



DIGITAL ASSET
INTELLIGENCE

RESEARCH REPORT
NR. 16 · 2026

COMPLIANCE · CROSS-RAIL-FORENSIK

Compliance-Blindstellen zwischen Krypto und Fiat

*Eine Qualitäts- und Schlüssigkeitsprüfung des Crystal-Intelligence-Reports
„Compliance Blindspots“ (2026), abgeglichen mit amtlichen und unabhängigen
Quellen – und was daraus für Ermittlungen und Compliance in Deutschland folgt.*

Compliance-Blindstellen zwischen Krypto und Fiat

Eine Qualitäts- und Schlüssigkeitsprüfung des Crystal-Intelligence-Reports „Compliance Blindspots“ (2026), abgeglichen mit amtlichen und unabhängigen Quellen – und was daraus für Ermittlungen und Compliance in Deutschland folgt.

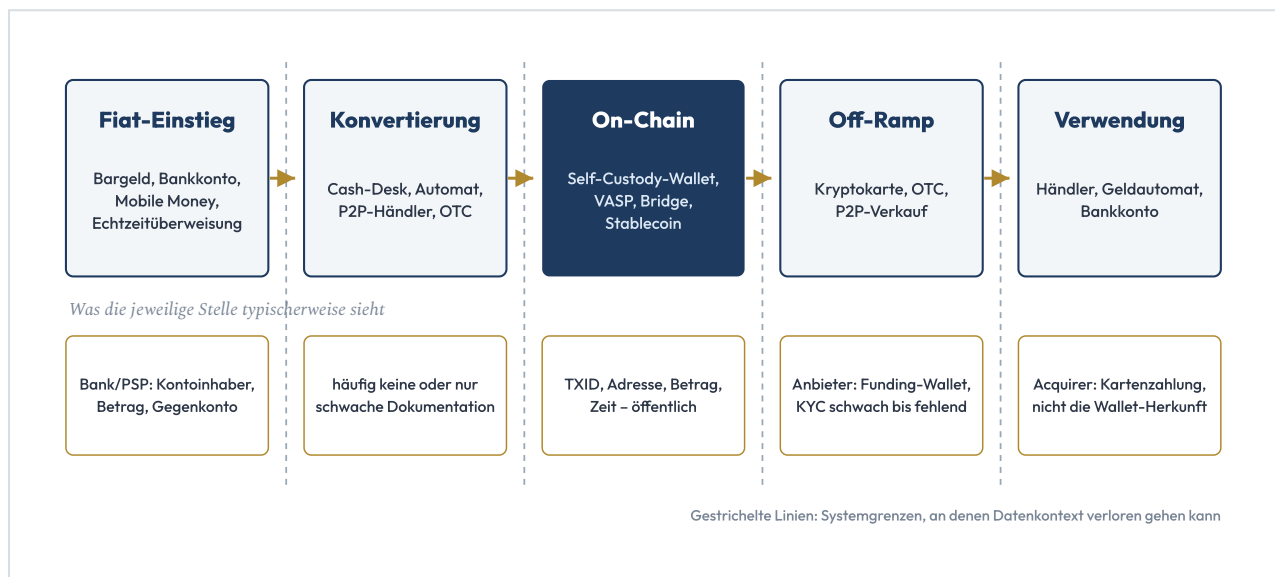


Abbildung 1: Die Cross-Rail-Kette. Jede Station sieht nur ihren Ausschnitt; an den Systemgrenzen geht Kontext verloren. Eigene Darstellung.

AUTOR	HERAUSGEBER
David Lüdtke Geschäftsführer · OSINT-Analyst & Krypto-Forensiker	Finanz Forensik GmbH finanz-forensik.de · postfach@finanz-forensik.de

Fachliche Analyse · erweiterte Deutschland-Fassung · Stand der Recherche: 24. September 2026 · keine Rechtsberatung im Einzelfall.
Fassung 2.1 ersetzt die Fassungen 1.0 und 2.0.

INHALT

- 01 Management Summary
- 02 Untersuchungsgegenstand und Methodik
- 03 Was Crystal tatsächlich zeigt
- 04 Qualitäts- und Schlüssigkeitsprüfung des Crystal-Reports
- 05 Externe Quellen: Wie weit lässt sich Crystal bestätigen?
- 06 Quellenmatrix: bestätigt, plausibel oder offen?
- 07 Deutschland: Markt, Regulierung und Ermittlungsrealität
- 08 Ein forensisches Modell für die Praxis: Cross-Rail Evidence
- 09 Red Flags und Indikatoren – richtig eingesetzt
- 10 Handlungsempfehlungen
- 11 Ausblick 2026/2027
- 12 Fazit
- 13 Quellen und weiterführende Literatur
- A Anhang: Nachrechnung der Crystal-Kennzahlen

01 Management Summary

Der Crystal-Intelligence-Report „Compliance Blindspots“ (veröffentlicht Juli 2026) beschreibt drei Übergangszonen, in denen klassische Blockchain-Analyse nur einen Teil des Risikobildes erfasst: physische Cash-to-Crypto-Dienste, die Abwicklung von P2P-Kryptogeschäften über Mobile-Money-Systeme und kryptofinanzierte Zahlungskarten. Die zentrale These – das größte Ermittlungs- und Complianceproblem liegt oft nicht innerhalb einer Blockchain, sondern an den Übergängen zwischen Zahlungswelten – ist überzeugend und wird von FATF, BIS, EBA, BaFin und FIU aus jeweils eigener Perspektive gestützt.

Die für diese Fassung vorgenommene Nachprüfung zeigt aber auch: Die These ist tragfähiger als ihre Zahlen. Mehrere Kennzahlen des Reports lassen sich intern nicht widerspruchsfrei nachrechnen, die Schlagzeilenwerte werden in einem Fall zu über 92 Prozent von Glücksspiel-Flüssen getragen, und die Länderauswahl für den Mobile-Money-Teil mischt Verbotsmärkte mit regulierten Märkten und bankbasierten Echtzeitsystemen. Für Gutachten und Compliance-Entscheidungen taugt der Report deshalb als Typologie und Suchhypothese – nicht als belastbare Mengenangabe.

83%

der befragten Jurisdiktionen mit Travel-Rule-Gesetz – 60 % davon (55 von 91) noch ohne Travel-Rule-Aufsichtsmaßnahme
FATF, Juli 2026

92,4%

des von Crystal ausgewiesenen High-Risk-Volumens bei Kryptokarten entfällt auf Glücksspiel
Crystal, eigene Nachrechnung

108.158

FIU-Verdachtsmeldungen digitaler
Finanzdienstleister 2025 (29 % aller
Meldungen)
FIU, Juli 2026

KERNURTEIL

Crystal identifiziert das richtige Problem, belegt es aber mit Zahlen, die teils nicht zusammenpassen, und formuliert einzelne Aussagen zu absolut. On-Chain-Daten beweisen weder die physische Bargeldübergabe noch den Zweck einer Mobile-Money-Zahlung. Sie können aber Risikobeziehungen sichtbar machen, sobald Wallets, Dienste, BIN-Strukturen oder Gegenparteien belastbar attribuiert sind. Die belastbarste Methode bleibt eine Cross-Rail-Forensik, die On-Chain-Analyse, OSINT, Provider-Attribution, Zahlungsdaten und rechtlich erlangte KYC-/Kontodaten zusammenführt – und für jede Aussage ihren Evidenzgrad offenlegt.

Die sieben wichtigsten Ergebnisse

- **Die Blindstelle ist ein Kontext-, kein Identitätsproblem.** Mobile-Money-Anbieter, Banken und Kartenprogramme kennen ihre Kunden häufig sehr wohl; ihnen fehlt der Zweck und das Folgeschehen. Für Ermittler heißt das: Die Identität ist oft per Auskunft erreichbar, der Zusammenhang muss forensisch hergestellt werden.
- **Interne Widersprüche im Crystal-Report.** Im Ägypten-Fallbeispiel weisen die Kennzahl-Kacheln Beträge aus (3,4 Mio. USD High-Risk-Zufluss, 534.000 USD Sanktionsbezug), die den im selben Diagramm genannten Gesamtzufluss von rund 452.000 USD um ein Vielfaches übersteigen. Auch die High-Risk-Summen im Kartenteil schwanken je nach Seite zwischen 161,7 und rund 167,6 Mio. USD.
- **Schlagzeilen- versus Substanzzisiko.** Von rund 166 Mio. USD High-Risk-Flüssen im Kartenteil entfallen 153,8 Mio. USD auf Glücksspiel. Sanktionen, Scams, gestohlene Mittel, Mixer, Darknet und Ransomware summieren sich zusammen auf etwa 13,8 Mio. USD; der Terrorfinanzierungsbezug beträgt rund 6.200 USD.

- **Konzentration statt Breite.** Ein einzelner Anbieter („Entity A“) steht für rund 479 Mio. USD Zuflüsse – etwa 40 Prozent des gesamten nachverfolgten Kartenvolumens von 1,18 Mrd. USD. Wachstumsaussagen für „den Markt“ sind damit stark von einem Akteur geprägt.
- **Die Regulierung verschiebt den Fokus auf ganze Konvertierungsketten.** FATF (März, Juli und September 2026), EU (TFR, MiCAR, ab Juli 2027 AMLR) und der deutsche Gesetzgeber (§ 15a GwG, GwGMeldV, KStTG) adressieren genau die Übergänge, die Crystal als blind beschreibt. Die Lücke liegt zunehmend im Vollzug, weniger im Recht.
- **Deutschland hat belegte und mögliche Entsprechungen der drei Kanäle:** Belegt sind illegal betriebene Krypto-Automaten (BaFin-Razzia 2024). Forensisch relevant, aber nicht als Krypto-Settlement nachgewiesen sind Echtzeitüberweisungen, Zahlungs-Apps und Neobank-Konten sowie Karten aus Drittstaaten-BINs. Für Marktvolumen und Verbreitung dieser drei Kanäle in Deutschland liegt keine belastbare amtliche Quantifizierung vor.
- **Für forensische Gutachten gilt:** Anbieterzahlen werden als Anbieterzahlen gekennzeichnet, vor Verwendung gegengerechnet und nur mit Datum, Bezugsbasis und Evidenzgrad zitiert. Jede Feststellung trägt einen Evidenztyp (On-Chain beobachtet, Provider-/Behördenauskunft, OSINT-korroboriert, Tool-Attribution, analytische Hypothese).

02 Untersuchungsgegenstand und Methodik

Gegenstand ist der 26-seitige Report „Compliance Blindspots – How criminals move value through the gaps between blockchain analytics, payment infrastructure, and physical cash conversion“ von Crystal Intelligence B.V. (Amsterdam), erschienen in der Reihe „Crystal Investigations“ mit Veröffentlichungsvermerk Juli 2026. Der Report fasst nach eigener Methodik drei zwischen Oktober 2025 und April 2026 veröffentlichte Crystal-Untersuchungen zusammen: eine physische Erhebung zu Cash-to-Crypto-Diensten, die Auswertung von 57.829 P2P-Anzeigen in zehn Märkten (November 2025 bis Januar 2026) sowie Blockchain-Forensik zu 45 VASPs (Januar 2023 bis Dezember 2025) und rund 120 Wallets aus dem Umfeld von knapp 100 Kartenanbietern (Januar 2024 bis Januar 2026).

Crystal weist selbst auf Grenzen hin: P2P-Anzeigen bilden Zahlungspräferenzen und keine bestätigten Volumina ab, VASP-Tracing erfasst keine Fiat-Werte, die Risikokategorisierung hängt von laufend aktualisierten Entity-Labels ab, und die Cash-Desk-Kartierung ist eine dokumentierte Teilmenge eines größeren Ökosystems.

2.1 Prüfverfahren dieser Fassung

Die Prüfung erfolgte in drei Schritten. Erstens wurden alle Kennzahlen des Reports gegeneinander nachgerechnet – Text gegen Grafik, Executive Summary gegen Detailseite, Summen gegen Einzelwerte (Anhang A). Zweitens wurde die Methodik auf Stichprobenlogik, Kategorienbildung und Bezugsbasen geprüft. Drittens wurden die Kernaussagen mit externen Quellen abgeglichen, wobei Gesetzestexte, Aufsichtsbehörden, FATF, BIS, Europol und amtliche deutsche Statistik Vorrang hatten.

BELEGKLASSE	BEDEUTUNG	BEHANDLUNG IM WHITEPAPER
A – Primärrecht / Aufsicht	Gesetz, Verordnung, Behördenleitlinie, FATF, BIS, Europol, FIU, Bundesbank	Belastbarer externer Referenzrahmen
B – Branchen- / Marktdaten	GSMA, Chainalysis, TRM Labs	Zur Größenordnung und Typologie; Methodik und Interessenlage beachten
C – Crystal-eigene Erhebung	Physisches Mapping, interne Entity-Labels, Provider-/BIN-Stichprobe	Originäre Crystal-Erkenntnis, nicht automatisch unabhängig verifiziert; nachgerechnet (Anhang A)
D – Investigative Recherche / Sekundärquellen	ICIJ, Fachmedien, Kanzlei- und Beraterpublikationen	Zur Kontextualisierung; Herkunft der Primärdaten wird geprüft und benannt

03 Was Crystal tatsächlich zeigt

3.1 Die strukturelle Lücke

Crystal beschreibt eine einfache, aber wichtige Systemgrenze: Banken, Kartennetzwerke, Mobile-Money-Anbieter und Kryptobörsen überwachen jeweils vor allem ihren eigenen Ausschnitt. Wird Wert zwischen diesen Systemen konvertiert, kann die Information über Herkunft, wirtschaftlichen Zweck oder Endnutzer verloren gehen. Dieselbe Zahlung kann in jedem Teilsystem unauffällig wirken: Eine P2P-Überweisung ist für den Mobile-Wallet-Anbieter eine inländische Zahlung; eine Einzahlung von einer Self-Custody-Adresse wirkt bei der Börse wie eine gewöhnliche Kryptoeinzahlung; eine Händlerzahlung verrät dem Acquirer nicht, welche Wallet die Karte zuvor finanziert hat.



Wert wechselt die Zahlungswelt – der Kontext bleibt zurück. An den Übergängen zwischen Bargeld, Bankkonto, Wallet und Karte entstehen die Blindstellen, die keine Einzelüberwachung schließt.

3.2 Die drei untersuchten Kanäle

KANAL	CRYSTAL-BEFUND	FORENSISCHE BEDEUTUNG
Cash-to-Crypto	Hunderte Dienste weltweit; Hongkong > 2,5 Mrd. USD Bargeldumsatz 2024; 33 % der identifizierten Aktivität mit Bezug zu unlicenzierten Börsen; 97 % der Mittel fließen weiter an große internationale Börsen.	Die Bargeldherkunft liegt vor dem sichtbaren On-Chain-Datensatz. Entscheidend ist die Attribution der Cash-Desk-Wallets. Die On-Chain-Analyse dieses Kanals kündigt Crystal erst für eine künftige Ausgabe an.
Mobile-Wallet-Settlement	57.829 P2P-Anzeigen in zehn Märkten; Mobile-Money-Anteil zwischen 48 % (Kolumbien) und 85 % (Elfenbeinküste); 45 VASPs mit 403 Mio. USD On-Chain-Flüssen.	Fiat-Zahlung und Kryptoerfüllung liegen in getrennten Systemen. Die Identität ist beim Wallet-Anbieter meist vorhanden, der Zweck nicht.
Kryptofinanzierte Karten	Knapp 100 Anbieter; 1,18 Mrd. USD On-Chain-Flüsse; 67,7 % ohne oder mit nur schwacher Identitätsprüfung; 54 BINs, davon 32 (59 %) mit No-KYC-Programmen; +66 % Zuflüsse 2025 gegenüber 2024.	Krypto wird in Kartenzahlungsfähigkeit überführt, bevor die Kartenüberwachung die Herkunft sieht. Die Funding-Wallet ist der letzte Punkt, an dem die Herkunft on-chain sichtbar ist.

ANALYTISCHER KERN

Die drei Kanäle unterscheiden sich technisch, folgen aber demselben Muster: Beim Übergang in ein anderes System wird der Datenkontext dünner. Entscheidend ist deshalb nicht, jedes Teilsystem maximal zu überwachen, sondern die Konvertierungspunkte zu identifizieren und Evidenz über Systemgrenzen hinweg zusammenzuführen.

04 Qualitäts- und Schlüssigkeitsprüfung des Crystal-Reports

Ein Anbieterbericht wird in Gutachten, Schriftsätzen und Compliance-Entscheidungen zitiert. Deshalb reicht es nicht, die Grundthese plausibel zu finden; die tragenden Zahlen müssen nachrechenbar sein. Die folgende Prüfung unterscheidet zwischen Befunden, die bestanden haben, und solchen, die vor einer Verwendung geklärt werden sollten. Die vollständige Nachrechnung enthält Anhang A.

4.1 Interne Konsistenz: Was sich nachrechnen lässt

Ein erheblicher Teil der Kennzahlen ist in sich stimmig. Die Einzelwerte der zehn Märkte summieren sich exakt auf 57.829 Anzeigen. Das Kartenwachstum von 66 Prozent ergibt sich präzise aus den Jahreswerten (689,8 gegenüber 415,5 Mio. USD). Die Anteile 67,7 Prozent (No-/Low-KYC), 87,9 Prozent (Website/SaaS) und 12,1 Prozent (Telegram) passen genau zu einer Grundgesamtheit von 99 Anbietern, also „knapp 100“. 32 von 54 BINs ergeben die angegebenen 59 Prozent.

4.2 Interne Konsistenz: Was nicht zusammenpasst

BEFUND	FUNDSTELLE IM REPORT	GEWICHT
Ägypten/Ebtoo – Größenordnung: Die Kacheln nennen 3,4 Mio. USD High-Risk-Zufluss (1,8 %), 1,4 Mio. USD mit Bezug zu illegalen Diensten und 534.000 USD Sanktionsbezug. Das Sankey-Diagramm derselben Seite weist aber nur 452.393 USD Gesamtzufluss aus; 1,9 % Sanktionsanteil entsprechen dort rund 8.600 USD. Die Kacheln setzen rechnerisch eine Basis von rund 189 Mio. USD voraus, die nirgends benannt ist.	S. 10	hoch
Ägypten/Ebtoo – Prozentwerte: Fließtext 2,9 % High-Risk-Zufluss (entspricht der Summe der roten Sankey-Kategorien), Kachel 1,8 %.	S. 10	mittel
Karten – High-Risk-Summe: Executive Summary „166 Mio. USD high-risk inflows“; Detailseite 161,7 Mio. USD; Tabellen-Gesamtsumme rund 167,6 Mio. USD, davon Eingang rund 162,9 Mio. USD; Prozentgrafik rechnet mit einer Basis von rund 166,4 Mio. USD.	S. 2, 13, 14	mittel
Karten – Ein- und Ausgang vermischt: Der Text nennt z. B. „3,8 Mio. USD mit Sanktionsbezug“ als Zufluss; laut Tabelle entfallen davon nur 2,55 Mio. USD auf Eingänge, 1,27 Mio. USD auf Ausgänge.	S. 13	mittel
BIN-Jurisdiktionen: Text: Hongkong 47 %, USA 16 %; Grafik: Hongkong 48 %, USA 19 %.	S. 15	gering
BIN-Zählung: 32 No-KYC-BINs (S. 14, 19) versus „22 unique BINs underpin every no-KYC crypto-card flow“ (S. 19) – das Verhältnis beider Zahlen wird nicht erklärt.	S. 14, 19	mittel
Bildunterschriften: Die Wachstumsgrafik der Karten trägt die Unterschrift der Mobile-Money-Grafik; die BIN-Grafik wiederholt die Unterschrift des Schemas.	S. 12, 15	gering (redaktionell)

4.3 Schlagzeile versus Substanz

Der Report stellt den High-Risk-Wert von rund 166 Mio. USD gleichrangig neben Sanktionen, Darknet, Ransomware und Terrorfinanzierung. Tatsächlich entfallen 153,8 Mio. USD (92,4 %) auf Glücksspiel. Online-Glücksspiel ist in vielen Rechtsordnungen erlaubnispflichtig oder verboten, in anderen legal – als Geldwäscheindikator ist es daher deutlich schwächer als ein Sanktions- oder Scam-Bezug. Die investigativ gewichtigen Kategorien summieren sich auf rund 13,8 Mio. USD, also gut ein Prozent der 1,18 Mrd. USD nachverfolgten Kartenflüsse. Der in der Executive Summary genannte Terrorfinanzierungsindikator beträgt rund 6.200 USD, davon 261 USD im Eingang.

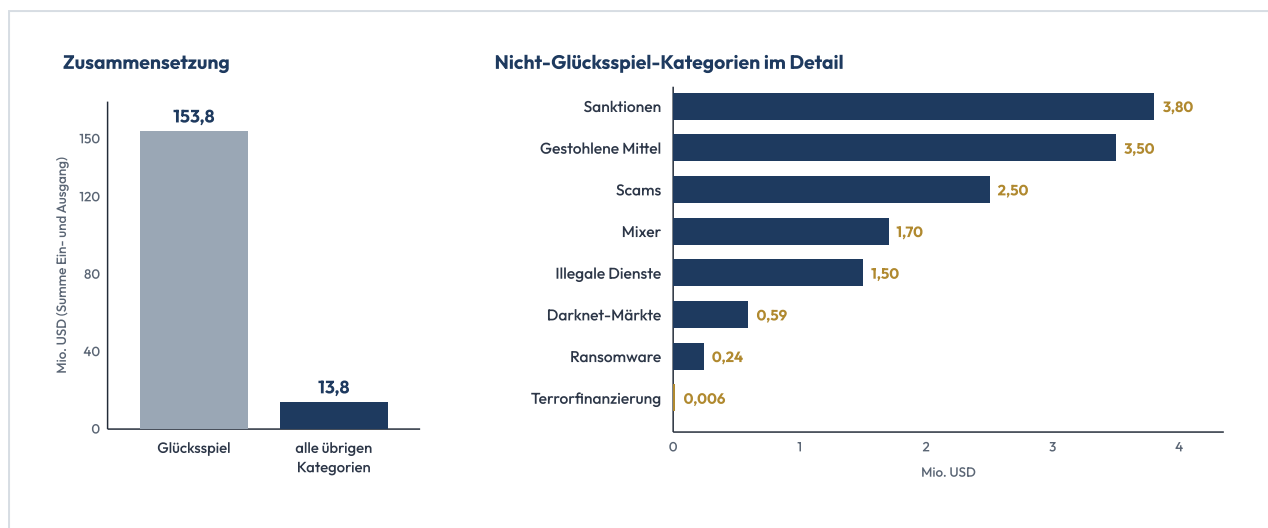


Abbildung 2: Zusammensetzung der von Crystal ausgewiesenen High-Risk-Flüsse bei Kryptokarten-Wallets (Summe aus Ein- und Ausgang). Datenquelle: Crystal Intelligence 2026, S. 13; eigene Darstellung.

Hinzu kommt eine starke Konzentration: „Entity A“, ein unlizenzierter Anbieter mit Sitz in Georgien, verbuchte auf TRON rund 478,8 Mio. USD Zuflüsse – etwa 40 Prozent aller von Crystal nachverfolgten Kartenflüsse. Ob das Marktwachstum von 66 Prozent breit getragen ist oder im Wesentlichen einen Anbieter widerspiegelt, lässt der Report offen.

4.4 Methodische Grenzen

- **Kategorienbildung „Mobile Financial Services“.** Für Indien zählt Crystal UPI und IMPS zu den mobilen Finanzdiensten. UPI ist ein kontobasiertes Echtzeitsystem, IMPS eine Interbanken-Überweisung; beide laufen über Bankkonten und sind nicht mit E-Geld-Wallets wie bKash oder Vodafone Cash vergleichbar. Indien stellt mit 18.147 Anzeigen gut 31 Prozent der Stichprobe und rund 34 Prozent aller als „mobil“ gewerteten Anzeigen. Die Aussage, die Zahlungen seien für den Anbieter „unsichtbar“, trifft auf bankbasierte Systeme so nicht zu.
- **„Verbotsmärkte“ als Rahmen.** Crystal erklärt die Verlagerung ins Mobile Money mit Kryptoverboten. Das passt für Ägypten, Algerien oder Bangladesch, aber nicht für alle zehn Märkte: Nigeria hat die Bankenrestriktion im Dezember 2023 aufgehoben und Digital Assets 2025 als Wertpapiere reguliert; Indien, die Philippinen oder Kolumbien kennen kein generelles Handelsverbot. Die Mobile-Money-Anteile dort spiegeln eher Zahlungsgewohnheiten als Verbotsumgehung. Die FATF-Übersicht vom Juli 2026 bestätigt die Mischung: Ägypten und Bangladesch geben ein Verbot an, Indien, Nigeria, Pakistan und die Philippinen nicht, Kolumbien ist unentschieden.
- **Identität vorhanden, Kontext fehlt.** Crystal beschreibt selbst eine „KYC-verifizierte“ Mobile-Money-Zahlung. Die Blindstelle ist deshalb vor allem eine Zweck- und Kontextlücke. Forensisch ist das eine gute Nachricht: Der Kontoinhaber ist per Auskunft grundsätzlich erreichbar.
- **Anzeigen sind keine Umsätze.** Anzahl der Anzeigen, Zahl der Händler und abgewickelter Volumen sind drei verschiedene Größen. Mehrfachanzeigen desselben Händlers und Plattformunterschiede werden nicht bereinigt ausgewiesen.
- **Herkunft der Hongkong-Zahl.** Für die 2,5 Mrd. USD Bargeldumsatz der Hongkonger Cash-Desks nennt der Report keine Herleitung (Hochrechnung, Selbstauskunft, On-Chain-Schätzung). Auch das ICIJ, das dieselbe Größenordnung berichtet, stützt sich auf Crystal; eine unabhängige Bestätigung existiert damit nicht.

- **Auswahlverzerrung.** Kartenanbieter wurden über Websites, SaaS-Plattformen und Telegram gefunden. Anbieter, die offen werben, sind überrepräsentiert; Aussagen über „den Markt“ sind Aussagen über den sichtbaren Teil des Marktes.
- **Innere Spannung der Kernaussage.** Einerseits heißt es, keine Blockchain-Analyse könne die Bargeldherkunft rückwirkend erkennen; andererseits soll Blockchain-Analyse die Kartenlücke „direkt“ schließen. Beides stimmt nur in einer engeren Fassung (siehe 4.5).
- **Interessenlage.** Der Report ist zugleich Forschungsarbeit und Produktkommunikation (Hinweis auf Crystal Expert, Demo-Angebot). Die Empfehlung, „physische Intelligence“ in Risikobewertungen zu integrieren, ist sachlich nachvollziehbar, deckt sich aber mit dem Leistungsangebot des Herausgebers. Das spricht nicht gegen die Befunde, wohl aber für eine unabhängige Gegenprüfung.

4.5 Präzisierung der zugespitzten Aussagen

WICHTIGE ABGRENZUNG

„Blockchain-Analyse kann die Bargeldherkunft nicht rückwirkend erkennen“ ist nur in enger Form richtig: Die Blockchain dokumentiert die physische Übergabe nicht. Sobald jedoch Wallets eines Cash-to-Crypto-Dienstes belastbar identifiziert sind, kann die On-Chain-Analyse zeigen, dass ein späterer Deposit direkt oder indirekt aus dieser Infrastruktur stammt. Was fehlt, ist der Beweis des konkreten Off-Chain-Vorgangs – nicht zwingend jede Risikospur.

Umgekehrt „schließt“ Blockchain-Analyse die Kartenlücke nicht allein: Sie zeigt die Herkunft der Funding-Wallet, nicht wer die Karte am Terminal einsetzt. Dafür braucht es Karten-, Issuer- und Acquirer-Daten.

4.6 Gesamturteil zur Schlüssigkeit

AUSSAGE	BELEGQUALITÄT	URTEIL
Compliance-Lücken entstehen an den Übergängen zwischen Zahlungssystemen	Durch FATF, BIS, EBA, BaFin, FIU extern gestützt	schlüssig
Cash-Desks speisen große Börsen mit „unauffälligen“ Einzahlungen (97 %)	Nur Crystal; Herleitung nicht offengelegt	plausibel, nicht verifiziert
Verbote verlagern P2P-Settlement in Mobile Money	Für einzelne Märkte plausibel; Länderauswahl und Kategorien uneinheitlich	teilweise schlüssig
Kryptokarten sind ein relevanter Off-Ramp mit schwacher KYC	Stichprobe von 99 Anbietern, Testregistrierungen	schlüssig als Typologie
166 Mio. USD High-Risk-Flüsse über Kryptokarten	Zu 92 % Glücksspiel; Summen inkonsistent	irreführend ohne Einordnung
Ägypten-Fallbeispiel (Ebtoo)	Kacheln und Diagramm um Größenordnungen verschieden	vor Verwendung klären

05 Externe Quellen: Wie weit lässt sich Crystal bestätigen?

5.1 FATF 2026: Drei Berichte, ein Befund

Im März 2026 warnte die FATF in ihrem Targeted Report zu Stablecoins und unhosted Wallets vor Risiken durch P2P-Transaktionen ohne regulierten Intermediär. Stablecoins seien auf über 250 Token und mehr als 300 Mrd. USD Marktkapitalisierung gewachsen; unter Berufung auf Chainalysis nennt die FATF einen Anteil von 84 Prozent am illegalen Transaktionsvolumen 2025. Einige Jurisdiktionen verlangen inzwischen, dass Emittenten Freeze- und Sperrfunktionen in Smart Contracts einbauen – für die Vermögenssicherung ein praktisch wichtiger Punkt.

Im Juli 2026 meldete die FATF in ihrem siebten Targeted Update, dass 83 Prozent (91 von 109) der befragten Jurisdiktionen Travel-Rule-Gesetze eingeführt haben, gegenüber 73 Prozent im Vorjahr. Zugleich hatten 60 Prozent dieser 91 Jurisdiktionen (55) zum Erhebungszeitpunkt noch keine Travel-Rule-bezogenen Feststellungen, Anordnungen, Aufsichts- oder Durchsetzungsmaßnahmen ergriffen (Rn. 25). Bemerkenswert: Die Executive Summary desselben Berichts spricht von „fast der Hälfte“ – ein Beispiel dafür, dass auch Primärquellen zwischen Zusammenfassung und Detailteil abweichen können und die Detailzahl maßgeblich ist. Die Angaben beruhen auf Selbstauskünften und wurden von der FATF nicht unabhängig verifiziert. Als fortbestehende Risikofelder nennt die FATF Stablecoins, Offshore-VASPs, selbst gehostete Wallets, OTC-Broker, Cross-Chain-Werkzeuge und DeFi – also im Kern die Crystal-Kanäle.

Am 3. September 2026 veröffentlichte die FATF einen Bericht zu Underground Banking und Hawala-ähnlichen Diensten (HOSSPs), den Deutschland gemeinsam mit Saudi-Arabien geleitet hat. Mehr als 80 Prozent der antwortenden Jurisdiktionen zählen diese Systeme zu den wichtigsten Kanälen professioneller Geldwäsche, knapp 90 Prozent bestätigen ihr Vorkommen, rund 70 Prozent berichten über zunehmenden Technikeinsatz. Die FATF definiert „digital hawala“ ausdrücklich unter Einbeziehung digitaler Zahlungssysteme und Kryptowerte und beschreibt Fälle mit mehr als 500 Mio. EUR, die binnen weniger Monate über bargeldbasierte Systeme bewegt wurden. Damit wird das Cross-Rail-Problem unabhängig bestätigt: Kriminelle bewegen Werte nicht in einem System, sondern zwischen mehreren.

5.2 EU, EBA und BaFin

Die EBA hat ihre ML/TF-Risikofaktorleitlinien auf Kryptowerte-Dienstleister erweitert und nennt Blockchain-Analytics ausdrücklich als Instrument der Risikominderung; die Leitlinien gelten seit Ende 2024 und erfassen auch Risiken aus selbst gehosteten Adressen. Die Transfer-of-Funds-Verordnung (EU) 2023/1113 und die EBA-Travel-Rule-Leitlinien verlangen Auftraggeber- und Begünstigtendaten bei Kryptotransfers. MiCAR verlangt für Kryptowerte-Dienstleistungen grundsätzlich eine Zulassung (mit der engen Ausnahme der Reverse Solicitation nach Art. 61); die EU-weite Übergangsfrist ist am 1. Juli 2026 ausgelaufen, in Deutschland bereits zum 31. Dezember 2025. Für Deutschland konkretisiert die BaFin in ihren Auslegungs- und Anwendungshinweisen die verstärkten Sorgfaltspflichten bei Transfers von oder zu selbst gehosteten Adressen (§ 15a GwG).

5.3 Mobile Money: Größenordnung bestätigt, Kryptonutzung nicht

Die GSMA weist für 2025 rund 2,3 Mrd. registrierte Mobile-Money-Konten, 593 Mio. monatlich aktive Konten und Transaktionen von mehr als 2 Billionen USD aus. Das belegt die Bedeutung von Mobile Money als Zahlungsinfrastruktur, bestätigt aber nicht Crystals länderspezifische P2P-Krypto-Anteile.

Zu beachten ist zudem die Definition: Bankbasierte Echtzeitsysteme wie UPI (Indien) oder Pix (Brasilien) fallen nicht unter Mobile Money im Sinne der GSMA. Crystals Kategorie ist damit weiter gefasst als die der Referenzquelle.

Eine hohe Mobile-Money-Nutzung ist kein Geldwäscheindikator. Relevant wird sie erst in Verbindung mit konkreten P2P-Krypto-Bezügen, unplausiblen Transfermustern, Gegenparteirisiken oder einer belegbaren Verbindung zu VASPs und unhosted Wallets.

5.4 BIS: Regulierungsarbitrage zwischen Zahlungsinstrumenten

BIS Paper 166 (März 2026) entwickelt einen Rahmen zur Bewertung von AML/CFT-Regimen über Bargeld, Bankgeld, Kryptowerte und digitales Zentralbankgeld hinweg und behandelt ausdrücklich Arbitrage zwischen den Instrumenten. Das ist konzeptionell nahezu deckungsgleich mit der Crystal-These: Unterschiedliche Pflichten verlagern Aktivität in den weniger überwachten Kanal. Bereits BIS Bulletin 111 (August 2025) schlug vor, die öffentliche Transaktionshistorie von Blockchains gezielt an den Kontaktpunkten zum Bankensystem zu nutzen. On-Chain-Transparenz ist also gerade an den Schnittstellen wertvoll, wenn sie mit Identitäts- und Zahlungsdaten verbunden wird.

5.5 Illicit-Volume-Daten: Rekordwerte, aber andere Treiber

TRM Labs schätzt das illegale Kryptovolumen 2025 auf 158 Mrd. USD (1,2 % des Gesamtvolumens), Chainalysis auf mindestens 154 Mrd. USD (unter 1 %). Beide Rekordwerte werden überwiegend von Sanktionsumgehung getragen, insbesondere vom rubelgedeckten Stablecoin A7A5. Bezeichnend für die Methodenabhängigkeit: Für denselben Token nennt Chainalysis ein Volumen von 93,3 Mrd. USD, TRM mehr als 72 Mrd. USD. Der oft zitierte Stablecoin-Anteil von 84 Prozent am illegalen Volumen spiegelt daher zu einem großen Teil staatlich organisierte Sanktionsumgehung wider und ist nicht ohne Weiteres auf Anlagebetrug oder die von Crystal untersuchten Kanäle übertragbar. In Berichten sind solche Werte als Anbieter-Schätzungen zu kennzeichnen.

5.6 Europol: Arbeitsteilige Infrastruktur, auch in Deutschland

Europol dokumentierte 2025 mehrere internationale Krypto-Betrugs- und Geldwäschenetzwerke. Im Juni 2025 wurde ein Investmentbetrugsnetzwerk mit mehr als 5.000 Opfern und rund 460 Mio. EUR gewaschenen Mitteln zerschlagen. Im Oktober und November 2025 folgten koordinierte Maßnahmen gegen ein Netzwerk mit mehr als 700 Mio. EUR gewaschenen Geldern – mit Durchsuchungen unter anderem in Deutschland – das neben gefälschten Handelsplattformen und Callcentern gezielt die Affiliate-Marketing-Infrastruktur der Betrugswerbung einschloss. Diese Fälle belegen nicht einen einzelnen Crystal-Kanal, bestätigen aber die operative Realität arbeitsteiliger, grenzüberschreitender Finanzinfrastrukturen.

06 Quellenmatrix: bestätigt, plausibel oder offen?

CRYSTAL-AUSSAGE	EXTERNE EVIDENZ	EINORDNUNG
Compliance-Lücke an Fiat/Krypto-Übergängen	FATF 2026a-d; BIS 2025/2026; EBA 2024; BaFin	Stark bestätigt
Unhosted Wallets / P2P erhöhen Sichtbarkeitsrisiken	FATF 2026a/b; EU-TFR; § 15a GwG	Stark bestätigt , aber risikobasiert zu behandeln; Self-Custody ist nicht per se illegitim
Mobile Wallets als Krypto-Settlement in bestimmten Märkten	GSMA bestätigt Skala; FATF „digital hawala“ bestätigt Cross-Rail-Nutzung	Strukturell plausibel ; Länderwerte nicht unabhängig verifiziert; Kategorie „mobil“ uneinheitlich
Mobile-Money-Zahlungen sind für Anbieter „unsichtbar“	Crystal selbst beschreibt KYC-verifizierte Transfers	Zu korrigieren : Identität vorhanden, Zweck fehlt
Hongkong-Cash-Desks > 2,5 Mrd. USD 2024	ICIJ berichtet dieselbe Größenordnung, stützt sich aber auf Crystal; Hongkong bereitet Lizenzregime für VA-Dealer vor (Gesetzentwurf 2026)	Plausibel , im Kern Crystal-basiert
67,7 % der Kartenanbieter ohne echte KYC	Keine gleichwertige unabhängige Stichprobe	Nicht unabhängig bestätigt ; intern konsistent
166 Mio. USD High-Risk-Flüsse über Kryptokarten	Crystal-Tabelle selbst: 92,4 % Glücksspiel	Einordnungsbedürftig ; Summen inkonsistent
Karten-BINs als Konzentrationspunkt	Karten-/Issuer-Struktur allgemein nachvollziehbar	Mechanismus plausibel , Zahlen proprietär
Stablecoins dominieren illegale On-Chain-Flüsse	FATF 2026a; Chainalysis 2026; TRM 2026	Bestätigt , aber stark von Sanktionsflüssen (A7A5) geprägt

07 Deutschland: Markt, Regulierung und Ermittlungsrealität

Crystal untersucht Schwellen- und Asienmärkte. Für deutsche Fälle ist die entscheidende Frage deshalb nicht, ob die Crystal-Zahlen hier gelten – sie gelten nicht –, sondern welche Entsprechungen die drei Kanäle im deutschen Zahlungsraum haben – und welche davon belegt, welche nur forensisch plausibel sind.

7.1 Belegte und mögliche Entsprechungen der drei Kanäle

CRYSTAL-KANAL	DEUTSCHE ENTSPRECHUNG	BELEGLAG E
Cash-to-Crypto	Belegt: illegal betriebene Krypto-Automaten (u. a. an Kiosken). Mögliche bzw. forensisch relevante Entsprechungen: Bargeld-OTC-Handel und unmittelbare Bargeldübergaben im Zusammenhang mit Kryptotransaktionen	BaFin-Razzia August 2024: 13 Krypto-Automaten an 35 Standorten beschlagnahmt, knapp 250.000 EUR Bargeld. Für physische OTC-/Cash-Desk-Strukturen liegt keine amtliche deutsche Volumenstatistik vor
Mobile-Wallet-Settlement	Mögliche Settlement-Rails im P2P-Kryptohandel: Echtzeitüberweisung, Zahlungs-Apps (z. B. PayPal, Wero), Neobank-Konten; Finanzagenten	Nicht als Krypto-Settlement belegt. Belegt ist nur die allgemeine Verbreitung (Bundesbank) und der Anstieg der FIU-Meldungen digitaler Finanzdienstleister 2025
Kryptofinanzierte Karten	Karten von Nicht-EU-Programmen (u. a. Hongkong- oder US-BINs), die an deutschen Terminals akzeptiert werden	Keine amtliche Zahl; Crystal nennt Westeuropa als Einsatzort im Fallbeispiel

7.2 Kennzahlen im Überblick

KENNZAH L / REGEL	DEUTSCHLAND 2024-2026	FORENSISCHE EINORDNUNG
FIU: Kryptobezug 2024	8.711 Verdachtsmeldungen; 3,3 % von 265.708	Kein Randphänomen; die Zahl misst Meldungen, nicht Straftaten
FIU: Kryptobezug 2025	Nicht mehr gesondert ausgewiesen	Zeitreihe bricht ab; Vergleich 2024/2025 nicht möglich
FIU: digitale Finanzdienstleister 2025	108.158 Meldungen; 29 % (2022: 43.190; 2023: 52.289; 2024: 34.357)	Zentraler Beobachtungspunkt für Betrug, Kontenkett en und Kryptotransfers
Bundesbank: Bargeld 2025	45 % der Alltagszahlungen; 71 % der Zahlungen zwischen Privatpersonen	Hybrider Zahlungsraum; Bargeld und Krypto zusammen denken
Bundesbank: Krypto-Nutzung 2025	4 % bereits gekauft/damit bezahlt; 10 % geplant	Überwiegend Investment, nicht Alltagszahlung
BaFin: Krypto-Automaten 2024	13 Automaten, 35 Standorte, ~250.000 EUR	Cash-to-Crypto existiert auch hier – ohne Volumenstatistik
GwGMeldV seit 1. März 2026	Blockchain-Transaktions-ID Pflichtangabe	Verdachtsmeldungen werden mit On-Chain-Daten verknüpfbar
MiCAR / K MAG	Übergangsfrist DE bis 31.12.2025; EU bis 1.7.2026	Zulassungsstatus als belastbarer OSINT-Prüfpunkt

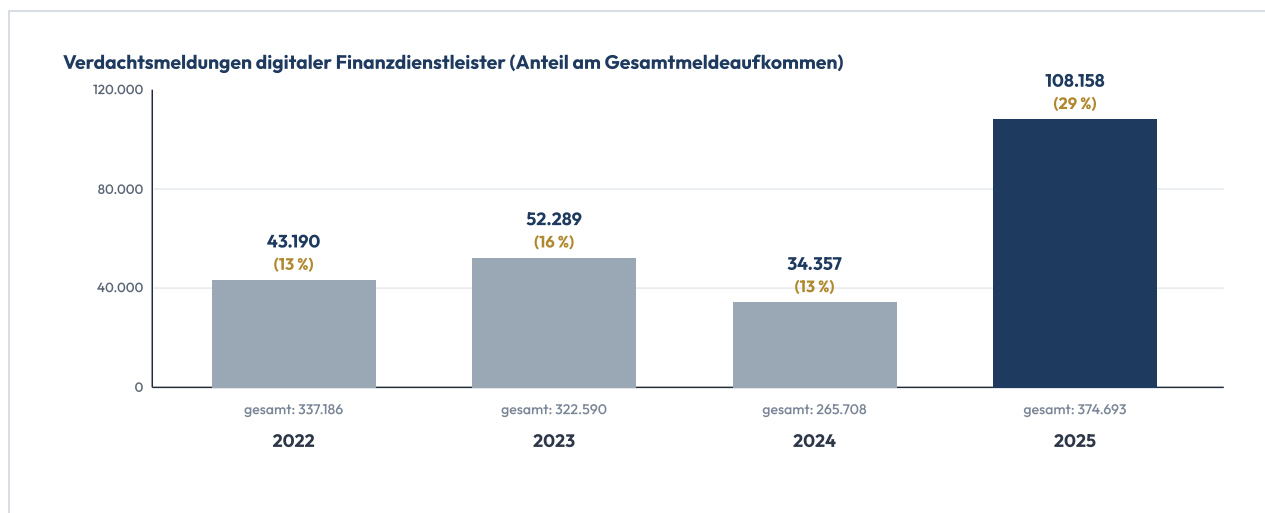


Abbildung 3: Verdachtsmeldungen digitaler Finanzdienstleister 2022–2025 mit Anteil am Gesamtmeldeaufkommen. 2024 war ein Tiefpunkt; gegenüber 2022 hat sich die Zahl etwa verzweieinhalbfacht, gegenüber 2024 mehr als verdreifacht. Quelle: FIU-Jahresbericht 2025, Tabelle 1. Eigene Darstellung.

7.3 FIU 2024 und 2025: Mehr Meldungen, weniger veröffentlichte Kryptokennzahlen

Der FIU-Jahresbericht 2024 wies 8.711 Verdachtsmeldungen mit Kryptobezug aus (3,3 % von 265.708 Meldungen) und machte Kryptowerte zum Schwerpunktthema. Am häufigsten genannt wurden Bitcoin, Ethereum, XRP, Tether und Litecoin; typische Anlässe waren Transfers zu Handelsplattformen, auffällige Wallet-Adressen und ungewöhnliche Transaktionsmuster.

Der im Juli 2026 veröffentlichte Jahresbericht 2025 verzeichnet 374.693 Verdachtsmeldungen (+41 %) mit rund 3,2 Mio. enthaltenen Transaktionen. Digitale Finanzdienstleister steigerten ihren Anteil auf 29 Prozent (2022 und 2024: je 13 Prozent, 2023: 16 Prozent); innerhalb dieses Segments steht Betrug und Untreue als Meldegrund vorn, kryptowertbezogene Auffälligkeiten folgen mit deutlichem Abstand. Die FIU führt das überproportionale Meldeaufkommen ausdrücklich auch auf eine erhöhte Risikoexposition zurück, unter anderem weil diese Anbieter kryptowertbezogene Transaktionen ermöglichen. Mit 106 Sofortmaßnahmen hielt die FIU Transaktionen von rund 751,8 Mio. EUR an. Eine gesonderte Gesamtzahl der Meldungen mit Kryptobezug veröffentlicht der Jahresbericht 2025 nicht mehr. Dadurch lässt sich aus der veröffentlichten Statistik nicht bestimmen, wie viele Betrugsverdachtsmeldungen zusätzlich einen Kryptobezug aufweisen; intern erstellt die FIU nach eigenen Angaben quartalsweise Sonderauswertungen zu Kryptowerten, bezeichnet deren Bedeutung für das Meldewesen als weiterhin hoch und hat ihr Anhaltspunktepapier zu Kryptowerten aktualisiert – die Ergebnisse werden im Jahresbericht aber nicht beziffert. Die seit März 2026 strukturiert erhobenen Kryptodaten könnten künftig wieder eine differenziertere statistische Auswertung ermöglichen, sofern die FIU entsprechende Kennzahlen veröffentlicht.

7.4 GwG-Meldeverordnung: Die TXID wird Pflicht

Die GwG-Meldeverordnung wurde am 1. September 2025 verkündet (BGBl. 2025 I Nr. 200) und ist am 1. März 2026 in Kraft getreten. Bei Transaktionen mit Kryptowerten tritt an die Stelle der Transaktionsnummer die Blockchain-Transaktions-ID; anzugeben sind zudem der Kryptowert, der Wechselkurs und der Anbieter. Nach § 4 GwGMeldV kann die FIU technische Verfahren einsetzen, um die Einhaltung der Formvorgaben und das Vorliegen der erforderlichen Angaben zu überprüfen. Nach Darstellung der FIU führt eine unterbliebene oder unvollständige Befüllung der Pflichtfelder in der Praxis dazu, dass die Meldung nicht übermittelt werden kann und technisch zurückgewiesen wird; bei

wiederholten oder systematischen Verstößen kommen aufsichtsrechtliche Maßnahmen in Betracht. Für Ermittlungen verbessert das die Anschlussfähigkeit zwischen Verdachtsmeldung und On-Chain-Analyse erheblich.

7.5 MiCAR und KMAG: Zulassung als Prüfpunkt

Die BaFin ist in Deutschland zuständige Behörde nach MiCAR. Nach § 50 KMAG erlosch die fortbestehende Erlaubnis für Altanbieter spätestens mit Ablauf des 31. Dezember 2025; EU-weit endete die Übergangsregelung am 1. Juli 2026. Seitdem ist der MiCAR-Zulassungs- oder Passporting-Status für alle an EU-Kunden gerichteten Angebote ein besonders belastbarer OSINT-Prüfpunkt (BaFin-Datenbank, ESMA-Register). Ein fehlender Zulassungsnachweis beweist für sich keine Straftat, ist bei einem an deutsche Kunden gerichteten Angebot aber ein relevanter Indikator für unerlaubte Geschäfte.

7.6 Self-Custody: § 15a GwG

Die Transfer-of-Funds-Verordnung gilt unmittelbar; § 15a GwG ergänzt sie. Anbieter müssen bei Kryptowertetransfers von oder zu selbst gehosteten Adressen das Geldwäsche-, Terrorismusfinanzierungs- und Sanktionsumgehungsrisiko ermitteln und angemessene Maßnahmen treffen – etwa die Identifizierung des Auftraggebers oder Begünstigten, die Ermittlung von Herkunft und Ziel der Kryptowerte oder eine verstärkte Überwachung. Nach § 10 GwG greifen bei Kryptowertetransfers außerhalb einer Geschäftsbeziehung ab 1.000 Euro die allgemeinen Sorgfaltspflichten. Self-Custody ist damit weder verboten noch automatisch verdächtig, löst aber eine dokumentierte, risikobasierte Prüfung aus.

7.7 Zahlungsverhalten: Deutschland bleibt hybrid

Laut Bundesbank-Studie 2025 (6.070 Befragte) wurden erstmals mehr Alltagszahlungen unbar als bar abgewickelt; Bargeld blieb mit 45 Prozent dennoch das meistgenutzte Einzelzahlungsmittel. Zwischen Privatpersonen liegt der Bargeldanteil bei 71 Prozent, 17 Prozent laufen über mobile oder Internetbezahlverfahren. Kreditinstitute im Euroraum müssen seit dem 9. Oktober 2025 auch das Versenden von Echtzeitüberweisungen anbieten; für Zahlungs- und E-Geld-Institute gilt eine längere Frist bis April 2027. Knapp ein Drittel der Befragten nutzt Echtzeitüberweisungen regelmäßig. Für P2P-Zahlungen nennen je rund 25 Prozent Überweisung bzw. PayPal als bevorzugtes Verfahren, Wero 1 Prozent – ein Kryptobezug wird dabei nicht erhoben.

4 Prozent haben Krypto-Token bereits gekauft oder damit bezahlt, weitere 10 Prozent planen es. Unter den Befragten mit Krypto-Erfahrung, also Personen, die Krypto-Token schon einmal gekauft oder damit bezahlt haben (n=139), gaben 92 Prozent an, die Token hauptsächlich zum Investieren zu nutzen. Wegen der kleinen Teilstichprobe ist dieser Wert vorsichtig zu verwenden. Für die Forensik folgt daraus: Der praktisch relevante Übergang ist häufiger Bankkonto → Börse/Wallet → Investment bzw. Rücktausch als die direkte Bezahlung mit Krypto. Ein- und Auszahlungswege sowie Self-Custody-Transfers sind besonders sorgfältig zu dokumentieren.

7.8 Deutsche Strafverfolgung: No-/Low-KYC-Infrastruktur ist real

Bei der Operation „Final Exchange“ schalteten BKA und ZIT im September 2024 47 in Deutschland gehostete Exchange-Dienste ab, denen bewusst mangelhafte KYC-Umsetzung vorgeworfen wurde. Ende April 2025 beschlagnahmten BKA und ZIT die Infrastruktur des Swapping-Dienstes eXch und sicherten Kryptowerte von rund 34 Mio. EUR sowie mehr als acht Terabyte Daten. Im August 2024 ging die BaFin mit Polizei und Bundesbank bundesweit gegen illegal betriebene Krypto-Automaten vor. Schnittstellenermittlungen sind in Deutschland damit gelebte Praxis.

7.9 BaFin-Warnungen: Plattformklone und Identitätsmissbrauch

BaFin-Warnungen aus 2025 dokumentieren serienmäßig aufgebaute, nahezu identische Investment-Websites ohne Erlaubnis sowie Identitätsmissbrauch zulasten etablierter Marktteilnehmer. Im August 2025 warnte die BaFin vor zwei Plattformreihen mit zusammen 28 damals bekannten Websites; in anderen Fällen behaupteten Betreiber wahrheitswidrig, Angebote stammten von der Börse Stuttgart bzw. der Baden-Württembergischen Wertpapierbörse. Domain-Historie, Impressum, Markenmissbrauch, Werbemittel und angebliche Lizenzangaben sind deshalb keine Nebeninformationen, sondern tragen die Off-Chain-Attribution.

7.10 Steuertransparenz: KStTG

Mit dem Kryptowerte-Steuertransparenz-Gesetz vom 22. Dezember 2025 (BGBl. 2025 I Nr. 352) hat Deutschland DAC8 umgesetzt; es ist am 24. Dezember 2025 in Kraft getreten. Die Sorgfalts- und Meldepflichten sind erstmals für das Kalenderjahr 2026 zu erfüllen. Anbieter müssen steuerliche Ansässigkeit feststellen und Transaktionsdaten jährlich bis zum 31. Juli des Folgejahres an das Bundeszentralamt für Steuern melden, erstmals also bis zum 31. Juli 2027. Die Daten erhöhen mittelfristig die Transparenz regulierter Anbieter, ersetzen aber weder strafprozessuale Auskünfte noch AML- und Blockchain-Analyse und erfassen private P2P-Transfers außerhalb meldepflichtiger Anbieter nicht.

7.11 Operation Chargeback: Zahlungsinfrastruktur als Teil der Tat

Der FIU-Jahresbericht 2025 stellt die Operation Chargeback als Schwerpunktfall dar: mehr als 4,3 Mio. betroffene Karteninhaber in 193 Ländern, ein geschätzter Schaden von über 300 Mio. EUR, rund 14 Mio. analysierte Transaktionen. Der Fall ist kein Kryptofall, zeigt aber dieselbe strukturelle Schwäche: Betrug, Zahlungsabwicklung, Scheinfirmen und Geldwäsche verteilen sich über mehrere regulierte Ebenen, sodass kein Beteiligter das Gesamtbild sieht.

WAS FÜR DEUTSCHLAND NICHT BELASTBAR BEZIFFERT IST

Keine amtliche deutsche Quelle quantifiziert das Volumen physischer Cash-to-Crypto-Umsätze, den Anteil von P2P-Kryptohandel über Echtzeitüberweisungen oder Zahlungs-Apps oder die Verbreitung von No-KYC-Kryptokarten in Deutschland. Die BaFin-Razzia belegt die Existenz illegaler Automaten, nicht deren Umsatz. Die Crystal-Zahlen dürfen daher nicht auf Deutschland hochgerechnet werden; sie sind als Typologie und Suchhypothese nutzbar, nicht als Prävalenznachweis.

08 Ein forensisches Modell für die Praxis: Cross-Rail Evidence

Aus der Analyse folgt ein erweitertes Ermittlungsmodell. Nicht die Blockchain allein, sondern die Verbindung der Beweisräume entscheidet. Ein belastbarer Fall sollte in fünf Ebenen dokumentiert werden:

EBENE	TYPISCHE DATEN	BEWEISFRAGE
1 • On-Chain	TXID, Adresse, Token, Betrag, Zeit, Chain, Smart-Contract- und Bridge-Interaktion	Was ist technisch nachweisbar passiert?
2 • Service-Attribution	Exchange-/VASP-Label, Kartenanbieter, BIN, Merchant, Bridge, Swap-Dienst	Welche Infrastruktur hat den Fluss übernommen?
3 • Off-Chain / OSINT	Websites, Domains, Messenger-Kanäle, Handelsregister, Lizenzstatus (BaFin, ESMA), Warnmeldungen	Wer steht hinter Dienst oder Infrastruktur?
4 • Zahlungs- und Identitätsdaten	Bankkonto, Echtzeitüberweisung, Mobile Wallet, Kartendaten, KYC, Login-/IP-Daten, Empfängerüberprüfung	Wer hat den Off-Chain-Schritt tatsächlich ausgeführt?
5 • Rechtliche Sicherung	Freeze-Anfrage, Auskunftersuchen, Sicherungsbeschluss, Rechtshilfe, Emittenten-Freeze bei Stablecoins	Wie wird aus Analyse eine verwertbare Maßnahme?

8.1 Evidenzgrade und Formulierungen

Damit eine probabilistische Wallet-Zuordnung nicht unbemerkt zur Tatsachenbehauptung wird, sollte jede zentrale Feststellung einen Evidenzgrad tragen. Bewährt hat sich eine fünfstufige Skala mit festen Formulierungen:

GRAD	GRUNDLAGE	FORMULIERUNGSBEISPIEL IM GUTACHTEN
E1 • On-Chain beobachtet	Reproduzierbare Transaktionsdaten	„Die Adresse X hat am ... Y USDT an Adresse Z übertragen (TXID ...).“
E2 • Behörden- oder Providerauskunft	Auskunft, KYC-Daten, Beschluss	„Nach Auskunft des Anbieters vom ... ist Inhaber des Kontos ...“
E3 • OSINT-korroboriert	Mehrere unabhängige offene Quellen	„Mehrere voneinander unabhängige Quellen ordnen die Domain ... dem Betreiber ... zu.“
E4 • Tool-Attribution	Label eines Analyseanbieters, mit Datum und Version	„Das Analysewerkzeug ... ordnet die Adresse (Stand ...) dem Dienst ... zu.“
E5 • Analytische Hypothese	Muster, Zeitkorrelation, Plausibilität	„Die zeitliche und betragsmäßige Übereinstimmung spricht dafür, dass ... Alternative Erklärungen: ...“

8.2 Zeitkorrelation als Brücke zwischen Systemen

Bei Echtzeitüberweisungen, Mobile Wallets, Karten und P2P-Handel ist die Zeitachse entscheidend. Gleiche oder korrespondierende Beträge, kurze Abstände, wiederkehrende Frequenzen und identische Gegenparteimuster können eine Hypothese stützen, ersetzen aber keine Identitätsfeststellung. Gute Berichte zeigen die Korrelation, nennen alternative Erklärungen und benennen die Auskunft, die den Zusammenhang verifizieren würde. Seit der schrittweisen Einführung der Empfängerüberprüfung bei Überweisungen in Euro (ab Oktober 2025) kann zudem das Ergebnis des Namensabgleichs ein zusätzlicher Anknüpfungspunkt sein.

8.3 Prüfschema für Anbieterstudien in Gutachten

Die Befunde aus Kapitel 4 lassen sich zu einem kurzen Prüfschema verallgemeinern, das vor jeder Übernahme einer Anbieterzahl in ein Gutachten oder eine Risikobewertung durchlaufen werden sollte:

- **Version und Datum:** Welche Fassung des Reports, welcher Datenstand, welcher Label-Stand?
- **Bezugsbasis:** Worauf bezieht sich der Prozentwert – Eingang, Ausgang oder Summe; Anbieter, Wallets oder Transaktionen?
- **Text-Grafik-Abgleich:** Stimmen Fließtext, Kacheln, Tabellen und Diagramme überein?
- **Stichprobe:** Wie wurde ausgewählt, wie groß ist sie, welche Verzerrungen sind naheliegend?
- **Zusammensetzung:** Welche Kategorie treibt den Schlagzeilenwert?
- **Konzentration:** Wie viel des Volumens entfällt auf einzelne Akteure?
- **Unabhängige Bestätigung:** Gibt es eine Quelle, die nicht auf denselben Daten beruht?
- **Interessenlage:** Ist die Studie zugleich Produktkommunikation?

09 Red Flags und Indikatoren – richtig eingesetzt

Crystal liefert praxisnahe Indikatoren. Ihre Stärke liegt in der Kombination, nicht in der isolierten Anwendung. Einzelmerkmale wie TRON-Nutzung, Self-Custody, Mobile Money oder runde Beträge sind für sich genommen kein Nachweis illegaler Aktivität. Die letzten drei Zeilen ergänzen deutsche Konstellationen.

INDIKATOR	WARUM RELEVANT	NICHT ÜBERINTERPRETIEREN
Neue Self-Custody-Wallet → schneller CEX-Deposit	Kann auf Cash-Desk- oder Intermediärnutzung hindeuten	Auch legitime Nutzer legen neue Wallets an und zahlen zeitnah ein
Viele kleine Zuflüsse → wenige große Abflüsse	Typisch für Aggregation, Brokerage, Sammelstrukturen	Kann legitime Zahlungsaggregation abbilden
Regelmäßige runde Beträge	Kann Off-Chain-Preis- oder Bargeldschwellen widerspiegeln	Allein schwach
P2P / Mobile Money + VASP-Bezug	Verbindet Fiat-Rail mit Kryptoerfüllung	Mobile Money ist massenhaft legitime Infrastruktur
TRON/BSC + Stablecoins	Niedrige Gebühren begünstigen schnelle, hochfrequente Transfers	Chainwahl ist kein Schuldindikator
No-/Low-KYC-Kartenanbieter	Schwache Identitätsbindung am Karten-Off-Ramp	Providerstatus und KYC-Praxis aktuell verifizieren
Bridge, Mixer, Chain-Hopping nach Deliktzufluss	Kann Layering verstärken	Bridges und DeFi sind auch legitime Standardfunktionen
DE: Serie von Echtzeitüberweisungen an Privatpersonen mit zeitnahe Kryptokauf beim Empfänger	Typisches Muster von P2P-Händlern und Finanzagenten	Auch private Kleinanzeigen- oder Familienzahlungen möglich
DE: Paper-Wallet oder Einzahlung nach Automatenkauf	Hinweis auf nicht zugelassene Automaten	Zugelassene, bankbetriebene Automaten existieren
DE: Kartenzahlung mit Drittstaaten-BIN aus Krypto-Funding	Off-Ramp außerhalb der EU-Aufsicht	BIN-Herkunft allein ist kein Verdacht

10 Handlungsempfehlungen

10.1 Für Ermittlungsbehörden und forensische Analysten

- **Nicht beim Exchange-Label stoppen:** Nach jedem identifizierten On-/Off-Ramp prüfen, welcher Fiat-, Karten-, Mobile-Money-, Echtzeit- oder OTC-Kanal dahinterstehen kann.
- **Service-Attribution versionieren:** Screenshots, Tool-Version, Datum und alternative Labels dokumentieren, weil sich Zuordnungen und Risikokategorien ändern.
- **Off-Chain-Beweisanforderungen früh formulieren:** Welche KYC-, IP-, Karten-, BIN-, Kontoinhaber- oder Merchant-Daten werden benötigt, um die On-Chain-Hypothese zu verifizieren?
- **Cross-Chain-Flüsse in einer Zeitleiste abbilden:** Bridge-Ausgang, Zielchain, Stablecoin-Swap und nachgelagerte Cash-Out-Adresse gemeinsam betrachten.
- **Sicherungsfähigkeit mitdenken:** Je näher der Fluss an einem regulierten Anbieter oder einem freeze-fähigen Stablecoin-Emittenten liegt, desto höher die Chance auf Sicherung – Zeit ist entscheidend.
- **Anbieterzahlen prüfen, bevor sie zitiert werden:** Prüfschema aus Abschnitt 8.3 anwenden.

10.2 Für Börsen, CASPs, Banken und Zahlungsdienstleister

- Risikobewertung nicht auf direkte Gegenparteien beschränken, sondern bekannte Offshore-, No-KYC- und Cash-to-Crypto-Infrastruktur als Kontext einbeziehen.
- Self-hosted Transfers nicht pauschal blockieren, sondern nach Herkunft, Ziel, Geografie, Gegenpartei und Muster differenzieren (§ 15a GwG).
- BIN-, Issuer- und Kartenprogrammrisiken mit On-Chain-Attribution verbinden, wo kryptofinanzierte Karten betroffen sind.
- Travel-Rule-Daten, Blockchain-Analytics und klassische Payment-Fraud-Signale in einer gemeinsamen Fallansicht zusammenführen.
- Verdachtsmeldungen vollständig nach GwGMeldV befüllen, insbesondere TXID, Kryptowert, Kurs und Anbieter.

10.3 Für Geschädigtenvertretung und Kanzleien

- Neben Wallet-Adresse und TXID immer auch Fiat-Belege sichern: IBANs, Echtzeitüberweisungsbelege einschließlich Ergebnis der Empfängerüberprüfung, Kartenabrechnungen, Zahlungs-App-Quittungen, Chats und Zeitstempel.
- Im Gutachten klar benennen, welche Stelle den Übergang in ein reguliertes System darstellt und welche Auskunft dort beantragt werden sollte.
- Die gesamte Beweiskette bis zu juristisch adressierbaren Gegenparteien aufbereiten, nicht nur den letzten sichtbaren Wallet-Hop.
- Begriffe wie „Täterwallet“ nur bei belastbarer personeller Zuordnung verwenden; sonst neutral von Empfangsadresse, Zwischenwallet, Cluster oder Service-Wallet sprechen.

10.4 Für Aufsicht und Gesetzgebung

- Kryptobezug in der FIU-Statistik wieder gesondert ausweisen – auf Basis der seit März 2026 strukturiert erfassten TXIDs.
- Die Settlement-Schicht (Echtzeitüberweisungen, Zahlungs-Apps, Neobanken) als eigenständiges Typologiefeld für P2P-Kryptohandel behandeln.
- Den Vollzug der Travel Rule und der MiCAR-Zulassungspflicht gegenüber Offshore-Anbietern priorisieren; die Rechtslage ist weitgehend vorhanden.

11 Ausblick 2026/2027

TERMIN	ENTWICKLUNG	BEDEUTUNG FÜR DIE BLINDSTELLEN
seit 24.12.2025	KStTG (DAC8) in Kraft; Pflichten ab Kalenderjahr 2026, erste Meldung bis 31.7.2027	Mehr Steuerdaten regulierter Anbieter; keine P2P-Abdeckung
seit 1.3.2026	GwGMeldV: TXID als Pflichtangabe	Verknüpfbarkeit Verdachtsmeldung ↔ Blockchain
seit 1.7.2026	EU-weites Ende der MiCAR-Übergangsfrist	An EU-Kunden gerichtete Dienstleistungen grundsätzlich zulassungspflichtig, soweit keine Ausnahme greift (insb. Reverse Solicitation, Art. 61 MiCAR)
2026	Hongkong: Gesetzentwurf für Lizenzen von VA-Dealern (OTC) und Verwahrern; Inkrafttreten offen	Könnte den von Crystal beschriebenen Cash-Desk-Markt formalisieren
10.7.2027	EU-Geldwäscheverordnung (AMLR) anwendbar; Art. 79: Verbot anonymer Konten einschließlich anonymer Kryptowertekonten und von Konten, die die Anonymisierung des Inhabers oder eine erhöhte Verschleierung von Transaktionen ermöglichen, ausdrücklich auch über anonymitätsverstärkende Coins; Art. 80: Barzahlungsobergrenze 10.000 EUR	Verlagert Druck weiter auf nicht regulierte P2P- und Offshore-Kanäle
2027/2028	AMLA (Sitz Frankfurt) koordiniert die europäische AML/CFT-Aufsicht; Auswahl der direkt beaufsichtigten Unternehmen 2027, direkte Aufsicht über bis zu 40 ausgewählte grenzüberschreitende Hochrisiko-Finanzunternehmen bzw. -gruppen ab 2028	Direkte EU-Aufsicht bleibt auf wenige große Akteure begrenzt; die Masse der Anbieter bleibt national beaufsichtigt
offen	Crystal kündigt On-Chain-Analysen zu Cash-Desks in einer Folgeausgabe an	Nachprüfung der 97%-Aussage wird möglich

Mit dichterer Regulierung der etablierten Übergänge steigt das Risiko einer Verlagerung in nicht regulierte P2P-Strukturen, Offshore-Dienste und digitale Hawala-Netzwerke. Das ist eine Einschätzung (Evidenzgrad E5), keine gemessene Tatsache; gestützt wird sie durch die FATF-Befunde zur Verbindung von Bankkonten, Fintechs, Instant Payments, Mobile Wallets und virtuellen Vermögenswerten. Für die Forensik bedeutet das eher mehr als weniger Schnittstellenarbeit.

12 Fazit

Crystal Intelligence trifft mit „Compliance Blindspots“ einen zentralen Punkt der modernen Finanzforensik: Die schwierigsten Stellen sind oft nicht die transparenten Blockchain-Transaktionen, sondern die Momente, in denen Wert zwischen Bargeld, Bank- oder Mobile-Money-Systemen, unhosted Wallets, VASPs und Karteninfrastruktur wechselt. Die externe Quellenlage 2026 stärkt diese Diagnose deutlich – bis hin zum FATF-Bericht vom September 2026 über digitale Hawala-Strukturen.

Als Datenquelle hält der Report dagegen einer genauen Prüfung nur teilweise stand. Größenordnungsfehler im Ägypten-Fallbeispiel, schwankende High-Risk-Summen, eine von Glücksspiel dominierte Schlagzeilenzahl und eine uneinheitliche Mobile-Money-Kategorie verbieten

es, einzelne Werte ungeprüft in Gutachten zu übernehmen. Für Deutschland gelten die Zahlen ohnehin nicht; hier liefern FIU, Bundesbank, BaFin und BKA eigene Anknüpfungspunkte, während die Quantifizierung der drei Kanäle weiterhin fehlt.

Die Konsequenz ist keine Abkehr von Blockchain-Forensik, sondern ihr Ausbau: On-Chain-Reproduzierbarkeit, Off-Chain-Attribution, Zahlungsdaten, OSINT, regulatorischer Status und eine gerichtsfest dokumentierte Beweiskette – verbunden durch offen ausgewiesene Evidenzgrade. Nicht „mehr Daten“ schließen die Blindstelle, sondern die saubere Verbindung der richtigen Datenräume. ■

Die Blockchain zeigt den Geldfluss. Die Identität entsteht an den Schnittstellen. Forensische Qualität entsteht dort, wo beides sauber verbunden, jede Zahl nachgerechnet und der Evidenzgrad jeder Aussage offengelegt wird.

LEITSATZ

13 Quellen und weiterführende Literatur

UNTERSUCHTER REPORT

Crystal Intelligence (2026): Compliance Blindspots: How criminals move value through the gaps between blockchain analytics, payment infrastructure, and physical cash conversion. Crystal Investigations, veröffentlicht Juli 2026, 26 S. – crystalintelligence.com/resources/compliance-blindspots-crypto-fiat-conversion-risk-2026/

INTERNATIONALE STANDARDS UND AUFSICHT

FATF (2026a): Targeted Report on Stablecoins and Unhosted Wallets – Peer-to-Peer Transactions. 3. März 2026. – fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html

FATF (2026b): Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. 16. Juli 2026 (insb. Rn. 24–25 und Annex A). – fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html

FATF (2026c): Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers. 11. März 2026. – fatf-gafi.org/en/publications/Virtualassets/Understanding-Mitigating-Risks-Offshore-VASPs.html

FATF (2026d): Investigating Professional Money Laundering, Underground Banking, and the Use of HOSSPs. 3. September 2026. – fatf-gafi.org/en/news/pml-underground-banking-hawala-hospps-2026.html

BIS (2026): From cash to crypto: towards a consistent regulatory approach to illicit payments. BIS Papers No 166, 3. März 2026. – bis.org/pub/bppdf/bisap166.htm

BIS (2025): An approach to anti-money laundering compliance for cryptoassets. BIS Bulletin 111, August 2025. – bis.org/publications/bulletin-111-approach-anti-money-laundering-compliance-cryptoassets

EBA (2024a): Guidelines on ML/TF risk factors – extension to crypto-asset service providers. 16. Januar 2024. – eba.europa.eu/publications-and-media/press-releases/eba-issues-guidance-crypto-asset-service-providers

EBA (2024b): Travel Rule Guidelines under Regulation (EU) 2023/1113. 4. Juli 2024. – eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and

Europol (2025a): Crypto investment fraud ring dismantled in Spain after defrauding 5,000 victims worldwide. 30. Juni 2025. – europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide

Europol (2025b): International takedown of cryptocurrency fraud network laundering over EUR 700 million. 4. Dezember 2025; ergänzend eucrim 4/2025. – europol.europa.eu/media-press/newsroom/news/international-takedown-of-cryptocurrency-fraud-network-laundering-over-eur-700-million

EU-RECHT

Verordnung (EU) 2023/1113 über Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte (TFR). – eur-lex.europa.eu/eli/reg/2023/1113/oj/eng/pdf

Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCAR), insbesondere Art. 59 und Art. 143 Abs. 3. – eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

Verordnung (EU) 2024/1624 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche (AMLR), anwendbar ab 10. Juli 2027, insbesondere Art. 79 (anonyme Konten) und Art. 80 (Barzahlungsobergrenze). – eur-lex.europa.eu/eli/reg/2024/1624/oj

Verordnung (EU) 2024/886 zu Echtzeitüberweisungen in Euro (Angebotspflicht, gestaffelte Fristen, Empfängerüberprüfung). – eur-lex.europa.eu/eli/reg/2024/886/oj

DEUTSCHLAND

FIU (2025): Jahresbericht 2024 – 265.708 Verdachtsmeldungen, davon 8.711 mit Kryptobezug. Veröffentlicht 10. Juni 2025. – zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2024.pdf?__blob=publicationFile&v=7

FIU (2026): Jahresbericht 2025 – 374.693 Verdachtsmeldungen; Tabelle 1 (digitale Finanzdienstleister 2022–2025); Abschnitt 3.1.1 (GwGMeldV); Abschnitt 5.1 (Sonderauswertungen Kryptowerte). Veröffentlicht Juli 2026. – zoll.de/SharedDocs/Downloads/DE/Links-fuer-Inhaltseiten/Fachthemen/FIU/fiu_jahresbericht_2025.pdf?__blob=publicationFile&v=2

Deutsche Bundesbank (2026): Zahlungsverhalten in Deutschland 2025. Stand Juli 2026. – bundesbank.de/de/publikationen/berichte/studien/zahlungsverhalten-in-deutschland-2025-997848

BaFin (2024): Pressemitteilung „BaFin-Razzia gegen Betreiber von Krypto-Automaten“, 20. August 2024. – bafin.de/SharedDocs/Veroeffentlichungen/DE/Pressemitteilung/2024/pm_2024_08_20_Krypto_Automaten.html

BaFin (2025a): Auslegungs- und Anwendungshinweise zum GwG, Stand Juli 2025, Abschnitt 7.6 (selbst gehostete Adressen). – bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_auas_2025_gw.pdf

BaFin (2025b): Warnung vor Plattformreihe „tägliche Gewinne zwischen 780 und 1800“, 19. August 2025. – bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/unerlaubte/2025/neu/meldung_2025_08_19_plattformreihe_tae_gliche_gewinne_zwischen_780_und_1800.html

BaFin (2025c): Warnung vor Plattformreihe „Verdienst für deutsche Staatsbürger von 200 bis 950“, 19. August 2025. – bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/unerlaubte/2025/neu/meldung_2025_08_19_plattformreihe_verdienst_fuer_deutsche_staatsbuergervon_200_bis_950.html

BaFin (2025d): Interactive Assets – Identitätsmissbrauch zulasten der Börse Stuttgart, 12. Februar 2025. – bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/unerlaubte/2025/meldung_2025_02_12_Interactive_Assets.html

BaFin: Kryptowerte-Dienstleistungen nach MiCAR – Zulassung, Aufsicht und Passporting. – bafin.de/DE/unternehmen-maerkte/erlaubnis-registrierung/geschaeft-krypto/kryptowerte-dienstleistungen/kryptowerte-dienstleistungen.html

BKA/ZIT (2024): 47 in Deutschland gehostete Exchange-Services abgeschaltet („Final Exchange“), 19. September 2024. – bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240919_PM_finalexchange.html

BKA/ZIT (2025): Krypto-Swapping-Dienst eXch abgeschaltet, 9. Mai 2025. – bka.de/DE/Presse/Listenseite_Pressemitteilungen/2025/Presse2025/250509_exch_abgeschaltet.html

GwG §§ 10, 15a; GwGMeldV (in Kraft seit 1. März 2026), insb. § 3 mit Anlage und § 4; – gesetze-im-internet.de/gwgmeldv/BJNR0C80A0025.html

KMAG, insbesondere § 50 (Übergangsvorschrift). – gesetze-im-internet.de/kmag/BJNR1B60B0024.html

KStTG vom 22. Dezember 2025 (BGBl. 2025 I Nr. 352, verkündet 23.12.2025), in Kraft seit 24. Dezember 2025; Pflichten erstmals für das Kalenderjahr 2026. – gesetze-im-internet.de/ksttg/BJNR1600B0025.html

MARKT- UND BRANCHENDATEN

GSMA (2026): State of the Industry Report on Mobile Money 2026. 24. März 2026. – gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/the-state-of-the-industry-report-on-mobile-money-2026/

Chainalysis (2026a): 2026 Crypto Crime Report – Introduction. – chainalysis.com/blog/2026-crypto-crime-report-introduction/

Chainalysis (2026b): Crypto Sanctions – 2026 Crypto Crime Report. – chainalysis.com/blog/crypto-sanctions-2026/

TRM Labs (2026): 2026 Crypto Crime Report. – trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report

INVESTIGATIVE RECHERCHE UND KONTEXT

ICIJ (2025): Crypto-to-cash services open up a new dirty money world (Coin Laundry). Die Hongkong-Zahl wird dort Crystal zugerechnet. – icij.org/investigations/coin-laundry/crypto-cash-desk-currency-exchange-money-laundering/

Hong Kong FSTB/SFC (2025/2026): Konsultationsschlussfolgerungen zu Lizenzregimen für VA-Dealing und -Verwahrung; Gesetzentwurf für 2026 angekündigt. – fstb.gov.hk/fsb/en/publication/consult/consult-policy.html

UNODC (2024): Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia. – unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

HINWEIS ZUR QUELLENKRITIK

Analyseanbieter wie Crystal, Chainalysis und TRM Labs arbeiten mit proprietären Entity-Datenbanken; ihre Volumenangaben sind nicht automatisch vergleichbar und werden hier zur Typologie- und Größenordnungseinordnung verwendet, nicht als amtliche Statistik. Sekundärquellen (Fachmedien, Kanzlei- und Beraterpublikationen) wurden nur zur Bestätigung von Primärangaben herangezogen. Bei gerichtlicher oder behördlicher Verwendung sind die fallbezogenen Transaktionsdaten und reproduzierbaren Nachweise entscheidend.

A Anhang: Nachrechnung der Crystal-Kennzahlen

Die folgende Tabelle dokumentiert die Nachrechnung. Seitenangaben beziehen sich auf die im Report aufgedruckten Seitenzahlen.

PRÜFPUNKT	ANGABE IM REPORT	NACHRECHNUNG	ERGEBNIS
P2P-Anzeigen gesamt	57.829 (S. 7, 23)	Summe der zehn Länderwerte = 57.829	stimmig
Gewichteter Mobile-Anteil	nicht angegeben	≈ 61 % über alle Anzeigen; ohne Indien ≈ 59 %	ergänzend
Anteil Indien an Stichprobe	18.147 Anzeigen (S. 8)	31,4 % aller Anzeigen; ≈ 34 % der als mobil gewerteten	Gewichtung beachten
Kartenwachstum 2025	+66 % (S. 12)	689,8 / 415,5 = 1,660	stimmig
Kartenvolumen gesamt	1,18 Mrd. USD (Jan 2024–Jan 2026)	2024 + 2025 = 1.105,3 Mio. USD; Rest ≈ 75 Mio. USD auf Januar 2026	plausibel, nicht direkt belegt
KYC-Anteile	67,7 % / 87,9 % / 12,1 % (S. 13)	= 67 / 87 / 12 von 99 Anbietern	stimmig
No-KYC-BIN- Anteil	32 von 54 = 59 % (S. 14)	59,3 %	stimmig
High-Risk-Karten gesamt	166 Mio. (S. 2); 161,7 Mio. (S. 13)	Tabellensumme ≈ 167,6 Mio.; Eingang ≈ 162,9 Mio.; Prozentbasis ≈ 166,4 Mio.	inkonsistent
Glücksspielanteil	92,4 % (S. 14)	153,8 / 166,4 = 92,4 %	stimmig bei Basis 166,4
Nicht-Glücksspiel- Kategorien	nicht angegeben	≈ 13,8 Mio. USD (Summe Ein-/Ausgang)	ergänzend
Entity A	478,8 Mio. USD Zufluss (S. 16)	≈ 40,6 % von 1.180 Mio. USD	Konzentration
Ebtoo Gesamtzufluss	452.393 USD (S. 10)	Sanktionsanteil 1,9 % ≈ 8.600 USD	–
Ebtoo Kacheln	3,4 Mio. (1,8 %); 534.000 USD Sanktionen	Implizite Basis ≈ 189 Mio. USD	Widerspruch zu 452.393 USD
BIN-Jurisdiktion	Text: HK 47 %, US 16 % (S. 15)	Grafik: HK 48 %, US 19 %	abweichend

AUTOR



David Lüttke

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

David Lüttke ist Geschäftsführer der Finanz Forensik GmbH, OSINT-Analyst und Krypto-Forensiker. Schwerpunkte sind Blockchain-Forensik, Wallet-Analyse, OSINT-gestützte Vermögensermittlung und die nachvollziehbare Aufbereitung digitaler Geldflüsse für Kanzleien, Unternehmen und Ermittlungsstellen.

Die Finanz Forensik GmbH verbindet technische Blockchain-Analyse mit OSINT und strukturierter Beweisdokumentation. Der Schwerpunkt liegt auf der Nachverfolgung digitaler Vermögenswerte, der Einordnung von Wallet- und Dienstleisterbeziehungen sowie der Aufbereitung verwertbarer Ermittlungsansätze für Kanzleien, Unternehmen und Behörden.

ARBEITSFELD	SCHWERPUNKT
Krypto-Forensik	Transaktionsnachverfolgung, Wallet-Strukturen, Cross-Chain- und Cash-Out-Analyse
OSINT	Anbieter-, Domain-, Firmen- und Infrastrukturrecherche sowie Lizenz- und Warnhinweise
Dokumentation	Nachvollziehbare Berichte mit vollständigen Hashes, Quellenangaben und klar getrennten Evidenzstufen

KONTAKT

Finanz Forensik GmbH · finanz-forensik.de · postfach@finanz-forensik.de · Stand: 24. September 2026

Herausgeber: Finanz Forensik GmbH · Würzburger Str. 59, 63639 Flörsbachtal · HRB 100521, Amtsgericht Hanau · USt-IdNr. DE454473675 · Geschäftsführung: Lydia Bonhard-Lüdtke, David Lüdtke. Fassung 2.1, Stand 24. September 2026. Zitiervorschlag: Finanz Forensik GmbH, Compliance-Blindstellen zwischen Krypto und Fiat, Fassung 2.1, 2026. Dieses Whitepaper dient der allgemeinen Information; es stellt keine Rechts-, Steuer- oder Anlageberatung dar und begründet kein Mandatsverhältnis. © 2026 Finanz Forensik GmbH — alle Rechte vorbehalten.