteiligten zu identifizieren. Er kann von jedermann eingesehen werden.

N. Privater Schlüssel (Private Key)

Der private Schlüssel (Private Key) ähnelt einer persönlichen Signatur oder PIN. Soll eine Transaktion stattfinden, muss der Wallet-Inhaber die Transaktionsdaten mit seinem privaten Schlüssel signieren. Sodann werden die Informationen an die Blockchain versandt und dort verifiziert. Der private Schlüssel ist nur für den jeweils Berechtigten einsehbar. Er sollte auch nur von diesem einsehbar sein, weil er den Zugriff auf die Token ermöglicht. Er wird nicht zusammen mit einem Token auf einen Erwerber übertragen.

Der private Schlüssel kann auch von einem Intermediär – ähnlich einer Depotbank – gehalten werden (Wallet Provider). Dies ist etwa deswegen sinnvoll, weil ein spezialisierter Verwahrer einen höheren technischen Schutz vor Hackerangriffen gewährleisten kann.

O. Selbst erfüllende Verträge (Smart Contracts)

Smart Contracts sind einer der Hauptanwendungsfälle von Blockchain-Technologie, können aber auch in gänzlich anderen Bereichen eingesetzt werden. Sie ermöglichen es (anonymen) Parteien, Transaktionen miteinander auszuführen. Der Begriff der Smart Contracts ist allerdings irreführend: Weder handelt es sich um Verträge, noch sind diese besonders schlau. Gemeint ist vielmehr eine automatisierte Erfüllung eines bereits geschlossenen Vertrages: Wenn bestimmte, von den Parteien definierte und digital überprüfbare Bedingungen erfüllt sind, soll die Erbringung der Leistungen automatisch durch einen Algorithmus in Gang gesetzt werden (Wenn-Dann-Algorithmus). Es bedarf insoweit keiner Mitwirkung der Parteien oder des Einsatzes eines Treuhänders mehr.

P. Schnittstelle (Oracle)

Smart Contracts brauchen einen vordefinierten Raum. Sofern sie auf eindeutig nachweisbare Tatsachen in der analogen Anwendung abstellen, muss dazu eine Verbindung hergestellt werden (z. B. ein Stromzähler, der Daten liefert). Diese Verbindung bezeichnet man als Schnittstelle (Oracle). Müssen dagegen wertungsoffene Voraussetzungen erfüllt sein („wichtiger Grund“, „Geschäftsgrundlage“, „Schutzpflicht“, etc.), können Smart Contracts ohne menschlichen Einflussnahme nicht funktionieren.

Q. Technikgestützte Willenserklärungen

Das Zustandekommen eines Vertrages unterliegt den allgemeinen Regeln des Zivilrechts. Das deutsche Recht erfordert insoweit Abgabe und Zugang zweier inhaltlich korrespondierender Willenserklärungen. Die Blockchain-Technologie entfaltet aus sich heraus keine Rechtswirkungen. Sie kann aber dazu genutzt werden, Willenserklärungen konkludent oder sogar automatisiert abzugeben. So lässt sich das Signieren einer Transaktion mit einem privaten Schlüssel potentiell als Abgabe einer Willenserklärung verstehen. Der Zugang der Willenserklärung kann darin gesehen werden, dass die validierte Transaktion in einem neuen Block gespeichert wird und endgültig Bestand hat. Diese technikgestützten Willenserklärungen können nach den allgemeinen Regeln der §§ 104 ff. BGB unwirksam sein (zum Ganzen: *Guggenberger*, in: Hoeren/Sieber/Holznagel, MMR-HdB, Teil 13.7 Rn. 10).

R. Initial Token Offering (ITO), Token Generating Event (TGE), Token Sale, Initial Coin Offering (ICO)

Token können zur Finanzierung eines Unternehmens oder Projekts genutzt werden. Die (erstmalige) Ausgabe neu geschaffener Token an Anleger wird als Initial Token Offering (ITO) oder Token Generating Event (TGE) bezeichnet. Einen besonders wichtigen Unterfall bildet das Initial Coin Offering (ICO). Dieses ähnelt allenfalls dem Namen nach einem Initial Public Offering. Zwar dient auch das ICO der Beschaffung von Kapital zur Geschäftsentwicklung eines Unternehmens. Im Detail ergeben sich erhebliche (strukturelle) Unterschiede: Bei einem ICO „schafft" ein Emittent zunächst neue Payment-Tokens, etwa Bitcoins auf einer dafür bereitgestellten Blockchain (z. B. Etherum). Sodann bietet der Emittent die neu geschaffenen Coins Investoren über eine Internetseite an. Die Investoren werden nur anhand eines sog. White Paper über das Geschäftsmodell des Emittenten informiert. Dieses White Paper ist deutlich kürzer als ein Wertpapierprospekt und erfüllt nicht die Anforderungen der Prospektregularien. Ein Intermediär – insbesondere eine Emissionsbank – wird nicht eingeschaltet. Im Gegenzug für das Zahlen von Fiat-Geld oder virtuellem Geld erhalten die Investoren Coins vom Emittenten.

S. Kryptobörse (Crypto Exchange)

Nachdem neue Token geschaffen und von Investoren erworben worden sind, besteht häufig das Bedürfnis nach einer Handels- und Deinvestitionsmöglichkeit. Dieses Bedürfnis soll durch sog. Kryptobörsen gestillt werden. Dabei handelt es sich um Handelsplattformen, auf denen Investoren ihre erworbenen Token verkaufen und neue Token von anderen Investoren erwerben können. Diese basieren oftmals auf einem Orderbuch. Anders als bei klassischen Venture Capital Beteiligungen sollen Kryptobörsen dafür sorgen, dass Investoren neue Token junger Unternehmen notfalls schnell wieder abstoßen können. Aufgrund eines liquiden Sekundärmarktes sollen mehr Investoren angereizt werden, sich an jungen Unternehmen zu beteiligen. Sofern die Börse auf der Blockchain Technologie aufbaut, wird auch der Begriff der „Decentralized Exchange" verwendet. Dabei kann die Börse gänzlich auf einem bereits vorhandenen Distributed Ledger aufbauen, oder sie verfügt über Anwendungen, die auf dem Register aufbauen und zu diesem in einer Wechselbeziehung stehen.

Ihre Ansprechpartner zu diesem Thema

Rechtsanwalt, Partner
Dr. Mirko Sickinger, LL.M.
T +49 221 20 52-596
F +49 221 20 52-1
m.sickinger@heuking.de

Rechtsanwalt
Dr. Martin Konstantin Thelen, LL.M.
T +49 221 20 52-481
F +49 221 20 52-1
mk.thelen@heuking.de