Dipl.-Ing. Mag. Dr. Bernhard Haslhofer
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik;
Forschungsgruppenleiter Complexity Science Hub, Wien

MMag. Dr. Markus Gumilar
Notarsubstitut in Hohenems

Mag. Isabella Pouzar-Hofmeister
Öffentliche Notarin in 1060 Wien

Digitale Krypto-Verlassenschaften

1. Einleitung

Mehr als 300.000 Österreicher besitzen Krypto-Vermögenswerte (wie Bitcoin oder Ethereum),[1] darunter viele Personen im mittleren oder höheren Lebensalter. Verstirbt eine dieser Personen, hinterlässt sie nicht nur einen analogen Nachlass, sondern auch einen digitalen (inklusive Krypto-Vermögenswerten).

Diese Thematik wird zunehmend auch für Sachverständige relevant, da diese im Rahmen eines Verlassenschaftsverfahrens zur Bewertung der vorhandenen Vermögenswerte zum Todeszeitpunkt herangezogen werden können. Sachverständige werden in der Regel durch den für das Verlassenschaftsverfahren zuständigen öffentlichen Notar in seiner Funktion als Gerichtskommissär bestellt.

Angesichts der in den letzten Jahren deutlich gestiegenen Zahl an digitalen Krypto-Verlassenschaften und der Erwartung, dass dieser Trend anhalten wird, widmet sich dieser Beitrag insbesondere der Frage, wie Krypto-Verlassenschaften aus technisch-forensischer Perspektive unter Berücksichtigung der aktuellen rechtlichen Rahmenbedingungen abgewickelt werden können.

Da dieses Thema sowohl technisch als auch rechtlich Neuland ist, stützt sich die vorgestellte Vorgehensweise vor allem auf empirische Erkenntnisse und die praktischen Erfahrungen des Sachverständigen und der involvierten Gerichtskommissäre. Mittelfristig sollen diese Erfahrungswerte in eine technisch und rechtlich standardisierte und verfahrensökonomisch vertretbare Methode überführt werden.

2. Hintergrund

2.1. Krypto-Vermögenswerte

Bitcoin und Ethereum sind die bekanntesten Krypto-Vermögenswerte, mit einer Marktkapitalisierung von inzwischen fast US-$ 2 Billionen. Zunehmend relevant werden auch sogenannte Stablecoins (wie beispielsweise Tether oder USDC), die eine 1:1-Bindung an traditionelle Währungen wie den US-Dollar versprechen. Darüber hinaus existieren tausende weitere Krypto-Assets, von denen jedoch nur wenige eine breite Nutzerbasis haben und daher im Kontext von Verlassenschaften von wenig Bedeutung sind. Für einen detaillierten Überblick über bekannte Krypto-Assets verweisen wir auf Online-Plattformen wie CoinMarketCap oder CoinGecko.

Aus technischer Sicht sind Krypto-Assets Einheiten, die im Zuge eines kompetitiven dezentralen Rechenprozesses (Mining) geschaffen und über Transaktionen sogenannten Adressen zugewiesen werden, welche wiederum in einer verteilten und öffentlich einsehbaren Datenstruktur (Blockchain) gespeichert sind. Eine Adresse ist – grob beschrieben – ein Hash-Wert, der von einem öffentlichen kryptografischen Schlüssel abgeleitet wurde. Wer den entsprechenden privaten Schlüssel besitzt, der von einem sogenannten Seed abgeleitet wird, kann somit über den der Adresse zugewiesenen Krypto-Vermögenswert verfügen. Geht dieser private Schlüssel verloren, sind auch die Vermögenswerte unwiederbringlich verloren und auch nicht mehr rekonstruierbar.

2.2. Aufbewahrungsmethoden

In Krypto-Asset-Systemen kann jeder Benutzer beliebig viele Schlüsselpaare generieren und damit die zugehörigen Adressen kontrollieren. Diese Paare werden oft in sogenannten Wallets zusammengefasst, sodass Vermögenswerte über mehrere Wallets verteilt sein können. Die zentrale Herausforderung für den Benutzer besteht in der sicheren Verwaltung der zugehörigen privaten Schlüssel. Grundsätzlich unterscheidet man dabei zwischen drei Aufbewahrungsmethoden:[2]

- **Krypto-Wechselbörse:** Ein Benutzer überträgt die Verwaltung seiner Krypto-Assets an einen Dritten, in der Regel eine Krypto-Wechselbörse (wie Binance, Kraken oder Bitpanda). Diese Institution verwaltet die Vermögenswerte in Wallets und kontrolliert auch die privaten Schlüssel. Das bedeutet, dass der Benutzer aus rein technischer Sicht in der Regel keinen direkten Zugriff auf seine Vermögenswerte hat.
- **Software-Wallet:** Ein Benutzer betreibt eine Software zur Verwaltung seiner Krypto-Assets auf seinem Computer oder Mobiltelefon. Bekannte Desktop-Software-Wallets sind Electrum, Exodus und Bitcoin Core. Bekannte Mobile Wallets sind Trust Wallet, MetaMask und Mycelium. Software-Wallets sind in der Regel mit dem Internet verbunden und werden daher auch als *„Hot Wallets“* bezeichnet.

- **Hardware-Wallet:** Ein Benutzer speichert die privaten Schlüssel auf einem externen, in der Regel PIN-geschützten Gerät. Dieses kann über eine Schnittstelle an einen Computer angeschlossen und in Kombination mit einer Software verwendet werden. Bekannte Hardware-Wallet-Hersteller sind Trezor und Ledger. Für weitere Hersteller, Abbildungen und technische Details verweisen wir auf die von INTERPOL kuratierte Liste bekannter Hardware-Wallets.[3]

Da die letzten beiden Methoden aus technischer Sicht lediglich private Schlüssel verwalten und ein privater Schlüssel aus einem Seed abgeleitet wird, besteht die Möglichkeit, ein Wallet zu rekonstruieren, wenn der Seed bekannt ist. Der Seed ist also der Master-Schlüssel, der Zugriff auf alle im Wallet gespeicherten Krypto-Assets ermöglicht. In der Praxis wird – wie in Abbildung 1 ersichtlich – der Seed entsprechend den Standards BIP-32[4] bzw BIP-39[5] oft in Form einer Reihe von Wörtern (eine sogenannte Seed-Phrase) gespeichert und meist in Papierform an einem sicheren Ort aufbewahrt.

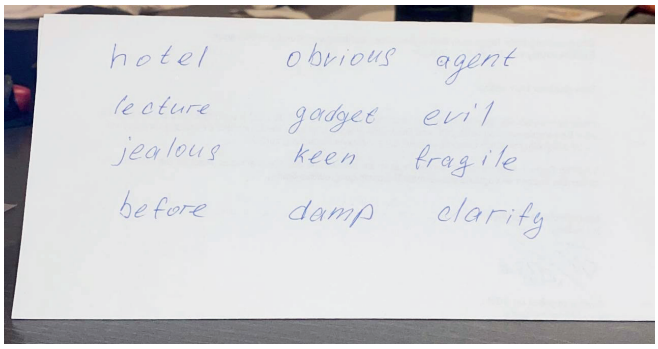

Abbildung 1: Mnemonic-Seed-Beispiel: Die angeführten Wortfolgen sind künstlich und entsprechen keinem echten Wallet (Quelle: https://en.bitcoin.it/wiki/Seed_phrase)

2.3. Rechtliche Perspektive

Das Verlassenschaftsverfahren dient der Abwicklung des Vermögens einer verstorbenen Person. Es wird überwiegend durch den Gerichtskommissär (einen Notar als Organ des Gerichts) nach den Regeln des AußStrG und GKG geführt.

Gerichtliche Beschlüsse werden ausschließlich durch das zuständige Bezirksgericht erlassen. Beispiele dafür sind die Beendigung des Verfahrens sowie Vertretungshandlungen, die nicht von der ordentlichen Verwaltung der Verlassenschaft in Art oder Umfang der Handlung umfasst sind (zB Verkäufe von Verlassenschaftsvermögen, die einen nicht unerheblichen Wert in Bezug auf das Gesamtvermögen der Verlassenschaft darstellen).

Zu Beginn steht die Todesfallaufnahme, in der der Gerichtskommissär erste Informationen erhält. Danach erhebt er unter anderem die vorhandenen Vermögenswerte.

Für die Bewertung von Vermögenswerten kann es von Gesetzes wegen (bei Beteiligung von schutzberechtigten Personen) oder aufgrund des Antrags einer berechtigten Person (zB eines Pflichtteilsberechtigten) erforderlich sein, einen Sachverständigen zur Schätzung von Nachlassvermögen beizuziehen.

Bestehen im Einzelfall konkrete Anhaltspunkte dafür, dass der Verstorbene über Krypto-Werte verfügte, kann es daher auch erforderlich sein, einen Sachverständigen beizuziehen. Der Gerichtskommissär legt den Aufgabenbereich des Sachverständigen fest. Seine Aufgabe kann von der reinen Feststellung des Werts bekannter Krypto-Bestände zum Todeszeitpunkt bis hin zur Ermittlung reichen, ob der Verstorbene zum Todeszeitpunkt Krypto-Assets hatte.

Das Verlassenschaftsverfahren endet mit der Einantwortung, mit welcher das Gericht den Nachlass den Erben zuweist. Daneben finden auch verkürzte Verfahren statt, wenn ein Nachlass überschuldet oder wenig Vermögen vorhanden ist.

3. Vorgehensweise

3.1. Vorbemerkung

Nachdem der Sachverständige vom Gerichtskommissär für die Erstellung eines Gutachtens bestellt wurde, ist eine Befundaufnahme durchzuführen, deren Ergebnisse schriftlich festgehalten werden müssen. Im Folgenden werden die wichtigsten Schritte der Befundaufnahme näher beschrieben: 1.) die Identifikation und Sicherstellung potenzieller Krypto-Vermögenswerte, 2.) deren forensische Analyse, 3.) die Bewertung dieser Vermögenswerte und 4.) gegebenenfalls deren Verwertung im Rahmen der Verlassenschaft. Diese Schritte werden im Weiteren detaillierter ausgeführt.

3.2. Identifikation und Sicherstellung

Dieser Schritt beginnt in der Regel mit einer Vor-Ort-Besichtigung des Wohnsitzes des Verstorbenen. Der Sachverständige fungiert dabei als Schätzmeister und hat die Aufgabe, Hinweise auf Krypto-Assets zu identifizieren und systematisch zu erfassen. In der Praxis bedeutet dies, vorhandene Dokumente zu sichten und Datenträger bzw elektronische Geräte aus dem Hausrat sicherzustellen. Da der Hausrat bzw die Dokumentensammlung sehr umfangreich sein kann, empfiehlt es sich, ein sogenanntes Triage-Verfahren anzuwenden, um Unterlagen, Datenträger und Geräte nach Plausibilität zu ordnen. So sind beispielsweise Dokumente in einem Tresor in der Regel wichtiger als solche in gewöhnlichen Aktenordnern; ebenso sind Datenträger eines bekannten Hardware-Wallet-Herstellers in der Regel relevanter als herkömmliche USB-Sticks.

Da es dem Sachverständigen während der Vor-Ort-Besichtigung in der Regel nicht möglich ist, den gesamten Hausrat zu durchsuchen, ist es ratsam, den für die Räumung zuständigen Personen oder Unternehmen klare Anweisungen zu geben, worauf sie bei der Entsorgung

achten sollen. Dafür kann beispielsweise eine Bilddokumentation bekannter Hardware-Wallets sowie Beispiele für Seed-Phrase-Notizen übergeben werden.

Zusätzlich wird empfohlen, im Rahmen der Befunderhebung das Gespräch mit den direkten Angehörigen oder nahestehenden Personen zu suchen. Es ist gut möglich, dass der Verstorbene zu Lebzeiten über seine Krypto-Investitionen gesprochen und Hinweise zur Verwahrung gegeben hat. Diese Informationen können dem Sachverständigen als Grundlage für die Identifikation von Krypto-Vermögenswerten dienen.

Es ist unbedingt das Grundprinzip des Parteiengehörs zu wahren. Der Sachverständige hat alle Parteien zur Befundaufnahme einzuladen und deren eingebrachte Informationen zu berücksichtigen.

3.3. Forensische Analyse

3.3.1. Allgemeines

Nach der Identifikation und Sicherstellung von Artefakten mit möglichem Krypto-Vermögensbezug müssen diese einer genaueren forensischen Analyse unterzogen werden. Die Vorgehensweise unterscheidet sich je nach Aufbewahrungsmethode bzw Natur des sichergestellten Artefakts.

3.3.2. Krypto-Börse

Ergibt sich ein Hinweis, dass der Verstorbene ein Benutzerkonto bei einer bekannten Krypto-Wechselbörse besaß, müssen die dortigen Bestände erfasst werden. Da die meisten Krypto-Börsen inzwischen eine Zwei-Faktor-Authentifizierung eingeführt haben, ist ein direkter Zugriff in der Regel nicht möglich, selbst wenn Benutzername und Passwort bekannt sind. Daher bleibt meist nur die Möglichkeit, ein Auskunftsersuchen an die Börse zu richten. Hierfür empfiehlt es sich, dass der Gerichtskommissär ein entsprechendes Schreiben mit Verweis auf die gesetzliche Grundlage aufsetzt und dieses gemeinsam mit den erforderlichen Unterlagen (zB Nachweis seiner Zuständigkeit, Sterbeurkunde) an die Krypto-Börse übermittelt. Der Gerichtskommissär leitet seine Befugnis zur Erhebung der Vermögenswerte aus § 9 GKG ab.

Alternativ kann der Gerichtskommissär einen Sachverständigen als Kurator für die Krypto-Vermögenswerte bestellen, der diese Schritte selbst durchführen kann. Bei Verlassenschaftsverfahren mit Auslandsberührung ist es beispielsweise nicht unüblich, dass Verlassenschaftskuratoren zur Feststellung von Vermögenswerten bestellt werden. Weiters ist es auch denkbar, dass der Gerichtskommissär im Wege der Rechtshilfe über das zuständige Bezirksgericht weitere Informationen einholen lässt. Das zuständige Bezirksgericht stellt sodann ein Rechtshilfeersuchen an das zuständige Gericht im betreffenden ausländischen Staat.

3.3.3. Hardware-Wallet

Wenn Hardware-Wallets sichergestellt wurden, müssen diese ebenfalls auf mögliche Krypto-Vermögenswerte untersucht werden. Da diese Wallets üblicherweise durch eine PIN geschützt sind, ist die klassische forensische Vorgehensweise (wie etwa die Erstellung eines forensischen Abbildes) in der Regel nicht durchführbar. Die Herausforderung besteht darin, die PINs für jedes Hardware-Wallet zu ermitteln, um eine Analyse durchführen zu können. PINs werden zB oft in der Nähe des Wallets (zB in der Verpackung) notiert. Es ist jedoch darauf zu achten, dass es in der Regel nur wenige Versuche gibt, die richtige PIN einzugeben, bevor sich das Hardware-Wallet selbst zerstört.

3.3.4. Seed-Phrase

Seed-Phrases werden häufig in Papierform aufbewahrt, typischerweise an einem sicheren Ort (zB in einem Tresor) und manchmal auch auf mehrere Personen verteilt, um zusätzliche Sicherheit zu gewährleisten. Wird eine solche Seed-Phrase sichergestellt, kann der Sachverständige die Wallets mithilfe eines Software-Wallets wiederherstellen und so auf die Vermögenswerte zugreifen. Man muss jedoch im Vorfeld wissen, mit welchem Hardware- bzw Software-Wallet die Seed-Phrase erstellt wurde, weil diese oft nicht kompatibel sind.

3.3.5. Endgeräte und Datenträger

Werden im Zuge der Sicherstellung Endgeräte (zB Laptop, Mobiltelefon) oder Datenträger im Hausrat gefunden und besteht der Verdacht, dass sich darauf Krypto-Vermögenswerte befinden könnten, ist eine umfassende forensische Datenträgeranalyse erforderlich. Dabei müssen die Geräte und Datenträger auf das Vorhandensein von Software-Wallets, elektronisch gespeicherten Seed-Phrases oder bekannten Krypto-Adressen untersucht werden.

3.4. Transaktionsanalyse und Bewertung

Nachdem der Zugriff auf Krypto-Wallets hergestellt wurde, können in der Regel die Krypto-Adressen, die der Verlassenschaft zuzuordnen sind, ausgelesen werden. Diese Adressen bilden die Grundlage für die Bewertung zum Todeszeitpunkt.

Für die Bewertung der Vermögenswerte kann sich der Sachverständige die Transparenz der Blockchain zunutze machen. Über diese sind für eine gegebene Adresse alle historischen eingehenden und ausgehenden Transaktionen abrufbar, wodurch der Bestand zu einem bestimmten Zeitpunkt berechnet werden kann. Für einfache Analysen können öffentliche Blockchain-Explorer-Tools verwendet werden. Diese Werkzeuge sind jedoch oft nur eingeschränkt nutzbar (beispielsweise durch das Fehlen von Funktionen zur Konvertierung von Werten zu historischen Wechselkursen) und eignen sich daher nur bedingt für eine vollständige Bewertung.

In der Praxis werden deshalb spezialisierte Krypto-Asset-Analysewerkzeuge eingesetzt, um diese Aufgabe zu bewältigen. Diese ermöglichen es, eine Adresse einzugeben und den Bestand der zugeordneten Krypto-Vermögenswerte unter Berücksichtigung historischer Wechselkurse abzurufen.

Da diese Tools in der Regel auch die Rekonstruktion historischer Geldflüsse ermöglichen, können sie dazu verwendet werden, die Geldflüsse zu verfolgen. Das bedeutet, dass es möglich ist, auf weitere, möglicherweise bislang unbekannte Wallets zu schließen, von denen der Verstorbene möglicherweise Krypto-Bestände auf seine Wallets überwiesen hat, oder Wallets zu identifizieren, die Vermögenswerte vom Verstorbenen erhalten haben.

Grundsätzlich ist die Krypto-Asset-Transaktionsanalyse ein sehr mächtiges forensisches Instrument, das es erlaubt, das historische Finanzverhalten des Verstorbenen nachzuvollziehen.

3.5. Verwertung

Aus Gründen der Vereinfachung ist zu empfehlen, dass nach Abschluss des Verlassenschaftsverfahrens die Verwertung stattfindet. In diesem Zusammenhang ist es denkbar, dass die Erben während des Verlassenschaftsverfahrens vereinbaren, dass einer von ihnen die Verwertung vornimmt. Eine solche Vereinbarung kann vor dem Gerichtskommissär zu Protokoll gegeben werden. Der so ermächtigte Erbe eröffnet bei einer vertrauenswürdigen Krypto-Wechselbörse, idealerweise innerhalb der nationalen oder europäischen Gerichtsbarkeit, ein Benutzerkonto auf seinen Namen. Die Vermögenswerte können dorthin gesammelt übertragen und in der Folge verwertet werden. Die Verteilung erfolgt dann entsprechend der getroffenen Vereinbarung.

4. Fazit, Herausforderungen und Ausblick

Digitale Krypto-Verlassenschaften gewinnen zunehmend an Bedeutung für Sachverständige, da diese von Notaren bzw Gerichtskommissären oft mit der Bewertung solcher Verlassenschaften betraut werden. In der Praxis sieht sich der Sachverständige jedoch mit mehreren Herausforderungen konfrontiert:

Erstens gibt es derzeit – abgesehen von diesem Beitrag – keine allgemeine Vorgehensweise, die rechtliche und technisch-forensische Aspekte integrativ abdeckt. Angesichts der rasant steigenden Fallzahlen besteht hier dringender Handlungsbedarf.

Zweitens wird der Sachverständige aus forensisch-technischer Sicht häufig mit der Tatsache konfrontiert, dass die Zugangsdaten oder die notwendigen Authentifizierungsfaktoren zu Hardware-Wallets oder Endgeräten nicht auffindbar sind. Bei Endgeräten besteht zwar die Möglichkeit einer klassischen forensischen Analyse, allerdings ist zu beachten, dass moderne verschlüsselte Geräte oft nicht mehr oder nur mit erheblichem Aufwand entsperrt werden können.

Drittens, wenn der Verstorbene seine Krypto-Vermögenswerte bei internationalen Krypto-Wechselbörsen aufbewahrt hat, stehen der Sachverständige und der Gerichtskommissär häufig vor dem Problem, dass Auskunftsersuchen entweder nicht oder nicht zufriedenstellend beantwortet werden.

Viertens ist der fehlende Zugang zu effizienten und wirtschaftlich vertretbaren Krypto-Asset-Analysewerkzeugen eine weitere Herausforderung. Dieses Problem wird jedoch zunehmend durch die Verfügbarkeit spezialisierter und kostengünstigerer Tools gemildert.

Perspektivisch ist davon auszugehen, dass die Bewertung von Krypto-Vermögenswerten zu einem Standardverfahren in Verlassenschaftsangelegenheiten wird. Dafür sind etablierte technisch-forensische Methoden sowie Werkzeuge notwendig, die die Arbeit des Sachverständigen effizient unterstützen. Mit diesem Beitrag wurde ein erster Grundstein für diese Entwicklungen gelegt und es ist zu erwarten, dass noch viele weitere Schritte folgen werden.

Anmerkungen:

1 *Saggese/Segalla/Sigmund/Raunig/Zangerl/Haslhofer*, Assessing the Solvency of Virtual Asset Service Providers: Are Current Standards Sufficient? Journal of Applied Economics 2024, 1.

2 Vgl *OSCE Mission to Skopje*, Handbook for dealing with virtual currencies in criminal proceedings (2022), online abrufbar unter https://www.osce.org/mission-to-skopje/522754.

3 Siehe https://github.com/INTERPOL-Innovation-Centre/HardwareWallets_DF_List.

4 Siehe https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.

5 Siehe https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki.

Korrespondenz:
Dipl.-Ing. Mag. Dr. Bernhard Haslhofer
Tel.: 0650 / 923 38 40
E-Mail: bernhard.haslhofer@gerichts-sv.at