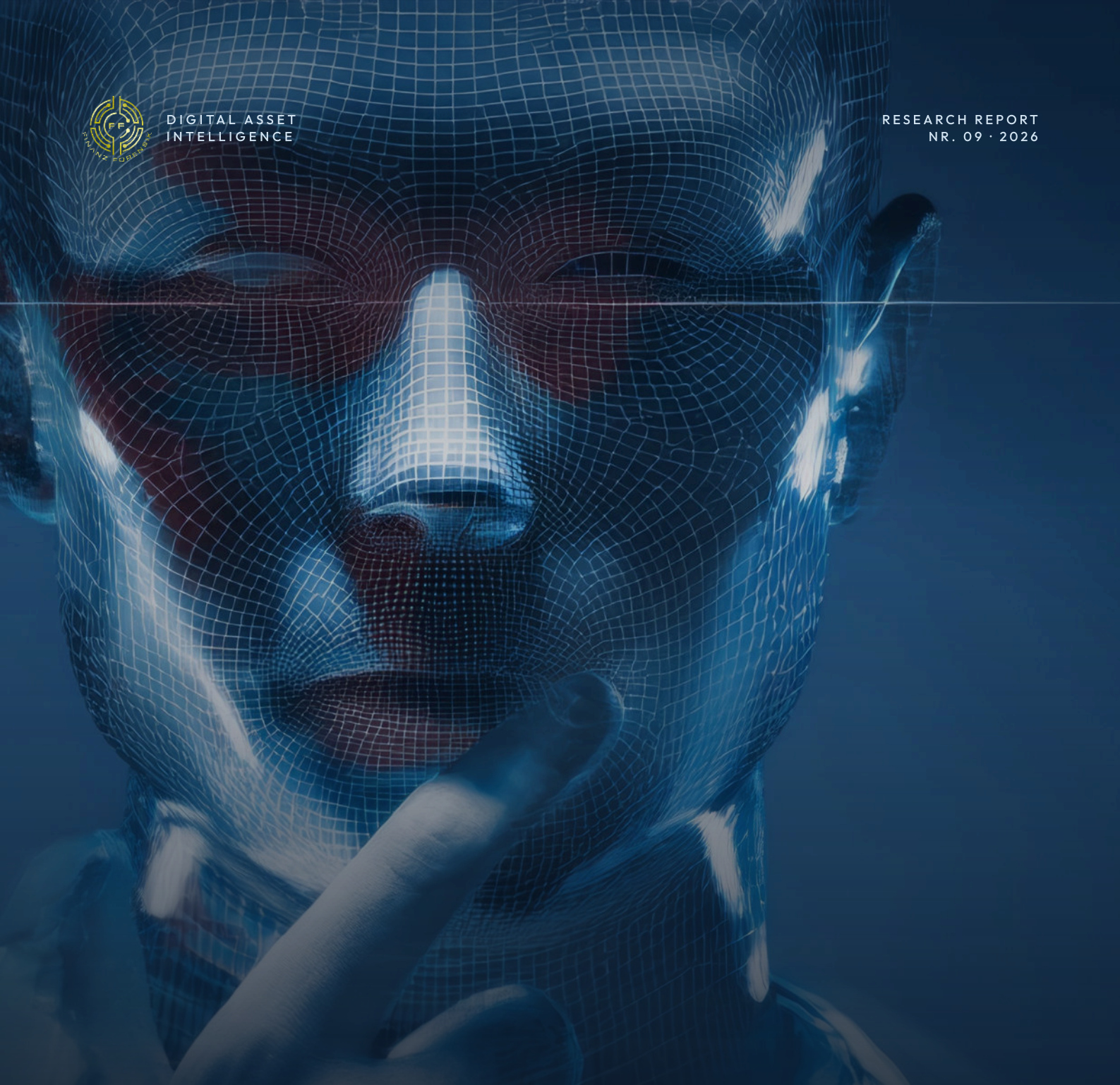


DIGITAL ASSET
INTELLIGENCE

RESEARCH REPORT
NR. 09 · 2026

TECHNOLOGIE · BLOCKCHAIN-FORENSIK

KI-gestützte Cybertrading-Betrugsnetzwerke

Wie autonome KI-Agenten den Anlagebetrug verändern werden — forensische Erkenntnisse, die Mathematik autonomer Geldwäsche und warum Blockchain-Forensik an Bedeutung gewinnt. 3. Auflage.

16 KAPITEL · 4 TEILE · 3 ANHÄNGE

FINANZ FORENSIK GMBH · FINANCIAL INTELLIGENCE

MANAGEMENT SUMMARY

Automatisierter Betrug hinterlässt mehr forensische Spuren — nicht weniger

Anlagebetrug war lange Handarbeit. Diese Grenze fällt gerade weg: Autonome KI-Agenten übernehmen Kontaktaufnahme, Vertrauensaufbau und den Betrieb gefälschter Plattformen. Doch die Auszahlungsmuster dahinter bleiben mathematisch nahezu erzwungen — und dadurch besser erkennbar.

17 Mrd. $
Krypto-Betrug & -Scams weltweit 2025 (Chainalysis)

4,5×
höherer Ertrag pro Fall bei KI-gestützten Scams (Chainalysis)

+1.400 %
Zuwachs bei Impersonation-Betrug im Jahresvergleich (Chainalysis)

11 %
aller Betrugsfälle beinhalten mittlerweile Deepfakes (Sumsub)

21 Mrd. $
Gesamtschaden Internetkriminalität USA 2025, +26 % (FBI IC3)

8,2 Mrd. $
jährliche Geldwäsche über verschachtelte VASP-Beziehungen (FATF)

Anlagebetrug war lange Zeit Handarbeit: Ein Täter, ein Skript, eine begrenzte Zahl an Opfern, die parallel „bearbeitet" werden konnten. Diese Grenze fällt gerade weg. Kriminelle Organisationen setzen zunehmend autonome KI-Agenten ein, die Kontaktaufnahme, Vertrauensaufbau, Beratungsgespräche und selbst den technischen Betrieb gefälschter Handelsplattformen eigenständig übernehmen.

Dieses Whitepaper verbindet zwei Arten von Erkenntnissen, die bewusst getrennt gehalten werden: Erstens extern erhobene, veröffentlichte Statistiken von Chainalysis, dem FBI, Sumsub und weiteren Institutionen (Kapitel 3) – diese sind wie gekennzeichnet Zahlen Dritter. Zweitens qualitative Beobachtungen aus der laufenden forensischen Fallarbeit von finanz-forensik.de (insbesondere Kapitel 6 bis 8) – hierbei handelt es sich ausdrücklich nicht um eine eigene Statistik oder repräsentative Stichprobe, sondern um wiederkehrende Muster, wie sie auch Lagebilder von Europol oder nationalen Sicherheitsbehörden auf Basis strukturierter Experteneinschätzung veröffentlichen.

Der eigentliche Beitrag dieses Whitepapers liegt weniger in weiteren Zahlen als in der Erklärung: Warum bleiben bestimmte Verschleierungsmuster trotz KI bestehen? Welchen mathematischen Zwängen unterliegt automatisierte Geldwäsche zwangsläufig? Und warum ist plausibel, dass Blockchain-Forensik durch die Automatisierung von Betrug nicht an Bedeutung verliert, sondern gewinnt? Diesen Fragen widmet sich Teil II dieses Dokuments.

METHODISCHER HINWEIS

Die in den Kapiteln 6 bis 9 dargestellten forensischen Beobachtungen und Modelle beruhen auf wiederkehrenden Mustern aus der Fallarbeit von finanz-forensik.de. Es handelt sich ausdrücklich nicht um eine statistische Hochrechnung, Prozentangabe oder repräsentative Stichprobe, sondern um qualitative, wiederholt beobachtete Regelmäßigkeiten – vergleichbar der Methodik von Lageberichten wie Europols Internet Organised Crime Threat Assessment (IOCTA), das ebenfalls auf strukturierten Experteneinschätzungen statt auf einem vollständig quantifizierten Datensatz beruht. Ausführliche Erläuterungen zur Methodik finden sich in Anhang C.

TEIL I

Lagebild

01 Einleitung: Vom Einzeltäter zum autonomen Betrugssystem

„Sha Zhu Pan“ – wörtlich „das Schwein schlachten“ – bezeichnet seit Jahren die Betrugsmasche, bei der Opfer über Wochen oder Monate hinweg emotional „gemästet“ werden, bevor ihnen scheinbar lukrative Investments in Kryptowährungen oder andere Anlageprodukte schmackhaft gemacht werden. Bislang erforderte dieses Modell viel menschliche Arbeitskraft: In Betrugsfabriken in Südostasien – oft betrieben mit Opfern von Menschenhandel als Zwangsarbeitskräften – verwalteten einzelne Täter jeweils nur eine begrenzte Zahl paralleler Kontakte.

Diese Beschränkung entfällt mit dem Einsatz generativer KI und autonomer KI-Agenten. Europol beschreibt, wie große Sprachmodelle wie ChatGPT es Betrügern ermöglichen, Nachrichten „schneller, deutlich authentischer und in erheblich größerem Maßstab“ zu verfassen. Der nächste Schritt ist bereits Realität: vollautomatisierte Agenten, die Konten anlegen, Beziehungen aufbauen, beraten, überzeugen und Gelder abschöpfen – ganz ohne menschlichen Bediener im Hintergrund.

„Kein menschlicher Betrüger verwaltet mehr einzelne Beziehungen – nur noch KI-Agenten, die rund um die Uhr, in mehreren Sprachen, Dutzende überzeugende ‚Experten‘-Identitäten parallel aufrechterhalten.“

SINNGEMÄSS NACH AKTUELLEN BRANCHENANALYSEN ZU AGENTISCHEM KI-BETRUG, 2026

---

02 Was passiert bereits heute?

Ein verbreitetes Missverständnis lautet: KI-gestützter Anlagebetrug sei ein Zukunftsszenario. Tatsächlich sind sämtliche in diesem Whitepaper beschriebenen Bausteine bereits im Einsatz:

- **Deepfake-Betrug:** Der Fall des Ingenieurbüros Arup (siehe Kapitel 4.5) zeigt bereits 2024 einen Schaden von 25 Millionen US-Dollar durch eine einzige Deepfake-Videokonferenz. Gefälschte „Quantum-AI“-Handelsplattformen mit Deepfakes bekannter Persönlichkeiten kosteten einen Betroffenen in Ontario rund 1,7 Millionen US-Dollar; im Juni 2026 warnte die südafrikanische Finanzaufsicht FSCA vor einem Deepfake-Betrug, der zwei bekannte Finanzjournalisten imitierte.
- **Autonome KI-Agenten:** Laut Sumsub tauchten bereits 2025 erste dokumentierte „AI fraud agents“ auf – autonome Systeme, die aus gescheiterten Versuchen lernen und ihre Taktik in Echtzeit an aktuelle Betrugspräventionsmaßnahmen anpassen.
- **Automatisierte Callcenter:** Threat-Intelligence-Analysen von Group-IB beschreiben KI-gestützte Scam-Callcenter, die synthetische Stimmen mit Sprachmodell-Coaching kombinieren, um Gesprächsverläufe in Echtzeit zu steuern.
- **Synthetische Identitäten im großen Stil:** Im Rahmen von „Project Déjà Vu“ deckte die Polizei in Toronto auf, dass eine einzelne Person mithilfe synthetischer Identitäten hunderte Konten bei Banken

und Finanzinstituten in Ontario eröffnet hatte – mit einem bestätigten Schaden von rund 2,9 Millionen US-Dollar.

- **Fraud-as-a-Service-Marktplätze:** Dark-LLM-Abonnements wie FraudGPT werden bereits heute kommerziell gehandelt – ein direkter Beleg dafür, dass die Bausteine für vollautomatisierten Betrug schon jetzt für wenig Geld verfügbar sind, nicht erst im Jahr 2030.

Auch das ungewöhnlich hohe Tempo internationaler Strafverfolgung 2026 – mehr Maßnahmen gegen Pig-Butchering-Netzwerke in vier Monaten als im gesamten vorangegangenen Jahrzehnt – ist selbst ein Indiz dafür, dass Behörden das Problem längst als akut und nicht als zukünftig einstufen.

03 Die Bedrohungslage im Überblick (externe Studien)

Die folgenden Kennzahlen stammen ausschließlich aus veröffentlichten Studien Dritter (Chainalysis, FBI IC3, Sumsub) und sind entsprechend gekennzeichnet. Sie sind naturgemäß mit den üblichen Einschränkungen solcher Erhebungen verbunden, insbesondere hoher Dunkelziffer bei nicht angezeigten Fällen:

17 Mrd. USD
durch Krypto-Betrug & -Scams erbeutet, weltweit 2025 (Chainalysis)

21 Mrd. USD
Gesamtschaden Internetkriminalität in den USA 2025, +26 % ggü. Vorjahr (FBI IC3)

4,5×
höherer Ertrag pro Fall bei KI-gestützten Scams ggü. klassischen Maschen (Chainalysis)

1.400 %
Zuwachs bei Impersonation-Betrug im Jahresvergleich (Chainalysis)

11 %
aller weltweiten Betrugsfälle beinhalten mittlerweile Deepfakes (Sumsub)

8,2 Mrd. USD
jährliche Geldwäscheflüsse über verschachtelte VASP-Beziehungen (FATF-Typologien 2026)

Auch in Deutschland und der EU ist die Entwicklung spürbar: BaFin und BKA warnten in den ersten Monaten des Jahres 2026 in mehr als 150 Einzelmeldungen vor unseriösen Krypto-Anbietern. Regional zeigt sich zudem ein Süd-Nord- bzw. West-Ost-Gefälle.

04 Anatomie eines KI-gestützten Betrugsnetzwerks

Was früher ein Callcenter mit geschultem Personal leistete, übernehmen zunehmend spezialisierte KI-Fähigkeiten, die sich zu einer durchgängigen technischen Pipeline zusammensetzen lassen. Die folgende, illustrative Architektur beschreibt, wie Betrug künftig tatsächlich organisiert sein könnte – nicht als Prognose einzelner Softwareprodukte, sondern als Modell der Funktionsaufteilung:

4.1 Grooming im industriellen Maßstab (Agent A/B)

KI-Agenten übernehmen die Kontaktaufnahme auf Dating-Plattformen, in sozialen Netzwerken oder Messenger-Diensten und pflegen dort parallel Dutzende bis Hunderte tiefgehende, individuell zugeschnittene „Beziehungen“. Besonders betroffen sind laut Sumsub die Bereiche Dating und Online-Medien, die mit einer Betrugsrate von 6,3 % mehr als doppelt so stark betroffen sind wie der Finanzsektor.

4.2 Die synthetische Brokerage (Agent C)

Der zweite Baustein ist die Fälschung ganzer Handelsplattformen. Täterorganisationen setzen mittlerweile komplette, KI-generierte Broker-Web- und -App-Erlebnisse auf – inklusive KYC-Onboarding, gebrandetem Kunden-Chat und frei erfundenen, aber plausibel wirkenden Live-Marktdaten.

4.3 Blockchain-Routing und Geldwäsche (Agent D/E)

Der dritte Baustein ist keine Täuschung mehr, sondern reine Infrastruktur: Sobald Gelder eingezahlt wurden, übernehmen automatisierte Prozesse Weiterleitung, Stückelung und Auswahl der Cash-out-Kanäle. Teil II dieses Whitepapers geht auf dieses Feld im Detail ein.

4.4 Recovery-Scam: der zweite Angriff (Agent F)

Ein oft übersehener, aber wachsender Baustein ist der sogenannte Recovery-Scam: Nachdem ein Opfer bereits Geld verloren hat, meldet sich – wiederum häufig KI-gestützt – ein vermeintlicher „Vermögensermittler", der gegen Vorkasse die Rückholung der verlorenen Gelder verspricht.

4.5 Deepfakes: der Verlust der letzten Gewissheit

Aus bereits drei bis fünf Sekunden Audiomaterial lässt sich heute eine Stimme mit rund 85 % Erkennungsgenauigkeit klonen; Video-Deepfakes sind mittlerweile überzeugend genug, um in Live-Videocalls für Führungskräfte oder vertraute Personen zu stehen. Wie real diese Bedrohung bereits ist, zeigt der Fall des britischen Ingenieurbüros Arup: Ein Mitarbeiter in Hongkong ließ sich durch eine Deepfake-Videokonferenz überzeugen, an der neben dem vermeintlichen CFO auch mehrere weitere, ihm bekannte Führungskräfte teilnahmen – sämtliche Teilnehmer außer ihm selbst waren KI-generiert. In der Folge veranlasste er 15 Überweisungen im Gesamtwert von rund 25 Millionen US-Dollar.

4.6 Fraud-as-a-Service: der Baukasten für jedermann

Auf einschlägigen Marktplätzen werden „Dark LLMs" wie FraudGPT für 30 bis 200 US-Dollar im Monat angeboten, synthetische Identitäten kosten teils nur rund 5 US-Dollar.

05 Typischer Ablauf eines Cybertrading-Betrugsfalls

Die einzelnen Bausteine aus Kapitel 4 greifen in der Praxis zu einem mehrstufigen Ablauf ineinander. In den von finanz-forensik.de begleiteten Fällen ließ sich dieser Ablauf – bei aller Varianz im Einzelfall – immer wieder in vergleichbarer Form beobachten:

- Erstkontakt, Vertrauensaufbau, erste Investmentempfehlung und Vertrauensbeweis (kleine, „verzinste" Auszahlungen).
- Eskalation zu größeren Summen, gelegentlich untermauert durch einen Deepfake-Videoanruf eines „Experten".
- Cash-out und Verschleierung über Zwischenadressen (Layering) und Stückelung (Smurfing) – Gegenstand von Teil II dieses Whitepapers.
- Abbruch des Kontakts, teils gefolgt von einem Recovery-Scam als zweitem Angriff auf dasselbe Opfer.

Vom einzelnen Betrüger zum autonomen Agentennetz. *Was früher menschliche Callcenter leisteten, verteilt sich zunehmend auf arbeitsteilige KI-Agenten — die Geldflüsse dahinter bleiben jedoch an dieselben Blockchain-Strukturen gebunden.*

TEIL II

Die Wissenschaft der Verschleierung

06 Forensische Beobachtungen: wiederkehrende Muster und ihre Ursachen

Dieses Kapitel beschreibt nicht nur, was sich in der forensischen Nachverfolgung von Cybertrading-Betrugsfällen wiederholt beobachten lässt, sondern vor allem, warum diese Muster auftreten – unabhängig davon, ob der jeweilige Fall menschlich oder KI-gestützt orchestriert wurde. Die Beobachtungen basieren auf der Auswertung von Blockchain-Transaktionsdaten aus mehreren von finanz-forensik.de bearbeiteten Fällen und werden hier – wie in Anhang C näher erläutert – bewusst qualitativ, anonymisiert und ohne Prozentangaben dargestellt.

6.1 Warum die Meldeschwelle zur Zwangsbedingung wird

Nahezu jedes regulierte Finanzsystem der Welt arbeitet mit harten Meldeschwellen: In den USA verlangt der Bank Secrecy Act die Meldung von Bartransaktionen oberhalb von 10.000 US-Dollar (Currency Transaction Report); die gezielte Aufteilung eines Betrags, um unterhalb dieser Schwelle zu bleiben, ist in den USA als eigener Straftatbestand („Structuring", 31 U.S.C. § 5324) sogar unabhängig von der Herkunft des Geldes strafbar. Auch die europäischen Geldwäsche-Richtlinien sowie die kryptospezifischen Transfer-of-Funds-Vorgaben unter MiCA/DAC8 arbeiten mit vergleichbaren Schwellenwerten für die verstärkte Identifizierung von Transaktionen. Die FATF benennt in ihren „Virtual Assets Red Flag Indicators" die „Stückelung von VA-Transaktionen … in Beträgen unterhalb von Aufzeichnungs- oder Meldeschwellen" ausdrücklich als eigenständiges Warnsignal.

Daraus folgt eine einfache, aber wichtige Einsicht: Stückelung ist keine kreative Erfindung findiger Täter, sondern die trivialste, naheliegendste Reaktion auf jedes System, das ausschließlich einzelne Transaktionen anhand eines festen Schwellenwerts prüft. Formal betrachtet: Prüft ein Kontrollsystem jede Einzeltransaktion mit Wert v gegen einen Schwellenwert T, dann ist die aufwandsärmste Umgehungsstrategie für einen Gesamtbetrag V die Aufteilung in $n \approx V/T$ Teilbeträge, die jeweils knapp unterhalb von T liegen. Diese Strategie ist unabhängig vom Intelligenzniveau des Akteurs – sie ist die dominante Antwort auf jede schwellenwertbasierte Kontrolle, ob sie nun von einem Menschen oder einem Optimierungsalgorithmus gewählt wird.

6.2 Warum generative KI dieses Problem nicht lösen kann

Generative KI – Sprachmodelle, Deepfakes, synthetische Stimmen – wirkt auf einer anderen Ebene als die in 6.1 beschriebene Zwangsbedingung: Sie verbessert die Überzeugungskraft, Personalisierung und Skalierung der Kontaktebene (Kapitel 4 und 5), nicht die regulatorisch-technische Ebene, auf der Meldeschwellen greifen. Ob eine Konversation von einem Menschen oder einem hochentwickelten Sprachmodell geführt wurde, ändert nichts daran, dass eine Einzahlung von 50.000 US-Dollar bei einer compliant arbeitenden Börse einen meldepflichtigen Schwellenwert auslöst.

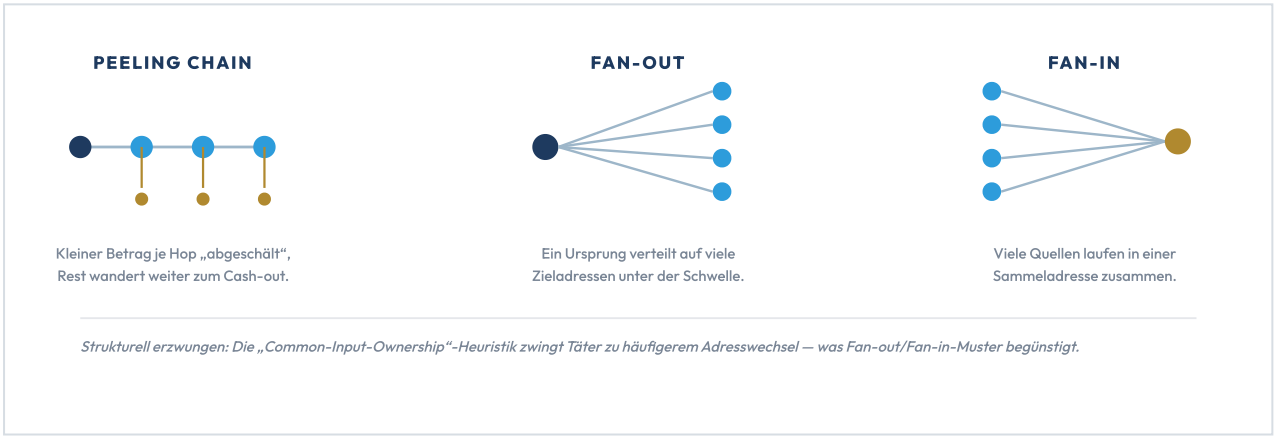
Daraus ergibt sich ein bemerkenswertes Paradox: Automatisiert eine Täterorganisation die Kontaktebene erfolgreich und vervielfacht dadurch das abgeschöpfte Gesamtvolumen, steigt zwangsläufig auch die Zahl der erforderlichen Stückelungstransaktionen – nicht ihre Zahl sinkt, sondern die schiere Menge an forensisch auffälligen Strukturierungs-Ereignissen wächst mit dem Erfolg der KI-gestützten Betrugsoperation mit.

6.3 Wiederkehrende Graphstrukturen: Peeling Chains, Fan-out und Fan-in

Blockchain-Forensik kennt seit den grundlegenden Arbeiten von Meiklejohn u. a. („A Fistful of Bitcoins“, 2013) sowie Möser, Böhme und Breuker („An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem“, 2013) mehrere wiederkehrende Strukturmotive in Transaktionsgraphen:

- **Peeling Chain:** Ein Guthaben wandert über eine Kette von Adressen, wobei bei jedem Schritt ein kleiner Betrag „abgeschält“ und der Rest an eine neue Wechseladresse weitergeleitet wird – bis es schließlich an einem Cash-out-Punkt endet.
- **Fan-out:** Ein einzelner Ursprung verteilt Gelder auf viele Zieladressen, um die Rückverfolgung zu erschweren und unterhalb von Meldeschwellen zu bleiben.
- **Fan-in (Konsolidierung):** Gelder aus vielen, augenscheinlich unabhängigen Quellen laufen in einer Sammeladresse zusammen, bevor sie gebündelt weiterverarbeitet werden.

Diese Motive sind nicht beliebig, sondern strukturell erzwungen: Die „Common-Input-Ownership“-Heuristik (Meiklejohn u. a.) erlaubt es, Adressen, die gemeinsam als Input einer Transaktion auftreten, demselben Akteur zuzuordnen – was Täter zu häufigerem Adresswechsel zwingt (mehr Hops), was wiederum Fan-out/Fan-in-Muster begünstigt. Genau diese Merkmale – 94 lokale und 72 aggregierte Nachbarschaftsmerkmale pro Transaktion im öffentlich verfügbaren „Elliptic“-Datensatz (Weber u. a., 2019) – bilden heute die Grundlage moderner, lernbasierter Erkennungsverfahren (siehe Kapitel 8).



Drei wiederkehrende Graphmotive in Transaktionsnetzwerken. *Diese Motive sind nicht beliebig, sondern Folge der Meldeschwellen (6.1) und der Clustering-Heuristiken. Sie bilden die Grundlage lernbasierter Erkennungsverfahren (Kapitel 8).*

6.4 Was sich durch KI verändert – und was strukturell gleich bleibt

Was sich verändert, ist nicht das „Wie“, sondern das „Wie schnell“ und „Wie parallel“: KI-Automatisierung erhöht die Geschwindigkeit zwischen einzelnen Hops und die Zahl gleichzeitig aktiver Fälle. Was strukturell gleich bleibt, ist die Notwendigkeit von Stückelung (6.1), die Begrenztheit tatsächlich nutzbarer Cash-out-Kanäle sowie die daraus entstehenden Graphmotive (6.3) – denn diese Zwänge liegen außerhalb dessen, was generative KI beeinflussen kann.

6.5 Neue Ermittlungsansätze

Aus den vorstehenden Beobachtungen leiten sich zwei komplementäre Ermittlungsansätze ab: Erstens der clusterübergreifende Abgleich wiederkehrender Zwischen- oder Sammelstrukturen über mehrere, augenscheinlich unabhängige Fälle hinweg. Zweitens die Fokussierung auf die begrenzte Zahl an Cash-out-Endpunkten statt auf die lückenlose Rekonstruktion jedes einzelnen, durch Automatisierung beliebig vervielfachbaren Zwischenschritts.

07 Die Mathematik autonomer Geldwäsche

Dieses Kapitel geht über die Beschreibung hinaus und schlägt ein einfaches, konzeptionelles Modell vor, um zu erklären, warum die in Kapitel 6 beobachteten Muster nahezu zwangsläufig entstehen – unabhängig davon, ob ein Mensch oder ein Algorithmus die Entscheidungen trifft. Das Modell erhebt keinen Anspruch auf empirische Validierung im strengen wissenschaftlichen Sinn, sondern dient als Analyserahmen.

7.1 Geldwäsche als Mehrzieloptimierung

Ein autonomer „Routing-Agent" – ob als explizite Software oder als implizites Entscheidungsmuster einer Tätergruppe – steht für jeden abzuwickelnden Betrag vor einem Optimierungsproblem mit mehreren, teils widersprüchlichen Zielgrößen. Diese Perspektive verschiebt die Fragestellung von „Wie verhalten sich Täter?" zu „Welches Optimierungsproblem müssen Täter grundsätzlich lösen – und was folgt daraus zwangsläufig für die beobachtbare Struktur?"

7.2 Die sechs Zieldimensionen

1 · ENTDECKUNGSRISIKO ↓

Minimierung des Entdeckungsrisikos: mehr Zwischenschritte, kleinere Tranchen, mehr Zeitverzögerung.

2 · LIQUIDITÄT ↑

Maximierung der Liquidität: Wahl von Zielplattformen, an denen der jeweilige Vermögenswert tatsächlich in ausreichendem Volumen und ohne Kursverzerrung in Fiat-Geld gewandelt werden kann.

3 · GEBÜHREN ↓

Minimierung der Gebühren: jeder zusätzliche Hop kostet Netzwerk- und Handelsgebühren – ein direkter Gegenspieler zur Risikominimierung durch mehr Hops.

4 · SANKTIONEN VERMEIDEN

Abgleich der Zieladressen und -entitäten gegen Sanktionslisten (z. B. OFAC SDN, EU-Konsolidierte Liste), um nicht bei einer sanktionierten oder ausgeschlossenen Plattform zu landen.

5 · CLUSTERING VERMEIDEN

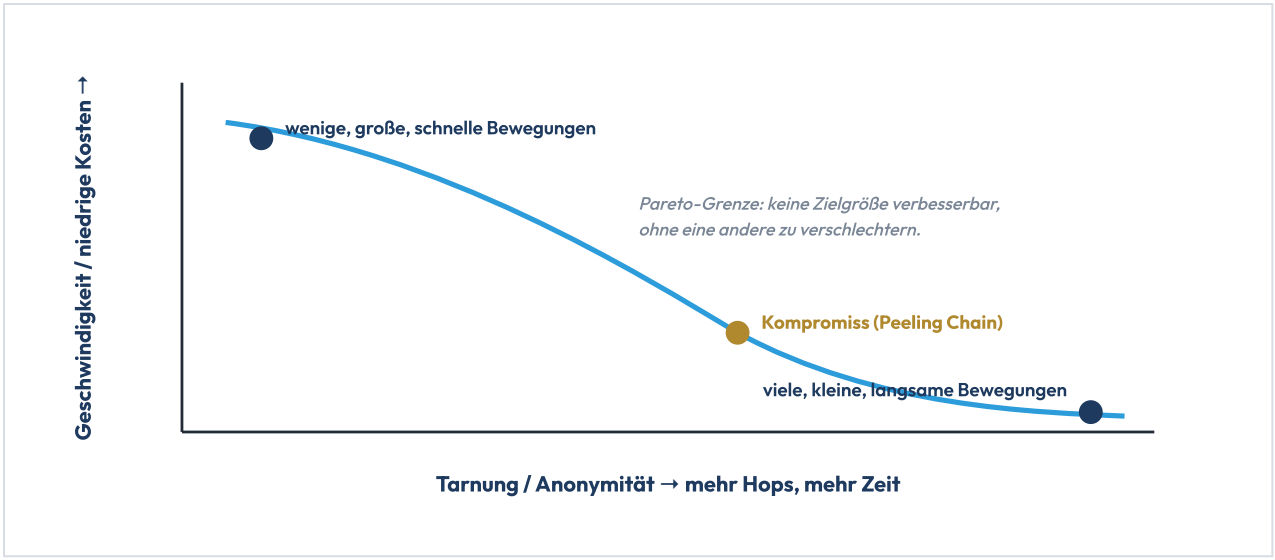
Umgehung bekannter Heuristiken (z. B. Common-Input-Ownership), was tendenziell zu mehr, nicht weniger Adresswechseln zwingt – ein Gegenspieler zur Gebührenminimierung.

6 · ZEIT ↓

Zeitoptimierung: schnelle Abwicklung verkürzt das Reaktionsfenster für Opfer, Börsen und Ermittler, erhöht aber zugleich die Auffälligkeit gegenüber geschwindigkeitsbasierten Betrugserkennungsregeln.

7.3 Zielkonflikte und die Pareto-Grenze

Die sechs Zielgrößen lassen sich nicht gleichzeitig optimal erfüllen: Risikominimierung und Vermeidung von Clustering verlangen tendenziell mehr Hops, mehr Zeit und mehr Adressen – Gebührenminimierung und Zeitoptimierung verlangen das Gegenteil. Es existiert daher kein einzelnes Optimum, sondern lediglich eine Pareto-Grenze nicht-dominierter Strategien: Jede reale Geldwäsche-Operation muss einen Punkt auf dieser Kurve wählen, und diese Wahl selbst ist ein beobachtbares Merkmal.



Die Pareto-Grenze der Geldwäsche-Optimierung. *Operationen, die Tarnung über Geschwindigkeit stellen, erzeugen viele kleine, langsame Bewegungen; Operationen, die Geschwindigkeit über Tarnung stellen, erzeugen wenige, große, schnelle Bewegungen. Diese „Revealed Preference" liefert eine Art Geldwäsche-Fingerabdruck der jeweiligen Operation.*

7.4 Warum Optimierung selbst Spuren erzeugt

Ein zentraler, auf den ersten Blick kontraintuitiver Punkt: Jede Optimierung im mathematischen Sinn bedeutet per Definition, auf gleichartige Ausgangsbedingungen mit gleichartigen Entscheidungen zu reagieren. Konsistenz ist das Wesen von Optimierung – und Konsistenz bedeutet Vorhersagbarkeit. Ein menschlicher Täter variiert unregelmäßig, macht Fehler, handelt aus Stimmung oder Ermüdung heraus – und liefert damit paradoxerweise weniger lernbares, generalisierbares Signal für musterbasierte Erkennungsverfahren als ein diszipliniert optimierender Agent es täte.

7.5 Von der Beobachtung zum Modell: Implikationen für die Graphstruktur

Das Modell aus 7.1 bis 7.4 erklärt die in Kapitel 6.3 beschriebenen Motive, statt sie nur zu beschreiben: Peeling Chains entstehen aus dem Kompromiss zwischen Risikominimierung und Gebührenminimierung (minimal ausreichende Tarnung bei begrenzten Kosten); Fan-in-Sammelpunkte entstehen aus der Liquiditätsanforderung, ausreichend Volumen für einen wirtschaftlich sinnvollen Cash-out zu bündeln; gelegentliche Treffer auf sanktionierte oder auffällige Plattformen entstehen aus unvollständiger oder verzögerter Aktualisierung der Sanktions- und Risikoprüfung (Ziel 4) relativ zu den übrigen fünf Zielen. Damit wird aus einer rein beschreibenden Forensik ein erklärendes Modell.

08 Warum Blockchain-Forensik an Bedeutung gewinnt – statt verliert

Eine verbreitete Annahme lautet: KI mache Täter unsichtbarer. Die in diesem Whitepaper entwickelte Argumentation legt das Gegenteil nahe.

8.1 Die Automatisierungs-Paradoxie

Wie in Kapitel 7.4 begründet, treffen automatisierte, optimierende Systeme konsistente, regelbasierte Entscheidungen unter vergleichbaren Bedingungen. Konsistente, wiederholte Entscheidungen erzeugen statistisch regelmäßige Muster – und genau solche Regelmäßigkeit ist die Grundvoraussetzung für musterbasierte, lernende Erkennungsverfahren.

8.2 Von regelbasierten zu lernenden Analyseverfahren

Frühe Blockchain-Forensik beruhte auf manuellen Heuristiken wie der Common-Input-Ownership- und der Wechseladressen-Heuristik (Meiklejohn u. a., 2013). Heute ermöglichen graphbasierte, lernende Verfahren – etwa Graph Convolutional Networks, trainiert auf öffentlich verfügbaren, gelabelten Datensätzen wie „Elliptic“ mit über 200.000 Bitcoin-Transaktionen (Weber u. a., 2019) – die automatisierte Erkennung subtiler struktureller und zeitlicher Signaturen, die einer rein manuellen Prüfung entgehen würden. Je stärker Täterorganisationen ihre Prozesse standardisieren und automatisieren (Kapitel 7), desto lernbarer und generalisierbarer wird das dabei entstehende Signal für solche Verfahren – Erkennungssysteme sollten gegenüber stark automatisierten Täterstrukturen tendenziell wirksamer werden, nicht schwächer.

8.3 Die Rolle des Menschen verschiebt sich, nicht verschwindet

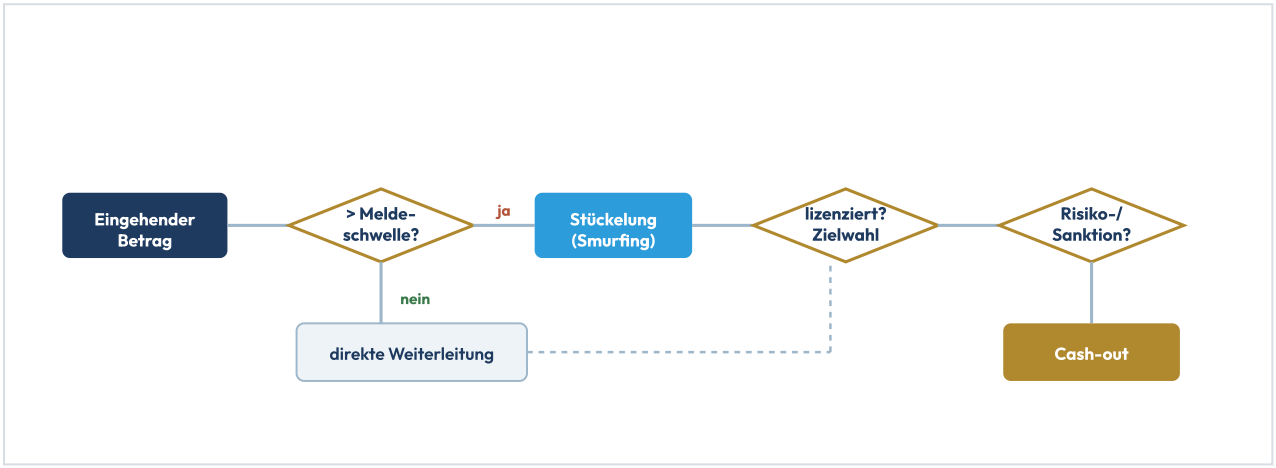
Menschliche forensische Analysten verschieben ihre Rolle von der manuellen Nachverfolgung jedes einzelnen Hops hin zur Kuratierung von Trainingsdaten, zur Validierung von Modellergebnissen und – entscheidend – zur rechtlich-investigativen Bewertung clusterübergreifender Treffer (Kapitel 6.5), die ein Modell allein nicht liefern kann. Die Kombination aus automatisierter, graphbasierter Cluster- und Risikoerkennung und erfahrungsbasierter Einzelfallbewertung ist genau der methodische Ansatz, auf dem die in diesem Whitepaper zusammengefassten Beobachtungen von finanz-forensik.de beruhen.

TEIL III

Die Zukunft der Ermittlung

09 Autonome Geldwäsche in der Praxis

Das in Kapitel 7 entwickelte Modell lässt sich als vereinfachter Entscheidungspfad illustrieren: Ein eingehender Betrag wird zunächst gegen bekannte Meldeschwellen geprüft; oberhalb der Schwelle erfolgt Stückelung, unterhalb direkte Weiterleitung; anschließend wird zwischen lizenzierten und unlizenzierten Zielplattformen gewählt, bevor eine abschließende Risikoprüfung den Cash-out freigibt.



Vereinfachter Entscheidungspfad eines Routing-Agenten. *Prüfung gegen Meldeschwellen → Stückelung oder direkte Weiterleitung → Wahl zwischen lizenzierter/unlizenzierter Zielplattform → abschließende Risikoprüfung vor Cash-out. Illustratives Modell, kein reales System.*

Dass dabei – wie in Kapitel 6.3 und 7.5 beschrieben – vereinzelt auch Plattformen mit Sanktionsbezug getroffen werden, bestätigt das Modell aus Kapitel 7: Selbst ein weitgehend optimierendes System produziert über Zeit hinweg Restrisiko in mindestens einer der sechs Zieldimensionen – und genau dort liegt der Ansatzpunkt für Ermittler.

10 Vom Sha Zhu Pan zum autonomen Multi-Agenten-System

Die Betrugsfabriken Südostasiens, in denen tausende – teils zur Arbeit gezwungene – Menschen Betrugsgespräche führen, bilden derzeit noch das organisatorische Rückgrat vieler Netzwerke. Internationale Ermittlungen haben diesem Modell 2026 empfindliche Schläge versetzt: Im April und Mai gelang FBI, Dubai Police und dem chinesischen Ministerium für öffentliche Sicherheit die Zerschlagung von mindestens neun Betrugszentren mit 276 Festnahmen; im Juni 2026 folgte eine multinationale Aktion unter Beteiligung von Meta, Microsoft, Starlink, Coinbase und Behörden.

Der ökonomische Druck aus genau dieser verschärften Strafverfolgung ist ein wesentlicher Treiber der Automatisierung: Je riskanter und teurer der Betrieb personalintensiver Betrugszentren wird, desto attraktiver werden KI-Agenten, die dieselbe „Beratungsleistung“ ohne Lohnkosten, Fluchtrisiko oder Aussagebereitschaft bei Festnahmen erbringen.

11 KI gegen KI: Das Wettrüsten

Die Abwehrseite setzt zunehmend ebenfalls auf KI, wodurch ein mehrstufiges Wettrüsten entsteht: Angreifer-KI generiert Täuschung, Verteidiger-KI erkennt Anomalien in Echtzeit, Forensik-KI unterstützt die Nachverfolgung abgeflossener Gelder (Kapitel 8), und Regulator-KI überwacht Märkte und Meldewege auf struktureller Ebene.

74 % der befragten Fraud- und AML-Verantwortlichen bei Banken und Fintechs bezeichnen KI-gestützten Betrug bereits heute als größte Bedrohung – zugleich geben 67 % an, für eine wirksame Abwehr noch nicht ausreichend aufgestellt zu sein. Als wirksamste technische Gegenmaßnahme gilt derzeit die sogenannte Liveness-Detection.

12 Warum klassische Ermittlungen künftig scheitern

- **Internationale Rechtshilfe ist zu langsam:** Ein Rechtshilfeersuchen kann Monate bis Jahre dauern, während ein Cash-out innerhalb von Stunden abgeschlossen ist.
- **Wallets wechseln in Sekunden:** Anders als ein Bankkonto lässt sich eine neue Kryptoadresse kostenlos und in Sekunden erzeugen.
- **Exchanges müssten automatisiert reagieren:** Manuell bearbeitete Auskunfts- und Einfrierungsersuchen bleiben strukturell im Rückstand gegenüber automatisiert agierenden Tätern.
- **Jurisdiktions-Hopping:** Täterorganisationen wählen gezielt Plattformen und Regionen mit schwacher Regulierung oder Sanktionsbezug für ihre Cash-out-Wege.

13 Regulatorische Antworten

Der EU AI Act stuft KI-Systeme zur Betrugserkennung und andere automatisierte Entscheidungsprozesse im Finanzsektor ausdrücklich als „hochriskant“ ein. Ab dem 2. August 2026 müssen entsprechende Systeme Anforderungen an Transparenz, Nachvollziehbarkeit und menschliche Aufsicht erfüllen; bei Verstößen drohen Bußgelder von bis zu 30 Millionen Euro. Parallel dazu intensivieren nationale Aufsichtsbehörden wie die BaFin ihre Verbraucherwarnungen.

14 Ausblick: 2030 – 2035 – 2040

HORIZONT	ERWARTETE ENTWICKLUNG
2030	Vollautomatisierte Multi-Agenten-Netzwerke werden zum Standard. Personalintensive Betrugszentren treten gegenüber schlanken, KI-agentengestützten Strukturen zunehmend in den Hintergrund. Auf der Verteidigungsseite wird breit einsetzbare Liveness- und Verhaltenserkennung zum Branchenstandard.
2035	Autonome Geldwäsche-Routing-Systeme werden zur Norm. Echtzeit-Risikobewertung bei der Wahl von Cash-out-Pfaden (Kapitel 7 und 9) dürfte sich von einem beobachtbaren Muster zu einer expliziten, systematisch eingesetzten Fähigkeit auf Täterseite entwickeln.
2040	Systemische statt fallbezogene Aufsicht. Die Unterscheidung zwischen „von Menschen initiiertem“ und „von KI initiiertem“ Betrug dürfte für die Strafverfolgung an Bedeutung verlieren; Aufsicht verschiebt sich zu struktureller Systemüberwachung.

TEIL IV

Praxis und Fazit

15 Gegenmaßnahmen: Empfehlungen für die Praxis

Für Institutionen ergibt sich die Notwendigkeit mehrschichtiger Verteidigung – Verhaltensanalyse, Gerätefingerabdruck, biometrische Liveness-Prüfung und Transaktionsmonitoring in Kombination. Eine vollständige Checkliste für Privatanleger und Unternehmen findet sich in Anhang A.

16 Fazit

KI-gestützte Cybertrading-Betrugsnetzwerke markieren einen qualitativen Bruch: Aus einem personal- und zeitintensiven Handwerk wird ein skalierbares, weitgehend automatisiertes Geschäftsmodell. Gleichzeitig zeigt die in Teil II entwickelte Argumentation: Die grundlegenden Auszahlungsmuster – Smurfing, Layering, begrenzte Cash-out-Kanäle – bleiben nicht nur bestehen, sie sind mathematisch nahezu erzwungen, und die zunehmende Automatisierung macht sie tendenziell besser, nicht schlechter erkennbar. ■

„Die größte Gefahr autonomer KI-Agenten liegt nicht darin, dass sie Menschen ersetzen. Sie liegt darin, dass sie Betrug schneller skalieren können, als Behörden, Banken und Ermittler ihre Schutzmechanismen anpassen können.“

FINANZ-FORENSIK.DE, JULI 2026

FÜR PRIVATANLEGER

- Unrealistische, garantierte Renditeversprechen hinterfragen – unabhängig davon, wie professionell die Plattform wirkt.
- Bei Drängen auf schnelle Entscheidungen oder emotionalem Druck bewusst innehalten.
- Video- oder Sprachanrufe vermeintlich bekannter Personen mit finanziellen Bitten über einen zweiten, unabhängigen Kanal verifizieren.
- Zahlungsaufforderungen an Krypto-Wallets oder über wenig regulierte Tauschdienste besonders kritisch prüfen.
- Lizenzierung des Anbieters bei der zuständigen Aufsichtsbehörde prüfen.
- Frühe „Gewinne“ nicht als Sicherheitsbeweis werten.
- Bei bereits erfolgtem Verlust: Vorsicht vor „Recovery“-Angeboten gegen Vorkasse.

FÜR UNTERNEHMEN

- Zahlungsfreigaben ab einer definierten Schwelle an einen zweiten, unabhängigen Verifikationskanal koppeln.
- Video-Autorisierungen kritisch prüfen: vorab vereinbarte Verifikationsmerkmale verlangen.
- Mitarbeiterschulungen an aktuelle Deepfake- und Social-Engineering-Maschen anpassen.
- Reaktionspläne für den Verdachtsfall vorab festlegen und testen.
- Bei Verdacht: zeitnahe Sicherung von Transaktionsdaten und frühzeitige forensische Nachverfolgung.

ANHANG B · GLOSSAR

Pig Butchering / Sha Zhu Pan — Betrugsmasche, bei der Opfer über einen längeren Zeitraum emotional gebunden und schrittweise zu Investments in eine gefälschte Handelsplattform bewegt werden.

Agentische KI — Autonome KI-Systeme, die mehrstufige Aufgaben ohne fortlaufende menschliche Steuerung eigenständig ausführen.

Multi-Agenten-Pipeline — Arbeitsteilige Architektur, in der unterschiedliche KI-Agenten jeweils einen Teilschritt des Betrugsprozesses übernehmen.

Structuring / Smurfing — Aufteilung größerer Geldbeträge in viele kleinere Transaktionen unterhalb von Meldeschwellen; in den USA eigener Straftatbestand (31 U.S.C. § 5324).

Layering / Wallet-Hopping — Weiterleitung von Geldern über mehrere Zwischenadressen, um die Herkunft zu verschleiern.

Peeling Chain — Kette von Transaktionen, bei der schrittweise kleine Beträge von einem wandernden Hauptguthaben „abgeschält" werden (Meiklejohn u. a., 2013).

Common-Input-Ownership-Heuristik — Forensische Annahme, dass Adressen, die gemeinsam als Input einer Transaktion auftreten, demselben Akteur gehören.

Graph Neural Network (GNN) — Lernverfahren, das Muster direkt auf Graphstrukturen (z. B. Transaktionsnetzwerken) erkennt; Grundlage moderner Blockchain-Forensik-Modelle.

Pareto-Grenze — Menge der Strategien, bei denen keine Zielgröße verbessert werden kann, ohne eine andere zu verschlechtern.

Routing-Agent — Konzeptionelles Modell eines Systems, das automatisiert den vermeintlich risikoärmsten Weiterleitungspfad wählt.

Nested VASP — Virtueller Vermögensdienstleister, der über das Konto eines anderen, größeren VASP operiert und dadurch eigene KYC-Pflichten teilweise umgeht.

Recovery-Scam — Nachfassbetrug, bei dem bereits geschädigte Opfer unter dem Vorwand der Vermögensrückholung erneut zu Zahlungen bewegt werden.

Liveness-Detection — Technisches Verfahren zur Prüfung, ob eine reale, physisch anwesende Person und kein synthetisches Abbild vorliegt.

ANHANG C · METHODISCHER HINWEIS ZUR DATENGRUNDLAGE

Dieses Whitepaper unterscheidet konsequent zwischen zwei Arten von Quellen. Erstens extern erhobene und veröffentlichte Statistiken (Kapitel 3), die als Zahlen Dritter gekennzeichnet sind und deren jeweilige Methodik den zitierten Originalquellen zu entnehmen ist. Zweitens qualitative Beobachtungen aus der forensischen Fallarbeit von finanz-forensik.de (Kapitel 5 bis 9), die ausdrücklich keine statistische Erhebung darstellen.

Diese qualitative Herangehensweise ist in der Sicherheits- und Kriminalitätsanalyse ein etabliertes und legitimes Vorgehen, insbesondere dort, wo belastbare, repräsentative Datensätze naturgemäß nicht existieren – etwa weil ein erheblicher Teil der Fälle nie angezeigt wird oder Tätergruppen keine überprüfbaren Statistiken offenlegen. Auch Europols Internet Organised Crime Threat Assessment (IOCTA) stützt sich methodisch auf strukturierte Experteneinschätzungen der Mitgliedstaaten statt auf einen einzigen, vollständig quantifizierten Datensatz. Nationale Lageberichte wie die des Bundesamts für Sicherheit in der Informationstechnik (BSI) verbinden ebenfalls qualitative Einordnungen mit punktuellen quantitativen Kennzahlen, je nachdem, was die Datenlage zulässt.

Konkret bedeutet dies für dieses Whitepaper: Wenn von „wiederholt beobachteten Mustern" die Rede ist, bezieht sich dies auf tatsächlich in mehreren, voneinander unabhängigen Fällen aus der Praxis von finanz-forensik.de festgestellte Regelmäßigkeiten – ohne Angabe von Fallzahlen, Prozentwerten oder einer Aussage zur Repräsentativität für die Gesamtheit aller Cybertrading-Betrugsfälle. Das in Kapitel 7 entwickelte mathematische Modell ist als analytischer Rahmen zu verstehen, der die beobachteten Regelmäßigkeiten plausibel erklärt, nicht als empirisch getestete und validierte Theorie.

QUELLEN & ÜBER FINANZ-FORENSIK.DE

finanz-forensik.de unterstützt Geschädigte, Kanzleien und Behörden bei der forensischen Nachverfolgung betrügerisch erlangter Vermögenswerte, insbesondere im Bereich Kryptowährungen und digitaler Zahlungsverkehr. Auf Basis von Blockchain-Analyse-Tools und enger Zusammenarbeit mit Handelsplattformen und Strafverfolgungsbehörden rekonstruieren wir Geldflüsse, identifizieren Auszahlungspunkte und unterstützen bei der Vorbereitung von Auskunfts- und Einfrierungsersuchen.

QUELLEN

Chainalysis: 2026 Crypto Crime Report – Scams, Introduction & Sanctions (chainalysis.com) · FBI Internet Crime Complaint Center (IC3): 2025 Internet Crime Report (ic3.gov) · Sumsub: Fraud Trends 2026; Identity Fraud Report 2025/2026 (sumsub.com) · Group-IB: Threat-Intelligence-Analysen zu KI-gestützten Scam-Callcentern, 2026 · Europol: Einschätzungen zum Einsatz von Sprachmodellen durch Betrugsnetzwerke, 2026; Internet Organised Crime Threat Assessment (IOCTA) · BaFin: Pressemitteilung „Aufsichtsbehörden warnen vor Finanzbetrug mit KI und Kryptowerten“, 12.02.2026 · FATF: Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, 2020; Typologien-Aktualisierung 2026 · Meiklejohn, S. et al.: „A Fistful of Bitcoins: Characterizing Payments Among Men with No Names“, IMC 2013 · Möser, M., Böhme, R., Breuker, D.: „An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem“, APWG eCrime 2013 · Weber, M. et al.: „Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics“, arXiv:1908.02591, 2019 (Elliptic-Datensatz) · CFO Dive / Fortune / Gulf News: Berichterstattung zum Arup-Deepfake-Betrugsfall, Hongkong, 2024 · Toronto Police Service: „Project Déjà Vu“ – Ermittlungen zu synthetischem Identitätsbetrug, 2026 · Cornell University (arXiv): Studie zu KI-gesteuerten Angriffs-Frameworks, 2024 · finanz-forensik.de: Aggregierte, anonymisierte qualitative Beobachtungen aus der forensischen Blockchain-Analyse von Cybertrading-Betrugsfällen, 2026.

Hinweis: Dieses Whitepaper kombiniert öffentlich zugängliche Studien und Behördendaten mit qualitativen, anonymisierten Beobachtungen aus eigener forensischer Fallarbeit (Stand Juli 2026, siehe methodischen Hinweis in Anhang C) und dient der allgemeinen Einordnung. Es ersetzt keine Rechts- oder Anlageberatung im Einzelfall. Alle schematischen Abbildungen sind illustrativ und stellen keine Abbildung eines konkreten, real identifizierten Systems dar; das in Kapitel 7 vorgestellte Optimierungsmodell ist ein analytischer Rahmen, keine empirisch validierte Theorie.

David Lüdtke

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

Zertifiziert als Crystal Expert (CECF · CEEI · CEUI). **Kontakt:** postfach@finanz-forensik.de · +49 6057 9189145 · www.finanz-forensik.de · **Herausgeber:** Finanz Forensik GmbH · Würzburger Str. 59, 63639 Flörsbachtal · HRB 100521, Amtsgericht Hanau · USt-IdNr. DE454473675 · Geschäftsführung: Lydia Bonhard-Lüdtke, David Lüdtke. Dieses Whitepaper gibt den Diskussions- und Datenstand Juli 2026 wieder und stellt keine Rechts-, Steuer- oder Anlageberatung dar. © 2026 Finanz Forensik GmbH.