

WHITEPAPER FÜR KANZLEIEN

Blockchain-Forensik in Gerichtsverfahren

Was Kanzleien über die technische Aufklärung von Krypto-Betrug wissen müssen — und wo die belegbaren Grenzen liegen.

Warum dieses Whitepaper

Kryptobetrug landet zunehmend auf den Schreibtischen von Kanzleien im Kapitalmarkt-, Bank- und Wirtschaftsstrafrecht. Mandantinnen und Mandanten haben Geld über vermeintliche Trading-Plattformen, Love-Scams oder „Cybertrading“ verloren — und die zentrale Frage lautet fast immer:

Wohin ist das Geld geflossen, und lässt sich das beweisen?

Die juristische Bewertung beherrschen Sie. Die **technische Rekonstruktion des Geldflusses** auf der Blockchain ist jedoch ein eigenes Handwerk — mit eigenen Werkzeugen, Methoden und Grenzen.

Dieses Whitepaper gibt Ihnen einen kompakten, ehrlichen Überblick: Was ist forensisch belegbar, wie sieht eine gerichtsverwertbare Dokumentation aus, und wann lohnt sich eine Analyse?

Wir schreiben bewusst nüchtern. BlockDetektiv verspricht keine Wiederbeschaffung und ist kein Rechtsdienstleister. Wir sind ein **neutraler forensischer Zulieferer** — die rechtliche Würdigung bleibt bei Ihnen.

INHALT

1. Warum Krypto-Spuren überprüfbar sind
2. Was forensisch belegbar ist — und was nicht
3. Wie eine gerichtsverwertbare Dokumentation aussieht
4. Typische Fallmuster und wo Forensik ansetzt
5. Zusammenarbeit Kanzlei ↔ Forensik
6. Checkliste: Wann lohnt sich eine forensische Analyse?

Warum Krypto-Spuren überprüfbar sind

Öffentliche Blockchains wie Bitcoin oder Ethereum sind ein **dauerhaftes, öffentlich einsehbares Kassenbuch**. Jede Transaktion — Betrag, Zeitpunkt, sendende und empfangende Adresse — ist unveränderlich gespeichert und für jeden nachprüfbar. Anders als bei einer klassischen Überweisung, die in den Systemen einzelner Banken verschwindet, bleibt der Krypto-Zahlungsweg technisch *rekonstruierbar*.

Betrüger nutzen zwar Pseudonymität: Eine Wallet-Adresse trägt keinen Klarnamen. Doch aus dem Verhalten der Adressen lassen sich Muster ableiten:

- **Clustering:** Mehrere Adressen, die technisch zusammengehören (z. B. gemeinsam als Eingänge einer Transaktion), werden einer Einheit zugeordnet.
- **Attribution:** Viele Adressen lassen sich bekannten Anlaufstellen zuordnen — vor allem **Krypto-Börsen**, die einer KYC-Pflicht unterliegen und damit für Behörden greifbar sind.
- **Geldfluss-Verfolgung (Tracing):** Der Weg der Gelder wird Schritt für Schritt („Hop“ für „Hop“) nachvollzogen, bis zu einer identifizierbaren Stelle.

Kernaussage

Auch wenn Gelder über viele Wallets, Bündelungen und sogar Mixer verschoben werden — auf der Blockchain bleibt in aller Regel eine **überprüfbare Spur**, der man methodisch folgen kann.

Was forensisch belegbar ist — und was nicht

Ehrlichkeit ist hier entscheidend, gerade vor Gericht. Eine seriöse Forensik benennt ihre Grenzen offen.

Belegbar

- Der **Geldfluss** von der Einzahlungs-Wallet über Zwischenstationen bis zu einer Anlaufstelle (häufig eine Börse).
- **Beträge, Zeitpunkte und Verknüpfungen** zwischen Adressen — objektiv aus der Blockchain ablesbar.
- **Zusammengehörigkeit** von Adressen über Clustering und wiederkehrende Muster.
- Die **Anlaufstelle**, an der Behörden über ein Auskunftersuchen ansetzen können.

Nicht (sicher) belegbar

- Der **Klarname** hinter einer Adresse — den liefern erst Dritte (z. B. eine Börse auf behördliches Ersuchen).
- Vollständige Rückverfolgung, wenn **Mixing-Dienste** oder Off-Chain-Vorgänge die Spur verschleiern (erschwert, nicht immer unmöglich).
- Eine **Garantie auf Wiederbeschaffung** — Forensik dokumentiert, sie holt kein Geld zurück.

Merksatz: Forensik zeigt, *was die Daten hergeben* — und sagt ehrlich, wo die Aussagekraft endet. Genau diese Transparenz macht eine Analyse vor Gericht belastbar.

Wie eine gerichtsverwertbare Dokumentation aussieht

Für die Verwertbarkeit zählt nicht das Ergebnis allein, sondern die **Nachvollziehbarkeit des Weges**. Eine belastbare forensische Dokumentation ist:

- **Methodentransparent:** Jeder Analyseschritt wird offengelegt — welche Adresse, welche Transaktion, welches Werkzeug, welche Annahme.
- **Quellen- und zeitgestützt:** Jede Aussage ist mit Transaktions-ID, Zeitstempel und überprüfbarer Quelle belegt und von Dritten reproduzierbar.
- **Lückenlos:** Der Geldfluss wird ohne unerklärte Sprünge dargestellt; Bündelungen und Weiterleitungen sind eingeordnet.
- **Trennscharf:** Fakten (aus der Blockchain) und Bewertung (Einordnung) sind klar getrennt.
- **Verständlich:** Aufbereitet so, dass Gericht und Anwaltschaft den technischen Sachverhalt nachvollziehen können — ohne Blockchain-Vorwissen.

Das Ergebnis ist ein Bericht, der als **gutachterliche Grundlage** in zivil- und strafrechtlichen Verfahren dienen kann. Die rechtliche Würdigung und Verwertung obliegt Gericht und Anwaltschaft.

Faustregel: **Was nicht nachvollziehbar dokumentiert ist, ist vor Gericht angreifbar.** Deshalb steht bei uns die Methodik über dem spektakulären Ergebnis.

Typische Fallmuster — und wo Forensik ansetzt

Fake-Broker / Cybertrading

Eine professionell wirkende „Trading-Plattform“ zeigt steigende Gewinne; bei der Auszahlung wird plötzlich eine „Steuer“ oder „Gebühr“ vorab verlangt, danach bricht der Kontakt ab. **Ansatz:** Einzahlungs-Transaktionen sichern, Geldfluss über die Hops verfolgen, Anlaufstelle dokumentieren.

Love-Scam / Pig Butchering

Über Wochen aufgebautes Vertrauen führt zu schrittweisen Einzahlungen in eine „exklusive“ App. **Ansatz:** Empfänger-Wallets clustern, wiederkehrende Bündelungsmuster erkennen, Gesamtbild rekonstruieren.

Recovery-Scam (der „zweite Betrug“)

Nach dem Verlust melden sich angebliche „Rückhol-Dienste“ gegen Vorkasse — und schädigen ein zweites Mal. **Ansatz:** Aufklärung, Beweissicherung, keine Vorschuss-Logik; genau hier ist ein neutraler Zulieferer Gold wert.

Fake-Support / Bitcoin-Automat

Angebliche Bank/Behörde drängt zu Zahlungen per Krypto-Automat oder Fernzugriff. **Ansatz:** Zahlungsadresse und Fluss sichern, Anlaufstelle für die Anzeige aufbereiten.

Zusammenarbeit Kanzlei ↔ Forensik

Wir arbeiten als **fester Zulieferer, mandatsbezogen oder für eine methodische Zweitmeinung** zu bestehenden Analysen. Der typische Ablauf:

1. **Kurzes Erstgespräch:** Wir klären unverbindlich, ob eine Analyse im konkreten Fall sinnvoll ist — und sagen auch ehrlich, wenn nicht.
2. **Beweissicherung:** Ihre Mandantschaft stellt Chatverläufe, Wallet-Adressen, Transaktions-IDs, Zahlungsbelege bereit.
3. **Forensische Analyse:** Geldfluss-Verfolgung, Clustering, Attribution — lückenlos dokumentiert.
4. **Übergabe:** Gerichtsverwertbarer Bericht als Grundlage für Ihre rechtlichen Schritte, inkl. Bereitschaft für Rückfragen.

Datenschutz & Vertraulichkeit

Alle Angaben werden DSGVO-konform, vertraulich, verschlüsselt und ausschließlich zweckgebunden verarbeitet. Wir sind kein Rechtsdienstleister im Sinne des RDG und geben keine Rückhol-Versprechen — dadurch entsteht **kein Interessenkonflikt** mit Ihrem Mandat.

Ihr Vorteil: Sie liefern die Rechtsseite, wir die belegbare technische Grundlage. Ein kleiner erster Testfall genügt, um die Zusammenarbeit zu prüfen.

Checkliste: Wann lohnt sich eine forensische Analyse?

- Es gibt **konkrete Krypto-Transaktionen** (Wallet-Adressen und/oder Transaktions-IDs liegen vor).
- Die Spuren sind **noch relativ aktuell** — je früher, desto belastbarer.
- Die Schadenshöhe rechtfertigt den Aufwand (oder mehrere Geschädigte bündeln sich).
- Ziel ist eine **Anzeige, ein Auskunftersuchen oder ein Zivilverfahren** — die Dokumentation soll als Grundlage dienen.
- Es besteht Bedarf an einer **neutralen, methodentransparenten Einordnung** (auch als Zweitmeinung).

Treffen mehrere Punkte zu, ist ein kurzes Erstgespräch der richtige nächste Schritt.

Über BlockDetektiv

BlockDetektiv ist auf forensische Krypto-Ermittlung und gerichtsverwertbare Beweissicherung spezialisiert — als neutraler Zulieferer für Kanzleien, Rechtsanwälte und Behörden. Ehrliche Positionierung: kein Rückhol-Versprechen, methodentransparente Dokumentation, offene Benennung der Grenzen.

Kontakt: blockdetektiv.de/fuer-kanzleien · kostenloses, unverbindliches Erstgespräch

Dieses Whitepaper dient der allgemeinen Information und stellt keine Rechtsberatung dar. BlockDetektiv ist kein Rechtsdienstleister im Sinne des RDG. © BlockDetektiv 2026.