DIGITAL ASSET
INTELLIGENCE

WHITEPAPER
2026

KRYPTO-FORENSIK · ASSET RECOVERY

Die Anatomie professioneller Krypto-Betrüger

Wie Täterinfrastrukturen wirklich arbeiten — und wie man Kryptowährungen zurückverfolgt, Wallet-Cluster aufdeckt und Vermögenswerte sichert.

14 KAPITEL · 8 FORENSISCHE ERKENNTNISSE

FINANZ FORENSIK GMBH · AUTOR: DAVID LÜDTKE

HINWEIS ZUR METHODIK & ZIEL

Wie professionelle Kryptobetrüger tatsächlich arbeiten

Kein weiteres Erklärstück über Blockchains, sondern die praxisnahe Antwort auf die Frage, wie Täter organisatorisch, technisch und wirtschaftlich vorgehen — und woran sich ihre Vorgehensweise forensisch festmachen lässt, um Kryptowährungen zurückzuverfolgen und Vermögenswerte zurückzuholen.

14–17 Mrd. USD
Krypto-Betrug weltweit 2025 (Chainalysis)

+253 %
Ø-Schaden je Zahlung 2024→2025 (782→2.764 USD)

≈ +1.400 %
Impersonation-Betrug 2025 (KI-Deepfakes)

84 %
der illegalen Zuflüsse in Stablecoins (2025)

HINWEIS ZUR METHODIK

Die Schlussfolgerungen beruhen auf den praktischen Erfahrungen der Finanz Forensik GmbH aus mehreren hundert kryptoforensischen Untersuchungen im deutschsprachigen Raum, ergänzt um öffentliche Quellen — ausdrücklich nicht als eigene statistische Auswertung. Alle Fallbeispiele, Wallet-Adressen, Beträge und Transaktionsverläufe sind, soweit nicht mit Quelle versehen, anonymisiert oder illustrativ konstruiert („Illustrativer Platzhalter") und lassen keine Rückschlüsse auf reale Geschädigte, Täter oder Verfahren zu.

Vier Opfer, eine Sammelwallet. *Unabhängige Zahlungsströme münden über unterschiedliche Layering-Pfade in derselben Sammelwallet und konvergieren am Cash-Out — genau das macht Täterinfrastrukturen forensisch angreifbar.*

1 Einleitung

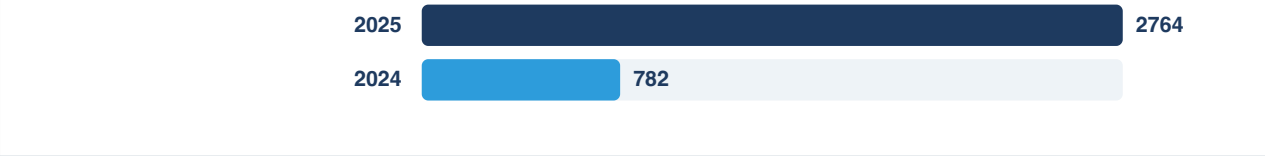
1.1 Die Entwicklung des Kryptobetrugs

Kryptowährungsbetrug hat sich von gelegentlichen Einzeltaten zu einem arbeitsteilig organisierten Geschäftsmodell entwickelt. Standen früher einzelne Täter mit begrenztem technischem Wissen dahinter, sind es heute spezialisierte, mitunter industriell anmutende Strukturen: Personen, die Opfer akquirieren (gefälschte Investmentplattformen, Romance- bzw. „Pig-Butchering"-Kontakte, Social-Media-Werbung), Personen, die die technische Infrastruktur betreiben (Wallets, Sammelstellen, Cross-Chain-Transfers), und Personen, die ausschließlich auf den Cash-Out in Fiat spezialisiert sind.

Diese Arbeitsteilung erschwert klassische Ermittlungsansätze, die auf eine einzelne verantwortliche Person zielen. Zugleich eröffnet sie neue forensische Ansatzpunkte: Wo Arbeitsteilung existiert, existieren auch Schnittstellen — und Schnittstellen hinterlassen Spuren, die sich per Blockchain-Analyse und Wallet Clustering sichtbar machen lassen.

1.2 Schadenssummen und Dunkelfeld

Nach dem 2026 Crypto Crime Report von Chainalysis wurden 2025 weltweit mindestens 14 Mrd. USD durch Kryptobetrug on-chain nachgewiesen; nach vollständiger Nacherfassung dürften es über 17 Mrd. USD sein — gegenüber rund 9,9 Mrd. USD im Vorjahr. Die durchschnittliche Schadenssumme pro Betrugszahlung stieg von 782 USD (2024) auf 2.764 USD (2025) — ein Plus von 253 %. Impersonation-Betrug wuchs um rund 1.400 %, getrieben von KI-Deepfakes.



Durchschnittliche Schadenssumme je Betrugszahlung (USD). *Anstieg um 253 % binnen eines Jahres (Chainalysis, 2026 Crypto Crime Report — Scams).*

Auch die allgemeine Cyberkriminalität in Deutschland liegt auf Höchststand: Das BKA registrierte für 2025 rund 334.000 Fälle Cybercrime im engeren Sinne bei einem von Bitkom geschätzten Gesamtschaden von 202,4 Mrd. Euro; gut 62 % der Taten wurden aus dem Ausland oder von unbekannten Tatorten begangen. Eine gesonderte Vollstatistik zu kryptobezogenen Schäden führt das BKA nicht — was das Dunkelfeld zusätzlich erschwert. Viele Fälle werden aus Scham oder der falschen Annahme, die Blockchain sei anonym, gar nicht angezeigt.

1.3 Die Professionalisierung der Täter

- Mehrsprachige, teils industriell organisierte Kontaktzentren zur Opferansprache
- Standardisierte technische Infrastruktur (Wallet-Generatoren, Layering-Skripte, vorbereitete Sammelwallets)
- Feste Kooperationen mit OTC-Brokern und etablierten Cash-Out-Kanälen
- Nutzung mehrerer Blockchains und Cross-Chain-Bridges zur systematischen Verschleierung
- Arbeitsteilige Rollen: Akquise, technische Abwicklung, Cash-Out, Geldwäsche

Wie industriell diese Strukturen agieren, zeigt die kambodschanische Huione-Gruppe, die nach Chainalysis-Daten über rund viereinhalb Jahre mehr als 98 Mrd. USD an Kryptowerten verarbeitete und mindestens 4 Mrd. USD aus illegalen Quellen wusch, bevor US-Behörden dem Netzwerk den Zugang zum Finanzsystem entzogen. Gegen den Vorsitzenden der „Prince Group" wurde Anklage wegen des Betriebs von Zwangsarbeits-Scam-Compounds erhoben. Professionalisierung bedeutet dabei nicht mehr Anonymität — im Gegenteil: Je standardisierter eine Infrastruktur arbeitet, desto wiederkehrender sind ihre Muster.

1.4 Warum klassische Ermittlungsansätze oft scheitern

Klassische Ansätze setzen bei der Identität einer Person an: Wer eröffnete das Konto, wer betrieb die Website, wer stand hinter der Nummer. Bei international agierenden, arbeitsteiligen Gruppen führt das ins Leere, weil kontaktierende Person, technische Infrastruktur und Cash-Out-Stelle unterschiedlichen, oft in verschiedenen Jurisdiktionen ansässigen Akteuren zuzurechnen sind.

1.5 Warum die Blockchain trotzdem Spuren hinterlässt

Eine öffentliche Blockchain ist kein anonymer, sondern ein pseudonymer und vollständig transparenter Raum. Jede Transaktion ist dauerhaft, unveränderlich und einsehbar. Was fehlt, ist nicht die Historie, sondern die Zuordnung einer Adresse zu einer realen Identität. Genau hier setzt professionelle Analyse an — durch Kombination von On-Chain-Mustern (Clustering, Zeitkorrelation, Bilanzanalyse) mit Off-Chain-Informationen (KYC-Daten, OSINT, Auskunftsersuchen) — bis idealerweise zu einem konkreten Cash-Out-Konto.

1

FORENSISCHE ERKENNTNIS NR. 1

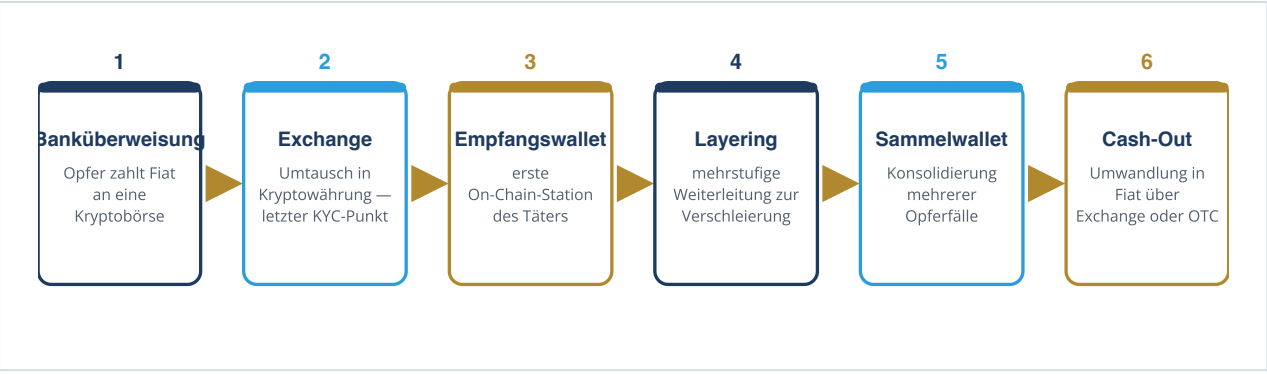
In nahezu allen von der Finanz Forensik GmbH untersuchten Fällen hinterließ die Täterinfrastruktur mehr verwertbare Spuren als die ursprüngliche Kontaktaufnahme zum Opfer. Während gefälschte Webseiten, Nummern und Chat-Accounts schnell gelöscht werden, bleiben die genutzten Wallet-Strukturen dauerhaft und unveränderlich auf der Blockchain nachvollziehbar.

KERNAUSSAGEN

- ✓ Kryptobetrug ist heute arbeitsteilig organisiert: Akquise, technische Abwicklung und Cash-Out liegen häufig in unterschiedlichen Händen.
- ✓ Allein 2025 wurden weltweit mindestens 14–17 Mrd. USD durch Krypto-Betrug erbeutet — Tendenz stark steigend.
- ✓ Klassische Ermittlungsansätze scheitern oft, weil sie auf eine Person zielen statt auf die Infrastruktur.
- ✓ Eine Blockchain ist pseudonym, nicht anonym — jede Transaktion bleibt dauerhaft und öffentlich nachvollziehbar.
- ✓ Die Täterinfrastruktur hinterlässt meist mehr Spuren als die ursprüngliche Kontaktaufnahme zum Opfer.

2 Der Lebenszyklus eines Kryptobetrugs

Um die Infrastruktur professioneller Täter zu verstehen, hilft die Betrachtung des typischen Wegs der Gelder vom Opfer bis zur Verwertung in Fiat als Prozess. Dieser Lebenszyklus wiederholt sich — mit Detailvariationen — in der Mehrheit der untersuchten Fälle und bildet das Grundgerüst jeder späteren Wallet-Analyse.



Der Lebenszyklus eines Kryptobetrugs in sechs Phasen. *Vier unabhängige Opferpfade münden typischerweise über unterschiedliches Layering in derselben Sammelwallet — und konvergieren am Cash-Out.*

Phase 1 — Banküberweisung. Der Betrug beginnt außerhalb der Blockchain, mit einer Banküberweisung oder Kartenzahlung an eine Kryptobörse. Forensisch die am einfachsten zu dokumentierende Phase (Kontoauszug + KYC-Daten der Exchange). Datum, Betrag, Empfänger-IBAN und Verwendungszweck bilden die Brücke zur On-Chain-Analyse.

Phase 2 — Exchange. Die Fiat-Einzahlung wird in Kryptowährung getauscht und an eine Täter-Wallet weitergeleitet. Dies ist der letzte Punkt mit direkter, KYC-gestützter Verbindung zwischen realer Person (Opfer) und Blockchain-Adresse, bevor die Gelder in die Täterinfrastruktur eintreten.

Phase 3 — Empfangswallet und Layering. Die empfangende Wallet ist meist nur die erste Station eines mehrstufigen Weiterleitungsprozesses (Layering), der Rückverfolgung erschweren und Tracing-Tools ermüden soll. In der Praxis sind Layering-Muster jedoch charakteristisch und wiedererkennbar.

Phase 4 — Sammelwallets und Cluster. Gelder aus mehreren Layering-Ketten — oft aus mehreren Opferfällen — laufen in einer begrenzten Zahl von Sammelwallets zusammen. Diese Konsolidierung ist aus Tätersicht wirtschaftlich sinnvoll und aus forensischer Sicht der wichtigste Ansatzpunkt für Wallet Clustering.

Phase 5 — Cash-Out. Am Ende steht die Umwandlung in Fiat oder verwertbare Form (Immobilien, Luxusgüter, OTC-Weiterverkauf). Der Cash-Out ist der verletzlichste Punkt, weil er regelmäßig eine regulierte, KYC-pflichtige Stelle involviert (Kapitel 7).

KERNAUSSAGEN

- ✓ Der Lebenszyklus folgt typischen Phasen: Banküberweisung, Exchange, Empfangswallet, Layering, Sammelwallet, Cash-Out.
- ✓ Die Banküberweisung ist forensisch am einfachsten zu dokumentieren — sie verknüpft eine reale Identität mit dem Fall.
- ✓ An der Exchange entsteht die letzte direkte, KYC-gestützte Verbindung zwischen Opfer und Blockchain-Adresse.
- ✓ Layering verschleiert den Geldfluss, hinterlässt aber charakteristische, wiedererkennbare Muster.
- ✓ Sammelwallets und der abschließende Cash-Out sind die verletzlichsten Punkte der gesamten Täterkette.

3 Die Infrastruktur moderner Täter

Professionelle Kryptobetrüger arbeiten selten mit einer einzelnen Wallet. Sie betreiben vollständige, wiederverwendbare Systeme aus Empfangs-, Zwischen- und Sammelwallets, ergänzt um Exchange-Konten, Stablecoin-Routen und OTC-Kontakte — der eigentliche Gegenstand jeder seriösen Wallet-Analyse.

BAUSTEIN	FUNKTION IN DER TÄTERINFRASTRUKTUR
Empfangswallets	Erste On-Chain-Station nach der Exchange; oft pro Opfer/Kampagne neu generiert. Markieren den eindeutigen Startpunkt eines Falls; über Zeitkorrelation mit anderen verknüpfbar.
Zwischenwallets / Layering	Reine Verschleierung; mehrere Weiterleitungen in kurzen Abständen, teils gleich große Teilbeträge („Peeling"/„Splitting"). Skript-Automatik hinterlässt regelmäßige Sekunden-/Minuten-Muster.
Sammelwallets	Organisatorisches Zentrum; hier laufen Gelder vieler Fälle zusammen. Fließen Gelder mehrerer unabhängiger Geschädigter hinein, ist das ein starkes Indiz für gemeinsame Täterschaft.
Exchange-Konten	Ohne Cash-Out-Kanal sind Kryptowerte wertlos. Strukturell notwendig — und der Punkt, an dem KYC/AML/Auskunftsersuchen am wirksamsten greifen.
Cross-Chain-Bridges	Transfer zwischen Blockchains erschwert die Analyse. Moderne Plattformen (z. B. Crystal Intelligence) bilden Cross-Chain-Bewegungen inzwischen durchgängig ab.
Stablecoins (USDT/USDC)	Bevorzugt für Sammelwallets/Cash-Out (keine Kursschwankung). 2025 rund 84 % der illegalen Zuflüsse — Emittenten-Kooperation (Freeze/Auskunft) erhöht Verfolgbarkeit.
OTC-Broker	Außerbörslicher Umtausch großer Beträge, teils ohne KYC. Bevorzugter Cash-Out-Weg — Bereich mit regulatorischem Nachholbedarf.

2 FORENSISCHE ERKENNTNIS NR. 2

Täterinfrastrukturen werden in aller Regel mehrfach verwendet, weil ihr Aufbau — insbesondere die Beschaffung funktionierender Exchange- und OTC-Zugänge — für die Täter selbst mit erheblichem Aufwand verbunden ist. Diese Wiederverwendung ist der zentrale Hebel forensischer Ermittlungen: Ein einzelner identifizierter Baustein führt häufig zu weiteren, bislang unbekannten Opferfällen.

KERNAUSSAGEN

- ✓ Professionelle Täter betreiben vollständige, wiederverwendbare Infrastruktursysteme statt einzelner Wallets.
- ✓ Empfangs- und Zwischenwallets dienen der Verschleierung; Sammelwallets sind das organisatorische Zentrum.
- ✓ Exchange-Konten sind der wertvollste Baustein, weil ohne sie erlangte Kryptowerte wertlos bleiben.
- ✓ Cross-Chain-Transfers und Stablecoins erschweren die Analyse, verhindern sie aber nicht — rund 84 % der illegalen Zuflüsse 2025 entfielen auf Stablecoins.
- ✓ Die Wiederverwendung dieser Bausteine über mehrere Opferfälle ist der zentrale Hebel forensischer Ermittlungen.

4 Die Ökonomie professioneller Kryptobetrüger

Die Bausteine erklären, woraus eine Täterinfrastruktur besteht — nicht, warum sie so aussieht. Die Antwort liegt in der Wirtschaftlichkeit: Professionelle Betrüger handeln als Unternehmer. Sie minimieren Aufwand, optimieren Kosten und automatisieren, wo es sich lohnt. Aus dieser betriebswirtschaftlichen Logik entstehen die wiederkehrenden Muster, die forensische Analyse überhaupt sichtbar macht.

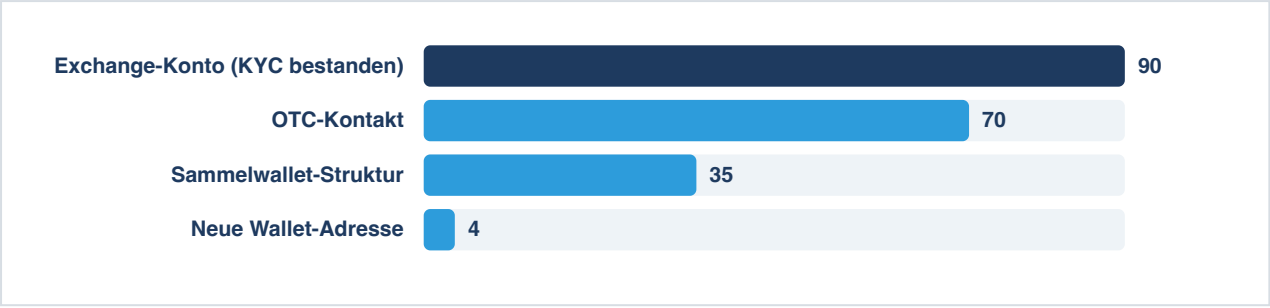
4.1 Täter denken in Grenzkosten, nicht in Verschleierungsmaximierung

Ein verbreitetes Missverständnis unterstellt Tätern, jede technisch mögliche Verschleierung auszuschöpfen. In der Praxis sind Infrastrukturen so komplex, wie es der Fall wirtschaftlich erfordert — nicht komplexer. Zusätzliches Layering, Cross-Chain-Sprünge oder Zwischenwallets kosten Zeit, Gas Fees und erhöhen die Fehlerwahrscheinlichkeit. Täter stoppen dort, wo der Grenzaufwand den Grenznutzen übersteigt.

4.2 Warum Infrastruktur mehrfach verwendet wird

Der Aufbau einer funktionierenden Infrastruktur kostet: Wallets generieren, Layering-Skripte konfigurieren, Cross-Chain-Routen testen und vor allem Exchange-/OTC-Zugänge beschaffen — häufig mit gefälschten Identitätsdokumenten, glaubwürdigem Kontoverlauf und OTC-Kontakten. Dieser Aufwand amortisiert sich erst über mehrere Nutzungen. Rationale Konsequenz: wiederholte Verwendung dersel-

ben Sammelwallets, Exchange-Konten und OTC-Kontakte über zahlreiche Opferfälle.



Relativer Beschaffungsaufwand einzelner Infrastrukturbausteine (illustrativ). *Je aufwendiger ein Baustein zu beschaffen ist, desto stärker wird er wiederverwendet — und desto belastbarer der spätere Cluster-Nachweis. Illustrative Werte zur Veranschaulichung der Grundlogik.*

4.3 Warum Wallets recycelt werden

Eine neue Wallet-Adresse ist technisch praktisch kostenlos — dennoch werden bekannte Zwischen- und Sammelwallets wiederverwendet. Grund ist die operative Komplexität: Jede Adresse muss überwacht, mit Gas versorgt und in die interne Buchhaltung integriert werden. Je größer und arbeitsteiliger eine Gruppe, desto mehr gleicht ihre Struktur einem klassischen Zahlungsverkehr mit festen Konten — und desto wertvoller wird die Kontinuität einzelner Adressen.

4.4–4.6 OTC, Exchange-Konten und rationale Wege

OTC-Broker bieten geringere/keine KYC-Anforderungen und den Umtausch großer Summen ohne Marktbewegung — beides senkt Entdeckungsrisiko und Kosten, um den Preis der Abhängigkeit von wenigen „verlässlichen" Kontakten. Eine Wallet ist beliebig reproduzierbar; ein unauffälliges Exchange-Konto mit Handelslimit und bestandener KYC ist es nicht — es ist ein knappes Wirtschaftsgut. Diese Knappheit erklärt, warum Cash-Out-Konten über viele unabhängige Fälle identisch bleiben, während vorgelagerte Wallets variiert werden. Täterinfrastruktur ist nie zufällig, sondern das Ergebnis rationaler Kosten-Nutzen-Abwägung — der eigentliche Grund, warum sich Muster wiederholen und Cash-Out-Punkte konvergieren.

3 FORENSISCHE ERKENNTNIS NR. 3

Die wirtschaftliche Logik der Täter ist der eigentliche Schlüssel zum Verständnis ihrer technischen Infrastruktur. Wer forensisch nach Mustern sucht, sucht im Kern nach den Stellen, an denen sich für Täter Wiederverwendung lohnt — und genau dort entstehen die belastbarsten Cluster-Nachweise.

KERNAUSSAGEN

- ✓ Täter handeln wirtschaftlich — nicht verschleierungs-, sondern grenzkosten-getrieben.
- ✓ Exchange-Konten sind wertvoller als Wallets, weil sie knapp und aufwendig zu beschaffen sind.
- ✓ Infrastruktur wird deshalb wiederverwendet — über viele Opferfälle hinweg.
- ✓ Genau daraus entstehen Wallet-Cluster und konvergierende Cash-Out-Punkte.
- ✓ Deshalb lohnt sich Bilanzanalyse mehr als isolierte Risk Scores.

5 Wallet Clustering

Wallet Clustering ordnet mehrere Blockchain-Adressen mit hinreichender Wahrscheinlichkeit demselben wirtschaftlichen Akteur zu — hier bewusst aus praktisch-ermittlerischer, nicht mathematisch-algorithmischer Perspektive: Woran erkennt ein Analyst, dass mehrere Wallets zusammengehören?

5.1 Woran erkennt man dieselben Täter?

- Wiederkehrende Sammelwallets, in die mehrere unabhängige Opferfälle münden
- Identische oder sehr ähnliche Layering-Muster (Zwischenschritte, Zeitabstände, Betragsstruktur)
- Gemeinsame Cash-Out-Adressen bei derselben Exchange
- Wiederverwendung derselben Zwischenwallets über mehrere Kampagnen hinweg
- Gemeinsame Nutzung derselben Bridge-Route zur selben Zielchain

5.2 Woran erkennt man dieselbe Infrastruktur?

Infrastruktur-Cluster bestehen auch dann fort, wenn sich die handelnden Personen ändern (z. B. wechselndes Personal im operativen Bereich). Kennzeichen sind gleichbleibende technische Muster — dieselbe Wallet-Generierungslogik, dasselbe Bridge-Protokoll, derselbe OTC-Kontakt — über längere Zeit, auch wenn einzelne vorgelagerte Wallets wechseln.

5.3 & 5.4 Mehrere Opfer, praktische Ansatzpunkte

Der zuverlässigste Indikator ist die nachweisbare Konvergenz unabhängiger Zahlungsströme in derselben Sammelwallet oder demselben Exchange-Konto innerhalb eines plausiblen Zeitfensters. OSINT (identische Kommunikationsmuster, Webseiten-Templates, Zahlungsaufforderungen) liefert unterstützende, nicht allein tragfähige Indizien.

ANSATZPUNKT	AUSSAGEKRAFT
Bilanzanalyse	Analyse der Zu- und Abflüsse einzelner Wallets über die Zeit — der methodisch stärkste Einzelbaustein (Kapitel 6).
Zeitkorrelation	Transaktionen in engem zeitlichen Zusammenhang (z. B. mehrere Empfangswallets, die binnen Minuten an dieselbe Sammelwallet leiten) deuten auf zentrale, koordinierte Steuerung.
Konsolidierungen	Gezieltes Zusammenführen von Guthaben aus mehreren Adressen in eine Zieladresse — eines der stärksten Cluster-Signale, da selten ohne gemeinsame Kontrolle.
Cash-Outs	Gemeinsamer Endpunkt mehrerer Ketten bei derselben Exchange/OTC-Adresse schließt den Kreis — mit Auskunftsersuchen oft der entscheidende Ansatz.

KERNAUSSAGEN

- ✓ Wallet Clustering ordnet mehrere Adressen demselben Akteur zu — praktisch, nicht rein mathematisch.
- ✓ Wiederkehrende Sammelwallets und identische Layering-Muster sind die stärksten Hinweise auf gemeinsame Täterschaft.
- ✓ Infrastruktur-Cluster bestehen auch dann fort, wenn sich die handelnden Personen ändern.
- ✓ Zeitkorrelation und Konsolidierungen liefern besonders belastbare Cluster-Signale.
- ✓ Der gemeinsame Cash-Out-Endpunkt schließt den Kreis und liefert oft den entscheidenden Ansatz.

6 Die Bilanzanalyse

Die Bilanzanalyse einzelner Wallets zählt zu den wirkungsvollsten, in der Praxis aber am wenigsten systematisch genutzten Werkzeugen — aus Sicht der Finanz Forensik GmbH der stärkste Einzelbaustein einer Wallet-Analyse, stärker als jeder automatisierte Risk Score. Statt einzelner Transaktionen wird der gesamte Kontostand einer Adresse über die Zeit nachvollzogen, vergleichbar einer Kontobewegungsanalyse im Bankwesen.

6.1 Warum Zu- und Abflüsse aussagekräftiger sind als Risk Scores

Risk Scores bewerten die Nähe einer Adresse zu bekannten illegalen Quellen (Mixer, Darknet, sanktionierte Adressen). Ein hoher Score ist ein nützlicher erster Hinweis, ersetzt aber keine inhaltliche Analyse. Aussagekräftiger ist die tatsächliche Bilanzbewegung: Wann und in welcher Höhe fließen Werte zu, wann und wohin ab — und ergibt sich ein wirtschaftlich sinnvolles Muster, das zur behaupteten Nutzung passt, oder nicht?

6.2 Die zentralen Fragen der Bilanzanalyse

- Wie viel Geld floss insgesamt durch die Adresse (kumulierter Zu- und Abfluss)?
- Wie hoch war der maximale Bestand, und wann wurde er erreicht?
- Wann erfolgte die Konsolidierung — das gezielte Zusammenführen aus mehreren Quellen?
- Wann begann der Cash-Out, und über welchen Zeitraum?
- Welche weiteren Opferfälle lassen sich anhand der Zuflusszeitpunkte derselben Infrastruktur zuordnen?
- Welche Exchange bzw. welcher OTC-Kontakt erhielt den größten Abflussanteil?

Diese Fragen sind kein Selbstzweck: Genau diese Informationstiefe benötigen Behörden, Staatsanwaltschaften und Anwälte, um ein Auskunftsersuchen zu formulieren, einen Vermögensarrest zu beantragen oder eine zivilrechtliche Klage schlüssig zu begründen (Kapitel 12/13).

> **Das typische Muster einer Sammelwallet**
>
> Der forensische Wert entsteht nicht durch eine isolierte Transaktion, sondern durch die Beobachtung: Eine Adresse ohne nennenswerte Historie wächst binnen kurzer Zeit auf ein Vielfaches ihres Zuflusses an, um anschließend vollständig an eine identifizierbare Exchange-Adresse zu fließen. Schneller Aufbau, punktueller Abfluss — bei legitimer Nutzung untypisch, bei professionellen Sammelwallets die Regel. [Illustrativer Platzhalter — konstruiertes Rechenbeispiel]

4 FORENSISCHE ERKENNTNIS NR. 4

Eine sorgfältige Bilanzanalyse liefert in der Praxis regelmäßig belastbarere Anhaltspunkte für eine gerichtsverwertbare Dokumentation als ein isolierter Risk Score, weil sie den wirtschaftlichen Sinnzusammenhang einer Adresse nachvollziehbar macht und die konkreten Fragen beantwortet, die Ermittler, Anwälte und Gerichte tatsächlich stellen.

KERNAUSSAGEN

- ✓ Die Bilanzanalyse verfolgt Zu- und Abflüsse einer Wallet über die Zeit — wie eine Kontobewegungsanalyse.
- ✓ Sie ist aussagekräftiger als ein isolierter Risk Score, weil sie den wirtschaftlichen Sinnzusammenhang zeigt.
- ✓ Sie beantwortet, was Ermittler brauchen: Höchststand, Konsolidierungszeitpunkt, Beginn des Cash-Out.
- ✓ Schneller Aufbau gefolgt von punktuellem Komplettabfluss ist das typische Sammelwallet-Muster.
- ✓ Genau diese Fragen bilden das Grundgerüst jedes gerichtsverwertbaren forensischen Berichts.

7 Die Bedeutung von Cash-Outs

Nicht jede Exchange im Geldfluss ist ein sinnvolles Ermittlungsziel — manche sind nur Durchgangsstation. Entscheidend ist die tatsächliche Cash-Out-Stelle: der Punkt, an dem Kryptowerte final in Fiat, andere Vermögenswerte oder verwertbare Form überführt werden.

7.1 Warum Cash-Outs der wichtigste Ermittlungsansatz sind

Cash-Out-Stellen sind der Punkt, an dem die Anonymitätsvorteile der Blockchain enden und regulatorische Instrumente greifen. Anders als eine Zwischenwallet unterliegt eine Exchange KYC-/AML-Pflichten und ist auskunftspflichtig. Da Täter aus wirtschaftlichen Gründen auf wenige Auszahlungspunkte beschränkt sind (Kapitel 4), ist die Cash-Out-Exchange häufig der Schlüssel zur realen Person.

7.2 KYC und AML als Hebel

KYC und AML verpflichten Exchanges, Identitäten zu verifizieren und verdächtige Muster zu melden. In der EU stützt sich das auf einen einheitlichen Rahmen: Die MiCA-Verordnung (EU) 2023/1114 etabliert seit Ende 2024 eine EU-weite Zulassungs- und Aufsichtspflicht für Kryptowertedienstleister (CASP). Ergänzend verpflichtet die Transfer-of-Funds-Regulation (VO (EU) 2023/1113, TFR) seit 30.12.2024 zur Übermittlung vollständiger Auftraggeber- und Begünstigtendaten — die EU-Umsetzung der FATF-„Travel Rule" (Empfehlung 16), konkretisiert in den EBA Travel Rule Guidelines (EBA/GL/2024/11). Ist eine Cash-Out-Adresse einer MiCA-lizenzierten Exchange zugeordnet, lässt sich über ein Auskunftsersuchen im Idealfall die Kontoinhaberschaft ermitteln — zunehmend auch die Kette vorangegangener Transfers.

7.3–7.5 Freeze, Datenanforderung, Vermögensarrest

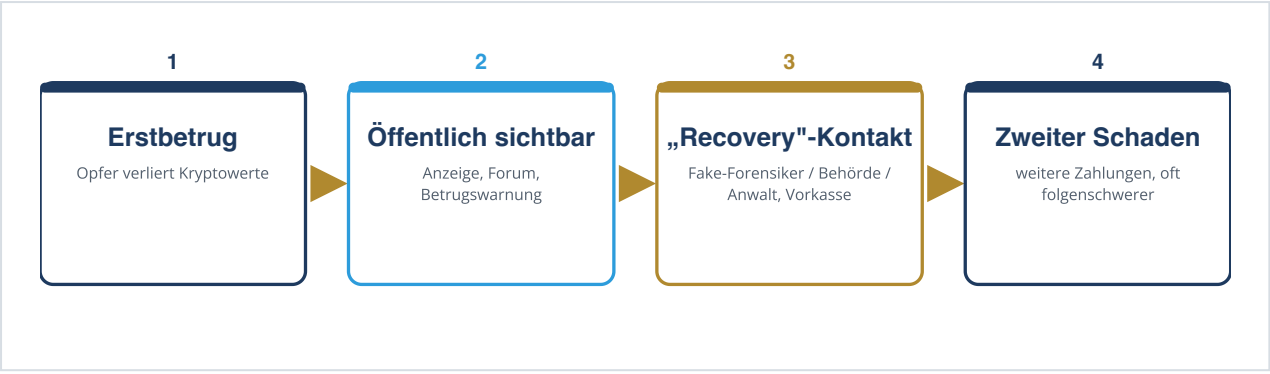
Viele größere Exchanges können Guthaben im Zusammenhang mit gemeldeten Betrugsfällen vorübergehend einfrieren („Freeze"). Eine zeitnahe, gut dokumentierte Freeze-Anfrage kann verhindern, dass Gelder vor Verfahrensabschluss weiter verschoben werden. Formale Datenanforderungen (strafprozessual über Rechtshilfeersuchen, zivilrechtlich über Auskunftsansprüche) richten sich an die Exchange der Cash-Out-Adresse; die Erfolgsaussichten hängen an der Qualität der forensischen Dokumentation (Kapitel 12). Zugeordnete Vermögenswerte eröffnen einen strafprozessualen Vermögensarrest (§§ 111e ff. StPO) zur Sicherung späterer Einziehung (§§ 73 ff. StGB) oder einen zivilrechtlichen Arrest.

KERNAUSSAGEN

- ✓ Nicht jede Exchange im Geldfluss ist ein Ermittlungsziel — entscheidend ist die tatsächliche Cash-Out-Stelle.
- ✓ MiCA und die Travel Rule (TFR) verpflichten Kryptodienstleister EU-weit zu KYC- und Auskunftspflichten.
- ✓ Cash-Out-Stellen sind der Punkt, an dem die Anonymitätsvorteile der Blockchain enden.
- ✓ Zeitnahe Freeze-Anfragen können verhindern, dass Gelder vor Verfahrensabschluss weiter verschoben werden.
- ✓ Identifizierte Cash-Out-Adressen eröffnen den Weg zu Vermögensarrest und Einziehung nach §§ 73 ff. StGB.

8 Recovery-Scams: Der zweite Betrug

Ein in der Literatur nahezu fehlendes, in der Praxis regelmäßiges Thema: der Recovery-Scam. In einem Satz — der zweite Betrug beginnt häufig unmittelbar nach dem ersten und richtet sich gezielt gegen Menschen, die durch den ursprünglichen Kryptobetrug bereits geschädigt und emotional verwundbar sind.



Der Recovery-Scam-Zyklus. *Vom ursprünglichen Betrug über die öffentliche Meldung bis zum zweiten, häufig folgenschwereren Vermögensschaden.*

Sobald ein Opfer öffentlich sichtbar wird (Anzeige, Forumsbeitrag, Bewertung auf einer Betrugswarnseite, Kontakt zu einer Kanzlei), gerät es häufig auf informelle „Listen" weiterverkaufter Opferdaten. Anti-Fraud-Ermittler beschreiben es unmissverständlich: Ist ein Opfer erst bekannt, folgt in vielen Fällen ein zweiter Kontaktversuch — durch angebliche Wiederbeschaffungs-Spezialisten (Chainalysis/Operation Shamrock, zit. n. cryptonews.com, Nov. 2025).

ERSCHEINUNGSFORM	VORGEHEN
Klassischer Recovery-Scam	„Recovery-Experten" kontaktieren proaktiv, behaupten, die Werte lokalisiert zu haben, verlangen eine Vorabgebühr. Nach Zahlung bricht der Kontakt ab oder es folgen weitere Gebühren.
Fake-Forensiker	Täter geben sich als Blockchain-Forensiker aus, präsentieren gefälschte, technisch wirkende Berichte und suggerieren eine baldige Rückführung — gegen Vorkasse.
Fake-Behörden	Angebliche Mitarbeiter von Polizei, Staatsanwaltschaft, BaFin oder internationalen Behörden fordern „Freigabegebühren" oder „Steuern" für die Auszahlung sichergestellter Werte.
Fake-Anwälte	Vorgeblich spezialisierte Anwälte hätten bereits ein Urteil erwirkt und verlangen Gerichts-/Vollstreckungskosten im Voraus.
Wallet Verification / Pay-to-Withdraw	Aufforderung, zur „Verifizierung" einen Betrag zu senden, oder vor jeder Auszahlung eine „Freischaltgebühr" — beide dienen nur weiteren Zahlungen.

Recovery-Scams nutzen den emotionalen Zustand nach dem Schaden aus: Hoffnung auf Wiedergutmachung, Scham über die erste Täuschung und der Wunsch nach schneller Korrektur senken die kritische Distanz erheblich.

> **Erkennungsmerkmale seriöser Krypto-Forensik**
>
> Seriöse Dienstleister verlangen keine Vorabzahlung für ein „garantiertes" Ergebnis — eine Analyse kann Auffindbarkeit dokumentieren, nie eine Rückholung garantieren. Sie treten unter nachprüfbarer Firmenidentität (Impressum, Kontakt, Berufserfahrung) auf, kontaktieren Geschädigte in der Regel nicht unaufgefordert und dokumentieren methodisch nachvollziehbar statt auf bloße Behauptungen gestützt.

5 FORENSISCHE ERKENNTNIS NR. 5

Der zweite Betrug ist kein Randphänomen, sondern eine regelmäßige Folgeerscheinung jedes öffentlich gewordenen Kryptobetrugsfalls. Aufklärung über Recovery-Scams sollte fester Bestandteil jeder ersten Kontaktaufnahme mit Geschädigten sein — nicht nachrangige Randnotiz.

KERNAUSSAGEN

- ✓ Der zweite Betrug beginnt häufig unmittelbar nach dem ersten — sobald ein Opfer öffentlich sichtbar wird.
- ✓ Fake-Forensiker, Fake-Behörden und Fake-Anwälte verlangen Vorabgebühren für eine angeblich sichere Rückholung.
- ✓ Wallet Verification und Pay-to-Withdraw sind gängige Varianten, weitere Zahlungen zu erzwingen.
- ✓ Seriöse Forensik-Dienstleister garantieren niemals ein Ergebnis und verlangen keine Vorkasse dafür.
- ✓ Aufklärung über Recovery-Scams gehört in jedes Erstgespräch — nicht an dessen Ende.

9 Täterinfrastrukturen erkennen: Anonymisierte Fallbeispiele

Hinweis

Die Fallbeispiele sind illustrativ und anonymisiert. Sie fassen wiederkehrende Muster aus vielen realen Untersuchungen zusammen, ohne einen konkreten, identifizierbaren Fall wiederzugeben. [Illustrative Platzhalter — konstruierte Fallbeispiele]

Fall A — Vier Opfer, eine Sammelwallet. Vier unabhängige Geschädigte meldeten separat Verluste bei derselben gefälschten Handelsplattform. Die Zahlungswege unterschieden sich zunächst deutlich (Exchanges, Empfangswallets, Layering-Tiefen). Die Analyse zeigte jedoch: Alle vier Ströme liefen nach drei bis fünf Zwischenschritten in derselben Sammelwallet zusammen — was die zunächst unzusammenhängenden Fälle einer Täterinfrastruktur zuordnete und gemeinsam gegenüber der Cash-Out-Exchange geltend machen ließ.

Fall B — Zwölf Wallets, eine Exchange-Adresse. Zwölf oberflächlich unabhängige Wallets wiesen keine direkten Verbindungen auf. Erst die Untersuchung der finalen Cash-Out-Transaktion zeigte: Alle zwölf zahlten an dieselbe Einzahlungsadresse eines Nutzerkontos bei einer bekannten Exchange. Typisch für Strukturen, die auf Wallet-Ebene bewusst verschleiern, auf Cash-Out-Ebene aber (Kapitel 4) auf wenige Konten angewiesen sind.

Fall C — Mehrere Blockchains, eine Exchange. Gezielte Nutzung mehrerer Chains über Cross-Chain-Bridges fragmentierte die Analyse. Dennoch dienten am Ende dieselbe Exchange und dasselbe Nutzerkonto als Cash-Out — ein Hinweis, dass Cross-Chain-Aktivität primär den Analyseprozess verschleiert, nicht zwingend eine diversifizierte Cash-Out-Struktur widerspiegelt.

6 FORENSISCHE ERKENNTNIS NR. 6

In allen drei Mustern lag der entscheidende forensische Ansatzpunkt nicht am Anfang, sondern am Ende der Täterkette — bei der Cash-Out-Adresse. Wallet-technische Verschleierung auf den vorgelagerten Stufen konnte die Konvergenz an der Auszahlungsstelle in keinem Beispiel verhindern.

KERNAUSSAGEN

- ✓ Vier unabhängige Opfer können über unterschiedliche Wege in derselben Sammelwallet zusammenlaufen.
- ✓ Zwölf oberflächlich unverbundene Wallets können am Ende bei demselben Exchange-Konto auszahlen.
- ✓ Cross-Chain-Aktivität über mehrere Blockchains mündet häufig dennoch in einer einzigen Exchange.
- ✓ In allen Mustern lag der entscheidende Ermittlungsansatz am Ende der Kette — nicht am Anfang.
- ✓ Wallet-technische Verschleierung verhindert die Konvergenz an der Cash-Out-Stelle in der Praxis kaum.

10 Die größten Irrtümer

In Gesprächen mit Geschädigten, Ermittlungsbehörden und Anwälten begegnen der Finanz Forensik GmbH regelmäßig dieselben Fehlannahmen über die Nachverfolgbarkeit von Kryptotransaktionen. Mythos gegen forensische Realität:

✕ MYTHOS	✓ REALITÄT
Ein hoher Risk Score bedeutet automatisch, dass der Inhaber der Adresse Täter ist.	Ein Risk Score bewertet die Nähe einer Adresse zu bekannten illegalen Aktivitäten. Er ist ein Hinweis, kein Beweis. Erst Bilanzanalyse und Wallet Clustering zeigen, ob und wie eine Adresse tatsächlich eingebunden ist.
✕ MYTHOS	✓ REALITÄT
Sobald Gelder durch einen Mixer geleitet wurden, sind Ermittlungen beendet.	Mixer erschweren die Analyse, beenden sie aber nicht zwangsläufig. Viele Implementierungen weisen eigene, bekannte Muster auf; moderne Tools bilden Ein- und Ausgänge weiter ab, und der Zufluss zum Mixer bleibt nachvollziehbar.
✕ MYTHOS	✓ REALITÄT
Wenn Kryptowerte weitergeleitet wurden, sind die Coins „verschwunden".	Kryptowerte verschwinden nicht. Jede Transaktion bleibt dauerhaft und öffentlich dokumentiert. Was fehlt, ist zunächst nur die Zuordnung zu einer realen Identität, nicht die Transaktionshistorie.
✕ MYTHOS	✓ REALITÄT
Eine gelöschte Wallet-App bedeutet, dass die Wallet nicht mehr existiert.	Eine Wallet ist keine App, sondern eine Adresse plus privater Schlüssel. Das Löschen der App entfernt nur die lokale Oberfläche; Adresse und Historie bleiben unverändert einsehbar.
✕ MYTHOS	✓ REALITÄT
Blockchain-Transaktionen sind vollständig anonym.	Öffentliche Blockchains sind pseudonym, nicht anonym. Jede Adresse und Transaktion ist einsehbar; es fehlt nur die direkte Identitätsverknüpfung, die sich über KYC, OSINT oder Verhaltensmuster oft herstellen lässt.
✕ MYTHOS	✓ REALITÄT
Ein Kontostand von 0 bedeutet, dass dort keine relevante Aktivität stattfand.	Null zeigt nur den aktuellen Zustand. Entscheidend ist die historische Bilanzbewegung — wie viel Wert wann zu- und wieder abgeflossen ist (Kapitel 6).
✕ MYTHOS	✓ REALITÄT
Stablecoins wie USDT können nicht zurückverfolgt werden.	Stablecoins sind ebenso nachvollziehbar wie andere Token. Zusätzlich können zentralisierte Emittenten (Tether, Circle) einzelne Adressen auf begründete Anfrage einfrieren — teils besser verfolgbar als andere Token.

KERNAUSSAGEN

- ✓ Ein hoher Risk Score ist ein Hinweis, kein Beweis für Täterschaft.
- ✓ Mixer erschweren Ermittlungen, beenden sie aber nicht — der Zufluss zum Mixer bleibt sichtbar.
- ✓ Weitergeleitete Kryptowerte verschwinden nicht; ihre Historie bleibt dauerhaft dokumentiert.
- ✓ Blockchains sind pseudonym, nicht anonym — die Zuordnung zu einer Identität lässt sich oft herstellen.
- ✓ Stablecoins wie USDT sind ebenso nachvollziehbar wie andere Token — teils besser über Emittenten-Freezes.

11 Technischer Gewahrsam ≠ Eigentum

Ein unterschätztes, rechtlich zentrales Thema: der Unterschied zwischen technischer Verfügungsgewalt über eine Blockchain-Adresse und der rechtlichen Zuordnung der Vermögenswerte — durch eine aktuelle obergerichtliche Entscheidung an praktischer Brisanz gewonnen.

11.1 Private Key als technischer, nicht rechtlicher Maßstab

Wer den privaten Schlüssel kontrolliert, kann technisch uneingeschränkt verfügen. Das ist von der Frage zu unterscheiden, wem die Werte rechtlich zuzuordnen sind. Ein Täter, der den Schlüssel einer Sammelwallet kontrolliert, in der nachweislich Gelder mehrerer Geschädigter zusammenfließen, ist nicht automatisch zivilrechtlicher Eigentümer.

11.2 Die Entscheidung des OLG Braunschweig (1 Ws 185/24)

Mit Beschluss vom 18.09.2024 (1 Ws 185/24) traf das OLG Braunschweig eine wegweisende, zugleich ambivalente Entscheidung. Ein Beschuldigter hatte im Rahmen eines Token-Projekts Zugriff auf die Seedphrase einer fremden Wallet erhalten und rund 25 Mio. Einheiten auf eigene Adressen übertragen. Das OLG bestätigte die Aufhebung eines zur Sicherung der Wertersatzeinziehung angeordneten Vermögensarrests (knapp 2,5 Mio. Euro) durch das LG Göttingen. Das Gericht verneinte Ausspähen von Daten (§ 202a StGB — Zugangsdaten waren bekannt und wurden bestimmungsgemäß verwendet), Computerbetrug (§ 263a StGB — eine Blockchain-Transaktion enthalte keine täuschungsäquivalente Erklärung) und Datenveränderung (§ 303a StGB — die Datenänderung werde durch das dezentrale Netzwerk selbst vorgenommen). Im Ergebnis blieb die faktische Aneignung durch bloße Verwendung eines bekannten Schlüssels strafrechtlich sanktionslos.

11.3–11.5 Konsequenz und zivilrechtliche Flanke

Technischer Zugriff allein begründet noch keine strafrechtlich relevante „Wegnahme" oder „Täuschung", insbesondere wenn er auf bekannten Zugangsdaten beruht und nur eine schuldrechtliche Nebenpflicht (etwa aus Treuhandabrede) verletzt. Wer sich allein auf strafrechtliche Instrumente verlässt, geht ein erhebliches Risiko ein — die zivilrechtliche Anspruchsgrundlage gewinnt Gewicht. Unabhängig von der strafrechtlichen Einordnung bleiben Herausgabe- (§ 985 BGB) und Bereicherungsansprüche (§ 812 BGB) regelmäßig eröffnet; § 985 setzt zwar traditionell eine „Sache" (§ 90 BGB) voraus — dogmatisch umstritten —, doch haben Gerichte eigentumsähnliche Herausgabe- und Vollstreckungsansprüche bereits anerkannt. Für die strafprozessuale Einziehung (§§ 73 ff. StGB) muss überhaupt eine taugliche Anknüpfungstat vorliegen; fehlt sie, entfällt die Vermögenssicherung und Geschädigte sind auf den Zivilweg verwiesen.

11.6 Praktische Konsequenz für Berichte

Forensische Berichte sollten konsequent zwischen technischer Feststellung („Adresse X kontrollierte zum Zeitpunkt Y die Verfügungsgewalt über Z Einheiten") und rechtlicher Bewertung (den beauftragenden Juristen vorbehalten) trennen — und von Beginn an so angelegt sein, dass sie sowohl eine strafprozessuale als auch, parallel und unabhängig, eine zivilrechtliche Anspruchsverfolgung nach §§ 985, 812 BGB tragen.

7 FORENSISCHE ERKENNTNIS NR. 7

Die Entscheidung des OLG Braunschweig (1 Ws 185/24) zeigt, dass technischer Zugriff auf eine Wallet strafrechtlich folgenlos bleiben kann, wenn keine tragfähige Anknüpfungstat vorliegt. Für die Praxis bedeutet dies, dass eine präzise, für Nicht-Techniker verständliche Dokumentation der Mittelflüsse nicht nur strafprozessual, sondern gerade auch zivilrechtlich — über §§ 985, 812 BGB — entscheidend für die Durchsetzbarkeit von Ansprüchen ist.

KERNAUSSAGEN

- ✓ Technischer Zugriff auf einen Private Key begründet noch kein zivilrechtliches Eigentum an den Werten.
- ✓ Das OLG Braunschweig (1 Ws 185/24) verneinte Diebstahl, Computerbetrug und Datenveränderung bei bloßer Schlüsselverwendung.
- ✓ Strafrecht ist kein Auffangbecken für jede Form digitaler Vertragsuntreue.
- ✓ §§ 985 und 812 BGB eröffnen unabhängig davon zivilrechtliche Herausgabe- und Bereicherungsansprüche.
- ✓ Eine präzise Dokumentation der Mittelflüsse ist zivilrechtlich mindestens so entscheidend wie strafprozessual.

12 Anforderungen an einen gerichtsverwertbaren Bericht

Eine technisch zutreffende Analyse wirkt nur, wenn sie so dokumentiert ist, dass sie vor Gericht, gegenüber Staatsanwaltschaften oder einer Exchange-Compliance-Abteilung Bestand hat. Mindestanforderungen:

ANFORDERUNG	INHALT
Dokumentation	Jeder Analyseschritt so dokumentiert, dass ein sachkundiger Dritter ihn ohne Rückfragen nachvollzieht — vollständige Adressen, Transaktions-Hashes, Zeitstempel, verwendete Werkzeuge (z. B. Crystal Intelligence, Maltego).
Quellenangaben	Jede Feststellung auf ihre Quelle zurückführbar (On-Chain-Beobachtung, Exchange-Auskunft, OSINT). Gesicherte Feststellungen und Vermutungen klar trennen.
Berechnungen	Summen, Kursumrechnungen zum Transaktionszeitpunkt, Bilanzverläufe nachvollziehbar und reproduzierbar hinterlegt (z. B. beigefügte Rohdatenexporte).
Nachvollziehbarkeit	Ein unabhängiger Sachverständiger muss dieselbe Analyse mit denselben Ausgangsdaten eigenständig nachvollziehen und zu denselben Ergebnissen gelangen können.
Screenshots & Hashes	Screenshots von Explorern/Plattformen sichern den Datenstand (Labels ändern sich); Transaktions-Hashes stets im Volltext.
Chain of Custody	Lückenlose Dokumentation, wer wann auf welche Daten zugriff und welche Schritte durchführte — Versionskontrolle, Tool-Versionen, Integritätsnachweise.

KERNAUSSAGEN

- ✓ Ein gerichtsverwertbarer Bericht dokumentiert jeden Schritt so, dass ein sachkundiger Dritter ihn ohne Rückfragen nachvollzieht.
- ✓ Jede Feststellung muss auf ihre Quelle zurückführbar sein — On-Chain, Exchange-Auskunft oder OSINT.
- ✓ Berechnungen und Bilanzverläufe müssen reproduzierbar hinterlegt sein, etwa durch Rohdatenexporte.
- ✓ Screenshots und vollständige Transaktions-Hashes sichern den Datenstand zum Untersuchungszeitpunkt.
- ✓ Eine lückenlose Chain of Custody ist Voraussetzung für die gerichtliche Verwertbarkeit.

13 Was Ermittlungsbehörden benötigen

13.1 Wie sollte ein Bericht aufgebaut sein?

- Knappe Zusammenfassung der Kernfeststellungen auf der ersten Seite (Executive Summary)
- Klare chronologische Darstellung des Geldflusses, idealerweise visuell unterstützt
- Getrennte Darstellung von gesicherten Fakten und forensischen Einschätzungen
- Konkrete, umsetzbare Handlungsempfehlungen (z. B. konkrete Exchange samt Kontaktweg für ein Auskunftsersuchen)
- Vollständige Anhänge mit Rohdaten, Adresslisten und Belegen

13.2 & 13.3 Was wirklich hilft — und was nicht

Den Ermittlungsfortschritt beschleunigen vor allem: die konkrete, namentlich benannte Cash-Out-Exchange samt Einzahlungsadresse, ein belastbarer zeitlicher Zusammenhang zwischen Zufluss und Abfluss sowie Hinweise auf weitere, bislang nicht gemeldete Opferfälle derselben Infrastruktur. Wenig hilfreich sind dagegen unstrukturierte Rohdatenexporte ohne Kontext, pauschale Risikoeinstufungen ohne Begründung und Spekulationen über Täteridentitäten ohne belastbare Indizien. Behörden profitieren von präziser, priorisierter Information — nicht von Datenmenge allein.

KERNAUSSAGEN

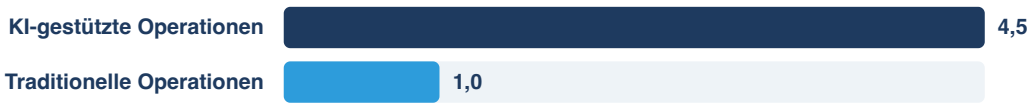
- ✓ Ein guter Bericht beginnt mit einer knappen Executive Summary der Kernfeststellungen.
- ✓ Gesicherte Fakten und forensische Einschätzungen gehören sauber getrennt dargestellt.
- ✓ Am hilfreichsten sind konkrete Cash-Out-Exchange, Einzahlungsadresse und Zeitkorrelation.
- ✓ Weitere, bislang unbekannte Opferfälle derselben Infrastruktur beschleunigen Ermittlungen zusätzlich.
- ✓ Unstrukturierte Datenmengen ohne Kontext oder unbegründete Spekulationen helfen Behörden kaum.

14 Die Zukunft der Kryptoforensik

Künstliche Intelligenz wird die Kryptoforensik nicht nur unterstützen, sondern grundlegend verändern — und die Entwicklung ist doppelgesichtig: Sie beschleunigt Ermittlungen erheblich und zugleich die Professionalisierung der Täterseite.

- Automatisierte Cluster-Erkennung über Millionen Adressen, in manuell nicht mehr leistbarem Umfang
- Automatisierte Bilanzanalyse (Kapitel 6), die Auffälligkeiten in Zu-/Abflussmustern in Echtzeit markiert
- Erkennung identischer Täterstrukturen über oberflächlich unabhängige Fälle hinweg
- Erkennung gleicher Cash-Out-Muster, selbst bei zuvor nie verbundenen Adressen
- Automatisierte Priorisierung von Ermittlungsansätzen nach Erfolgswahrscheinlichkeit und Schadenshöhe

Wie real die Verschiebung ist, zeigt die Täterseite: Nach Chainalysis-Daten erzielten KI-gestützte Betrugsoperationen 2025 im Schnitt ein 4,5-faches Umsatzvolumen gegenüber traditionellen Fällen — u. a. durch Deepfake-Videos vermeintlicher Führungskräfte, Behördenvertreter und Influencer sowie Phishing-as-a-Service. Wenn Täter KI zur Skalierung nutzen, ist KI auf Ermittlerseite kein optionales Zusatzwerkzeug mehr, sondern notwendige Voraussetzung.



Umsatzvolumen KI-gestützter vs. traditioneller Betrugsoperationen (2025). *KI-gestützte Operationen erzielten im Schnitt das 4,5-Fache (Chainalysis, 2026 Crypto Crime Report — Scams).*

Da Täterinfrastrukturen grenzüberschreitend operieren, hängt der Erfolg zunehmend von internationaler Kooperation ab (Europol, Interpol, Rechtshilfe). Die größte Wirkung entsteht, wo Finanzermittlungen, Sanktionsrecht und Strafverfolgung ineinandergreifen (Huione-Zerschlagung, Prince-Group-Sanktionen). MiCA und die Travel Rule (TFR) schaffen seit Ende 2024 einen einheitlichen, auskunftspflichtigen EU-Rahmen und dürften die Rückverfolgbarkeit von Cash-Outs zwischen regulierten Anbietern erheblich erleichtern; die Behandlung von Self-Hosted-Wallets bleibt in Überprüfung. Zu erwarten ist eine zunehmende Verschränkung von OSINT und On-Chain-Analyse sowie eine wachsende Rolle privater Forensik-Dienstleister als Bindeglied zwischen Geschädigten, Exchanges und Behörden.

8 FORENSISCHE ERKENNTNIS NR. 8

Künstliche Intelligenz ist keine Zukunftsvision mehr, sondern bereits heute fester Bestandteil sowohl der Täter- als auch der Ermittlerseite. Wer als Dienstleister, Kanzlei oder Behörde nicht in KI-gestützte Analysewerkzeuge investiert, wird mittelfristig gegenüber zunehmend KI-gestützten Täterstrukturen strukturell im Nachteil sein.

KERNAUSSAGEN

- ✓ Künstliche Intelligenz verändert die Kryptoforensik grundlegend, nicht nur unterstützend.
- ✓ KI-gestützte Betrugsoperationen erzielten 2025 ein 4,5-faches Umsatzvolumen gegenüber traditionellen Methoden.
- ✓ Automatisierte Cluster- und Bilanzanalyse verschieben Analystenzeit von der Auffindung zur Verifikation.
- ✓ MiCA und die Travel Rule (TFR) schaffen seit Ende 2024 einen einheitlichen, auskunftspflichtigen EU-Rahmen.
- ✓ Wer nicht in KI-gestützte Analyse investiert, gerät gegenüber KI-gestützten Täterstrukturen ins Hintertreffen.

§ Glossar

AML
Anti-Money-Laundering — regulatorische Vorgaben zur Geldwäschebekämpfung.

Adresse
Öffentlich sichtbarer Identifikator auf einer Blockchain, dem Werte zugeordnet werden.

Asset Recovery
Rechtliche und forensische Bemühungen zur Rückführung entzogener Vermögenswerte.

Auskunftsersuchen
Formale Anfrage an eine Exchange oder Behörde zur Herausgabe von Kontodaten.

Bereicherungsanspruch
Anspruch aus § 812 BGB auf Rückabwicklung einer rechtsgrundlosen Vermögensverschiebung.

Bilanzanalyse
Analyse der Zu- und Abflüsse einer Wallet über die Zeit (Kapitel 6).

Blockchain-Analyse
Systematische Untersuchung von Transaktionsdaten zur Aufklärung von Geldflüssen.

Bridge
Technischer Mechanismus zum Transfer von Werten zwischen Blockchains.

CASP
Crypto-Asset Service Provider — nach MiCA lizenzierter Kryptowertedienstleister.

Cash-Out
Umwandlung von Kryptowerten in Fiat oder andere verwertbare Vermögenswerte.

CEX
Centralized Exchange — zentralisierte, regulierte Handelsplattform.

Chain of Custody
Lückenlose Dokumentation des Umgangs mit Beweismitteln.

Clustering
Zuordnung mehrerer Adressen zu einem gemeinsamen wirtschaftlichen Akteur.

Computerbetrug
§ 263a StGB; bei bloßer Blockchain-Transaktion nach OLG Braunschweig regelmäßig nicht einschlägig.

Cross-Chain-Transfer
Übertragung von Werten zwischen unterschiedlichen Blockchain-Netzwerken.

DEX
Decentralized Exchange — dezentrale Handelsplattform ohne zentrale Verwahrstelle.

EBA
European Banking Authority — u. a. zuständig für die Travel Rule Guidelines.

Einziehung
Strafprozessuale Vermögensabschöpfung nach §§ 73 ff. StGB.

Empfangswallet
Erste On-Chain-Adresse, die Gelder von einer Exchange empfängt.

FATF
Financial Action Task Force — Urheberin der „Travel Rule" (Empfehlung 16).

Freeze
Vorübergehendes Einfrieren eines Kontos/Guthabens durch Exchange oder Behörde.

Gas Fee
Transaktionsgebühr für die Verarbeitung einer Blockchain-Transaktion.

Hash
Eindeutiger kryptografischer Fingerabdruck, u. a. zur Identifikation einer Transaktion.

Herausgabeanspruch
Anspruch aus § 985 BGB auf Rückgabe einer Sache bzw. eines eigentumsähnlichen Werts.

Impersonation-Betrug
Betrug, bei dem sich Täter als Behörden, Unternehmen oder bekannte Personen ausgeben.

KYC
Know Your Customer — Identitätsprüfung von Kunden durch regulierte Anbieter.

Layering
Mehrstufige Weiterleitung von Geldern zur Verschleierung der Herkunft.

Mixer
Dienst zur Vermischung von Kryptowerten mehrerer Nutzer zur Verschleierung.

MiCA
Markets in Crypto-Assets — VO (EU) 2023/1114 zur Regulierung von Kryptowerten/-diensten.

OSINT
Open Source Intelligence — Recherche auf Basis öffentlich zugänglicher Quellen.

OTC-Broker
Anbieter für den außerbörslichen Handel großer Kryptowert-Mengen.

Pay-to-Withdraw
Recovery-Scam-Variante mit wiederholten Gebühren vor angeblicher Auszahlung.

Peeling
Layering-Technik: wiederholtes Abspalten kleiner Beträge von einer größeren Summe.

Pig Butchering
Betrug, bei dem Opfer über längere Zeit emotional und finanziell manipuliert werden.

Private Key
Geheimer kryptografischer Schlüssel zur Verfügung über eine Wallet.

Pseudonymität
Adressen sind öffentlich, aber nicht direkt einer Identität zugeordnet.

Recovery-Scam
Zweiter Betrug an bereits Geschädigten unter dem Vorwand der Rückholung (Kapitel 8).

Risk Score
Automatisierte Risikoeinstufung einer Adresse anhand ihrer Historie.

Romance Scam
Betrug über eine vorgetäuschte romantische Beziehung.

Sammelwallet
Adresse, in der Gelder aus mehreren Quellen konsolidiert werden.

Self-Hosted Address
Private Wallet-Adresse, nicht bei einem regulierten Dienstleister verwahrt.

Splitting
Aufteilung eines Betrags in mehrere gleich große Teilbeträge zur Verschleierung.

Stablecoin
Kryptowert mit an eine Referenzwährung (meist USD) gekoppeltem Wert.

Täterökonomie
Kosten-Nutzen-Logik hinter Aufbau und Wiederverwendung von Täterinfrastruktur (Kapitel 4).

Transaktions-Hash
Eindeutiger Identifikator einer einzelnen Blockchain-Transaktion.

Travel Rule
Pflicht (FATF-Empf. 16, EU: VO 2023/1113) zur Übermittlung von Auftraggeber-/Empfängerdaten.

TFR
Transfer of Funds Regulation — VO (EU) 2023/1113, EU-Umsetzung der Travel Rule.

UTXO
Unspent Transaction Output — Guthabenmodell u. a. bei Bitcoin.

Vermögensarrest
Vorläufige Sicherung von Vermögenswerten nach §§ 111e ff. StPO.

Wallet Clustering
Zuordnung mehrerer Adressen zu einem gemeinsamen Akteur (Kapitel 5).

Zeitkorrelation
Analysemethode, die zeitlich eng beieinanderliegende Transaktionen in Zusammenhang setzt.

Zwischenwallet
Adresse, die im Layering Gelder nur vorübergehend hält.

QUELLEN

ANALYSE & DATEN
Chainalysis, 2026 Crypto Crime Report — Scams (2026) · Crystal Intelligence (Blockchain-Analyse) · Maltego (OSINT/Link-Analyse) · Europol (Berichte org. Kriminalität) · BKA, Bundeslagebild Cybercrime 2025 · BSI.

REGULIERUNG
VO (EU) 2023/1114 (MiCA) · VO (EU) 2023/1113 (TFR) · EBA/GL/2024/11 (Travel Rule Guidelines) · FATF-Empfehlung 16.

RECHT
OLG Braunschweig, Beschluss v. 18.09.2024 — 1 Ws 185/24 · §§ 202a, 263a, 303a, 73 ff. StGB · §§ 111e ff. StPO · §§ 90, 812, 985 BGB.

Neben der praktischen Ermittlungserfahrung der Finanz Forensik GmbH. Stand: 2026.

UNSERE LEISTUNGEN

Die Finanz Forensik GmbH ist auf Krypto-Forensik, Blockchain-Analyse, OSINT-Ermittlungen und Asset Recovery spezialisiert — für Geschädigte, Kanzleien, Wirtschaftsprüfer und Ermittlungsbehörden.

LEISTUNG	WAS SIE ERHALTEN
Blockchain-Analyse & Tracing	Rückverfolgung von Geldflüssen über Layering, Cross-Chain und Sammelwallets bis zur tatsächlichen Cash-Out-Stelle.
Wallet Clustering	Zuordnung mehrerer Adressen und Opferfälle zu einer gemeinsamen Täterinfrastruktur über Bilanzanalyse, Zeitkorrelation und Konsolidierungen.
Bilanzanalyse	Nachvollziehbare Zu-/Abfluss- und Höchststandsanalyse einzelner Wallets als Grundlage für Auskunftsersuchen und Vermögensarrest.
OSINT-Ermittlung	Verknüpfung von On-Chain-Strukturen mit öffentlich zugänglichen Off-Chain-Spuren der Täter.
Gerichtsverwertbarer Bericht	Dokumentation mit vollständigen Hashes, Quellenangaben, reproduzierbaren Berechnungen und lückenloser Chain of Custody.
Asset Recovery & Behördenzuarbeit	Aufbereitung für Freeze-Anfragen, Auskunftsersuchen, Vermögensarrest (§§ 111e ff. StPO) und zivilrechtliche Ansprüche (§§ 985, 812 BGB).

ÜBER DEN AUTOR

David Lüdtke

Geschäftsführer · OSINT-Analyst & Krypto-Forensiker · Finanz Forensik GmbH

Gerichtsfeste Kryptotransaktionsanalysen, OSINT-gestützte Vermögensermittlung und gutachterliche Aufbereitung für Strafverteidiger, Insolvenzverwalter und Unternehmen. Zertifiziert als Crystal Expert (CECF · CEEI · CEUI). **Kontakt:** postfach@finanz-forensik.de · www.finanz-forensik.de

Herausgeber: Finanz Forensik GmbH · Krypto-Forensik · Blockchain-Analyse · OSINT-Ermittlungen · Asset Recovery · www.finanz-forensik.de · Ansprechpartner: David Lüdtke, postfach@finanz-forensik.de. Dieses Whitepaper dient der allgemeinen Information und gibt den Diskussions-, Rechts- und Datenstand 2026 wieder; es stellt keine Rechtsberatung dar. Fallbeispiele sind anonymisiert oder illustrativ.