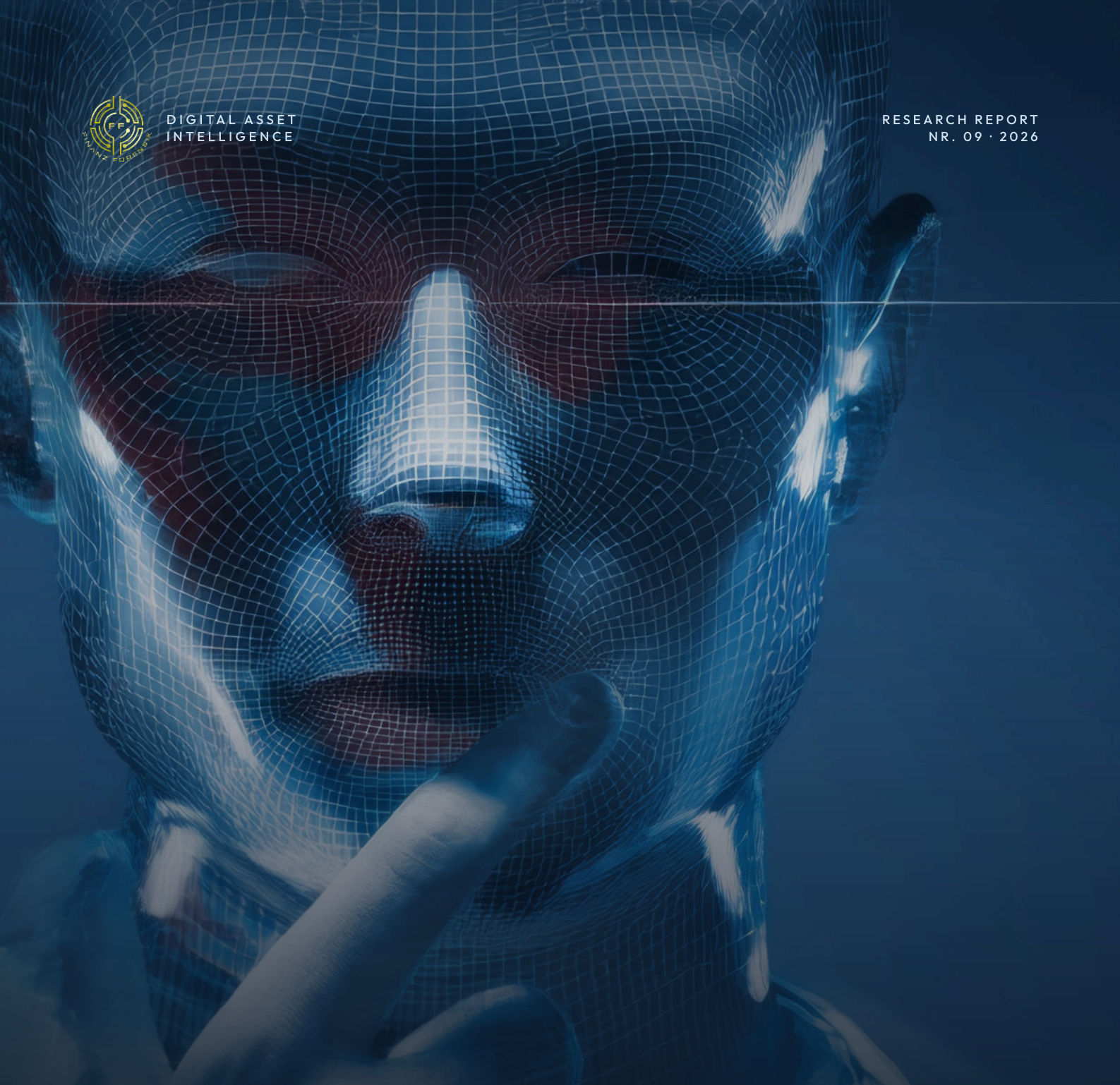


DIGITAL ASSET
INTELLIGENCE

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 · MODELL

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.

FINANZ·FORENSIK · FINANCIAL INTELLIGENCE & BLOCKCHAIN FORENSICS RESEARCH REPORT 09 / 2026

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.

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.

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 IOCTA, das ebenfalls auf strukturierten Experteneinschätzungen beruht. Ausführliche Erläuterungen in Anhang C. Die in Kapitel 3 genannten Kennzahlen stammen ausschließlich aus veröffentlichten Studien Dritter und sind entsprechend gekennzeichnet.

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 Krypto-Investments 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 Agenten. Europol beschreibt, wie große Sprachmodelle 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 Bausteine bereits im Einsatz:

- **Deepfake-Betrug:** Der Fall des Ingenieurbüros Arup zeigt bereits 2024 einen Schaden von 25 Millionen US-Dollar durch eine einzige Deepfake-Videokonferenz. Im Juni 2026 warnte die südafrikanische 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 anpassen.
- **Automatisierte Callcenter:** Group-IB beschreibt KI-gestützte Scam-Callcenter, die synthetische Stimmen mit Sprachmodell-Coaching kombinieren, um Gesprächsverläufe in Echtzeit zu steuern.
- **Synthetische Identitäten:** Im Rahmen von „Project Déjà Vu“ deckte die Polizei in Toronto auf, dass eine einzelne Person mithilfe synthetischer Identitäten hunderte Konten eröffnet hatte — bestätigter Schaden rund 2,9 Millionen US-Dollar.
- **Fraud-as-a-Service:** Dark-LLM-Abonnements wie FraudGPT werden bereits kommerziell gehandelt — die Bausteine für vollautomatisierten Betrug sind schon jetzt für wenig Geld verfügbar.

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 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, FATF) und sind mit den üblichen Einschränkungen solcher Erhebungen verbunden, insbesondere hoher Dunkelziffer. Die sechs Leitkennzahlen sind bereits auf der Auftaktseite zusammengefasst. Auch in Deutschland ist die Entwicklung spürbar: BaFin und BKA warnten in den ersten Monaten 2026 in mehr als 150 Einzelmeldungen vor unseriösen Krypto-Anbietern.

04 Anatomie eines KI-gestützten Betrugsnetzwerks

Was früher ein Callcenter mit geschultem Personal leistete, übernehmen zunehmend spezialisierte KI-Fähigkeiten, die sich zu einer durchgängigen Pipeline zusammensetzen lassen. Die folgende, illustrative Architektur beschreibt die Funktionsaufteilung — nicht als Prognose einzelner Softwareprodukte:

AGENT A/B · GROOMING

KI-Agenten übernehmen Kontaktaufnahme auf Dating- und Messenger-Plattformen und pflegen parallel Dutzende bis Hunderte individuell zugeschnittene „Beziehungen". Laut Sumsub sind Dating und Online-Medien mit 6,3 % Betrugsrate mehr als doppelt so stark betroffen wie der Finanzsektor.

AGENT C · SYNTHETISCHE BROKERAGE

Fälschung ganzer Handelsplattformen: komplette KI-generierte Broker-Web- und -App-Erlebnisse inklusive KYC-Onboarding, gebrandetem Kunden-Chat und frei erfundenen, aber plausibel wirkenden Live-Marktdaten.

AGENT D/E · ROUTING & GELDWÄSCHE

Keine Täuschung mehr, sondern reine Infrastruktur: Sobald Gelder eingezahlt sind, übernehmen automatisierte Prozesse Weiterleitung, Stückelung und Auswahl der Cash-out-Kanäle. Teil II geht darauf im Detail ein.

AGENT F · RECOVERY-SCAM

Nachdem ein Opfer bereits Geld verloren hat, meldet sich — wiederum häufig KI-gestützt — ein vermeintlicher „Vermögensermittler", der gegen Vorkasse die Rückholung verspricht (siehe Research Report Nr. 08).

DEEPFAKES

Aus drei bis fünf Sekunden Audio lässt sich eine Stimme mit rund 85 % Genauigkeit klonen; Video-Deepfakes sind überzeugend genug für Live-Videocalls. Im Arup-Fall veranlasste ein Mitarbeiter nach einer Deepfake-Konferenz 15 Überweisungen über rund 25 Mio. US-Dollar.

FRAUD-AS-A-SERVICE

„Dark LLMs" wie FraudGPT werden für 30 bis 200 US-Dollar im Monat angeboten, synthetische Identitäten teils für nur rund 5 US-Dollar — der Baukasten für jedermann.

05 Typischer Ablauf eines Cybertrading-Betrugsfalls

Die Bausteine aus Kapitel 4 greifen zu einem mehrstufigen Ablauf ineinander, der sich in den von finanz-forensik.de begleiteten Fällen immer wieder in vergleichbarer Form beobachten ließ:

- 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.

- 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 wiederholt beobachten lässt, sondern vor allem, warum diese Muster auftreten — unabhängig davon, ob der Fall menschlich oder KI-gestützt orchestriert wurde.

6.1 Warum die Meldeschwelle zur Zwangsbedingung wird

Nahezu jedes regulierte Finanzsystem arbeitet mit harten Meldeschwellen: In den USA verlangt der Bank Secrecy Act die Meldung von Bartransaktionen oberhalb von 10.000 US-Dollar; die gezielte Aufteilung eines Betrags, um darunter zu bleiben, ist als eigener Straftatbestand („Structuring", 31 U.S.C. § 5324) strafbar. Auch europäische Geldwäsche-Richtlinien und die kryptospezifischen Transfer-of-Funds-Vorgaben unter MiCA/DAC8 arbeiten mit Schwellenwerten. Die FATF benennt in ihren „Virtual Assets Red Flag Indicators" die Stückelung unterhalb von Meldeschwellen ausdrücklich als Warnsignal.

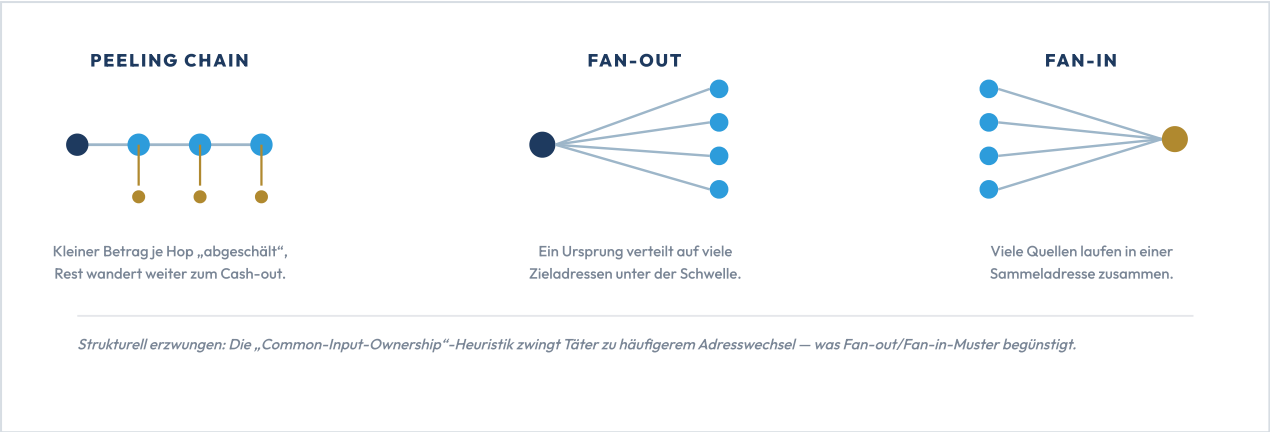
Daraus folgt: Stückelung ist keine kreative Erfindung findiger Täter, sondern die trivialste Reaktion auf jedes System, das einzelne Transaktionen anhand eines festen Schwellenwerts prüft. Formal: Prüft ein Kontrollsystem jede Transaktion mit Wert v gegen einen Schwellenwert T, dann ist die aufwandsärmste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

6.2 Warum generative KI dieses Problem nicht lösen kann

Generative KI wirkt auf einer anderen Ebene als diese Zwangsbedingung: Sie verbessert Überzeugungskraft, Personalisierung und Skalierung der Kontaktebene, nicht die regulatorisch-technische Ebene, auf der Meldeschwellen greifen. Ob eine Konversation von einem Menschen oder einem 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 Paradox: Automatisiert eine Täterorganisation die Kontaktebene erfolgreich und vervielfacht das abgeschöpfte Volumen, steigt zwangsläufig auch die Zahl der erforderlichen Stückelungstransaktionen — die Menge forensisch auffälliger Strukturierungs-Ereignisse wächst mit dem Erfolg der Operation.

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

Blockchain-Forensik kennt seit den Arbeiten von Meiklejohn u. a. („A Fistful of Bitcoins", 2013) und Möser/Böhme/Breuker (2013) mehrere Strukturmotive in Transaktionsgraphen:



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 gleich bleibt

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

6.5 Neue Ermittlungsansätze

Daraus leiten sich zwei komplementäre Ansätze 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, beliebig vervielfachbaren Zwischenschritts.

07 Die Mathematik autonomer Geldwäsche

Dieses Kapitel schlägt ein einfaches, konzeptionelles Modell vor, um zu erklären, warum die beobachteten Muster nahezu zwangsläufig entstehen. Das Modell erhebt keinen Anspruch auf empirische Validierung, 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. Das verschiebt die Frage 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 ↓

Mehr Zwischenschritte, kleinere Tranchen, mehr Zeitverzögerung.

2 · LIQUIDITÄT ↑

Zielplattformen, an denen der Wert tatsächlich in ausreichendem Volumen und ohne Kursverzerrung in Fiat wandelbar ist.

3 · GEBÜHREN ↓

Jeder Hop kostet Netzwerk- und Handelsgebühren — direkter Gegenspieler zur Risikominimierung.

4 · SANKTIONEN VERMEIDEN

Abgleich der Zieladressen gegen Sanktionslisten (OFAC SDN, EU-Liste), um nicht bei sanktionierten Plattformen zu landen.

5 · CLUSTERING VERMEIDEN

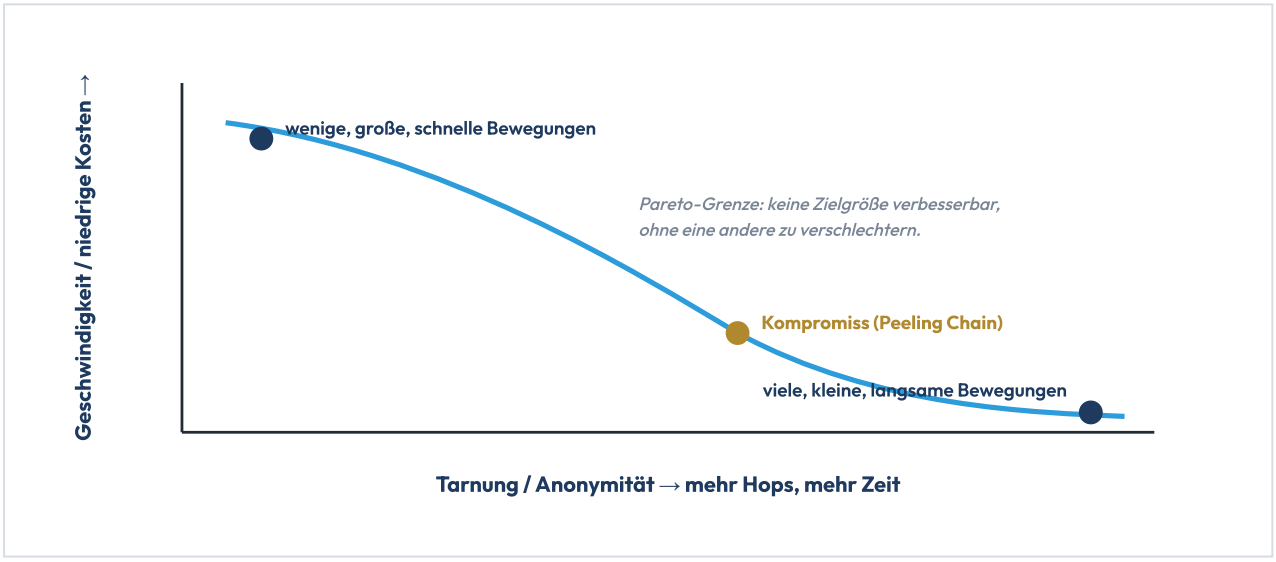
Umgehung bekannter Heuristiken (Common-Input-Ownership) zwingt zu mehr Adresswechseln — Gegenspieler zur Gebührenminimierung.

6 · ZEIT ↓

Schnelle Abwicklung verkürzt das Reaktionsfenster, erhöht aber die Auffälligkeit gegenüber geschwindigkeitsbasierten Regeln.

7.3 Zielkonflikte und die Pareto-Grenze

Die sechs Zielgrößen lassen sich nicht gleichzeitig optimal erfüllen: Risikominimierung und Clustering-Vermeidung verlangen mehr Hops, mehr Zeit, mehr Adressen — Gebühren- und Zeitoptimierung verlangen das Gegenteil. Es existiert daher kein einzelnes Optimum, sondern eine Pareto-Grenze nicht-dominierter Strategien.



Die Pareto-Grenze der Geldwäsche-Optimierung. *Jede reale Operation wählt einen Punkt auf dieser Kurve — und diese Wahl ist selbst ein beobachtbares Merkmal, eine Art „Geldwäsche-Fingerabdruck" (Revealed Preference).*

7.4 Warum Optimierung selbst Spuren erzeugt

Ein zentraler, kontraintuitiver Punkt: Jede Optimierung im mathematischen Sinn bedeutet, 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 — und liefert damit paradoxerweise weniger lernbares, generalisierbares Signal als ein diszipliniert optimierender Agent.

7.5 Von der Beobachtung zum Modell

Das Modell erklärt die Motive aus 6.3, statt sie nur zu beschreiben: Peeling Chains entstehen aus dem Kompromiss zwischen Risiko- und Gebührenminimierung; Fan-in-Sammelpunkte aus der Liquiditätsanforderung, ausreichend Volumen für einen sinnvollen Cash-out zu bündeln; gelegentliche

Treffer auf sanktionierte Plattformen aus unvollständiger Aktualisierung der Sanktionsprüfung relativ zu den übrigen Zielen. Damit wird aus beschreibender Forensik ein erklärendes Modell.

08 Warum Blockchain-Forensik an Bedeutung gewinnt — statt verliert

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

8.1 Die Automatisierungs-Paradoxie

Automatisierte, optimierende Systeme treffen 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 (Common-Input-Ownership, Wechseladressen). Heute ermöglichen graphbasierte, lernende Verfahren — etwa Graph Convolutional Networks, trainiert auf gelabelten Datensätzen wie „Elliptic“ mit über 200.000 Bitcoin-Transaktionen (Weber u. a., 2019, mit 94 lokalen und 72 aggregierten Merkmalen je Transaktion) — die automatisierte Erkennung subtiler struktureller und zeitlicher Signaturen. Je stärker Täterorganisationen standardisieren und automatisieren, desto lernbarer wird das Signal — Erkennungssysteme sollten gegenüber stark automatisierten Strukturen tendenziell wirksamer werden, nicht schwächer.

8.3 Die Rolle des Menschen verschiebt sich, nicht verschwindet

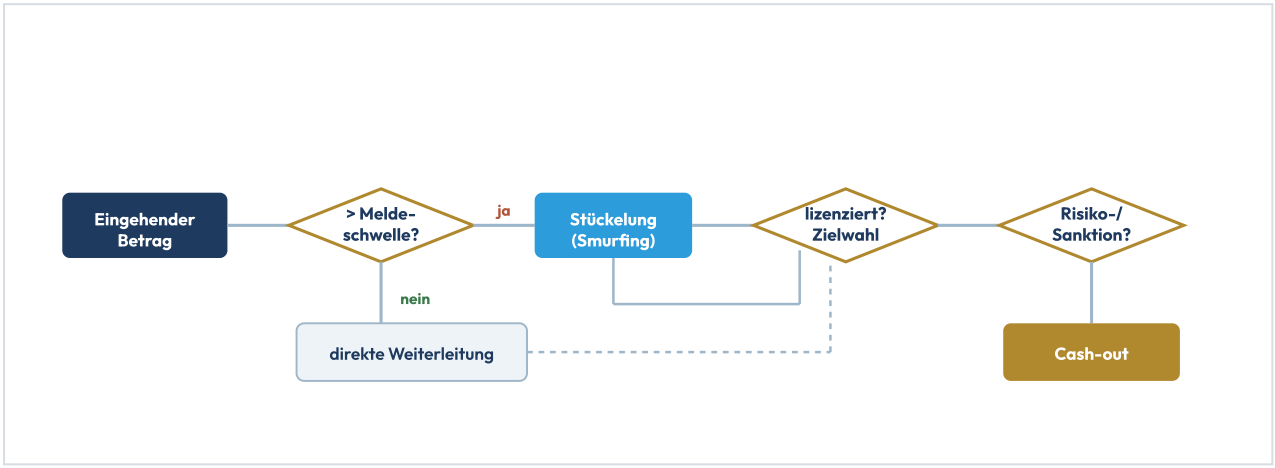
Menschliche Analysten verschieben ihre Rolle von der manuellen Nachverfolgung jedes einzelnen Hops hin zur Kuratierung von Trainingsdaten, zur Validierung von Modellergebnissen und — entscheidend — zur rechtlich-investigativen Bewertung clusterübergreifender Treffer. Die Kombination aus automatisierter, graphbasierter Cluster- und Risikoerkennung und erfahrungsbasierter Einzelfallbewertung ist genau der methodische Ansatz von finanz-forensik.de.

TEIL III

Die Zukunft der Ermittlung

09 Autonome Geldwäsche in der Praxis

Das Modell aus Kapitel 7 lässt sich als vereinfachter Entscheidungspfad illustrieren:



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

Dass dabei vereinzelt auch Plattformen mit Sanktionsbezug getroffen werden, bestätigt das Modell aus Kapitel 7: Selbst ein weitgehend optimierendes System produziert über Zeit 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 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 dieser verschärften Strafverfolgung ist ein wesentlicher Treiber der Automatisierung: Je riskanter und teurer personalintensive Betrugszentren werden, desto attraktiver werden KI-Agenten, die dieselbe „Beratungsleistung“ ohne Lohnkosten, Fluchtrisiko oder Aussagebereitschaft erbringen.

11 KI gegen KI: das Wettrüsten

Die Abwehrseite setzt zunehmend ebenfalls auf KI: Angreifer-KI generiert Täuschung, Verteidiger-KI erkennt Anomalien in Echtzeit, Forensik-KI unterstützt die Nachverfolgung abgeflossener Gelder, Regulator-KI überwacht Märkte 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 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.
- **Jurisdiktions-Hopping:** Täter 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 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 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 zurück. 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 entwickelt sich vom beobachtbaren Muster zu einer explizit eingesetzten Fähigkeit auf Täterseite.
2040	Systemische statt fallbezogene Aufsicht; die Unterscheidung zwischen „von Menschen initiiertem" und „von KI initiiertem" Betrug verliert für die Strafverfolgung an Bedeutung.

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.

FÜR PRIVATANLEGER

Garantierte Renditeversprechen hinterfragen. Bei Drängen bewusst innehalten. Video-/Sprachanrufe vermeintlich bekannter Personen über einen zweiten, unabhängigen Kanal verifizieren. Lizenzierung bei der Aufsichtsbehörde prüfen. Frühe „Gewinne“ nicht als Sicherheitsbeweis werten. Bei bereits erfolgtem Verlust: Vorsicht vor „Recovery“-Angeboten gegen Vorkasse.

FÜR UNTERNEHMEN

Zahlungsfreigaben ab definierter Schwelle an einen zweiten, unabhängigen Verifikationskanal koppeln. Video-Autorisierungen mit vorab vereinbarten Merkmalen prüfen. Mitarbeiterschulungen an aktuelle Deepfake-Maschen anpassen. Reaktionspläne vorab festlegen und testen.

IM VERDACHTSFALL

Zeitnahe Sicherung von Transaktionsdaten und frühzeitige forensische Nachverfolgung. Transaktions-Hashes, Wallet-Adressen und Off-Ramp-Bezüge sind on-chain dauerhaft — die Zuordnung zur Gegenpartei unterliegt jedoch Löschfristen bei Exchanges.

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

ANHANG · GLOSSAR

Pig Butchering / Sha Zhu Pan — Masche, bei der Opfer über längere Zeit emotional gebunden und schrittweise zu Investments in eine gefälschte Plattform bewegt werden. · **Agentische KI** — autonome Systeme, die mehrstufige Aufgaben ohne fortlaufende menschliche Steuerung ausführen. · **Multi-Agenten-Pipeline** — arbeitsteilige Architektur, in der KI-Agenten jeweils einen Teilschritt übernehmen. · **Structuring / Smurfing** — Aufteilung größerer Beträge in viele kleinere Transaktionen unterhalb von Meldeschwellen (31 U.S.C. § 5324). · **Layering / Wallet-Hopping** — Weiterleitung über mehrere Zwischenadressen zur Verschleierung. · **Peeling Chain** — Kette, bei der schrittweise kleine Beträge abgeschält werden. · **Common-Input-Ownership** — Annahme, dass Adressen, die gemeinsam als Input auftreten, demselben Akteur gehören. · **GNN** — Graph Neural Network; erkennt Muster direkt auf Transaktionsgraphen. · **Pareto-Grenze** — Menge der Strategien, bei denen keine Zielgröße ohne Verschlechterung einer anderen verbesserbar ist. · **Nested VASP** — Dienstleister, der über das Konto eines größeren VASP operiert und eigene KYC-Pflichten teilweise umgeht. · **Liveness-Detection** — Prüfung, ob eine reale, physisch anwesende Person und kein synthetisches Abbild vorliegt.

ANHANG C · METHODIK & QUELLEN

Dieses Whitepaper unterscheidet konsequent zwischen extern erhobenen, veröffentlichten Statistiken (Kapitel 3, als Zahlen Dritter gekennzeichnet) und qualitativen Beobachtungen aus der Fallarbeit von finanz-forensik.de (Kapitel 5–9), die ausdrücklich keine statistische Erhebung darstellen. Diese qualitative Herangehensweise ist in der Sicherheits- und Kriminalitätsanalyse etabliert — auch Europols IOCTA und BSI-Lageberichte stützen sich auf strukturierte Experteneinschätzungen. Das in Kapitel 7 entwickelte Modell ist ein analytischer Rahmen, keine empirisch validierte Theorie.

QUELLEN (AUSWAHL)

Chainalysis: 2026 Crypto Crime Report · FBI IC3: 2025 Internet Crime Report · Sumsub: Fraud Trends 2026; Identity Fraud Report 2025/2026 · Group-IB: Threat-Intelligence zu KI-Scam-Callcentern, 2026 · Europol: IOCTA; Einschätzungen zum Einsatz von Sprachmodellen, 2026 · BaFin: PM „Aufsichtsbehörden warnen vor Finanzbetrug mit KI und Kryptowerten“, 12.02.2026 · FATF: Virtual Assets Red Flag Indicators, 2020; Typologien 2026 · Meiklejohn u. a., „A Fistful of Bitcoins“, IMC 2013 · Möser/Böhme/Breuker, APWG eCrime 2013 · Weber u. a., arXiv:1908.02591, 2019 (Elliptic) · Toronto Police Service, „Project Déjà Vu“, 2026 · CFO Dive / Fortune / Gulf News: Arup-Deepfake-Fall, 2024.

Kombiniert öffentlich zugängliche Studien und Behördendaten mit qualitativen, anonymisierten Beobachtungen aus eigener forensischer Fallarbeit (Stand Juli 2026). Ersetzt keine Rechts- oder Anlageberatung. Alle schematischen Abbildungen sind illustrativ.

ÜBER DEN AUTOR

David Lüdtke

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

Auf Basis von Blockchain-Analyse-Tools und enger Zusammenarbeit mit Handelsplattformen und Strafverfolgungsbehörden rekonstruiert Finanz Forensik Geldflüsse, identifiziert Auszahlungspunkte und unterstützt bei der Vorbereitung von Auskunfts- und Einfrierungsersuchen. Zertifiziert als Crystal Expert (CECF · CEEI · CEUI). **Kontakt:** postfach@finanz-forensik.de · +49 6057 772 994 86 · 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 dient der allgemeinen Information und gibt den Diskussions- und Datenstand Juli 2026 wieder; es stellt keine Rechts-, Steuer- oder Anlageberatung dar.