Kryptowährungen als Nachlassbestandteil – rechtliche Grundlagen und „digitale Vorsorge“

Dr. *Cyril H. Hergenröder,* M.A., Europajurist (Univ. Würzburg), Aschaffenburg/Würzburg*

Die zunehmende Digitalisierung des Alltags stellt wie viele andere Rechtsgebiete auch das Erbrecht vor neue, dogmatische wie praktische Herausforderungen. Zu den besonders werthaltigen Bestandteilen des „digitalen Nachlasses“ zählt insbesondere ein etwaig vorhandenes Guthaben des Erblassers an Kryptowährungen. Um einen sicheren und praktikablen Übergang entsprechender Vermögenswerte auf die Erben zu gewährleisten, kommt es auf eine möglichst umfassende „digitale Vorsorge“ des Erblassers zu Lebzeiten an.

A. Problemaufriss

Kryptowährungen wie beispielsweise Bitcoin, Ripple, Ethereum oder Litecoin sind als digitale Anlage- und Zahlungsinstrumente ein immer noch relativ junges Phänomen der Finanz- und Spekulationswirtschaft, welches gleichwohl im Alltag, auch infolge hohen medialen Interesses, nicht unerhebliche Relevanz erlangt hat. Entsprechende Currency- oder Payment-Token werden mittlerweile als Zahlungsmittel eingesetzt sowie auf Online-Börsen gehandelt, wobei ihr faktischer Wert sich nach Angebot und Nachfrage auf einschlägigen Kryptobörsen bestimmt.[1] Prägendes Merkmal kryptographischer Währungen ist dabei ihre hohe Volatilität, die sie zu einem beliebten Anlage- und Spekulationsobjekt macht. Rasanten Kursgewinnen folgen mitunter ebenso starke Kurseinschnitte bzw. -abstürze.

Im Zusammenhang mit der allgemein zunehmenden Bedeutung des digitalen Nachlasses verstorbener Personen rückte in jüngerer Zeit die erbrechtliche Behandlung kryptographischer Vermögenswerte in den Fokus juristischer Betrachtung. Mitursächlich dafür dürfte eine Bundestagsanfrage aus dem Jahr 2018 gewesen sein, welche unter Bezugnahme auf den Fall eines verstorbenen US-amerikanischen „Krypto-Millionärs“ die Zugriffsmöglichkeiten der Erben auf kryptographische Vermögenswerte nach deutschem Recht aufwarf.[2] Gleichwohl erscheint der Themenkreis „Kryptowährungen im Erbrecht“ trotz verschiedener zwischenzeitlich vorhandener Untersuchungen, darunter auch zu erbschaftssteuerlichen Aspekten,[3] insgesamt noch relativ wenig ausgeleuchtet.[4] Auch existiert soweit ersichtlich bis dato noch keine einschlägige Rechtsprechung, was die Bedeutung des Themas gerade mit Blick auf eine bestmögliche Nachlassvorsorge zukünftiger Erblasser und deren rechtliche Beratung allerdings nicht schmälert.

Der vorliegende Beitrag widmet sich zunächst in gebotener Kürze den für den Umgang mit entsprechenden Nachlasswerten maßgeblichen technischen Grundlagen (B.). Daran anschließend erfolgt eine Darstellung der rechtlichen Rahmenbedingungen betreffend kryptographische Nachlassbestandteile (C.), um schließlich unter Berücksichtigung des aktuellen Meinungsstands aufzuzeigen, ob und in welcher Form eine „digitale Vorsorge“ zu Lebzeiten sinnvoll ist (D.). Die Geltung deutschen Rechts wird dabei im Rahmen der nachfolgenden Ausführungen stets vorausgesetzt.[5]

B. Technische Voraussetzungen

Unter Kryptowährungen versteht man virtuelle, im Rahmen eines dezentral organisierten Computernetzwerks geschöpfte und verwaltete Ersatzwährungen, die auf verschlüsselten Datenmengen basieren.[6] Sie werden grundsätzlich nicht von einer Zentralbank oder öffentlichen

* Der Autor ist Staatsanwalt sowie Wissenschaftlicher Mitarbeiter am Lehrstuhl für Deutsche und Europäische Rechtsgeschichte, Kirchenrecht und Bürgerliches Recht an der Julius-Maximilians-Universität Würzburg (Prof. Dr. Anja Amend-Traut).

1 *Blum/Heuser*, in: Gsell/Krüger/Lorenz/Reymann (Hrsg.), beck-online Großkommentar, Stand: 15.6.2021, § 2311 Rn. 53; *Kälberer*, BC 2021, 417 (420); *d'Avoine/Hamacher*, ZIP 2022, 6 (7).

2 Zum Wortlaut sowohl der Anfrage als auch der Antwort der Bundesregierung vom 28.6.2018 siehe BT-Drs. 19/3068, S. 29.

3 Vgl. dazu überblicksweise *Amend-Traut/Hergenröder*, ZEV 2019, 113 (120) sowie eingehend die Darstellung bei *Stein/Lupberger*, DStR 2019, 311 (313 ff.) und *von Oertzen/Grosse*, DStR 2020, 1651 (1652 ff.).

4 Ebenso *Möller/Shmatenko*, in: Hoeren/Sieber/Holznagel (Hrsg.), Handbuch Multimedia-Recht, 57. EL September 2021, Teil 13.6 Rn. 81.

5 Vgl. *Medler*, ZEV 2020, 262 (265).

6 *Klinger*, in: Bengel/Reimann (Hrsg.), Handbuch der Testamentsvollstreckung, 7. Aufl. 2020, § 5 Rn. 676; *Blum/Heuser*, (Fn. 1), Rn. 49; *Amend-Traut/Hergenröder*, (Fn. 3), (114).

Stelle emittiert oder garantiert.[7] Vielmehr verwalten die Nutzer des frei über einen Client zugänglichen Peer-to-Peer-Computernetzwerks gemeinsam die Historie aller zwischen den Nutzern transferierten Werte über eine Art dezentrales virtuelles Bestands- oder Kontenbuch.[8] Die einzelnen digitalen Werteinheiten, welche als Tauschmittel akzeptiert und auf elektronischem Weg übertragen und gehandelt werden können, werden als Token bezeichnet.[9] Diese sind, trotz gelegentlich anzutreffender plakativer Bezeichnung als „digitale Münze", nicht real verkörpert und stellen auch keine abgrenzbaren virtuellen Datenmengen dar. Sie existieren vielmehr lediglich als rein digitale Information über die innerhalb eines Peer-to-Peer-Netzwerks getätigten Guthabentransaktionen. Zu diesem Zweck werden alle Transaktionen einer Kryptowährung linear und dezentral in Form einer sogenannten Blockchain fortgeschrieben. Diese funktioniert wie ein Register, bestehend aus einer Reihe von nacheinander geschalteten Einträgen, in denen die relevanten Informationen, insbesondere zu Transaktionen digitaler Token, hinterlegt sind.[10]

Das dem einzelnen Teilnehmer des Netzwerks auf der Blockchain zugeordnete Kryptoguthaben wird in passwortgeschützten Wallets ermittelt und angezeigt. Diese ähneln insoweit einem Benutzerkonto beim Online-Banking[11] und existieren als Hardware-Wallets, Desktop-Wallets, Web-Wallets oder physisch verkörpert in Papierform.[12] Jedem Wallet ist mindestens ein vom genutzten Client generiertes kryptographisches Schlüsselpaar in Form eines öffentlichen und eines privaten Schlüssels zugewiesen, die aus einer Abfolge von Zahlen und Buchstaben bestehen.[13] Während der Public Key einer Kontonummer entspricht und für alle Netzwerkteilnehmer einsehbar ist,[14] dient der grundsätzlich nur dem jeweiligen Nutzer bekannte und zumeist verschlüsselt gespeicherte Private Key dazu, auf das Kryptovermögen zuzugreifen und ausgehende Transaktionen durch ein Signaturverfahren zu autorisieren.[15] Er kann entweder in dem Wallet des Nutzers oder auf einem externen Speichermedium gespeichert oder auf einem Blatt Papier niedergelegt werden.[16] Darüber hinaus können sogenannte Seeds zum Einsatz kommen, die aus einer Aneinanderreihung mehrerer Wörter bestehen und einen zentralen Zugang zu mehreren in einem Wallet vorhandenen Private Keys ermöglichen.[17]

Ein eigenständiger Vermögenswert kommt bei alledem wirtschaftlich betrachtet weder der Datenmenge innerhalb des Netzwerks noch der Zuordnung derselben zum Public Key eines Wallets zu.[18] Wirtschaftlicher Bezugspunkt ist vielmehr der Private Key, der den Zugriff auf die einem Wallet zugeordneten Kryptowährungsguthaben und somit die Möglichkeit zu Transaktionen oder zur Umwandlung der Kryptowährung in Fiat-Geld ermöglicht.[19] Kann infolge eines fehlenden Private Keys nicht mehr auf ein Wallet zugegriffen werden, so sind eine Interaktion im Peer-to-Peer-Netzwerk und damit einhergehende Transaktionen nicht mehr möglich.[20]

C. Kryptowährungen als Nachlassbestandteil

E ist im gesetzlichen Güterstand mit M verheiratet. Sie haben drei gemeinsame Kinder. Am 1.7.2021 erwarb E 15 Bitcoins, wobei der durchschnittliche Kurswert eines Bitcoins zu diesem Zeitpunkt 28.318,51 Euro betrug. Sie führt ein Online-Wallet beim Anbieter X, bei welchem sie sich mittels einer App einloggt. Der Private Key wird vom Anbieter in diesem Wallet verwaltet. Am 1.7.2022 stirbt E, ohne eine letztwillige Verfügung errichtet zu haben. Zu diesem Zeitpunkt enthält ihr Wallet weiterhin die 15 Bitcoins. Der Bitcoin-Kurs weist zum Zeitpunkt ihres Todes noch einen durchschnittlichen Kurswert von 18.534,04 Euro auf.

I. Erbrechtliche Grundsätze betreffend kryptographische Nachlasswerte

Programmatischer Ausgangspunkt der Blockchain-Technologie ist deren Unabhängigkeit von staatlichen Institutionen. Auch die einzelnen Token einer Kryptowährung werden dem jeweiligen Nutzer eines Peer-to-Peer-Netzwerks konzeptionell allein durch technische Berechtigung und nicht etwa durch eine genuin juristische Eigentumsposition zugewiesen.[21] Auch deshalb ist die Rechtsnatur von Kryptowährungen wie beispielweise Bitcoin bis dato nicht endgültig geklärt.

Ein dingliches Recht am Eintrag in der Blockchain und damit am einzelnen Token gibt es nach herrschender Meinung jedenfalls nicht. Im geschriebenen Recht ist die Inhaberschaft an Kryptowährungseinheiten bis dato jedenfalls

---

7 *Kälberer*, (Fn. 1), (420); *d'Avoine/Hamacher*, (Fn. 1). Allerdings existieren zwischenzeitlich vereinzelt auch staatliche Kryptowährungen, darunter die E-Krone in Schweden oder der Petro in Venezuela. Vgl. hierzu *Rathmann*, 3 staatliche Kryptowährungen – Welche Länder haben ihre eigenen digitalen Währungen?, cryptoticker.io, https://cryptoticker.io/de/3-staatliche-kryptowaehrungen-welche-laender-haben-ihre-eigenen-digitalen-waehrungen/, Abruf v. 14.7.2022.

8 Dies wird als Distributed-Ledger-Technologie bezeichnet. Vgl. etwa *Ammann*, CR 2018, 379; *Schlund/Pongratz*, DStR 2018, 598; *d'Avoine/Hamacher*, (Fn. 1).

9 *Kälberer*, (Fn. 1), (420).

10 *Weiss*, NJW 2022, 1343; *Perleberg-Kölbel/Kuckenburg*, FuR 2022, 312.

11 *Weiss*, (Fn. 10), 1343.

12 *Klinger*, (Fn. 6), § 5 Rn. 678. Zur Unterscheidung zwischen sogenannten Hot Wallets und Cold Wallets siehe *Medler*, (Fn. 5), (264).

13 *Badstuber*, DGVZ 2019, 246.

14 *Blum/Heuser*, (Fn. 1), Rn. 51; *Weiss*, JuS 2019, 1050 (1052); *d'Avoine/Hamacher*, (Fn. 1), (7).

15 *Blum/Heuser*, (Fn. 1), Rn. 51; *Badstuber*, (Fn. 13), (247).

16 *Badstuber*, (Fn. 13), (247).

17 *Klinger*, (Fn. 6), § 5 Rn. 679.

18 *Klinger*, (Fn. 6), § 5 Rn. 676.

19 *Von Oertzen/Grosse*, (Fn. 3), (1652).

20 *Blum/Heuser*, (Fn. 1), Rn. 53.2; *Förster/Fast*, ZAP 2022, 227 (230).

21 *Weiss*, (Fn. 10), (1344).

nicht als dingliches Recht anerkannt.[22] Nach überzeugender Auffassung stellen die in der Blockchain abgebildeten kryptographischen Währungseinheiten ebenso wie die kryptographischen Schlüssel eines Netzwerkteilnehmers zudem mangels Körperlichkeit keine eigentumsfähigen Sachen im Sinne der §§ 90, 903 ff. BGB dar, weshalb eine Eigentumsübertragung nach den §§ 929 ff. BGB nicht in Betracht kommt.[23] Zwar kann sich eine Vertragspartei gegenüber einer anderen schuldrechtlich zur Übertragung von Kryptowährungseinheiten verpflichten.[24] Der nachfolgende dingliche Vollzug einer entsprechenden Transaktion stellt jedoch lediglich einen Realakt dar.[25] Auch existieren im Zusammenhang mit blockchainbasierten Kryptowährungen keine nach §§ 413, 398 S. 1 BGB an andere Nutzer des maßgeblichen Netzwerks abtretbaren Forderungen, da die einzelnen Token keinen Anspruch gegen einen bestimmten Dritten verkörpern.[26] Kryptographische Schlüssel und Krypto-Token sind vor diesem Hintergrund im Ergebnis als sogenannte sonstige Gegenstände im Sinne von § 453 Abs. 1 BGB anzusehen.[27]

Aus erbrechtlicher Perspektive betrachtet zählt der einem Kryptoguthaben inhärente Vermögenswert zunächst zweifelsohne zum sogenannten digitalen Nachlass eines Erblassers.[28] Hierunter ist die Gesamtheit der Rechtsverhältnisse des Erblassers betreffend informationstechnische Systeme einschließlich des gesamten elektronischen Datenbestandes des Erblassers zu verstehen.[29] Der Terminus beinhaltet somit eine gesetzlich nicht speziell geregelte Bezeichnung für die gesamte digitale Hinterlassenschaft eines Erblassers, begründet jedoch keine „Sonderkategorie" von Nachlasswerten, da das deutsche Bürgerliche Recht nicht zwischen analogem und digitalem Nachlass unterscheidet.[30] Mit dem Tod einer Person, dem sogenannten Erbfall, geht vielmehr das gesamte analoge wie digitale Vermögen des Erblassers gem. § 1922 Abs. 1 BGB im Wege der Gesamtrechtsnachfolge als Ganzes und unmittelbar auf den oder die Erben über. Dieser Grundsatz der Universalsukzession findet ohne weiteres auch auf den digitalen Nachlass und damit auch auf etwaige zur Erbschaft rechnende Kryptowährungsguthaben Anwendung.[31]

Im gewählten Beispielsfall bestimmt sich die Erbfolge mangels einer letztwilligen Verfügung nach der gesetzlichen Erbfolge gem. §§ 1924 ff. BGB. Als Ehegatte der E würde M gem. § 1931 Abs. 1 BGB neben den Kindern als Erben erster Ordnung grundsätzlich ein Viertel des Nachlasses erben, wobei sich sein Erbteil im Wege des pauschalen Zugewinnausgleichs nach §§ 1931 Abs. 3, 1371 Abs. 1 BGB auf eine Hälfte erhöhen würde. Die drei gemeinsamen Kinder würden daneben gem. § 1924 Abs. 1 und 4 BGB jeweils Erben zu einem Sechstel. Der Nachlass der E, zu dem auch das ihr bei Lebzeiten zugewiesene Kryptowährungsguthaben zählt, würde gem. § 2032 Abs. 1 BGB als gemeinschaftliches Vermögen auf die aus M und den Kindern bestehende Erbengemeinschaft übergehen.

Näher zu prüfen ist allerdings, in welcher Form diese Vermögenswerte vor dem Hintergrund ihrer oben bereits skizzierten rechtlichen Einordnung in concreto auf die Erben der E übergehen. Nicht in den Nachlass des Erblassers fallen nach dem bisher Gesagten die in der Blockchain gespeicherten Transaktionsdaten, welche das virtuelle Kryptoguthaben des Nutzers abbilden, da diesem keine Rechtsinhaberschaft an den fraglichen Daten zukommt.[32] Auch werden die den kryptografischen Währungseinheiten zugrundeliegenden Daten nicht auf einem physischen Datenträger des jeweiligen Nutzers gespeichert, wodurch das Eigentum am Speichermedium auch die rechtliche Zuordnung der darauf enthaltenen Daten umfassen könnte.[33] Schließlich bestehen innerhalb des jeweils genutzten Peer-to-Peer-Netzwerks hinsichtlich der in diesem gespeicherten Datenmengen auch keine Forderungen des einzelnen Nutzers gegenüber anderen Teilnehmern, welche im Wege der Universalsukzession auf die Erben übergehen könnten. Im Ergebnis ist nach mittlerweile gefestigter Ansicht auf den Private Key als Bezugsobjekt der Universalsukzession nach § 1922 Abs. 1 BGB abzustellen, da dieser dem Erblasser die faktische Verfügungsgewalt über sein Kryptoguthaben eröffnet, ohne dass die aus der Inhaberschaft am privaten Schlüssel resultierende faktische Verfügungsgewalt für sich betrachtet eine Rechtsposition darstellt.[34] In welcher Form der Private Key auf die Erben übergeht, hängt dabei maßgeblich von dessen Speicherort ab. Nutzt der Erblasser ein ausschließlich online geführtes Wallet, so bestehen zwischen ihm und dem Dienstanbieter schuldrechtliche Beziehungen, in die seine Erben nach § 1922 Abs. 1 BGB

---

22 *Badstuber*, (Fn. 13), (249).

23 *Amend-Traut/Hergenröder*, (Fn. 3), (117); *Schlund/Pongratz*, (Fn. 8), (600); *Omlor*, ZRP 2018, 85 (87); *Shmatenko/Möllenkamp*, MMR 2018, 495 (497); *Medler*, (Fn. 5), (264); *von Oertzen/Grosse*, (Fn. 3); *Weiss*, (Fn. 10), (1344); *Förster/Fast*, (Fn. 20), (230). Abweichender Auffassung ist insoweit hingegen *Walter*, NJW 2019, 3609 (3611 ff.), der eine analoge Anwendung des § 90 BGB und damit einhergehend auch der §§ 929 ff. BGB diskutiert.

24 Vgl. näher *Weiss*, (Fn. 10), (1344) mit Hinweis auch darauf, dass die Einführung von § 327 Abs. 1 S. 2 BGB insoweit kein anderes Ergebnis in dinglicher Hinsicht zeitigt, sowie *Schlund/Pongratz*, (Fn. 8), (600).

25 *Weiss*, (Fn. 10), (1344).

26 *Amend-Traut/Hergenröder*, (Fn. 3), (117); *Badstuber*, (Fn. 13), (248); *von Oertzen/Grosse*, (Fn. 3); *Förster/Fast*, (Fn. 20), (230).

27 Vgl. *von Oertzen/Grosse*, (Fn. 3), m. w. N.

28 *Kössinger*, in: Nieder/Kössinger (Hrsg.), Handbuch der Testamentsgestaltung, 6. Aufl. 2020, Rn. 100.

29 *Deusch*, ZEV 2014, 2 f.; *Kössinger*, (Fn. 28), Rn. 100.

30 *Förster/Fast*, (Fn. 20); *Preuß*, in: Gsell/Krüger/Lorenz/Reymann (Hrsg.), beck-online. Großkommentar, Stand: 1.5.2022, § 1922 Rn. 384.

31 *Amend-Traut/Hergenröder*, (Fn. 3), (117); *Medler*, (Fn. 5), (264).

32 *Amend-Traut/Hergenröder*, (Fn. 3), (118); *Möller/Shmatenko*, (Fn. 4), Rn. 81.

33 *Amend-Traut/Hergenröder*, (Fn. 3), (117); *Burandt/Pein*, EE 2019, 81 ff.

34 Vgl. hierzu ausführlich *Amend-Traut/Hergenröder*, (Fn. 3) sowie *Medler*, (Fn. 5), (264); *Blum/Heuser*, (Fn. 1), Rn. 53.1; *von Oertzen/Grosse*, (Fn. 3), (1652); *Förster/Fast*, (Fn. 20), (230). Demgegenüber stellt *Klinger*, (Fn. 6), Rn. 678 wohl auf das Wallet als eigentlichen Nachlassbestandteil ab, während der Private Key lediglich den Zugang hierzu eröffne.

eintreten.[35] Im oben gewählten Beispielsfall erlangen Es Erben somit einen Anspruch gegen den Wallet-Betreiber auf Auskunft sowie Zugang zum Wallet und dem darin enthaltenen privaten Schlüssel.[36] Ist das Wallet des Erblassers mitsamt dem privaten Schlüssel hingegen auf einem physisch verkörperten Speichermedium wie beispielsweise einem USB-Stick, einem Smartphone oder einem PC oder Tablet gesichert, gehen die auf dem jeweiligen physischen Datenträger enthaltenen Daten mitsamt dem Sacheigentum am Datenträger auf die Erben über.[37] Selbiges gilt für einen in Papierform gesicherten Private Key, da entsprechende Schriftstücke ebenfalls als Nachlassbestandteil auf die Erben übergehen.[38]

II. Praktischer Umgang mit kryptographischen Nachlasswerten

In der Erbrechtspraxis sind über die dargestellten rechtlichen Grundsätze hinaus im Umgang mit kryptographischen Nachlasswerten zwei Faktoren von besonderer Relevanz. Zum einen kommt es ebenso wie bei anderen Nachlassbestandteilen wie beispielsweise Aktiendepots oder Bankschließfächern darauf an, dass die begünstigten Erben überhaupt Kenntnis von entsprechenden Vermögenswerten des Erblassers und vom Übergang derselben auf seine Person haben. Zum anderen müssen die Erben auch tatsächlichen Zugriff auf das Kryptoguthaben erlangen.

Stirbt ein Erblasser wie E im oben gewählten Beispielsfall, ohne eine letztwillige Verfügung errichtet zu haben, besteht für die Erben zwingend die Notwendigkeit, sich innerhalb der Ausschlagungsfrist des § 1944 Abs. 1 BGB einen Überblick über Bestand und Werthaltigkeit des Nachlasses zu verschaffen. Dies betrifft im Besonderen den digitalen Nachlass, zu dem neben Benutzerkonten bei verschiedensten Online-Diensten wie beispielsweise Facebook oder vergleichbaren Social-Media-Plattformen auch das Kryptoguthaben des Erblassers zählt. Die Recherche nach digitalen Nachlassbestandteilen kann die Erben vor erhebliche praktische Probleme stellen, sofern sie nicht bereits diesbezügliche Kenntnis besitzen. Hatte der Erblasser ein mit dem Public Key seines Wallets korrespondierendes Bankkonto eröffnet, über welches Transaktionen abgewickelt werden, können die Erben beispielsweise über etwaige vorhandene Kontoauszüge Kenntnis von entsprechenden Vermögenswerten des Erblassers erlangen und von der verantwortlichen Bank Auskunft zum Bankvertrag und Konto verlangen.[39] Alternativ können auf im Nachlass befindlichen Smartphones installierte Krypto-Apps Aufschluss über existente Wallets geben.

Die notwendige Kenntnis der Erben von der Existenz rein virtuell existierender Vermögenswerte reicht allerdings nicht aus. Darüber hinaus müssen die Erben das auf sie übergegangene Recht des Erblassers auch nachweisen und auf das Kryptoguthaben faktisch zugreifen können.[40] Entsprechend der oben getätigten Überlegungen ist entscheidend, dass die Erben über den Private Key sowie über vorhandene Wallet-Passwörter verfügen, da die Inhaberschaft am Private Key ihnen die faktische Verfügungsgewalt über das dem Erblasser zuzuordnende Kryptovermögen verschafft und somit Transaktionen über dieses oder dessen Umwandlung in Fiat-Geld über eine Kryptobörse ermöglicht. Hat der Erblasser zur Speicherung seines Wallets und seiner privaten Schlüssel ein physisches Speichermedium, zum Beispiel einen USB-Stick oder eine PC-Festplatte, gewählt oder seine privaten Schlüssel auf einem Papierausdruck gesichert, muss folglich gewährleistet sein, dass die Erben Kenntnis von der Existenz entsprechender Trägermedien und deren Verwahrungsort erlangen. Wurde der Private Key des Erblassers hingegen nicht von ihm gespeichert, sondern vom Online-Wallet-Anbieter im Rahmen eines Kryptoverwahrgeschäfts verwahrt, so besaß der Erblasser selbst gegebenenfalls keine Kenntnis vom Private Key, sondern loggte sich zwecks Zugriffs auf sein Krypto-Guthaben und zur Legitimation seiner Transaktionen mit vorhandenen Zugangsdaten zu einer Benutzeroberfläche oder App ein.[41] In diesem Fall bedürfen die Erben notwendigerweise der entsprechenden Zugangsdaten und Passwörter. Sollten ihnen diese nicht bekannt sein, besteht gegen den jeweiligen Dienstanbieter ein Auskunfts- und Herausgabeanspruch.[42]

Erlangen die Erben im Ergebnis keine Kenntnis von den notwendigen Schlüsseln und Passwörtern, bleibt ihnen die Verfügungsgewalt über ein etwaig zum Nachlass zählendes Kryptoguthaben endgültig verwehrt, woraus sich für sie, neben dem Verlust gegebenenfalls erheblicher wirtschaftlicher Werte, weitere Risiken ergeben können. Denn der

---

35 *Amend-Traut/Hergenröder*, (Fn. 3), (118); hierzu auch *Burandt/Pein*, (Fn. 33); *Förster/Fast*, (Fn. 20), (231).

36 *Von Oertzen/Grosse*, (Fn. 3), (1652); *Medler*, (Fn. 5), (264). Manche Online-Dienstleister ermöglichen es den Erben im Übrigen in ihren AGB explizit, das Wallet des Erblassers fortzuführen, vgl. *Burandt/Pein*, EE 2019, 153 m. w. N.

37 *Amend-Traut/Hergenröder*, (Fn. 3), (118); *von Oertzen/Grosse*, (Fn. 3), (1652); *Naczinsky*, ZEV 2021, 227; *Förster/Fast*, (Fn. 20), (231). An den auf dem jeweiligen Speichermedium befindlichen elektronischen Daten erwirbt der Erbe hingegen kein Eigentum, da diese als solche mangels abgrenzbarer Körperlichkeit keine Sachen sind. Vgl. *Förster/Fast*, (Fn. 20) unter Verweis auf *OLG Brandenburg* NJW-RR 2020, 54.

38 *Naczinsky*, (Fn. 37).

39 Zum Auskunftsanspruch der Erben vgl. allgemein *Preuß*, (Fn. 30), Rn. 249 ff.

40 *Medler*, (Fn. 5), (264). Zu den Möglichkeiten und Schwierigkeiten eines Nachweises insbesondere bei Fehlen einer letztwilligen Verfügung vgl. *Naczinsky*, (Fn. 37), (231).

41 Vgl. *d'Avoine/Hamacher*, (Fn. 1) (8) mit näherer Erläuterung zur Unterscheidung zwischen custodian wallets und non-custodian wallets.

42 Vgl. *Medler*, (Fn. 5), (264). Dieser ist jedoch nur dann zielführend, wenn der Wallet-Anbieter tatsächlich selbst Zugriff auf den Private Key hat und die Zugangsdaten auf Verlangen neu erteilen kann. Zudem kann die Rechtsdurchsetzung erschwert sein, wenn der Wallet-Anbieter seinen Sitz im Ausland hat. Vgl. *Medler*, (Fn. 5), (265) und *Naczinsky*, ZEV 2020, 665 (668).

Umstand, dass ein Erbe keinen Zugriff auf das ihm zugefallene Kryptoguthaben hat, ändert nichts daran, dass ein Nachlassübergang stattgefunden hat, soweit das Recht des Erben an dem Vermögenswert nachweisbar ist.[43] Dies hat insbesondere Auswirkungen auf Pflichtteils- und Vermächtnisansprüche, denen sich die Erben ausgesetzt sehen können.[44]

D. Nachlassvorsorge

Die voranstehenden Überlegungen haben aufgezeigt, dass im Fall des Todes eines Erblassers die in seinem Nachlass befindlichen kryptographischen Vermögenswerte zwar im Wege der Universalsukzession grundsätzlich ohne weiteres auf seine Erben übergehen können. Entscheidend ist allerdings, dass diese nicht allein Kenntnis davon haben, dass entsprechende Vermögenswerte überhaupt existieren, sondern darüber hinaus auch sicheren Zugriff auf die zur Erlangung der Verfügungsgewalt erforderlichen Zugangsdaten, Passwörter und kryptographischen Schlüssel erhalten. Des Weiteren muss den Erben seitens des Erblassers durch Mitteilung des Verwahrungsorts auch der uneingeschränkte Zugriff auf diejenigen Speichermedien ermöglicht werden, auf denen er Wallet und Private Key gesichert hat. Um diese Bedingungen in der Situation eines Erbfalls gewährleisten zu können, kommt es auf eine möglichst rechtssichere und zugleich praktikable „digitale Nachlassvorsorge" durch spätere Erblasser an. Diesbezüglich existieren für den Erblasser – ungeachtet etwaig vorhandener Vorgaben des Wallet-Anbieters für den Fall des Versterbens eines Nutzers[45] – verschiedene denkbare Möglichkeiten.

Zunächst ist festzuhalten, dass eine ausreichende Information der Rechtsnachfolger des Erblassers nicht zwingend an die Errichtung einer letztwilligen Verfügung geknüpft ist, wiewohl sich eine solche gegebenenfalls anbieten mag, insbesondere angesichts des Umstands, dass gerade ein eigenhändiges Testament gem. § 2247 BGB recht unkompliziert abgefasst werden kann.[46] Entscheidend ist vielmehr, dass der Erblasser ein praktikables Vorgehen wählt, welches einen möglichst rechtssicheren Rechtswechsel garantiert. Ausreichend und hilfreich für die gesetzlichen Erben könnte insoweit bereits eine schlichte Auflistung aller Passwörter und Zugangscodes sowie kryptographischer Schlüssel in Gestalt einer „digitalen Vorsorgemappe" sein.[47] Diese könnte auf einem PC, einem USB-Stick oder in einer Cloud gespeichert oder physisch ausgedruckt und verwahrt bzw. einer Vertrauensperson übergeben werden.[48] Nutzt der Erblasser für den Zugriff auf sein Wallet ein Smartphone, so muss die Auflistung auch die zur Nutzung desselben erforderliche PIN bzw. eine Abbildung des genutzten Entsperrmusters enthalten.[49] Allerdings gilt es seitens des Erblassers zu berücksichtigen, diese Liste möglichst in regelmäßigen Abständen zu aktualisieren, gerade im Fall häufiger, aus Gründen der IT-Sicherheit empfehlenswerter Passwortwechsel.[50] Im Übrigen ist zu beachten, dass bei zu offener Verwahrung im Bereich der eigenen Wohnung oder bei Übergabe an eine andere Person naturgemäß ein Risiko des Zugriffs durch Dritte oder des Verlusts besteht.[51] Greift ein Erblasser hingegen auf online geführte Passworthinterlegungsdienste zurück, können Passwörter und sonstige Zugangsdaten zwar auf dem Server des Anbieters gespeichert und im Todesfall gegen Nachweis an die Erben herausgegeben werden. Diesbezüglich ergeben sich allerdings Bedenken hinsichtlich der Datensicherheit, insbesondere im Fall eines Hackings, sowie das Risiko, dass der betreffende Dienst vor Ableben des Erblassers eingestellt wird.[52]

Eine denkbare Alternative bestünde darin, das vom Erblasser erstellte Verzeichnis über dessen sämtliche Internetaktivitäten und Accounts samt zugehöriger Passwörter auf einem USB-Stick oder einer externen Festplatte zu speichern und dieses Speichermedium bzw. das Verzeichnis wiederum mittels eines Passworts zu schützen.[53] In diesem Fall könnten das Passwort und die Information zum Aufbewahrungsort des Speichermediums an einen Bevollmächtigten übergeben werden, während das Speichermedium selbst beim Erblasser verbleibt.[54] Bei dieser Vorgehensweise kann problemlos und jederzeit eine Aktualisierung der im Verzeichnis enthaltenen Passwörter und Zugangsdaten vorgenommen werden. Als Bevollmächtigter könnte etwa ein zukünftiger Erbe ausgewählt werden. Ebenso könnte das Masterpasswort zusammen mit einer

---

43 *Blum/Heuser*, (Fn. 1), Rn. 53.1.

44 Vgl. vertiefend *Amend-Traut/Hergenröder*, (Fn. 3), (118 ff.).

45 *Preuß*, (Fn. 30), Rn. 387.1 m. w. N.; *Leipold*, in: Säcker/Rixecker/Oetker/Limperg (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Aufl. 2020, § 1922 Rn. 47 f.

46 Zu den Errichtungsvoraussetzungen und zur inhaltlichen Ausgestaltung eines eigenhändigen Testaments vgl. beispielsweise die Darstellung bei *Horn*, NJW 2016, 3500.

47 Vgl. für den digitalen Nachlass allgemein *Steiner/Holzer*, ZEV 2015, 262 (265); *Pruns*, ErbR 2018, 614 (621); *Naczinsky*, (Fn. 42), (668).

48 *Preuß*, (Fn. 30), Rn. 387.1.

49 Vgl. *Pruns*, (Fn. 47), (621).

50 Vgl. hierzu *Steiner/Holzer*, ZEV 2015, 262 (265) sowie *Bundesministerium der Justiz,* Erben und Vererben – Erläuterungen zum Erbrecht, bmj.de, https://www.bmj.de/SharedDocs/Publikationen/DE/Erben_Vererben.pdf;jsessionid=8F1A98DB641972BD0F289715358571EA.2_cid297?__blob=publicationFile&v=39, S. 24, Abruf v. 11.7.2022.

51 Vgl. *Raude*, RNotZ 2017, 17 (24); *Naczinsky*, (Fn. 42), (669).

52 Vgl. *Gloser*, DNotZ 2015, 4 (10); *Raude*, (Fn. 51), (23); *Naczinsky*, (Fn. 42), (669).

53 *Gloser*, (Fn. 52), (13); *Pruns*, (Fn. 47), (621).

54 Zu diesem Vorschlag *Steiner/Holzer*, (Fn. 47), (265). Allgemein wird im Zusammenhang mit dem digitalen Nachlass eine notariell beurkundete „Vorsorgevollmacht für digitale Angelegenheiten" mit darin enthaltenen, möglichst konkreten Handlungsanweisungen für den Bevollmächtigten als Vorsorgemöglichkeit für den Todesfall vorgeschlagen. Vgl. etwa *Steiner/Holzer*, (Fn. 47), (265); *Raude*, (Fn. 51), (24). Eine Aufnahme digitaler Zugangsdaten, insbesondere der Passwörter für ein Kryptowallet oder des Private Key, in solch eine Vorsorgevollmacht erschiene allerdings aus Gründen der Datensicherheit nicht zielführend, da die Vollmacht gerade dazu dient, im Rechtsverkehr gegenüber Dritten vorgelegt zu werden. Vgl. *Gloser*, (Fn. 52), (9); *Raude*, (Fn. 51), (25); *Naczinsky*, (Fn. 42), (669).

konkreten Handlungsanweisung, an wen unter welchen Voraussetzungen die Urkunde übergeben werden soll, in einer notariellen Vorsorgeurkunde niedergelegt und beim Notar verwahrt werden.[55]

Wird im Übrigen durch den Erblasser eine letztwillige Verfügung, etwa in Gestalt eines eigenhändigen Testaments, errichtet, könnten etwaige Zugangsdaten, Passwörter und kryptographische Schlüssel grundsätzlich auch unmittelbar in diese aufgenommen oder als Anlage dazu genommen werden.[56] Eine solche Vorgehensweise bietet sich allerdings aus mehreren Gesichtspunkten nicht an. Zum einen wird der Inhalt der letztwilligen Verfügung im Testamentseröffnungsverfahren nach §§ 348 ff. FamFG durch das Nachlassgericht an die Beteiligten bekanntgegeben.[57] Im Fall einer Eröffnung nach § 348 Abs. 3 FamFG erfolgt dabei eine schriftliche Bekanntgabe durch vollständige Übersendung der letztwilligen Verfügung an die Beteiligten, darunter auch die Pflichtteilsberechtigten. Dies begründet ein gewisses Missbrauchspotenzial.[58] Zudem erscheint dieses Vorgehen auch insoweit nicht praktikabel, als je nach Errichtungszeitpunkt bis zum Ableben ein mehrfacher Wechsel von Zugangsdaten und Passwörtern stattfinden könnte, was ein regelmäßiges „Update" der letztwilligen Verfügung erforderlich machen würde.[59] Besonders aufwendig wären Konten- oder Passwortänderungen dann, wenn die Auflistung in einem notariellen oder einem amtlich verwahrten Testament niedergelegt sein sollte, da eine Abänderung in solchen Fällen eine entsprechende Kostenfolge nach sich zöge.[60]

Vor dem Hintergrund der jeweiligen Vorzüge und Schwächen der voranstehend aufgezeigten Vorsorgemöglichkeiten zur Sicherung des Zugriffs der Erben auf das digitale Erbe des Erblassers und insbesondere auf das von ihm hinterlassene Kryptovermögen bietet sich im Ergebnis eine sogenannte Kombinationslösung an.[61] Bei dieser wird neben einer testamentarischen Regelung des analogen wie digitalen Nachlasses auch eine aktuelle und vollständige Auflistung über das digitale Vermögen samt Passwörtern, Zugangsdaten und privaten kryptographischen Schlüsseln erstellt, auf welche das Testament verweist. Diese Aufstellung kann sodann auf einem lokalen Speicherträger mittels eines Masterpassworts verschlüsselt und der Speicherträger sodann an einem sicheren, auch für die Erben leicht zugänglichen Ort wie beispielsweise einem Bankschließfach verwahrt werden. Das Masterpasswort kann in einer digitalen Vorsorgeurkunde festgehalten werden, die beim Notar verbleibt. Auf diese wird dann im Testament ebenfalls Bezug genommen, wobei die digitale Vorsorgeurkunde so zu gestalten ist, dass nur die Erben oder etwaige Vermächtnisnehmer gegen Nachweis Kenntnis vom Dokument nehmen dürfen.[62] Alternativ oder ergänzend kann auch ein Bevollmächtigter im Wege einer postmortalen Vollmacht damit beauftragt werden, im erforderlichen Fall auf die hinterlegte Auflistung zuzugreifen und notwendige Schritte zu unternehmen.[63]

E. Fazit

Ein vorhandenes Kryptowährungsguthaben zählt zum digitalen Nachlass eines Erblassers und geht mit dem Erbfall grundsätzlich ohne Weiteres im Wege der Universalsukzession auf dessen Erben über. Maßgeblicher erbrechtlicher Bezugspunkt ist dabei der sogenannte Private Key, der dem Nutzer eines Peer-to-Peer-Netzwerks die faktische Verfügungsgewalt über das ihm auf der Blockchain zugeordnete Kryptoguthaben verleiht. Den rechtssicheren Übergang dieses Private Keys und damit der Zugriffsmöglichkeit auf ein vorhandenes Wallet zu garantieren, ist Aufgabe einer möglichst umfassenden digitalen Vorsorge. Diesbezüglich besteht in der Praxis Beratungspotential, welches in der Zukunft den digitalen Nachlass im Allgemeinen und Kryptowährungen im Besonderen betreffend voraussichtlich noch weiter zunehmen wird.

55 *Gloser*, (Fn. 52), (11); *Raude*, (Fn. 51), (25).

56 Vgl. *Medler*, (Fn. 5), (267).

57 *Preuß*, (Fn. 30), Rn. 387.1; *Förster/Fast*, (Fn. 20), (232).

58 Vgl. *Gloser*, (Fn. 52); *Förster/Fast*, (Fn. 20), (233).

59 *Leipold*, (Fn. 45), Rn. 48; *Naczinsky*, (Fn. 42), (669); *Förster/Fast*, (Fn. 20), (233).

60 *Naczinsky*, (Fn. 42), (669).

61 Hierzu näher *Deusch*, (Fn. 29), (7); *Medler*, (Fn. 5), (267).

62 *Raude*, (Fn. 51), (26); *Naczinsky*, (Fn. 42); *Förster/Fast*, (Fn. 20), (234).

63 Hierzu und zu den Schwächen einer postmortalen Vollmacht näher *Naczinsky*, (Fn. 42).