TOBIAS KREMP

WHITEPAPER FÜR ERMITTLER UND COMPLIANCE

Blockchain verstehen.

Grundlagen, Transaktionen, Seed Phrases und Geldwäschemuster; erklärt an Beispielen, die im Kopf bleiben.

> **Für wen dieses Papier geschrieben ist**
>
> Polizeibeamte im Streifen- und Ermittlungsdienst, Staatsanwälte, Finanzermittler sowie AML- und Compliance-Verantwortliche bei Banken, Fintechs und Zahlungsdienstleistern.
>
> Vorkenntnisse sind nicht erforderlich. Alle Fallbeispiele sind frei erfunden und dienen ausschließlich der Veranschaulichung.

digitale-enteignung.de
Stand: Juli 2026 · Version 1.0

Inhalt

01 | Warum dieses Papier

Kryptowährungen sind längst in der Fallbearbeitung angekommen. Die Anzeige wegen Anlagebetrugs, bei der das Opfer „USDT an eine Trading-Plattform“ überwiesen hat. Die Wohnungsdurchsuchung, bei der ein Zettel mit zwölf handgeschriebenen Wörtern am Kühlschrank hängt. Der Verdachtsfall in der Bank, bei dem ein Kunde binnen drei Wochen 45.000 Euro an eine Kryptobörse transferiert. Wer solche Sachverhalte bearbeitet, braucht kein Informatikstudium. Ein belastbares Grundverständnis genügt, um die richtigen ersten Schritte zu gehen und die richtigen Fragen zu stellen.

Dieses Whitepaper erklärt die Grundlagen so, dass sie hängen bleiben: mit Bildern aus dem Alltag, anhand realitätsnahen Fällen und mit Schaubildern zum Wiedererkennen. Am Ende stehen eine Checkliste für die ersten 24 Stunden und ein Glossar mit den 20 wichtigsten Begriffen.

Eine gute Nachricht vorweg: Die Blockchain ist für die Strafverfolgung kein Feind. Sie ist ein Beweismittel, das nie schläft, nichts vergisst und jedem offensteht. Kein Bankgeheimnis, keine Löschfristen, keine verlorenen Kontoauszüge. Wer die Grundmechanik versteht, hat gegenüber klassischen Finanzermittlungen einen seltenen Vorteil: Der komplette Zahlungsverkehr liegt offen.

02 | Was eine Blockchain ist: das gläserne Kassenbuch

Man stelle sich eine Kleinstadt vor, die ihr gesamtes Geldwesen über ein einziges Kassenbuch abwickelt. Dieses Buch liegt nicht im Rathaus. Es hängt als Kopie in jedem Schaufenster der Stadt, und alle Kopien werden im Minutentakt abgeglichen. Wer jemandem Geld überweisen will, ruft es öffentlich aus: „Seite 4.812, Eintrag 17: Anna zahlt 50 an Bruno.“ Alle Aushänge übernehmen den Eintrag gleichzeitig.

Gefälscht werden kann in diesem System praktisch nichts. Wollte jemand einen alten Eintrag ändern, müsste er sämtliche Kopien in sämtlichen Schaufenstern zugleich manipulieren, und zwar rückwirkend. Genau das leistet eine Blockchain, nur weltweit und automatisiert: Tausende Computer (Nodes) halten identische Kopien desselben Registers und einigen sich laufend auf den gültigen Stand.

Blöcke: Seiten mit Siegel

Die Einträge werden nicht einzeln abgelegt. Sie werden gebündelt, etwa alle zehn Minuten bei Bitcoin, und als „Block“ an das Register angehängt; daher der Name Blockchain, Kette aus Blöcken. Jeder Block erhält ein digitales Siegel, den sogenannten Hash: eine Prüfsumme, die sich aus dem gesamten Inhalt des Blocks errechnet. Ändert sich auch nur ein Komma im Block, ändert sich das komplette Siegel.

Der entscheidende Kniff: Jeder neue Block enthält das Siegel seines Vorgängers. Die Seiten des Kassenbuchs sind dadurch untrennbar miteinander vernäht. Wer Seite 100 fälschen will, macht

damit automatisch die Siegel aller Seiten ab 101 ungültig. Das Netzwerk erkennt den Bruch sofort und verwirft die Fälschung.

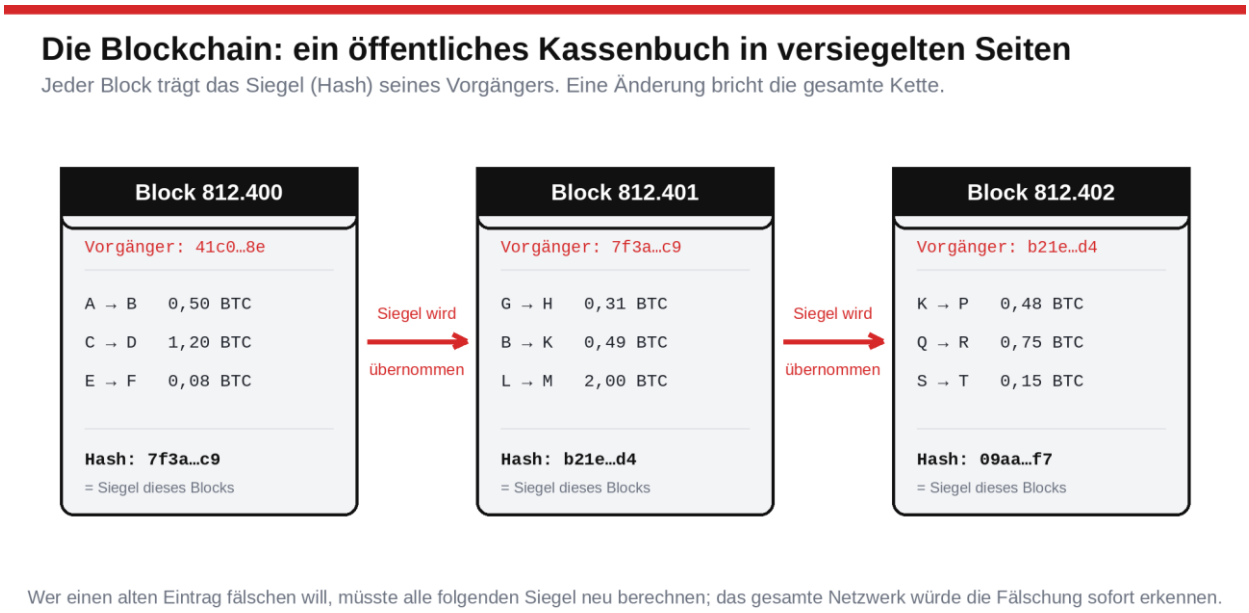

Abb. 1: Blöcke sind versiegelte Kassenbuchseiten. Jede Seite trägt das Siegel der vorherigen.

Merksatz

Eine Blockchain ist ein öffentliches Kassenbuch, von dem tausende identische Kopien existieren. Einträge können nur hinzugefügt, nie geändert oder gelöscht werden.

Für die Ermittlungspraxis heißt das: Was einmal auf der Blockchain steht, steht dort für immer. Beweismittelverlust durch Zeitablauf gibt es on-chain nicht.

03 | Eine Transaktion lesen

Ein Beispiel. Herr Bergmann, 61, hat auf eine angebliche Krypto-Anlageplattform eingezahlt. In seiner Anzeige legt er einen Screenshot vor: eine Buchstaben-Zahlen-Kolonne, ein Betrag, ein Datum. Was auf den ersten Blick kryptisch wirkt, folgt einem festen Schema. Jede Transaktion auf jeder Blockchain besteht im Kern aus fünf Angaben:

- **TXID (Transaktions-ID):** eine lange Zeichenkette, die die Zahlung weltweit einmalig kennzeichnet. Am besten als Aktenzeichen der Zahlung merken. Mit der TXID lässt sich jede Transaktion sekundenschnell in einem Block Explorer aufrufen.
- **Absenderadresse:** die Adresse, von der die Coins stammen.
- **Empfängeradresse:** die Adresse, an die die Coins gehen.
- **Betrag:** auf bis zu acht Nachkommastellen genau, inklusive einer kleinen Netzwerkgebühr.
- **Zeitstempel und Bestätigungen:** wann die Zahlung in einen Block aufgenommen wurde und wie viele Blöcke seitdem folgten. Ab etwa sechs Bestätigungen gilt eine Bitcoin-Zahlung als praktisch unumkehrbar.

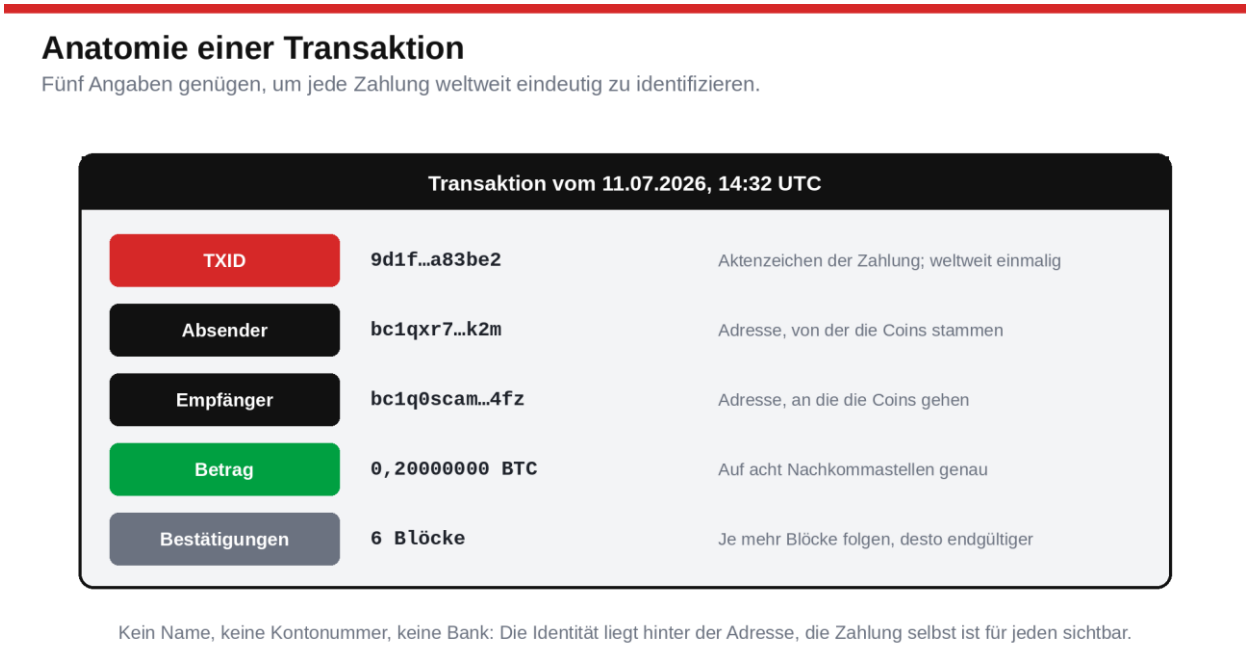

Abb. 2: Die fünf Bestandteile jeder Transaktion am Beispiel der Zahlung von Herrn Bergmann.

Was fehlt, fällt sofort auf: Es gibt keinen Namen, keine IBAN, keine Bank. An die Stelle des Kontoinhabers tritt die Adresse, eine Art Nummernschild ohne öffentliches Halterregister. Die Zahlung selbst ist für jedermann sichtbar; die Person dahinter zunächst nicht. Wie diese Lücke geschlossen wird, behandeln die Kapitel 07 und 09.

> **Praxishinweis für die Anzeigenaufnahme**
>
> Vom Geschädigten immer erfragen beziehungsweise sichern: TXIDs aller Zahlungen, verwendete Empfängeradressen, Name der Plattform samt URL, Screenshots des Chatverlaufs, genutzte eigene Börse oder Wallet-App.

> Eine einzige vollständige TXID ist wertvoller als zehn Seiten Sachverhaltsschilderung: Sie ist der Einstiegspunkt für die gesamte Finanzermittlung.

04 | Zwei Buchungslogiken: Geldscheine gegen Girokonto

Nicht alle Blockchains rechnen gleich. Für die Auswertung ist ein Unterschied zentral, und er lässt sich mit Bargeld und Girokonto erklären.

Bitcoin: die Geldschein-Logik (UTXO)

Bitcoin kennt keine Kontostände. Es kennt einzelne „Scheine“ unterschiedlicher Größe, technisch UTXOs genannt (Unspent Transaction Outputs, unverbrauchte Zahlungsausgänge). Wer 0,7 BTC zahlen will und nur einen Schein zu 1,0 BTC besitzt, gibt den ganzen Schein aus und erhält 0,3 BTC als Wechselgeld zurück; meist auf eine frische, automatisch erzeugte eigene Adresse. Dieses Wechselgeld heißt Change.

Für die Analyse ist Change Gold wert. Fließt aus einer Transaktion ein Teilbetrag an eine nagelneue Adresse, die kurz darauf weiterverwendet wird, gehört diese Adresse mit hoher Wahrscheinlichkeit demselben Inhaber wie die Absenderadresse. Analysetools wie Chainalysis Reactor nutzen genau solche Heuristiken (Change Output Detection, Common Input Ownership), um zehntausende Adressen zu einem Cluster, also zu einem mutmaßlich gemeinsamen Inhaber, zusammenzufassen.

Ethereum und Tron: die Girokonto-Logik (Account-Modell)

Ethereum und Tron führen dagegen echte Kontostände. Eine Adresse ist ein Konto; Zahlungen buchen ab und schreiben gut, Wechselgeld existiert nicht. Konten werden typischerweise dauerhaft wiederverwendet. Das macht die Historie einer einzelnen Adresse besonders übersichtlich: Ein Blick genügt, um sämtliche Ein- und Ausgänge seit Erstellung zu sehen.

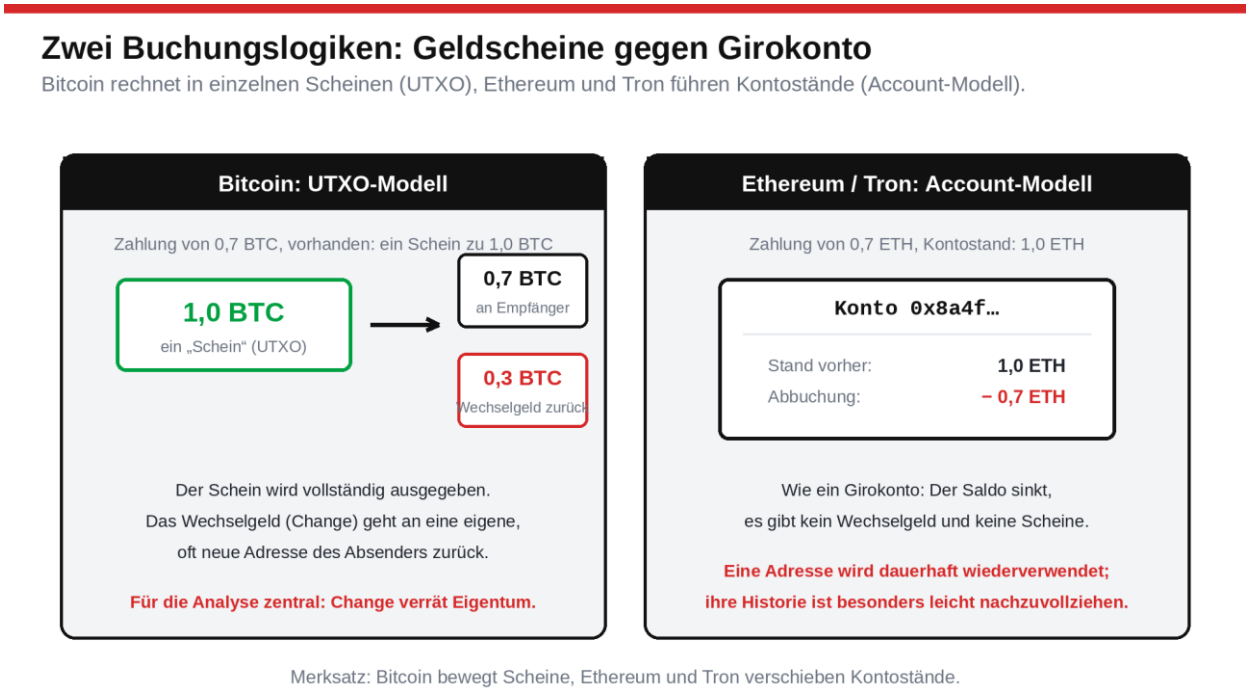

Abb. 3: Bitcoin bewegt Scheine samt Wechselgeld, Ethereum und Tron verschieben Kontostände.

Warum das in der Praxis zählt

Betrugsnetzwerke im Bereich Anlagebetrug arbeiten heute überwiegend mit USDT auf Tron (Kürzel: USDT-TRC20), gerade wegen niedriger Gebühren und einfacher Handhabung.

USDT ist dabei ein Token, kein eigenes Netzwerk: Derselbe „Dollar-Coin“ existiert auf Tron, Ethereum und weiteren Chains. Für die Nachverfolgung ist immer entscheidend, auf welchem Netzwerk die Zahlung lief; das verrät das Adressformat (Kapitel 06).

05 | Wallet, Private Key, Seed Phrase: der Generalschlüssel

Ein zweiter erfundener Fall. Bei Familie Krüger arbeitet eine Woche lang ein Handwerkertrupp. Am Kühlschrank hängt ein Zettel mit zwölf nummerierten Wörtern: „1. ozean 2. tiger 3. lampe …“. Einer der Arbeiter fotografiert den Zettel im Vorbeigehen. Drei Tage später sind sämtliche Kryptobestände der Familie verschwunden, 27.000 Euro. Kein Einbruch, kein Hacking, kein gestohlenes Passwort. Das Foto genügte.

Die drei Ebenen

- **Wallet:** die Verwaltungssoftware oder das Gerät (App, Browser-Erweiterung, USB-Stick-ähnliche Hardware-Wallet). Wichtig: In der Wallet liegen keine Coins. Die Coins liegen immer auf der Blockchain; die Wallet verwahrt nur die Schlüssel.
- **Private Key:** der geheime Schlüssel zu einer einzelnen Adresse. Wer ihn kennt, kann über die Coins dieser Adresse verfügen. Vergleichbar mit dem Schlüssel zu einer einzelnen Tür.
- **Seed Phrase:** zwölf oder 24 Wörter aus einer festen Wortliste, aus denen sich sämtliche Private Keys und Adressen einer Wallet mathematisch neu erzeugen lassen. Der Generalschlüssel zum ganzen Gebäude.

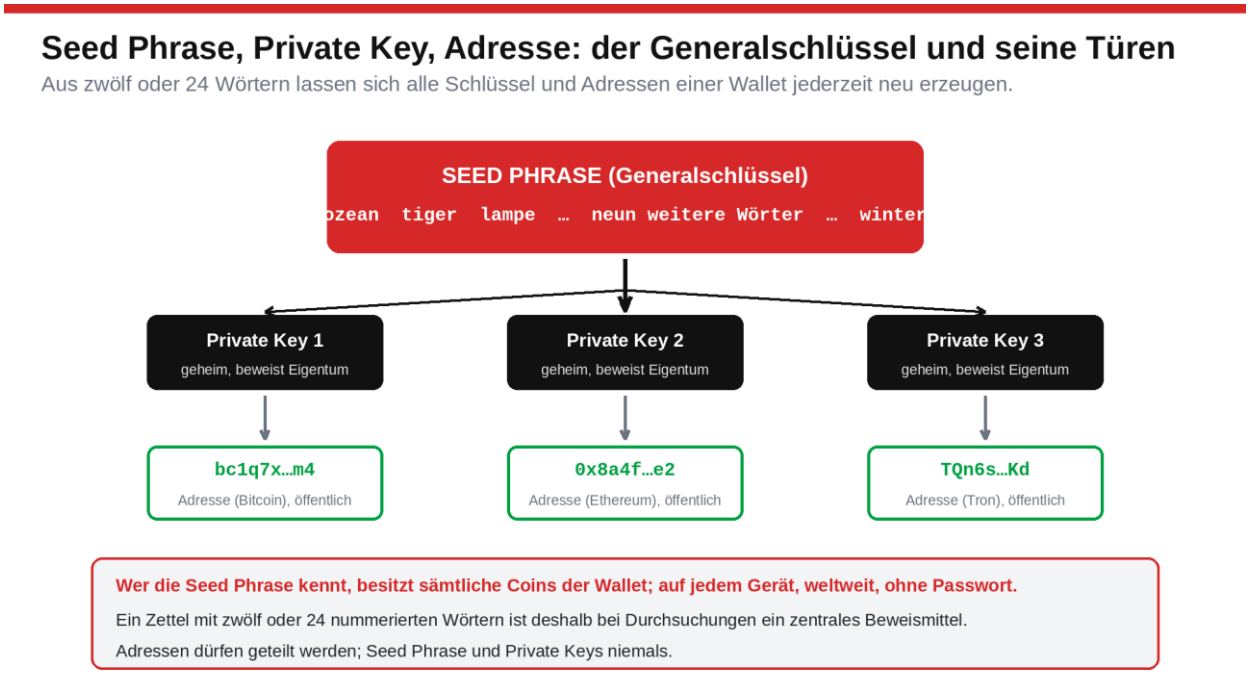

Abb. 4: Aus der Seed Phrase entstehen alle Schlüssel, aus den Schlüsseln alle Adressen.

Die Seed Phrase ist bewusst so gebaut, dass sie auf Papier passt. Sie funktioniert geräteunabhängig und weltweit: Wer die zwölf Wörter in eine beliebige Wallet-App eingibt, hat vollständigen Zugriff auf sämtliche zugehörigen Bestände. Ein Passwort, eine PIN oder das Originalgerät sind dafür nicht erforderlich. Deshalb war das Kühlschrank-Foto im Fall Krüger der komplette Diebstahl.

Bedeutung für Durchsuchung und Sicherstellung

Zettel, Notizbücher oder Metallplatten mit 12 oder 24 nummerierten Wörtern sind potenziell der Zugriff auf Vermögen in unbegrenzter Höhe und entsprechend zu dokumentieren und zu sichern.

Ebenso relevant: Hardware-Wallets (kleine USB-ähnliche Geräte, z. B. mit Display), Recovery-Karten in Originalverpackungen von Wallet-Herstellern, Fotos solcher Zettel auf Smartphones.

Zeitfaktor beachten: Wer die Seed Phrase besitzt, kann Bestände jederzeit von jedem Ort der Welt wegbewegen. Vermögenssichernde Maßnahmen dulden keinen Aufschub.

06 | Adressen erkennen und im Block Explorer prüfen

Adressen sehen aus wie Zeichensalat, folgen aber strengen Formatregeln. Schon die ersten Zeichen verraten das Netzwerk, und das Netzwerk entscheidet, mit welchem Werkzeug weitergearbeitet wird.

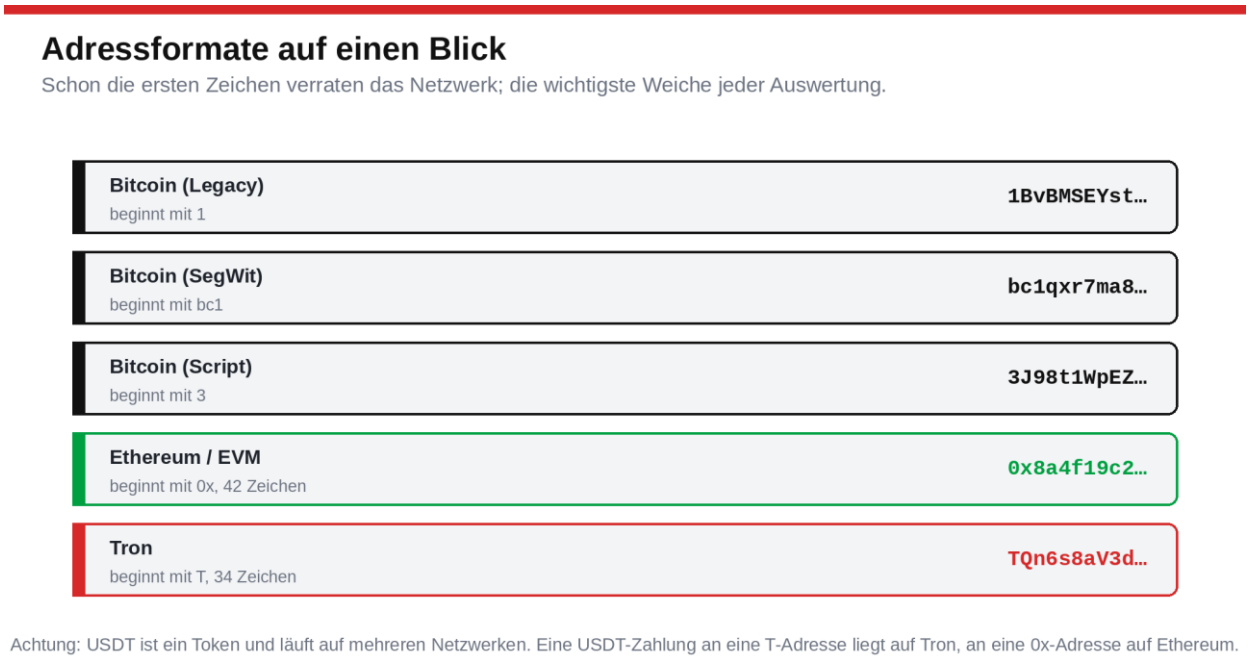

Abb. 5: Die gängigsten Adressformate. Der Anfang der Adresse verrät die Blockchain.

Der Block Explorer: das öffentliche Fahndungsbuch

Ein Block Explorer ist eine frei zugängliche Website, die das Kassenbuch durchsuchbar macht: für Bitcoin etwa mempool.space oder blockchain.com, für Ethereum etherscan.io, für Tron tronscan.org. Kosten: keine. Anmeldung: keine. Spezialsoftware: keine. Für die ersten Schritte einer Auswertung reicht der Explorer vollkommen aus.

Der Ablauf ist immer gleich. Adresse oder TXID in das Suchfeld einfügen und ablesen:

- Gesamtein- und -ausgänge der Adresse sowie aktueller Bestand: Liegt dort noch Vermögen? Dann kann eine Sicherung in Betracht kommen.
- Alle Transaktionen mit Zeitstempel: Passt der Zahlungszeitpunkt zur Aussage des Geschädigten? Damit lässt sich der Sachverhalt objektiv verifizieren.
- Gegenadressen jeder Zahlung: Wohin floss das Geld weiter? Jede Gegenadresse ist der nächste Knoten der Spur.
- Bei Tron und Ethereum zusätzlich: welche Token (etwa USDT) bewegt wurden.

> **Faustregel**
> Block Explorer beantworten die Frage „Was ist passiert?“. Kommerzielle Analysetools wie Chainalysis Reactor oder TRM Labs beantworten die Frage „Wem gehört das?“, weil sie

> Adressen zu Clustern bündeln und bekannte Dienste (Börsen, Mixer, Scam-Wallets) benennen.
>
> Erst Explorer, dann Analysetool: Diese Reihenfolge spart Lizenzkosten und schärft den Blick.

07 | Pseudonym, nicht anonym

Der hartnäckigste Irrtum über Kryptowährungen lautet: „Bitcoin ist anonym." Richtig ist: Bitcoin ist pseudonym. Der Unterschied trägt ganze Ermittlungsverfahren.

Anonym wäre ein Bargeldkoffer, der den Besitzer wechselt: keine Aufzeichnung, keine Spur, kein Nachweis. Pseudonym ist ein Nummernschild ohne öffentliches Halterregister: Jede Fahrt wird lückenlos protokolliert, für immer und für jeden einsehbar. Unbekannt ist zunächst nur, wer am Steuer sitzt. Sobald das Pseudonym ein einziges Mal mit einer Identität verknüpft wird, fällt die gesamte protokollierte Historie auf diese Person zurück; rückwirkend bis zur allerersten Transaktion.

Wo Pseudonyme zerbrechen

- **Börsen mit Identitätsprüfung (KYC):** die mit Abstand wichtigste Bruchstelle, ausführlich in Kapitel 09.
- **Wiederverwendung von Adressen:** Wer dieselbe Adresse für Schwarzmarkt und Gehaltseingang nutzt, verknüpft beide Welten selbst.
- **Öffentliche Spuren:** eine Spendenadresse im Social-Media-Profil, eine Adresse in einem Forumspost, ein Erpresserschreiben: alles verwertbare Verknüpfungen.
- **Eigene Fehler der Täter:** Testüberweisungen vom Privatkonto, vergessene Change-Adressen, Zahlungen an Bekannte.

Hinzu kommt der Faktor Zeit, und er arbeitet ausnahmslos für die Strafverfolgung. Klassische Bankunterlagen unterliegen Aufbewahrungsfristen; Blockchain-Daten nicht. Eine Transaktion aus dem Jahr 2015 lässt sich 2026 genauso auswerten wie am Tag ihrer Ausführung. Analysetools werden zudem laufend besser: Cluster, die vor fünf Jahren unbenannt waren, tragen heute Labels. Kalte Spuren tauen on-chain regelmäßig wieder auf.

> **Merksatz**
>
> Die Blockchain vergisst nichts, und sie verzeiht nichts. Ein einziger Identitätsbezug genügt, um Jahre an Transaktionshistorie einer Person zuzuordnen.

08 | Muster der Verschleierung

Wer gestohlene oder ertrogene Coins besitzt, hat ein Problem: Die Herkunft klebt an ihnen, sichtbar für jedes Analysetool. Täter versuchen deshalb, die Spur zu verwischen. Die vier häufigsten Muster lassen sich mit Alltagsbildern beschreiben, und alle vier hinterlassen selbst wieder charakteristische Spuren.

Peel Chain: die Zwiebeltechnik

Von einem großen Betrag wird Schicht für Schicht ein kleiner Teil „abgeschält“ und zu einer Börse oder einem Aufkäufer geschickt; der Rest wandert jeweils auf eine frische Adresse weiter. Es entsteht eine lange Kette aus Einmal-Adressen mit stets ähnlichem Bild: großer Durchlaufposten, kleine Abzweigung. Genau diese Regelmäßigkeit macht Peel Chains in Graphenansichten auf einen Blick erkennbar.

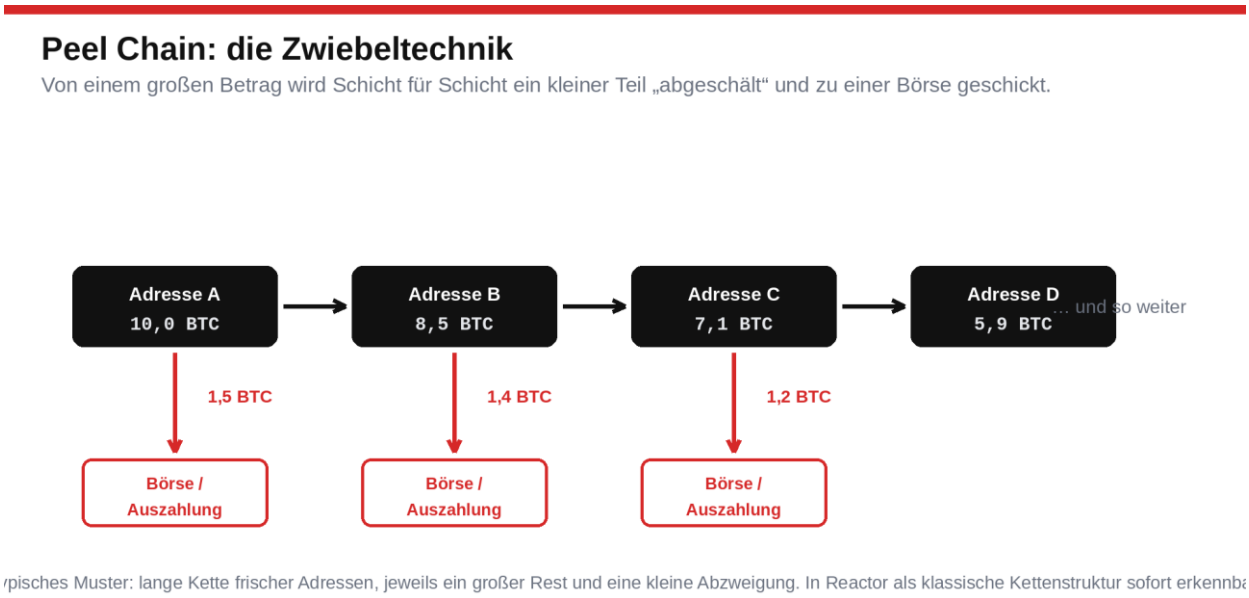

Abb. 6: Peel Chain. Der Hauptbetrag wandert weiter, kleine Tranchen zweigen zur Auszahlung ab.

Consolidation: das Sammelbecken

Das Gegenstück zur Peel Chain: Viele kleine Zuflüsse, etwa die Einzahlungen hunderter Betrugsopfer, laufen in wenigen Sammeladressen zusammen, bevor der Gesamtbetrag weiterbewegt wird. Für Ermittlungen ist das ein Geschenk: Eine einzige identifizierte Sammeladresse verbindet sämtliche Opfer eines Netzwerks und bündelt getrennte Verfahren zu einem Gesamtbild.

Mixer: der große Topf

Ein Mixer (auch Tumbler) funktioniert wie ein Topf, in den viele Personen ihre Münzen werfen, um anschließend „andere“ Münzen in gleicher Höhe zu entnehmen. Die direkte Verbindung zwischen Ein- und Auszahlung reißt ab. Vollständig verschwindet sie trotzdem selten: Beträge, Zeitfenster und Verhaltensmuster erlauben in vielen Fällen eine Zuordnung (Demixing), und die bloße Mixer-Nutzung ist ein gewichtiges Indiz für Verschleierungsabsicht, das auch beweisrechtlich Bedeutung gewinnen kann.

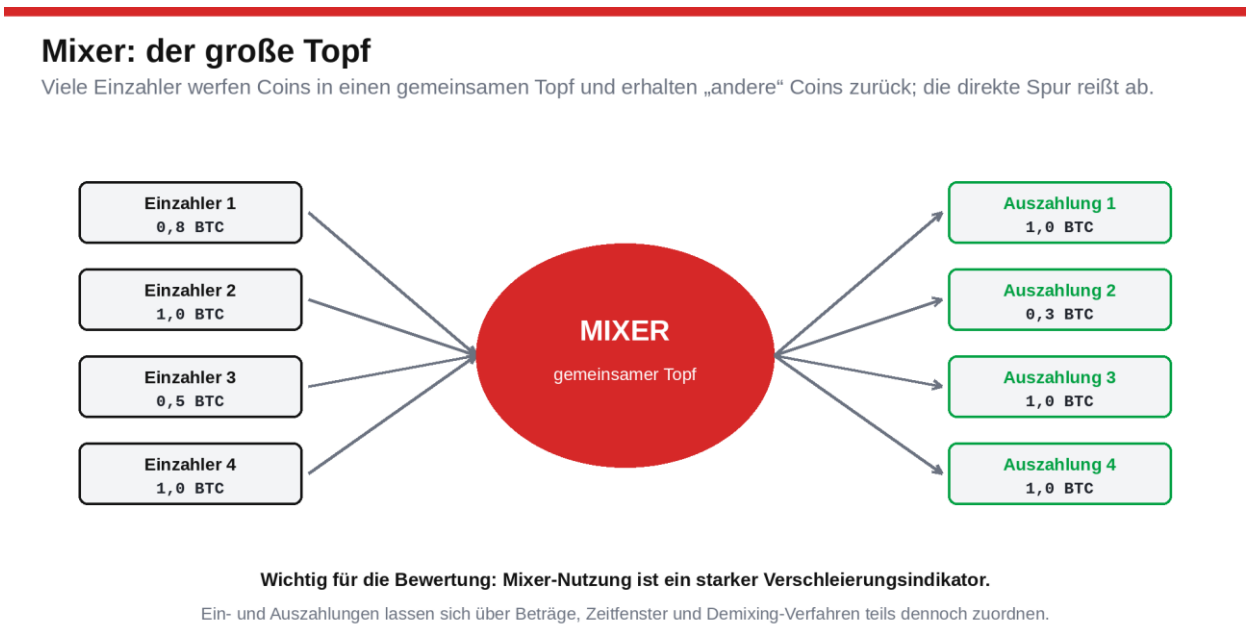

Abb. 7: Mixer-Prinzip. Der gemeinsame Topf kappt die direkte Spur; Muster bleiben.

Chain Hopping: der Fahrzeugwechsel

Fluchtfahrer wechseln das Auto, Geldwäscher wechseln die Blockchain: Bitcoin wird über eine Brücke (Bridge) oder eine Tauschplattform in USDT auf Tron getauscht, von dort weiter in Ether, und so fort. Jeder Wechsel soll den Verfolger abschütteln, weil klassische Werkzeuge an der Netzwerkgrenze enden. Moderne Analysetools verfolgen Bridge-Übergänge zunehmend automatisch; zudem entsteht an jeder Tauschstelle ein Dienstleister, der Aufzeichnungen führt und als Auskunftsadressat in Betracht kommt.

Der rote Faden aller vier Muster

Verschleierung vernichtet die Spur nicht, sie verlängert sie nur. Jede zusätzliche Station kostet die Täter Gebühren und Zeit und erzeugt neue Datenpunkte: Adressen, Zeitstempel, Dienstleister.

Ermittlungspraktisch gilt: dem Geld bis zum nächsten Dienstleister folgen. Dort warten Aufzeichnungen, und Aufzeichnungen bedeuten Auskunftsersuchen.

09 | Die Börse als Schlüsselstelle: KYC und Auskunftsersuchen

Irgendwann wollen Täter reales Geld sehen: Euro auf einem Konto, Bargeld in der Hand. Der Weg dorthin führt fast immer über eine Kryptobörse (Exchange) oder einen vergleichbaren Dienstleister. Und regulierte Dienstleister müssen ihre Kunden kennen: Das Kürzel KYC steht für „Know Your Customer“ und meint die Identifizierungspflicht nach Geldwäscherecht.

Eine Börse verwahrt damit genau das, was der Blockchain fehlt: Namen. Ausweiskopien, Selfie-Videos aus dem Verifikationsprozess, E-Mail-Adressen, Telefonnummern, IP-Protokolle, verknüpfte Bankverbindungen, Login-Zeiten, Gerätedaten. Führt eine verfolgte Spur zu einer Einzahladresse einer Börse, verwandelt ein erfolgreiches Auskunftsersuchen das Pseudonym in eine Person.

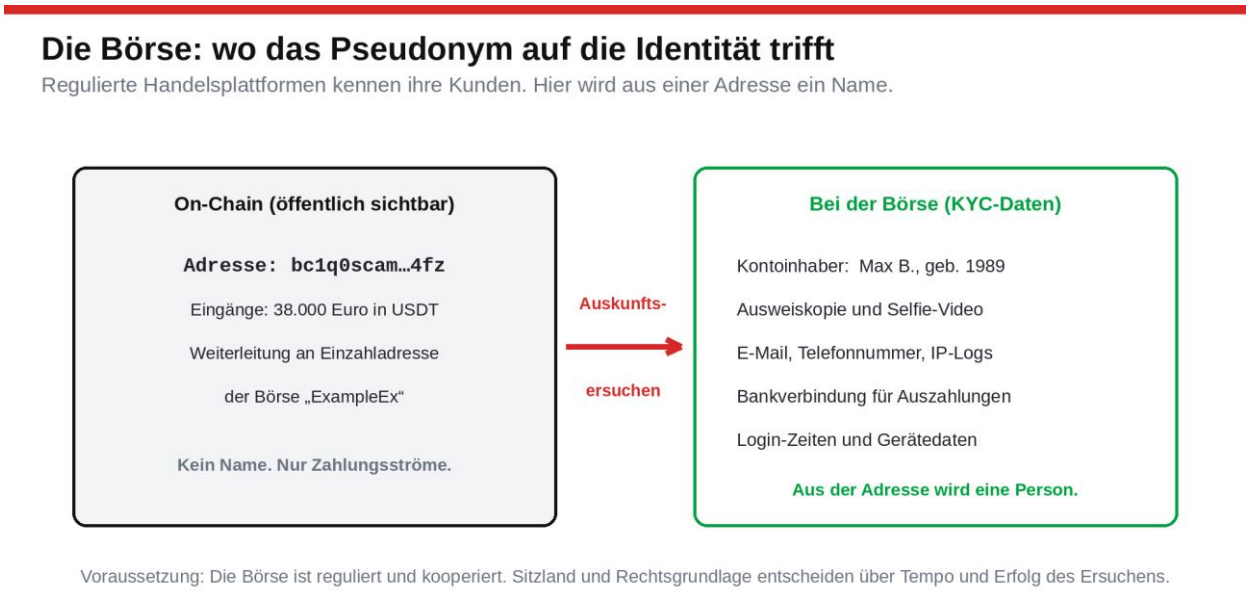

Abb. 8: An der Börse trifft die öffentliche Zahlungsspur auf gespeicherte Identitätsdaten.

Was über Erfolg und Tempo entscheidet

- **Zuordnung der Adresse:** Analysetools erkennen die Einzahladressen großer Börsen zuverlässig; im Zweifel bestätigt die Börse selbst, ob eine Adresse zu ihr gehört.
- **Sitzland und Regulierung:** In der EU zugelassene Anbieter (seit MiCA mit einheitlicher Lizenzpflicht) sind über Rechtshilfe- und Auskunftswege gut erreichbar. Anbieter in kooperationsunwilligen Jurisdiktionen bleiben schwierig; auch das ist eine ermittlungsrelevante Erkenntnis über das Netzwerk.
- **LEA-Kanäle:** Die meisten großen Börsen unterhalten eigene Law-Enforcement-Portale oder -Postfächer mit definierten Anforderungen an Ersuchen. Präzise Ersuchen (Adresse, TXID, Zeitraum, Rechtsgrundlage) werden deutlich schneller beantwortet als Pauschalanfragen.
- **Eile bei Guthaben:** Liegt auf dem Börsenkonto noch Vermögen, kommt eine Sperr- beziehungsweise Sicherungsbitte in Betracht, bevor die Auskunft im Detail bearbeitet wird. Bei zentral verwalteten Stablecoins wie USDT kann der Herausgeber Adressen technisch einfrieren; ein solcher Freeze sichert Vermögen, ersetzt aber kein Verfahren und garantiert keine Rückzahlung an Geschädigte.

Merksatz

Die Blockchain zeigt das Wohin, die Börse kennt das Wer. Jede Krypto-Finanzermittlung läuft auf denselben Moment zu: den Übergang der Spur in einen Dienstleister mit Kundendaten.

10 | Ein Fall von Anfang bis Ende: „Sandra M. und die Trading-App“

Zum Abschluss ein durchgehendes, frei erfundenes Beispiel, das die Bausteine der vorigen Kapitel zusammensetzt. Der Ablauf entspricht der Typologie, die internationale Berichte als „Pig Butchering“ beschreiben: Opfer werden über Wochen emotional aufgebaut (gemästet) und anschließend finanziell ausgenommen (geschlachtet).

Phase 1: der Aufbau

Sandra M., 47, Bürokauffrau, erhält über ein soziales Netzwerk eine Kontaktanfrage von „David“, angeblich Finanzanalyst in Singapur. Wochenlang geht es um Alltag, Familie, Urlaubspläne; von Geld keine Rede. Dann zeigt David beiläufig Screenshots seiner Gewinne auf einer Trading-Plattform und bietet an, ihr den Einstieg zu zeigen.

Phase 2: die Einzahlungen

Sandra registriert sich bei einer deutschen Kryptobörse, durchläuft dort die Identitätsprüfung und kauft USDT. Nach Davids Anleitung überweist sie die Token an eine Tron-Adresse der „Plattform“: zunächst 500 Euro, nach ersten angeblichen Gewinnen 4.500 Euro, später in drei Tranchen weitere 33.000 Euro. Gesamtschaden: 38.000 Euro. Die App zeigt derweil ein Depot von angeblich 61.000 Euro. Als Sandra auszahlen will, verlangt die Plattform eine „Steuer“ von 15%. Spätestens hier zerreißt die Illusion, und Sandra erstattet Anzeige.

Phase 3: die Auswertung

Die Anzeige enthält, was Kapitel 03 empfiehlt: alle TXIDs, die Empfängeradresse (Format T…, also Tron), Screenshots der App und des Chats. Der Blick in den Block Explorer bestätigt die Zahlungen auf die Minute. Die Empfängeradresse zeigt außerdem Eingänge von über 40 weiteren Adressen in vergleichbaren Stückelungen: mutmaßlich weitere Geschädigte, der Fall ist Teil einer Serie.

Die Analyse mit einem kommerziellen Tool zeichnet das bekannte Bild: Die Opfergelder laufen in einer Sammeladresse zusammen (Consolidation), werden dort mit Geldern anderer Kampagnen vermischt und in mehreren Tranchen an die Einzahladressen zweier Börsen im Ausland weitergeleitet. Auf einer der Adressen liegen zum Auswertungszeitpunkt noch rund 210.000 USDT.

Phase 4: die Maßnahmen

- Sicherungsersuchen an die Börse mit Guthaben, parallel Anregung eines Freezes der Sammeladresse beim Stablecoin-Herausgeber.
- Auskunftsersuchen zu Kontoinhaber, KYC-Unterlagen, IP-Protokollen und verknüpften Bankverbindungen über die LEA-Kanäle beider Börsen.
- Abgleich der über 40 einzahlenden Adressen mit anderen Verfahren: Zusammenführung der Serie, Identifikation weiterer Geschädigter über deren KYC-Börsen.
- Sandras eigene Börse kennt ihre Identität ohnehin; ihre Auszahlungsadresse dient als verifizierter Startpunkt der Beweiskette.

Ob am Ende Täter im Ausland gefasst werden, entscheidet die internationale Kooperation. Gesichert ist etwas anderes: eine lückenlose, gerichtsfeste Dokumentation des Geldflusses vom Konto der Geschädigten bis zur letzten bekannten Station, die Verknüpfung dutzender Einzelfälle zu einer Serie und die reale Chance auf Vermögenssicherung. Vor zwanzig Jahren hätte derselbe Fall mit Auslandsüberweisungen an Briefkastenfirmen geendet; heute liegt der komplette Zahlungsweg offen.

11 | Checkliste: die ersten 24 Stunden

Zehn Punkte für den Erstzugriff bei Sachverhalten mit Kryptobezug, gleich ob Anzeigenaufnahme, Durchsuchung oder Verdachtsmeldung:

- **1. TXIDs sichern.** Jede Transaktions-ID vollständig dokumentieren; Copy-and-paste statt Abschrift, ein Zeichen Unterschied macht die ID wertlos.
- **2. Adressen sichern.** Alle bekannten Empfänger- und Absenderadressen erfassen und das Netzwerk anhand des Formats notieren (1/3/bc1 = Bitcoin, 0x = Ethereum, T = Tron).
- **3. Plattform dokumentieren.** URL, App-Name, Screenshots der Oberfläche und des angeblichen Depots; betrügerische Seiten verschwinden oft binnen Tagen.
- **4. Kommunikation sichern.** Chatverläufe vollständig exportieren, Profile der Kontaktpersonen mit Screenshots festhalten.
- **5. Eigene Börse des Geschädigten erfragen.** Dort liegen verifizierte Daten und die Auszahlungshistorie; der saubere Startpunkt der Beweiskette.
- **6. Block Explorer nutzen.** Zahlungen verifizieren, Restguthaben auf Zieladressen prüfen, unmittelbare Weiterleitungen notieren.
- **7. Bei Guthaben: Eile.** Restbestände auf Täteradressen oder Börsenkonten können jederzeit abfließen; Sicherungsmaßnahmen und Freeze-Anregungen priorisieren.
- **8. Bei Durchsuchungen: Seed Phrases.** Zettel und Platten mit 12/24 Wörtern, Hardware-Wallets, Recovery-Karten und Fotos davon auf Geräten gezielt suchen und sichern.
- **9. Serienbezug prüfen.** Empfängeradressen mit anderen Verfahren und öffentlichen Scam-Datenbanken abgleichen; Einzelfälle sind selten Einzelfälle.
- **10. Spezialisierte Stellen einbinden.** Für Clusteranalyse, VASP-Recherche und internationale Ersuchen frühzeitig die zuständigen Fachdienststellen beziehungsweise die Compliance-Eskalationswege nutzen.

12 | Glossar

Adresse	Öffentliche Kennung für den Empfang von Coins; vergleichbar einem Nummernschild ohne öffentliches Halterregister.
Block	Gebündelte, versiegelte „Seite“ des Kassenbuchs mit vielen Transaktionen; verweist stets auf den Vorgängerblock.
Block Explorer	Frei zugängliche Website zum Durchsuchen einer Blockchain (z. B. mempool.space, etherscan.io, tronscan.org).
Bridge	Dienst zum Übertragen von Werten zwischen zwei Blockchains; typisches Werkzeug beim Chain Hopping.
Chain Hopping	Wiederholter Wechsel zwischen Blockchains zur Verschleierung der Spur; der „Fahrzeugwechsel“ der Geldwäsche.
Change	Wechselgeld einer Bitcoin-Transaktion; fließt an eine (oft neue) Adresse des Absenders zurück und verrät dadurch Eigentum.
Cluster	Gruppe von Adressen, die Analysetools demselben Inhaber zuordnen, etwa über gemeinsame Verwendung in Transaktionen.
Cold Wallet	Schlüsselverwahrung ohne Internetverbindung, z. B. Hardware-Wallet oder Papier; Gegenstück: Hot Wallet.
Hash	Digitale Prüfsumme („Siegel“) über Daten; jede noch so kleine Änderung erzeugt einen völlig anderen Hash.
KYC	„Know Your Customer“: geldwäscherechtliche Pflicht regulierter Dienstleister zur Identifizierung ihrer Kunden.
Layering	Verschleierungsphase der Geldwäsche: Aufsplitten, Weiterleiten und Tauschen inkriminierter Gelder über viele Stationen.
MiCA	EU-Verordnung über Märkte für Kryptowerte; einheitlicher Zulassungs- und Aufsichtsrahmen für Kryptodienstleister in der EU.
Mixer / Tumbler	Dienst, der Coins vieler Nutzer vermischt, um die direkte Zahlungsspur zu kappen; starker Verschleierungsindikator.
Peel Chain	Kettenmuster, bei dem von einem großen Betrag wiederholt kleine Tranchen „abgeschält“ und ausgezahlt werden.
Private Key	Geheimer Schlüssel zu einer Adresse; wer ihn kennt, verfügt über deren Coins.
Seed Phrase	12 oder 24 Wörter, aus denen alle Schlüssel und Adressen einer Wallet wiederherstellbar sind; der Generalschlüssel.
Stablecoin	Kryptowert mit stabilem Zielwert, meist 1 US-Dollar (z. B. USDT, USDC); Standardzahlungsmittel heutiger Betrugsnetzwerke.

TXID	Weltweit einmalige Kennung einer Transaktion; das „Aktenzeichen“ jeder Zahlung.
UTXO	Unverbrauchter Zahlungsausgang bei Bitcoin; die „Geldscheine“, aus denen Zahlungen zusammengesetzt werden.
VASP / CASP	Anbieter von Kryptodienstleistungen (Börsen, Verwahrer, Tauschdienste); Adressaten von Auskunftsersuchen.

Über diese Publikation

Dieses Whitepaper erscheint auf digitale-enteignung.de, der Publikationsplattform von Tobias Kremp zu Finanzkriminalität, Blockchain-Forensik und der Mechanik der digitalen Enteignung. Sämtliche Fallbeispiele, Namen und Beträge sind frei erfunden; Übereinstimmungen mit realen Personen oder Verfahren wären zufällig.

HINWEIS: Alle Inhalte sind rein privater Natur. Der Autor schreibt als unabhängiger Experte und Publizist (Art. 5 GG) auf Basis öffentlich zugänglicher Quellen. Die Beiträge sind keine offiziellen Stellungnahmen einer Behörde und ersetzen keine Rechtsberatung.