Von Oliver Christian Schroen, Stand 25.01.2021

Was sind sogenannte „Kryptoassets“ der Sorte „Bitcoin“?

Eine Abhandlung zur steuerlichen Beurteilung aufbauend auf einem Beispiel und einer Analogie aus der Realwelt.

(Genderhinweis: Alle verwendeten Begriffe sind, wo möglich, als d/w/m zu verstehen.)

I. Einleitung

In dieser Abhandlung werde ich zu zeigen versuchen, worum es sich handelt, wenn jemand ein sogenanntes „Kryptoasset“ wie z.B. „Bitcoin“ „erwirbt“. Dies ist nötig, damit ggf. vorhandene unzutreffende Bilder als Trugbilder entlarvt werden und somit möglichst klar wird, worüber steuerlich eigentlich entschieden werden soll, damit es zu keinen unzutreffenden Rechtsfolgen allein aufgrund unzureichenden Wissens über die tatsächlichen Vorgänge kommt. Es existieren leider eine Menge Fehlvorstellungen, vor allem unzutreffende visuelle Vorstellungen von etwas tatsächlich Unsichtbarem.

Es scheint hierbei leider häufig auch wie bei Goethes Faust im 1. Teil, Studierzimmer 2, zuzugehen:

Der Schüler glaubt mit dem Universalgelehrten Dr. Faust zu sprechen, gerät aber an Mephisto, der ihn täuscht und auf des Schülers Hinweis *„Doch ein Begriff muß bei dem Worte sein.“* nur antwortet: *„Schon gut! Nur muß man sich nicht allzu ängstlich quälen/Denn eben wo Begriffe fehlen,/Da stellt ein Wort zur rechten Zeit sich ein./Mit Worten läßt sich trefflich streiten,/Mit Worten ein System bereiten,/An Worte läßt sich trefflich glauben,/Von einem Wort läßt sich kein Jota rauben.“*

Mit solch einer Haltung wird der Begriff, also die Bedeutung, als obsolet erklärt, wenn man nur schöne altbekannte Wörter (Zeichen) verwendet, die nicht die Bedeutung der bezeichneten Tatsache korrekt beschreiben, sondern nur einen Schein der Bekanntschaft und damit ein nur scheinbares Wissen, bzgl. der Bedeutung des Bezeichneten erzeugen.

Zur Klärung bzgl. der zu bezeichnenden Tatsachen gehe ich in folgenden Schritten vor:

Das Kapitel „II. Sensibilisierung“ soll dafür sensibilisieren, dass es bei neuen Erscheinungen in der virtuellen Welt steuerlich relevant und demzufolge entscheidend ist, zwischen der „Dokumentation eines Etwas“ und dem „dokumentierten Etwas selbst“ zu unterscheiden. Hierzu verwende ich zunächst das Beispiel des Grundbuchs, in dem u.a. die real existierenden Grundstücke und die diesbezüglichen jeweiligen Eigentumsverhältnisse dokumentiert sind.

Im Kapitel III. „Realwelt …“ wird - aufbauend auf dem Beispiel des Grundbuchs - eine Einordnung von „Kryptoassets“ wie z.B. „Bitcoins“ anhand der Realwelt entwickelt. Dies erfolgt mittels einer Analogie über „analoge Coins“ in der Realwelt. In „Fazit 1“ am Ende dieses Kapitels werden die wichtigsten Ergebnisse zusammengestellt.

Sind die realweltlichen analogen Grundlagen geklärt, wird in Kapitel IV. „Virtuelle Welt …“ das zuvor für den realweltlichen Bereich Dargestellte quasi in die virtuelle Welt übertragen und anhand dieser Ergebnisse die Vorgänge bei „Kryptoassets“ wie z.B. „Bitcoin“ genauer beleuchtet. In „Fazit 2“ am Ende dieses Kapitels werden die wichtigsten Ergebnisse zusammengestellt.

In Kapitel V. „Übersicht…“ erfolgt eine tabellarische Übersicht, welche die wichtigsten Eigenschaften von Coins und deren Dokumentation in der Realwelt und der virtuellen Welt gegenüberstellt. Sie dient auch zur späteren schnellen Vergegenwärtigung.

Mit Kapitel VI. „Fragen zur steuerlichen Beurteilung“ schließt diese Abhandlung. Die hier gestellten Fragen sollen sicherstellen, dass bei einer steuerlichen Würdigung möglichst klar herausgearbeitet werden kann, worüber eigentlich entschieden werden soll, insbesondere wenn es um die Qualifizierung einer „Kryptowährung“ als Wirtschaftsgut geht. (In Anlehnung an: FG Nürnberg, Beschluss v. 08.04.2020 – 3 V 1239/19 Rd.Nr. 35)

Die im Text eingerückt zu findenden *„Exkurse“* dienen nur einer weiteren Vertiefung des Verständnisses, sind jedoch zum Erfassen der notwendigen Grundlagen nicht von großer Relevanz und können zunächst übersprungen werden.

II. Sensibilisierung

Angenommen jemand möchte eine Immobilie in Deutschland erwerben. Hierbei ist es ihm sehr wichtig, darauf vertrauen zu können, dass der Veräußerer auch berechtigt ist, ihm die Immobilie zu verkaufen. Ebenso möchte er später als neuer Eigentümer nachweisen können, dass er wiederum berechtigt ist, diese Immobilie weiterveräußern zu dürfen.

Dies wird in Deutschland insbesondere durch die Dokumentation im sogenannten Grundbuch erreicht, denn es werden dort alle Eigentumswechsel verschriftlicht. Geht das Eigentum an einer Immobilie nacheinander von einem auf den jeweils nächsten Eigentümer über, so bleibt die Dokumentation über alle Eigentümerwechsel im Grundbuch über Jahrzehnte und länger erhalten.

Im Grundbuch kann man idealerweise - vom ersten Eigentümer an - alle Eigentümerwechsel und die jeweils aktuellen Eigentümer der Immobilie/des Grundstücks chronologisch aufgereiht, vorstellbar wie die Kettenglieder einer Kette, schriftlich niedergelegt finden. Ob die Dokumentation der Eigentumswechsel in einem Grundbuch in Papierform oder elektronisch stattfindet, ist gleichgültig, wenn sie gegen Fälschung abgesichert ist.

Auch eine nicht dokumentierte Historie an Verkäufen von irgendwelchen Dingen, für die in der Regel eine Form, z.B. ein schriftlicher Kaufvertrag nicht erforderlich ist, wäre dennoch eine Historie an Verkäufen und i.d.R. auch von Eigentumsübergängen an diesen Dingen. Da die meisten Menschen sowohl ausreichend vergesslich als auch zumindest zum Teil hin und wieder unehrlich sind oder sein könnten, kann eine möglichst fälschungssichere Verkaufsdokumentation bzgl. verkaufter Dinge ratsam sein. Deshalb sind beispielsweise für Grundstücksverkäufe insbesondere folgende Dokumentationen, nämlich die notarielle Beurkundung und die sich daraus ergebenden Eintragungen im Grundbuch, gesetzlich vorgeschrieben.

Das Grundbuch bietet die Möglichkeit reale Vermögenswerte, die Grundstücke, und die jeweilige Eigentümerstellung fälschungssicher analog oder auch digital abzubilden, zu dokumentieren.

Ein Grundbuch in dem ein Grundstück dokumentiert ist, das aber real nicht existiert, bildet insoweit keinerlei Vermögenswert ab; weder analog noch digital, weshalb auch ein Notar nicht berechtigt ist, wissentlich einen Übertragungsvertrag über das Eigentum an einem nicht real existierenden Grundstück zu beurkunden.

Angenommen es käme - zumindest theoretisch denkbar - doch dazu, dass im Grundbuch ein vorgeblicher „Eigentumswechsel“ an einem nicht real existierenden Grundstück dokumentiert wurde, würde dadurch ein neues reales Grundstück entstehen? Nein, selbstverständlich nicht, weil nur die Historie über ein bestehendes Grundstück substanziell sein kann.

Auch spätere weitere Eintragungen im Grundbuch könnten auf dieser fehlenden Grundlage kein reales Grundstück entstehen lassen. Übrig bliebe allein eine Dokumentation über den angeblichen Übergang von „Eigentum“ an einem Gegenstand an dem die Begründung von Eigentum - wegen mangelnder realer Existenz - tatsächlich gar nicht möglich und auch denklogisch nicht vorstellbar ist.

Es handelte sich vielmehr um eine Dokumentation von (Schein-)Aktionen bezüglich eines real nicht existenten Etwas; faktisch ein „Grundbuch ohne Grundstück“.

So geht es in der nachfolgenden Darstellung ebenso ausschließlich um die reine Dokumentation von Aktionen, ohne dass diese Aktionen irgendetwas mit Eigentum oder anderen kodifizierten wirksam begründeten Ansprüchen an etwas Realem zu tun hätten (§ 194 BGB).

In dieser Abhandlung wird ausdrücklich nur auf „Kryptoassets“ ohne jeglichen Anspruch nach § 194 BGB, also „anspruchslose Kryptoassets“, eingegangen. Andere „Kryptoassets“, die ein tatsächlich existierendes Etwas, wie Grundstücke, Anteile an Kapitalgesellschaften usw. lediglich digital abbilden, werden hier nicht beleuchtet, weil sich die steuerliche Bestimmung und die ggf. nachfolgende Besteuerung von Tatbeständen mit diesen, sich nach dem jeweils Abgebildeten richtet.

Statt der Bezeichnung „Kryptoasset“ wird nachfolgend die auch Bezeichnung „Signaturkette“ verwendet.

III. Realwelt – „analog dokumentierte Signaturkette“

Um nun eine Brücke zum IV. Kapitel zu schlagen, wird nachfolgend zunächst eine Analogie aus der Realwelt bemüht. Hierfür gehen wir jedoch zunächst von der maßgebenden Definition des „Coin“ im System „Bitcoin“ aus.

Das „Bitcoin Whitepaper“ definiert einen „elektronischen Coin“ „als eine Kette von digitalen Signaturen, als Signaturkette. („We define an electronic coin as a chain of digital signatures.“). Dies klingt komplizierter als es ist.

Folgendes analoge Bild soll hier zunächst für die notwendige Klarheit sorgen.

Es muss an dieser Stelle betont werden, dass es nachfolgend ausschließlich um die Dokumentation einer Historie geht und nicht um die Historie selbst.

Um Licht ins Dunkel zu bringen, bietet es sich an, zunächst von der bekannten Realwelt auszugehen.

Hierfür brauchen wir

1. einen Bogen Papier,
2. Personen, die nacheinander etwas auf dieses Papier schreiben, dies handschriftlich signieren und anschließend das Papier jeweils an eine andere Person ihrer Wahl weitergeben sowie
3. eine „dritte Partei“, die darüber wacht, dass diese Personen auch die sind, für die sie sich ausgeben.

Das Ergebnis dieses Vorgangs soll sodann als Kette von analog dokumentierter Signaturen bzw. als „analoge Signaturkette“ bezeichnet werden - im Gegensatz zu der im Bitcoin Whitepaper genannten Kette von digitalen Signaturen, also der „digital dokumentierten Signaturkette“, der „digitalen Signaturkette“.

Diese „analog dokumentierte Signaturkette“ kann auch als „analoger Coin“ im Gegensatz zu dem vorgenannten „elektronischen Coin“ bezeichnet werden, weil sich in dieser Dokumentationsform eine manuelle Unterschrift („Signatur“) an die nächste reiht.

Form der Entstehung einer neuen „analog dokumentierten Signaturkette“

Eine „analog dokumentierte Signaturkette“ könnte beispielsweise dadurch entstehen, dass eine Person (A) ihren eigenen Namen auf einen Bogen Papier schreibt, sich also selbst schriftlich benennt (z.B.: „1. Benannter = A“) ansonsten aber nichts Weiteres auf das Papier schreibt. Zusätzlich könnte die Person den Bogen aber auch mit einer Überschrift versehen, z.B. „analogi-coin“ und soweit gewünscht, eine beliebige Zahl mit ergänzenden Bezeichnung, wie z.B. „100 Logoi“ oder „1 Logoi“ hinzufügen.

Das so beschriftete Papier, auf dem nur der „1. Benannte“ (A) steht, soll dann z.B. „analogi-coin-Start“ heißen.

Nun könnte eine weitere Person, die (B), hinzutreten, die auf diesem Papier verewigt sein möchte, z.B. weil auch sie dokumentiert haben möchte, jemand anderen benennen zu können. Vielleicht wäre sie sogar bereit, dem (A) für diese Möglichkeit etwas zu zahlen. Auf welche Art und Weise eine solche Benennungsmöglichkeit (A) an (B) dokumentiert werden könnte, wird im nächsten Absatz unter dem Begriff „Signierung“ erläutert.

Form der Benennung - die „Signierung“- als Form für das Anfügen neuer Glieder/„Signierungsmöglichkeit“

Diesem Start der auf Papier dokumentierten „Signaturkette“ („analogi-coin-Start“) werden jeweils neue zusätzliche Glieder durch den nachfolgend beschriebenen Vorgang angefügt, welcher ab jetzt jeweils „Signierung“ genannt werden soll. Dadurch wird die Historie fortlaufend dokumentiert.

Diese „Signierung“ erfolgt, indem derjenige, dessen Name zuletzt auf das Papier geschrieben wurde - hier der (A) -, sich überlegt, wen er als nächstes in der „Signaturkette“ vermerkt haben möchte, d.h. wen er „neu-benennen“ möchte, z.B. die (B).

Der (A) könnte die (B) durch einfaches Sagen von: *„Ich benenne die (B)“* benennen. Das wäre aber für die (B) i.d.R. wenig zufriedenstellend, da (B) später entweder die Historie nicht lückenlos aufsagen könnte oder/und ihr nur wenige Menschen vertrauen und diese Historie nur wenige glauben würden und sie zudem dem (A) vertrauen müsste.

Deshalb notiert er deren Namen und weitere Identifizierungs-Daten der „Neu-Benannten“ (B), das aktuelle Datum und ggf. die aktuelle Uhrzeit auf dem Papier und signiert abschließend handschriftlich.

Durch jede „Signierung“ verändert sich die „Signaturkette“, indem sie jeweils um ein Glied verlängert wird. Die vorangehenden Einträge verändern sich dadurch jedoch nicht.

Diese „Neu-Benennungen“ müssen zwingend zeitlich nacheinander erfolgen - möglich aber auch in unregelmäßigen auch größeren Zeitabständen – weil immer nur einer, nämlich der in der Dokumentation „Letzt-Benannte“, eine weitere „Signierung“ vornehmen kann, d.h. die „Signierungsmöglichkeit“ erhalten, kann.

Der „Neu-Benannte“ – hier (B) - erhält die Papier-Dokumentation der Signaturkette, der Historie, ausgehändigt. Diese kann er dann behalten oder nach freier Wahl an eine andere Person weitergeben.

Da die Dokumentation über „100 Logoi“ oder „1 Logoi“ oder noch anders überschrieben sein kann, muss zunächst klargestellt werden, dass eine Dokumentation über „100 Logoi“ nichts Anderes ist, als 100 getrennte Dokumentationen über jeweils „1 Logoi“.

Hier besteht ausnahmsweise das Ganze (Dokumentation über „100 Logoi“) aus der Summe seiner Teile (nämlich 100 getrennte Dokumentationen über jeweils „1 Logoi“), denn die Historie aller 100 Signaturketten ist völlig identisch mit der Historie der als Bündel zusammengefassten Signaturkette, deren Dokumentation mit „100 Logoi“ überschrieben ist.

> ***Exkurs: Teilung von „Signaturketten“:***
>
> *Auch ist es denkbar, dass eine „Signaturkette“ geteilt wird, indem bei der „Signierung“ nur ein bestimmter Teil, z.B. 30/100 mit der „Neu-Benannten“ (B) und 70/100 mit der „Neu-Benannten“ (C) verknüpft werden. Alternativ könnte sich der (A) selbst – statt der (C) - als „Neu-Benannten“ (A) mit den z.B. 70/100 verknüpfen.*
>
> *Bei einer Teilung der „Signaturkette“ muss eine Fotokopie der bisherigen „Papier-Signaturkette“ gefertigt werden, aus der die genaue Teilung und die anteiligen Benennungen auch quantitativ ersichtlich sind. Dazu müssen vorher auf der bisherigen „Papier-Signaturkette“ z.B. die „Neu-Benannte“ (B) zu 30/100 und die „Neu-Benannte“ (C) zu 70/100 notiert werden. Sodann wird eine Kopie hiervon erstellt. Eine „Neu-Benannte“ erhält die bisherige „Papier-Signaturkette“ die andere eine Kopie derselben.*
>
> *Ab erfolgter Teilung einer „Papier-Signaturkette“ sprechen wir von mehreren - im Beispiel von zwei - voneinander völlig unabhängigen „Signaturketten“, die einerseits weiter geteilt werden können und andererseits aber auch wieder teilweise oder vollständig zu jeweils einer „Signaturkette“ vereinigt werden können. Würde der (A) bei einer „Signierung“ beispielsweise die (B) zu 30/100 benennen und die (C) nicht zu 70/100 sondern versehentlich oder absichtlich nur zu 7/100, blieben 63/100 mit dem „Letzt-Benannten“, dem (A) weiter verknüpft.*
>
> *Behält sich der (A) weder Original noch Kopie zurück, könnte er für diese 63/100 keine „Neu-Benennung“ mehr initiieren. Die „Signaturkette“ wäre und bliebe teilweise, hier zu 63/100, beendet, weil faktisch nicht mehr identifizierbar. Deshalb sollte geregelt werden, dass eine „Neu-Benennung“ nur gültig ist, wenn die Summe auf dem Original und den Kopien nach Teilung immer zusammen 100/100 der „Signaturkette“ vor Teilung darstellen.*
>
> *Eventuell kann es angezeigt sein, Maßnahmen vorzusehen, um weitere Fälschungsmöglichkeiten auszuschließen, wie z.B. die Angabe auf allen Kopien und dem Original, wie viele Exemplare mit Teilmengen nach der Teilung jeweils vorhanden sind.*

Form der „Verifizierung“ - notarielle Beglaubigung

Wenn sichergestellt werden soll, dass bei einer „Signierung“ der jeweils Signierende auch der ist, für den er sich ausgibt und, dass dies auch für alle Vorgänger galt, könnte es sinnvoll sein, sich auf eine Form der zu dokumentierenden „Verifizierung“ zu einigen bzw. diese zu bestimmen. Für das zuvor erläuterte Anfügen neuer Kettenglieder ist eine Verifizierung zwar nicht notwendig, aber sinnvoll.

So kann der Schöpfer des jeweiligen „analogi-coin-Starts“ eine notwendige Form für eine solche „Verifizierung“ vorgeben. Sie könnte z.B. besagen, dass bei jeder Benennung, also „Signierung“, die jeweilige Unterschrift des „Letzt-Benannten“ vor dem Notar vorzunehmen ist. Der Notar prüft z.B. anhand des Personalausweises, ob der „Letzt-Benannte“ der ist, der die „Neu-Benennung“ unterschreibt und beglaubigt sodann die Unterschrift mit seinem Dienstsiegel und seiner eigenen Unterschrift. Auch könnte z.B. geregelt werden, dass die Verifizierung auch durch den „Neu-Benannten“ oder durch einen vom „Neu-Benannten“ bevollmächtigten Vertreter erfolgen kann.

Exkurs: Verifikation bei Teilung von „Signaturketten“:

Es sollte unbedingt geregelt sein, dass bei einer Teilung einer „Signaturkette“ ein Notar die Übereinstimmung der Kopie/n mit dem Original auf jeder Kopie beglaubigt. So soll vermieden werden, dass plötzlich zu viele Kopien, und damit mehr als 100/100, unautorisiert im Umlauf sind. Auch für weitere Nachweisprobleme könnte es sinnvoll sein, andere - ggf. auch notarielle - Verifizierungsmöglichkeiten in Betracht zu ziehen.

Form der „Dokumentation“

Es kann festgelegt werden, dass als gültige Dokumentation, die „Papierform mit notariell beglaubigten Unterschriften“ und ggf. „notariell beglaubigten Original-/Kopienübereinstimmungen“ gilt (nachfolgend auch: „beglaubigte Papierform“).

Es geht hierbei ausschließlich um die Form der „Dokumentation“, welcher die „Signierung“ und die „Verifizierung“ derselben in ihrer jeweiligen vorgegebenen Form vorausging.

Fazit 1 :

Da die „analog dokumentierte Signaturkette“ auch als „analoger Coin“ im Gegensatz zu dem o.g. „elektronischen Coin“ (Bitcoin Whitepaper) bezeichnet werden kann, sind die Begriffe „analoge Signaturkette“, „analoger Coin“ und „Signierungshistorie“ gleichbedeutend.

Die „Signierungsmöglichkeit“ ist also nicht identisch mit dem Coin. Diese Möglichkeit ist nicht die Historie und erst recht nicht die Dokumentation dieser Historie. Somit ist die analoge „Neu-Benennungsmöglichkeit“, bzw. „Signierungsmöglichkeit“ NICHT der „analoge Coin“, die „analoge Signaturkette“ bzw. die „Signierungshistorie“.

Der „Coin“/die „analoge Signaturkette“ bildet weder einen Anspruch (§ 194 BGB) - worauf auch immer - ab, noch erhält der jeweils „Letzt-Benannte“ einen Anspruch (§ 194 BGB) auf etwas Bestimmtes oder auch nur Bestimmbares. Das Gleiche gilt für die Dokumentation der „analogen Signaturkette“.

Der „Letzt-Benannte“ hat lediglich die Möglichkeit, die nächste „Signierung“ zu initiieren, also eine Person seiner Wahl zu benennen („analoge Signierungsmöglichkeit“), was bereits mit einem einfachen Sagen von: *„Ich benenne die (B)“* bewerkstelligt werden könnte.

Nicht mehr - aber auch nicht weniger!

Die jeweilige dokumentierte „analoge Signaturkette“ beinhaltet lediglich die Darstellung der erfolgten „Benennungen“ und ggf. „Verifizierungen“ (z.B. der Beglaubigungen), hat aber keinen darüberhinausgehenden Inhalt/Gehalt; sie stellt also nur eine Form ohne weiteren Inhalt dar, vergleichbar einem „Grundbuch ohne Grundstück“; substanzlos.

Ein „analoger Coin“, eine „analog dokumentierte Signaturkette“, die Historie, befindet sich mangels physischer Existenz an keinem bestimmten Ort. Lediglich die zentrale „Dokumentation“ der „analogen Signaturkette“ befindet sich jeweils bei dem, der den Bogen Papier aktuell in seinem Besitz hat. Von diesem könnte die „Dokumentation“ physisch vernichtet werden. Würde dies erfolgen, wäre die „Dokumentation“ der bisherigen „Benennungen“ und „Verifizierungen“ zerstört. Die „Dokumentation“ hätte nun auch keine Form mehr und wäre somit plötzlich physisch inexistent.

Der „Coin“, die „Signaturkette“, also die „Benennungshistorie“ selbst, wäre jedoch nicht verschwunden. Sie wäre nur nicht mehr dokumentiert und somit auch nicht mehr nachweisbar. Allerdings kann es ab endgültiger Zerstörung der „Dokumentation“ auch zu keinen spielregelkonformen weiteren Benennungen mehr kommen.

Die zuvor erläuterte „analog dokumentierte Signaturkette“ hat keinen wirklichen Inhalt/Gehalt.

Sie besteht nur aus nacheinander erfolgten und verifizierten Benennungen, die auf Papier dokumentiert sind. Mit anderen Worten: Eine bloße Form ohne Inhalt, ohne Substanz und ohne intrinsischen Wert.

Die Dokumentation auf Papier ist wie ein „Grundbuch ohne Grundstücke“.

Übergang aus der realen in die virtuelle Welt

Möchte jemand sich beispielsweise die Kosten für diese Verifizierungsform (Beglaubigung durch den Notar) sparen, oder aus anderen Gründen keine dritte Partei involviert sehen, z.B. wegen des Wunsches auf Privatheit, aber dennoch eine gewisse, das Vertrauen in einen Notar ersetzende, Sicherheit behalten, könnte er einen Ausweg darin erblicken von der realen Welt in die virtuelle digitale Welt zu wechseln.

Demnach könnten zu diesem Zweck die drei Formen, nämlich die „Form der Signierung", die „Form der Verifizierung" und die „Form der Dokumentation" beispielsweise in ein Blockchain-Netzwerk verlagert werden.

Ein Inhalt/Gehalt (außer der „Dokumentation" der „Benennungen" und ggf. der „Verifizierungen") kann - mangels Existenz – auch nicht verlagert werden.

Es würden somit nur die jeweiligen drei Formen vom Analogen hin zum Digitalen verändert.

Dadurch würde auch kein Inhalt/Gehalt neu entstehen oder hinzugefügt; erst recht kein Anspruch gem. § 194 BGB entstehen.

IV. Virtuelle Welt – „digitale Signaturkette"

Form der „Dokumentation"

Ein Blockchain-Netzwerk dient insbesondere einer möglichst fälschungssicheren Dokumentation.

Es ersetzt die „beglaubigte Papierform". Es dokumentiert die erfolgten gültigen „Neu-Benennungen", die „Signierungen" und somit die Historie.

Statt des zuvor benutzten Begriffs der „Signierung" wird im Bitcoin-Blockchain-Netzwerk der Begriff der „Transaktion" verwendet.

Die Dokumentationen von allen erfolgten „Transaktionen" - bei denen jedoch tatsächlich nichts, erst recht kein Anspruch (§ 194 BGB), übertragen wird - und somit alle Transaktionshistorien aller „digitaler Signaturketten" („elektronischer Coins"), können von jedem Ort auf der Welt mit funktionierendem Internetzugang und Computer-Hard-/und Software von jedem jederzeit eingesehen werden.

Eine Anfragemöglichkeit bei einer geografisch bestimmbaren Dokumentationsstelle, somit einer dritten Partei, ist weder erforderlich noch tatsächlich möglich.

Das Bitcoin-Blockchain-Netzwerk ist an keinem bestimmten Ort zu lokalisieren. Es befindet sich zugleich überall und nirgends. Auch gibt es kein Original, von dem es Kopien geben könnte. Tatsächlich bestehen nur - potentiell - unendlich viele, Quasi-Original-Exemplare der „Dokumentation" aller Transaktionshistorien, mithin eine dezentrale Dokumentation aller Transaktionen.

Die Blockchain-Technologie gehört zu der Gruppe der Distributed-Ledger-Technologien (DLT).

Form der „Verifizierung"

Diese digitale „Dokumentation" soll - wie die analoge - vor der Gefahr von Verfälschungen so weitgehend wie möglich geschützt werden.

Deshalb müssen bei einem Blockchain-Netzwerk neue Einträge („Transaktionen") bevor sie endgültig im Netzwerk aufgenommen/dokumentiert werden, verifiziert werden. Hier existieren verschiedene Verfahren der „Verifizierung".

Welches Verfahren im jeweiligen Blockchain-Netzwerk gelten soll, kann durch den Schöpfer des Netzwerks von Beginn an im Protokoll bestimmt werden oder/und ggf. später - ggf. auch durch die Nutzer - geändert werden.

Für die Bitcoin-Blockchain und zurzeit noch die Ethereum-Blockchain gilt ein konsensuales, also ein nichtautoritär direktives, Verifizierungsverfahren. Es ist das sogenannte „Proof-of-Work-Verfahren".

Dieses wird durch die sogenannten „Nodes“, das sind mit dem Blockchain-Netzwerk verbundenen Computer, am Laufen gehalten. Diese „Nodes“ übernehmen sozusagen die Arbeit des Notars und verifizieren die „gewünschten“ „Transaktionen“, d.h. die gewünschten Verlängerungen der „Signaturketten“, welche von den jeweils „Letzt-Benannten“ der „Signaturketten“ initiiert wurden und von einem sogenannten „Miner“ (s.u.) dem Netzwerk vorgeschlagen wurde.

Exkurs: Ein „Neu-Benannter“ ist hier keine bestimmte Person.

Wichtig für die steuerliche Einordnung ist, dass im Gegensatz zu einer „analog dokumentierten Signaturkette“ in einer „digitalen Signaturkette“ der „Erst-Benannte“, der „Letzt-Benannte“ und der „Neu-Benannte“ nicht bestimmte Personen bzw. bestimmte Steuerpflichtige sind.

Zur Verlängerung einer „digitalen Signaturkette“, also für die Initiierung einer „Transaktion“, werden sowohl für den „Erst-Benannten“, den „Letzt-Benannten“ als auch für den „Neu-Benannten“ - an Stelle von Namen usw. - jeweils ein sogenannter „Öffentlicher Schlüssel“, ein „Public Key“, angegeben.

Diese „Öffentlichen Schlüssel“ sind grundsätzlich von jedem frei und anonym erzeugbar und daher vom System her nicht von vorneherein einer bestimmten Person bzw. einem bestimmten Steuerpflichtigen zugeordnet. So ist es möglich, sich nahezu unendlich viele „Öffentlichen Schlüssel“ zu erzeugen und dann für jede „Transaktion“ einen anderen zu verwenden, was interessanterweise auch der Erzeuger des „Bitcoin“ in seinem „Whitepaper“ empfiehlt. So kann es auch dazu kommen, dass bei einer Transaktion beide „Öffentliche Schlüssel“ („Public Keys“) zu derselben Person gehören.

Im Bitcoin-Netzwerk wird dieser „Öffentliche Schlüssel“ in einer verkürzten Darstellung als „Bitcoin-Adresse“ bezeichnet.

Ein „Öffentlicher Schlüssel“ („Public Key“) des Bitcoin-Blockchain-Netzwerkes könnte so aussehen:

04eedc5d392b8608b35b919da1b8ba3615cc305895309a6a9c6acda482b5c1e5ac6bcd896f15757143d7898a83ac2a23fdefd1f33960352b972876a80ba95481d6 .

Eine hieraus abgeleitete Kurzversion, die sogenannte "Bitcoin-Adresse", würde so aussehen:

1Bavq5jaxqV58Z88iPRZmqisEXsrjwTc8W .

Form der Entstehung einer neuen digitalen Signaturkette durch Mining

Der „Miner“, z.B. der „Antminer“, ist ein spezialisierter Hochleistungscomputer, der von einer oder mehreren natürlichen oder juristischen Personen (Betreiber) betrieben wird.

Häufig wird auch der Betreiber als „Miner“ bezeichnet. Daher ist es insbesondere für steuerliche Zwecke entscheidend, welche Bedeutung dem Begriff „Miner“ im jeweiligen Diskurs zugedacht wird.

Im Bitcoin-Blockchain-Netzwerk ist programmtechnisch vorgegeben, dass neue „Signaturketten“ nur durch das „Proof-of-Work-Verfahren“ (PoW) aktiviert werden.

Hierbei versuchen die „Miner“ eine gültige Lösung für ein vom Netzwerk vorgegebenes mathematisches Rätsel zu finden, indem sie sehr viele Rateversuche sehr schnell hintereinander durchführen. Dies kann verglichen werden mit dem Versuch, ein technisch perfektes Zahlenschloss mit mehreren richtigen Lösungen - allein durch Ausprobieren d.h. ohne technische Hilfsmittel und manuelle Geschicklichkeit - zu „knacken“.

Je mehr Versuche jemand in einer bestimmten Zeitspanne ausprobiert, umso wahrscheinlicher ist es, dass er eine der passenden Lösungen als Erster findet. Allerdings kann es zu jedem dieser mathematischen Rätsel immer nur einen einzigen Gewinner geben: Nämlich immer nur den, der auf eine der vielen gültigen Lösungen zuerst getippt hat.

Eine Garantie auf den „Hauptgewinn“ gibt es - wie in jeder Lotterie üblich - nicht. Es ist aber durchaus möglich, wenn auch nicht sehr wahrscheinlich, wie beim Lotto, dass ein Versuch, ein Tipp, ausreicht, um die richtige Zahl zu erraten.

Da die „Miner“ für ihre Arbeit sehr viel Strom benötigen, entstehen dem Betreiber durch die Arbeit („work“) der „Miner“ erhebliche Kosten für elektrischen Strom und außerdem für die Unterbringung und den Betrieb der „Miner“.

Damit die Betreiber dennoch ihre „Miner“ arbeiten lassen, winkt ihnen z.B. im Bitcoin-Netzwerk - zurzeit noch - im Erfolgsfall ein „Gewinn“. Gewinner ist nur der „Miner“, der als Erster eine gültige Lösung errät und diese, sehr

vereinfacht beschrieben, auch als Erster an das Netzwerk sendet und dort dann die nachfolgende „Verifizierung“ erfolgreich verläuft. Alle anderen haben verloren und können nur auf das nächste Spiel hoffen.

Exkurs: Blockchain

In einer sehr vereinfachenden Beschreibung kann man sich eine Blockchain vorstellen als eine Reihe aneinandergereihter Blöcke, welche elektronische Daten enthalten. Nachdem in einer Blockchain der erste „Block“ („Genesis-Block“) erzeugt wurde, wird an diesen ein zweiter „Block“ angehängt. Aus den Daten des ersten „Blocks“ und weiterer Daten werden Werte ermittelt, die garantieren, dass überprüft werden kann, ob der angehängte „Block“ ein gültiger „Block“ ist. Dann folgt der dritte „Block“ und so weiter.

Ein „Miner“ erzeugt einen leeren „Block“ und packt in diesen die von ihm ausgewählten „Transaktionswünsche“, die an das Blockchain-Netzwerk gesandt wurden.

Man könnte ein Blockchain-Netzwerk auch so programmieren, dass jede einzelne Transaktion in ihren eigenen einzelnen „Block“ eingefügt werden müsste. Das wäre jedoch nicht effektiv.

Der „Miner“ nimmt aus der Menge der an das Netzwerk geschickten „Transaktionswünsche“, i.d.R. die für den Betreiber des „Miners“ wirtschaftlich interessantesten in seinen „Block“. Das sind jene, bei denen die Initiatoren der „Transaktionswünsche“ für den Erfolgsfall eine möglichst hohe sogenannte „transaction-fee“ ausgelobt haben.

Diese „transaction-fee“ bekommt er - genauso wie den o.g. Gewinn - erst, wenn er als erster eine gültige Lösung für das o.g. mathematische Rätsel erraten hat und dann seinen „Block“ mit den darin von ihm aufgenommenen „Transaktionswünschen“ bzgl. der diversen „Signaturketten“ an das Netzwerk gesendet hat und dieser „Block“ insgesamt verifiziert wurde. Früher wurde die „transaction-fee“ zusammen mit dem o.g. Gewinn als „Blockreward“ bezeichnet; heute meint man mit „Blockreward“ i.d.R. nur isoliert den o.g. Gewinn.

Die „transaction-fee“ ist wie auch der o.g. „Gewinn“ nichts in der Realwelt Existierendes. Er besteht weder aus Geld noch anderem, was einen Anspruch nach § 194 BGB darstellen, verschaffen oder garantieren würde, sondern ist vielmehr wiederum nur ein Signaturkettenbündel von z.B. „5 Satoshi“, zu verstehen lediglich als „Neu-Benennungsmöglichkeit“ /„Signaturmöglichkeit“ bzgl. der bis zu fünf „1-Satoshi-Signaturketten“ s.u. .

Statt „Gewinn“ wird nachfolgend auch der Fachbegriff, der „Blockreward“, verwendet. Dieser „Blockreward“ ist zurzeit mit 6,25 Bitcoin (BTC) bezeichnet.

Ca. alle 10 Minuten entsteht ein Gewinn, ein neuer „Blockreward“. Er wird jeweils als das erste Glied einer neuen digitalen „Signaturkette“, eines neuen „Coins“, protokollgesteuert vom Netzwerk - sozusagen automatisch - aktiviert.

Der Betreiber lässt für den Fall seines Gewinns dem Netzwerk vorab durch seinen „Miner“ mitteilen, welcher der „Erst-Benannte“, also der zuerst benannte „Öffentliche Schlüssel“ („Public Key“) ist, mit welchem der „Blockreward“ verknüpft werden soll.

Meistens wird er eine Verknüpfung vorgeben, welche ihm selbst die weitere Benennung ermöglicht.

Diese Benennungs-Möglichkeit ist alles, was der „Miner“, bzw. dessen Betreiber, gewinnt, d.h. eine „Signaturmöglichkeit“ s.u. .

Das bedeutet, dass der Miner, bzw. dessen Betreiber, mit dem „Blockreward“ nichts in der Realwelt gewonnen hätte, erst recht kein Geld oder etwas Anderes, was einen Anspruch nach § 194 BGB darstellen, verschaffen oder garantieren würde. Er erhält eben nur den Beginn eines Signaturkettenbündels von 6,25 BTC, zu verstehen lediglich als „Signaturmöglichkeit“ s.u. .

Diese neue digitale „Signaturkette“ kann fortan durch Benennungen („Transaktionen“), zuerst nur vom „Erst-Benannten“, danach von allen später Benannten verlängert werden.

Da programmtechnisch im Protokoll vorgegeben wurde, dass ein Bitcoin in 100.000.000 kleinste virtuelle Einheiten, „Satoshi“ genannt, aufgeteilt werden kann, können aus einem „Blockreward“ von 6,25 Bitcoin (BTC) potentiell bis zu 625.000.000 einzelne Signaturketten, die jeweils mit einem anderen Öffentlichen Schlüssel (Public Key) verknüpft werden könnten, hervorgehen. Oder anders dargestellt: Den „Blockreward“ kann man sich auch vorstellen, als ein als gedachtes Bündel, zunächst parallel verlaufender Signaturketten, welches zumindest potentiell in bis zu 625.000.000 einzelne Signaturketten aufgespalten und auch wieder teilweise oder vollständig zusammengeführt werden kann.

Exkurs: Der „Blockreward" wird weder hergestellt noch angeschafft.

Den „Blockreward" wird vom ratenden „Miner", bzw. dessen Betreiber, weder hergestellt noch angeschafft.

Der ratende „Miner", bzw. dessen Betreiber, beherrscht nicht den Herstellungsprozess, denn er kann weder auf die Quantität, die Qualität noch den Zeitpunkt der Aktivierung des „Blockreward", einwirken.

Somit kann er - steuerlich - nicht als Hersteller der „Blockreward" qualifiziert werden.

Auch kann - steuerlich - keine Anschaffung durch den ratenden „Miner", bzw. dessen Betreiber, vorliegen, da er den vom System selbst lediglich aktivierten „Blockreward" nicht von einem Rechtsvorgänger erwirbt. Vielleicht könnte es etwas Drittes sein, ein „Autonomes Emergieren" im System?

Die vom Protokoll vorgegebene maximal mögliche Anzahl an „Signaturketten" im Bitcoin-Netzwerk beträgt ca. 100.000.000 x 21.000.000, welche nach und nach durch das System selbst, jeweils als „Blockreward", aktiviert werden.

Die maximale Anzahl an „Signaturketten" im Etherum-Netzwerk ist bis jetzt nicht endgültig begrenzt. In anderen Blockchain-Netzwerken wird die Anzahl der Signaturketten teilweise von einzelnen Akteuren bestimmt.

Die Anzahl der „Signaturketten"/„Coins" eines Blockchain-Netzwerkes ist irrelevant für deren grundsätzliche steuerliche Beurteilung.

Die Dokumentation über die Historie von „1 Bitcoin" ist nichts Anderes als die Historie von 100.000.000 getrennten Dokumentationen über jeweils „1 Satoshi".

Hier besteht ausnahmsweise das Ganze (Dokumentation über „1 Bitcoin") aus der Summe seiner Teile, (nämlich 100.000.000 getrennte Dokumentationen über jeweils „1 Satoshi"), denn die Historie aller 100.0000.000 Signaturketten ist völlig identisch mit der Historie der als Bündel zusammengefassten Signaturkette, deren Dokumentation mit „1 Bitcoin" beschrieben wird.

Form der Benennung - „Transaktion" – als Form für das Anfügen neuer Glieder/"Signaturmöglichkeit"

Wer hat nun die Möglichkeit zu initiieren, dass einer „Signaturkette" ein weiteres Glied angehängt werden soll, also einem anderen „Öffentlichen Schlüssel" („Public Key") die nächste „Signaturmöglichkeit" eröffnet werden soll?

Wie oben bereits dargestellt, benennt der „Miner" dem Netzwerk, welchem „Öffentlichen Schlüssel" („Public Key") der Gewinn, der „Blockreward", zugeordnet werden soll.

Nur wer auch den zu einem „Öffentlichen Schlüssel" („Public Key") jeweils zugehörigen „Privaten Schlüssel" („Private Key") kennt, dem ist es möglich, eine Verlängerung der Dokumentation der „Signaturkette", hier „Transaktion" genannt, zu initiieren. *(„Not your keys, not your Bitcoin!".)*

„Public-Key" und „Private-Key" bilden gemeinsam das sogenannte „kryptografische Schlüsselpaar".

Jeder, der dieses „kryptografische Schlüsselpaar" kennt, kann eine Transaktion initiieren, indem er beim Bitcoin-Blockchain-Netzwerk eine Verlängerung der „Signaturkette", sozusagen eine „Neu-Benennung" /„Neu-Verknüpfung" mit einem anderen „Öffentlichen Schlüssel" („Public Key") beantragt/wünscht.

Hierbei muss er seinen „Privaten Schlüssel" („Private Key") zur „digitalen Signatur" einsetzen. Dies hat - sehr vereinfacht ausgedrückt - im Ergebnis die gleiche Funktion wie die höchstpersönliche handschriftliche Signatur des Signierenden bei der im vorigen Kapitel beschriebenen „analogen Signierung", ohne welche, gemäß der geltenden Spielregeln, keine „Neu-Benennung" bzw. "Neu-Verknüpfung" erfolgen kann.

Die „Miner" können - müssen jedoch nicht - diesen Neuverknüpfungswunsch entgegennehmen, d.h. in ihren neuen „Block" aufnehmen. Sofern sie mit ihrem Raten (s.o.) erfolgreich sind, gelangt die aufgenommene „Transaktion" zusammen mit vielen anderen „Transaktionen" in den neuen „Block" an das bisherige Ende der Bitcoin-Blockchain, wo der „Block"/die „Transaktionen" von den „Nodes" verifiziert werden können (s.o.).

Die Bitcoin-Blockchain dient, wie oben beschrieben, der dezentralen „Dokumentation" aller bisher erfolgter „Transaktionen" bezüglich aller „Signaturketten"/„Coins". Die Rückverfolgbarkeit der Kettenglieder einer

„Signaturkette“ ist jedoch nicht so leicht möglich, da es i.d.R. zu Aufspaltungen der „Blockreward“ und später auch wieder zu Bündelungen mit anderen „Signaturketten“ kommt. So verändert sich die Anzahl aller „Signaturketten“ permanent.

Exkurs: Wallet

Das „kryptografische Schlüsselpaar“ wird in einer sogenannten „Wallet“ verwahrt. Dieses Schlüsselpaar könnte sich jemand in seinem Gehirn einprägen („Brain-Wallet“) oder auf ein Stück Papier schreiben („Paper-Wallet“), in Metall prägen oder in einem elektronischen/technischen Gerät oder auf noch andere Weise speichern.

In einer sogenannten „Wallet“ befindet sich mindestens ein „kryptografisches Schlüsselpaar“, ohne dessen jeweilige Kenntnis und Verwendung eine „Neu-Benennung“/„Transaktion“ nicht möglich ist.

In der Wallet, z.B. „Paper-Wallet“, befindet sich kein „elektronischer Coin“ also keine „digitale Signaturkette“.

Das bedeutet nicht zwangsläufig, dass es keine technischen Geräte geben könne, in denen neben dem „kryptografischen Schlüsselpaar“ auch eine „Dokumentation“ der „digitale Signaturkette“ teilweise oder vollständig gespeichert werden könnte.

Fazit 2 :

Da die „digitale Signaturkette“ auch als „elektronischer Coin“ im Gegensatz zu dem o.g. „analogen Coin“ bezeichnet werden kann, sind die Begriffe „digitale Signaturkette“, „elektronischer Coin“ und „Signaturhistorie“ gleichbedeutend.

Die „Signaturmöglichkeit“ ist also nicht identisch mit dem Coin.

Somit ist die digitale „Neu-Benennungsmöglichkeit“, bzw. „Signaturmöglichkeit“ NICHT der „elektronische Coin“, die „digitale Signaturkette“ bzw. die „Signaturhistorie“.

Der „Coin“/die „digitale Signaturkette“ bildet weder einen Anspruch (§ 194 BGB) auf irgendetwas ab, noch erhält der jeweils „Letzt-Benannte“, der über die Kenntnis des „Kryptografischen Schlüsselpaares“ verfügt, einen Anspruch (§ 194 BGB) auf etwas. Das gleiche gilt für die Dokumentation der „digitalen Signaturkette“.

Der „Letzt-Benannte“ hat lediglich die Möglichkeit, die nächste „Transaktion“ zu initiieren, also eine „Bitcoinadresse“/ einen „Öffentlichen Schlüssel“ („Public Key“) seiner Wahl zu benennen („digitale Signaturmöglichkeit“).

Nicht mehr - aber auch nicht weniger!

Die jeweilige dokumentierte „digitale Signaturkette“ beinhaltet lediglich die erfolgten „Benennungen“ und ggf. „Verifizierungen“, hat aber sonst keinen darüberhinausgehenden Inhalt/Gehalt; sie stellt also nur eine Form ohne weiteren Inhalt dar, vergleichbar einem „Grundbuch ohne Grundstück“; substanzlos. Ein „elektronischer Coin“, eine „digitale Signaturkette“, befindet sich mangels physischer Existenz an keinem bestimmten Ort. Lediglich die dezentrale „Dokumentation“ der erfolgten „Transaktionen“ bzgl. der „digitalen Signaturketten“ „befindet“ sich in der Blockchain.

Die Blockchain, als Dokumentationsform, „befindet“ sich überall, wo sie technisch heruntergeladen wird.

Eine „digitale Signaturkette“, die Historie, kann mangels physischer Existenz weder in Besitz genommen noch zerstört werden. Lediglich die Dokumentationsform, die Blockchain, kann inaktiv werden und bleiben, wenn bzw. solange es keine „Miner“ und/oder „Nodes“ o.ä. gibt, die Transaktionswünsche erfüllen bzw. Verifizierungstätigkeiten erledigen.

Der „Coin“, die „Signaturkette“, also die „Benennungshistorie“ selbst, wäre jedoch nicht verschwunden. Sie wäre nur nicht mehr dokumentiert. Allerdings kann es ab endgültiger Zerstörung der „Dokumentation“ auch zu keinen formgerechten weiteren Benennungen mehr kommen.

Die zuvor erläuterte „digitale Signaturkette“ hat, wie die „analog dokumentierte Signaturkette“, keinen wirklichen Inhalt/Gehalt.

Sie besteht nur aus nacheinander erfolgten und verifizierten Benennungen, die in der Blockchain dokumentiert sind.

Mit anderen Worten: Eine bloße Form ohne Inhalt und ohne intrinsischen Wert.

Die Dokumentation in der Blockchain ist wie ein „Grundbuch ohne Grundstücke“.

Und wer bezahlt für so etwas?

Oder warum sollte jemand reales Geld (Fiat-Geld, wie z.B. Euro) oder einen anderen Anspruch im Sinne von § 194 BGB für eine intrinsisch wertlose analoge „Signierungsmöglichkeit“ bzw. digitale „Signaturmöglichkeit“ hingeben?

Ganz einfach: Weil er es möchte!

Oder aus Hoffnung, dass er jemanden findet, der ebenso hofft, jemanden zu finden, der ihm für diese Möglichkeit mehr gibt, als er selbst dafür gegeben hat.

Wer beispielsweise für eine „Signaturmöglichkeit“ im System „Jesus Coin (JC)“ bezahlte, erhoffte sich vielleicht, wie im „Whitepaper“ angedeutet, vor der Hölle bewahrt zu bleiben (Zitat von Seite 13: *“If you don’t immediately buy Jesus Coin after reading this whitepaper, you’re going to hell.”*). Ob für einen Ablassbrief in analoger Form oder in digitaler Form bezahlt wird, ist zumindest ertragsteuerlich unerheblich. Es kommt auf den Inhalt und nicht auf die Form an.

Dasselbe muss dann auch für alle anderen analogen und digitalen „Signaturmöglichkeiten“ ohne Anspruch auf „Sündenvergebung“ oder andere diesweltlich nicht nachprüfbaren Versprechen oder Ansprüche (§ 194 BGB) gelten!

V. Überblick und Vergleich bzgl. der wichtigsten Eigenschaften der Dokumentationen von dokumentierten Coins (=Signaturketten)

	„analog (dokumentiert)“	**„digital (dokumentiert)“**
Physische Beschaffenheit oder Substanz des Coins (=Signaturkette)	keine, da nur HISTORIE	keine, da nur HISTORIE
DOKUMENTATION DER HISTORIE :		
Form der Entstehung, des Beginns, der Dokumentation eines „Coins“, einer Signaturkette	Beschreiben eines Bogens Papier, insbesondere mit den Angaben des sich selbst „Erst-Benannten“ („coin-Start“).	Aktivierung, z.B. eines „Blockreward“, durch Verknüpfung mit einem „Public-Key“ aufgrund eines programmierten Blockchain-Protokolls (z.B. BTC -> PoW).
Form der dokumentierten Benennung	Schreiben auf Papier mit eigenhändiger Unterschrift („Signierung“). Benennung selbst formlos möglich, i.d.R. jedoch nur durch geschäftsfähige Person.	Elektronisches Initiieren einer kryptografisch signierten „Transaktion“ Bei Dokumentations-Erfolg, ggf. Realakt. Benennung selbst formlos möglich. Die Benennungs-Dokumentation in der Blockchain kann auch durch geschäftsunfähige Person erfolgen.
Form der dokumentierten Verifizierung	Durch lebende Person / Notar oder benannte Person oder von dieser bevollmächtigte Person.	Computernetzwerk bzw. dessen Betreiber / “Nodes“ (z.B. BTC -> PoW).
Form der Dokumentation	Papier – zentral	Blockchain – dezentral

	„analog (dokumentiert)“	**„digital (dokumentiert)“**
Teilbarkeit des Coins, der „Signaturkette“, = Trennung der zukünftigen Historie	Jede aus einem Bündel an Signaturketten abgespaltene Signaturkette ist eine eigene Signaturkette und kann ab Trennung für sich gesondert weitergeführt werden. Somit ist nur die kleinste Signaturkette (je nach Angabe im „coin-Start“) nicht teilbar.	Jede aus einem Bündel an Signatur-ketten abgespaltene Signaturkette ist eine eigene Signaturkette und kann ab Trennung für sich gesondert weitergeführt werden. Somit ist nur die kleinste Signaturkette (z.B. 1 Satoshi im Bitcoin-Netzwerk) nicht teilbar.
Inhalt/Gehalt des Coins, der „Signaturkette“	Erfolgte „Signierungen“ (=Benennungen).	Erfolgte „Transaktionen“ (=Benennungen).
Umkehrbarkeit/Fälschbarkeit der Dokumentation der Benennungen	Umkehrbarkeit bzw. Fälschbarkeit der Dokumentation von „Signierungen“ evtl. möglich, deshalb Vertrauen in dritte Partei bzw. zuvor Benannten notwendig.	Umkehrbarkeit bzw. Fälschbarkeit der Dokumentation von „Transaktionen“ grundsätzlich nicht möglich, deshalb kein Vertrauen in dritte Partei notwendig.
Nutzungsmöglichkeiten des Coins, der „Signaturkette“, bzw. der Dokumentation der Historie	Grundsätzlich nicht vorgegeben.	Grundsätzlich nicht vorgegeben.
Wert der „Signierungsmöglichkeit“ bzw. „Signaturmöglichkeit“	Kein intrinsischer Wert bzw. Nutz-/Verbrauchswert Extern kann ihr jeweils ein Wert (in Bargeld oder Anspruch gem. § 194 BGB) beigemessen werden. Er erscheint nur zum jeweiligen Realisationszeitpunkt.	Kein intrinsischer Wert bzw. Nutz-/Verbrauchswert Extern kann ihr jeweils ein Wert (in Bargeld oder Anspruch gem. § 194 BGB) beigemessen werden. Er erscheint nur zum jeweiligen Realisationszeitpunkt.

VI. Fragen zur steuerlichen Beurteilung

Für die steuerliche Beurteilung der hier dargestellten Tatsachen wären insbesondere folgende Fragen zu klären:

1. **Kann eine Signaturkette, sei sie analog oder digital dokumentiert, die schon ursprünglich keinerlei Anspruch (§ 194 BGB) gegenüber wem auch immer begründet oder abbildet, und deren Verlängerung auch keinen solchen Anspruch nachträglich entstehen lässt oder vermittelt („anspruchslose Signaturkette"), ein Wirtschaftsgut im ertragsteuerlichen Sinne sein?**
   Die Beurteilung sollte berücksichtigen, dass jeder jederzeit eine analog dokumentierte Signaturkette starten kann und jeder, der diesbezügliche technische Expertise hat, neue digital dokumentierte Signaturketten nach dem ERC20-Standard herstellen und damit neu starten lassen kann.

   Hierbei könnte zu beachten sein:

   a.
   Zurzeit (25. Januar 2021) sind 8.311 sogenannte „Kryptowährungen" (insbesondere „anspruchslose Signaturketten") auf „coinmarketcap.com" gelistet.
   Hinzu kommen unzählbare weitere noch nicht oder nicht mehr dort gelistete sogenannte „Kryptowährungen". „Analoge Coins" wird es vermutlich sehr viel weniger geben.

   Alles was für die Wirtschaftsguteigenschaft von „anspruchslosen Signaturketten"/"**digitalen Signaturketten"** vorgebracht wird,

   - muss für **alle** „anspruchslosen Signaturketten" /"**digitalen Signaturketten gleichermaßen** gelten

   oder

   - es muss eine sachgerechte, geeignete, relevante und offensichtliche Unterscheidung zwischen den „anspruchslosen Signaturketten" /"**digitalen Signaturketten"** erfolgen, die der Steuerpflichtige vor seinem Tätigwerden kennen können muss, um sich an einschlägig existierende **gesetzliche** Vorgaben und Restriktionen halten zu können.

   b.
   Was für „anspruchslose Signaturketten"/"**digitale Signaturketten"** gilt,

   - muss für alle „anspruchslosen Signaturketten" gelten, somit auch für **„analoge Signaturketten"**

   oder

   - es muss eine sachgerechte, geeignete, relevante und offensichtliche Unterscheidung zwischen den „anspruchslosen Signaturketten"/"**digitalen Signaturketten"** einerseits und **„analogen Signaturketten"** andererseits erfolgen, die auch - unter dem Gesichtspunkt der Technologieneutralität betrachtet - eine steuerliche Ungleichbehandlung erlaubt und zu begründen geeignet ist, die der Steuerpflichtige vor seinem Tätigwerden kennen können muss, um sich an einschlägig existierende **gesetzliche** Vorgaben und Restriktionen halten zu können.

Siehe auch Prof. Dr. Bofinger (EX-Wirtschaftsweiser) über Bitcoin in ntv vom 13.01.2021:

„Ökonomisch ist das Prinzip doch sehr einfach. Jemand gibt ein Spielgeld heraus und bringt andere dazu, ihm dafür echtes Geld zu geben. Es ist dasselbe, als wenn ich jetzt '100 Bofinger' auf einen Zettel schreiben würde und Menschen finde, die mir dafür 100 Euro geben, ohne dass ich ihnen gegenüber irgendeine Einlösungsverpflichtung habe. Bei Bitcoin ist dieses Prinzip lediglich in einem Informatik-Nebel verborgen." (https://www.n-tv.de/wirtschaft/Bofinger-zerlegt-Bitcoin-Hype-article22288515.html)

2. Wenn man die Wirtschaftsguteigenschaft für „anspruchslose Signaturketten" bejaht, ergibt sich die weitere Frage, wie die „Anschaffung" oder „Veräußerung" im ertragsteuerlichen Sinne jeweils begründet werden kann?

Hierbei könnte zu beachten sein:

a. Zurechnung

Hier kommt der Klärung der Frage der bürgerlich-rechtlichen Zurechnung gem. § 39 Abs. 1 AO und der ggf. möglichen wirtschaftlichen Zurechnung gem. § 39 Abs. 2 AO richtungsweisende Bedeutung zu.
Da es kein bürgerlich-rechtliches Eigentum oder einen Anspruch (§ 194 BGB) an „anspruchslosen Signaturketten" geben kann, kann es auch keine Person geben, die als anderer als der Eigentümer die tatsächliche Herrschaft über ein Wirtschaftsgut in der Weise ausübt, dass sie den **Eigentümer im Regelfall für die gewöhnliche Nutzungsdauer** von der Einwirkung auf das Wirtschaftsgut wirtschaftlich ausschließen kann.

Somit würde es keinen wirtschaftlichen Eigentümer (§ 39 Abs. 2 AO) geben, da es zumindest gem. Gesetzeswortlaut für die Annahme von wirtschaftlichem Eigentum zuvor zwingend des Eigentums - bzw. vielleicht ausreichend, zumindest eines Anspruchs nach § 194 BGB - eines anderen bürgerlich-rechtlichen Rechteinhabers bedarf (§ 39 Abs. 1 AO).

Was wäre die gewöhnliche Nutzungsdauer einer „anspruchslosen Signaturkette"?

Wem wäre eine „Paper-Wallet" zuzurechnen, wenn es mehrere Papierkopien oder Fotos davon gibt?

b. Übergang der Zurechnung

Auch wäre dann die Möglichkeit des Übergangs des ggf. fingierten wirtschaftlichen Eigentums zu prüfen. Denn es gibt zumindest keine reguläre Anschaffung/Veräußerung mangels Rechtsvorgängers, da es eben keine Ansprüche gem. § 194 BGB gibt, die übertragen werden könnten.
Wie würden bei Off-Chain Geschäften, z.B. Verkauf einer „Paper-Wallet", die gerade nicht in der Blockchain dokumentiert sind, also Weitergabe des „kryptografischen Schlüsselpaares" verfahren?
Wem würde das ggf. existierende Wirtschaftsgut bei Verkauf nur einer von unendlich vielen Papierkopien oder eines Fotos zugerechnet?

3. Selbst soweit die Wirtschaftsguteigenschaft für „anspruchslose Signaturketten“ festgestellt wäre, und § 23 EStG grundsätzlich anwendbar wäre, müssten die jeweils anzunehmenden Zeitpunkte der Anschaffung/der Veräußerung untersucht und festgestellt werden.

Hierbei könnte zu beachten sein:

a. zu „anspruchslose Signaturketten“ - Realisierung
Erst dadurch, dass die wirtschaftliche Leistungsfähigkeit, d. h. Kaufkraft, gesteigert wird, kann es zu einer Gewinnrealisierung kommen.
Erst wenn „anspruchslosen Signaturketten“ wieder in einen Anspruch (§ 194 BGB) z.B. Euro „getauscht“ werden (BFH IX 73/98), kommt es zu einer Realisierung eines Veräußerungspreises.
Das bedeutet andererseits, dass es zu keiner Realisierung eines Veräußerungspreises kommen kann, solange im virtuellen Bereich von einer „anspruchslosen Signaturketten“ zu einer anderen „anspruchslosen Signaturketten“ gewechselt wird, also nur virtuelle, d.h. nicht reale, Vorgänge stattfinden.

Eine Umrechnungspflicht von „anspruchslosen Signaturketten“ in Euro ist außerdem gesetzlich, zumindest für nicht im Betriebsvermögen befindliche Wirtschaftsgüter, nicht vorgesehen.

In dem nachfolgend teilweise zitierten BFH-Urteil ging es um den unmittelbaren Tausch von verschiedenen Wirtschaftsgütern in ausländischer Währung, somit ohne das Handlungsumfeld zu verlassen, also zwischendurch in die einzige in Deutschland unbegrenzt zu akzeptierende Währung (damals DM, heute EURO nach § 14 BbankG) zu tauschen.

Wichtig ist hierbei vorab festzuhalten, dass „anspruchslose Signaturketten“ keine Währung und auch keine „andere Währung“ im Sinne des zitierten BFH-Urteils sein können, da sie nicht den geforderten gesetzlichen Status einer Währung besitzen, weshalb außerdem auch das in § 23 EStG erwähnte FiFo-Verfahren nicht zwingend anzuwenden ist. Nun wird unterstellt, dass „anspruchslose Signaturketten“ zu den im KWG definierten „Kryptowerten“ gehören.

KWG § 1 Abs. 11 Nr. 10
*„Kryptowerte im Sinne dieses Gesetzes sind **digitale Darstellungen 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.**“*

> Soll nun die **Darstellung eines Wertes** oder der **dargestellte Wert** oder beides besteuert werden? Eine Digitalfotografie einer Immobilie würde die Kriterien *„auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann.“* erfüllen? Hätte diese Darstellung den Wert des Dargestellten?

Im BFH-Urteil v. 02.05.2000 - IX R 73/98 BStBl 2000 II S. 614) heißt es unter:

II. 2. a)
*„Der sich durch Währungsschwankungen ergebende Kursgewinn wird mithin nicht schon durch den Transfer eines Fremdwährungsguthabens von einem Konto auf ein anderes oder durch Gewährung eines Darlehens in Fremdwährung und Rückfluss der Darlehensvaluta in Fremdwährung gemäß § 23 Abs. 1 Nr. 1 Buchst. b EStG realisiert. Die Verlagerung des Fremdwährungsguthabens führt als solche zu keinem Vermögenszuwachs des Steuerpflichtigen und zu **keiner Steigerung seiner wirtschaftlichen Leistungsfähigkeit** (vgl. Wellmann, Deutsche Steuer-Zeitung - DStZ -1997, 253 , 254).*

Die Wertsteigerung im Privatvermögen in Form des erzielten Kursgewinns wird gemäß § 23 EStG erst dann durch einen marktoffenbaren Veräußerungsvorgang ***realisiert und damit steuerbar, wenn die ausländische Währung in DM (oder eine andere Währung) rückgetauscht wird.***
Erst in dem durch den günstigen Rücktausch erhöhten DM-Betrag (oder Betrag in einer anderen Währung) liegt der Zufluss des "Veräußerungspreises" *i.S. von § 23 letzter Absatz i.V.m. § 11 Abs. 1 EStG."*

II. 2. b)
*„**Zu Unrecht** vertritt das FA die Auffassung, beim Rückfluss des als Festgeld angelegten Fremdwährungs-kapitals und bei dessen erneuter Anlage müssten die Beträge auch dann in DM ausgedrückt werden**, wenn tatsächlich kein Rückumtausch in DM erfolgt sei.** Zwar können Fremdwährungsforderungen im Betriebsvermögen nach Maßgabe der bilanzsteuerrechtlichen Grundsätze ggf. in DM umzurechnen sein (vgl. § 244 des Handelsgesetzbuches - HGB -; BFH-Urteil vom 19. Januar 1978 IV R 61/73 , BFHE 124, 327 , BStBl II 1978, 295).* ***Das gilt jedoch nicht für Fremdwährungskapital im Privatvermögen*** *(Wellmann, DStZ 1997, 253 , 254; a. A. FG München, Urteil vom 7.Januar 1987 XIII 181/85 E , EFG 1987, 356).* ***Insoweit fehlt es an einer entsprechenden Rechtsgrundlage. Fremdwährungsbeträge im Privatvermögen sind vielmehr erst dann in DM umzurechnen, wenn sie dem Steuerpflichtigen als Einnahmen gemäß § 8 Abs. 1, § 11 Abs. 1 EStG zufließen."***

b. „anspruchslose Signaturketten" - On-Chain und Off-Chain - Zeitpunkte

Sollten Veräußerungsgeschäfte im Rahmen des § 23 EStG zu berücksichtigen sein, so wäre weiter zu untersuchen, worin das für den Zeitpunkt der Anschaffung/Veräußerung maßgebende Verpflichtungsgeschäft besteht. Wäre zwischen On-Chain und Off-Chain Aktionen zu unterscheiden?

4. Gibt es ertragsteuerlich <u>relevante</u> Unterschiede zwischen „Geschäften" mit Bezug zu <u>anspruchslosen digital dokumentierten</u> Signaturketten bzw. <u>anspruchslosen analog dokumentierten</u> Signaturketten, die zu einer unterschiedlichen und begründeten steuerlichen Beurteilung führen dürfen?

Hierbei könnte zu beachten sein:

Wäre eine entgeltliche Übertragung des Eigentums an einem Grundstück, welches im Grundbuch eingetragen ist, aber nachweislich real nicht existiert, eine Veräußerung von Grundstücken (§ 23 Abs. 1 Nr. 1 EStG) oder eines anderen Wirtschaftsgutes (§ 23 Abs. 1 Nr. 2 EStG) oder würde es überhaupt nicht unter die Tatbestände des § 23 EStG fallen, da Veräußerungsgeschäfte mit „Formen ohne Inhalt" - an denen kein Eigentum begründet werden kann - dort nicht expliziert geregelt sind? Würde die 1-jährige oder die 10-jährige „Spekulationsfrist" gelten? Wie wäre es mit der Digitalfotografie eines Grundstücks?

Wie verhält es sich mit den **<u>anspruchslosen digital dokumentierten</u>** Signaturketten bzw. **<u>anspruchslosen analog dokumentierten</u>** Signaturketten, die in § 23 EStG auch nicht als Wirtschaftsgüter ausdrücklich genannt sind?

5. Was wird in der Wallet aufbewahrt?

Laut BMF gilt:
27. Februar 2018 BETREFF Umsatzsteuerliche Behandlung von Bitcoin und anderen sog. virtuellen Währungen; EuGH-Urteil vom 22. Oktober 2015, C-264/14, Hedqvist GZIII C 3 - S 7160-b/13/10001 DOK 2018/0163969

Seite 3
b) „Wallet“ Die „Wallets“ (elektronische Geldbörsen) werden auf dem Computer, Tablet oder Smartphone gespeichert und dienen **der Aufbewahrung der sog. virtuellen Währung.**

Es werden in der „Wallet“ (z.B. Paper-Wallet) nur der Private-Key und der Public-Key aufbewahrt.
Das wäre dann gem. BMF die virtuelle Währung.
Wenn das so zuträfe, dann wäre nur ein OFF-CHAIN Geschäft ggf. nach § 23 EStG ein Geschäft mit einem Wirtschaftsgut, also ein (Mit-)Inkenntnissetzen der beiden Zeichenfolgen (Private-Key und Public-Key)?
Das „Ans-Ende-einer-Signaturkette-Gesetztwerden“ (ON-CHAIN) wäre dann kein Veräußerungsgeschäft nach § 23 EStG.

6. Eine „objektiv werthaltige Position“?

Laut gefestigter BFH muss ein Vermögenswert eine „objektiv werthaltige Position“ sein, um ertragsteuerlich als „Wirtschaftsgut“ zu gelten. Dass etwas zu einem bestimmten Zeitpunkt einen Wert hat, ist banal, so hat die Leistung eines Dienstleisters auch zu einem bestimmten Zeitpunkt einen bestimmten Wert. Das Wort „werthaltig“ hat die Bedeutung in der Zeit ausgedehnter zu sein, etwa so: Wert habend, und diesen auch (voraussichtlich) über einen längeren Zeitraum beibehaltend.
Diese „Werthaltigkeit“ muss dann aber auch noch „objektiv“ vorliegen. Das ist bei sog. „Kryptowährungen“ gerade nicht der Fall.

Hierzu ein Zitat aus der NZZ vom 11.01.2021:

„Damit lässt sich eine Schwankungsbreite für den ‘richtigen Preis’ zwischen ‘Null und sehr viel mehr’ ableiten», heisst es fast schon scherzhaft in einer Analyse der DZ Bank, des Dachgremiums der deutschen Genossenschaftsbanken, vom Freitag (8. 1).“
(https://www.nzz.ch/finanzen/bitcoin-kryptowaehrungen-im-ueberblick-ld.1336477)

7. Bei allen obigen Erwägungen ist zu beachten:

Abgabenordnung (AO)

§ 85 Besteuerungsgrundsätze

Die Finanzbehörden haben die Steuern nach Maßgabe der Gesetze gleichmäßig festzusetzen und zu erheben.

Insbesondere haben sie sicherzustellen, dass Steuern nicht verkürzt, **zu Unrecht erhoben** oder Steuererstattungen und Steuervergütungen nicht zu Unrecht gewährt oder versagt **werden.**

§ 88 Untersuchungsgrundsatz

(1) Die Finanzbehörde ermittelt den Sachverhalt von Amts wegen.

Dabei hat sie **alle für den Einzelfall bedeutsamen**,

auch die für die Beteiligten günstigen Umstände zu berücksichtigen.

(2) Die Finanzbehörde bestimmt Art und Umfang der Ermittlungen nach den Umständen des Einzelfalls sowie **nach den Grundsätzen der Gleichmäßigkeit, Gesetzmäßigkeit und Verhältnismäßigkeit**; an das Vorbringen und an die Beweisanträge der Beteiligten ist sie nicht gebunden. Bei der Entscheidung über Art und Umfang der Ermittlungen können allgemeine Erfahrungen der Finanzbehörden sowie Wirtschaftlichkeit und Zweckmäßigkeit berücksichtigt werden.

LINKS:

Zu Jesus Coin (JC)

Gelistet auf coinmarketcap.com: https://coinmarketcap.com/de/currencies/jesus-coin/

Whitepaper: https://www.chainwhy.com/upload/default/20180629/cc7814b402a92dd452854e8638a3082c.pdf

Transaktionen auf etherscan: https://etherscan.io/address/0xe2d82dc7da0e6f882e96846451f4fabcc8f90528#tokentxns