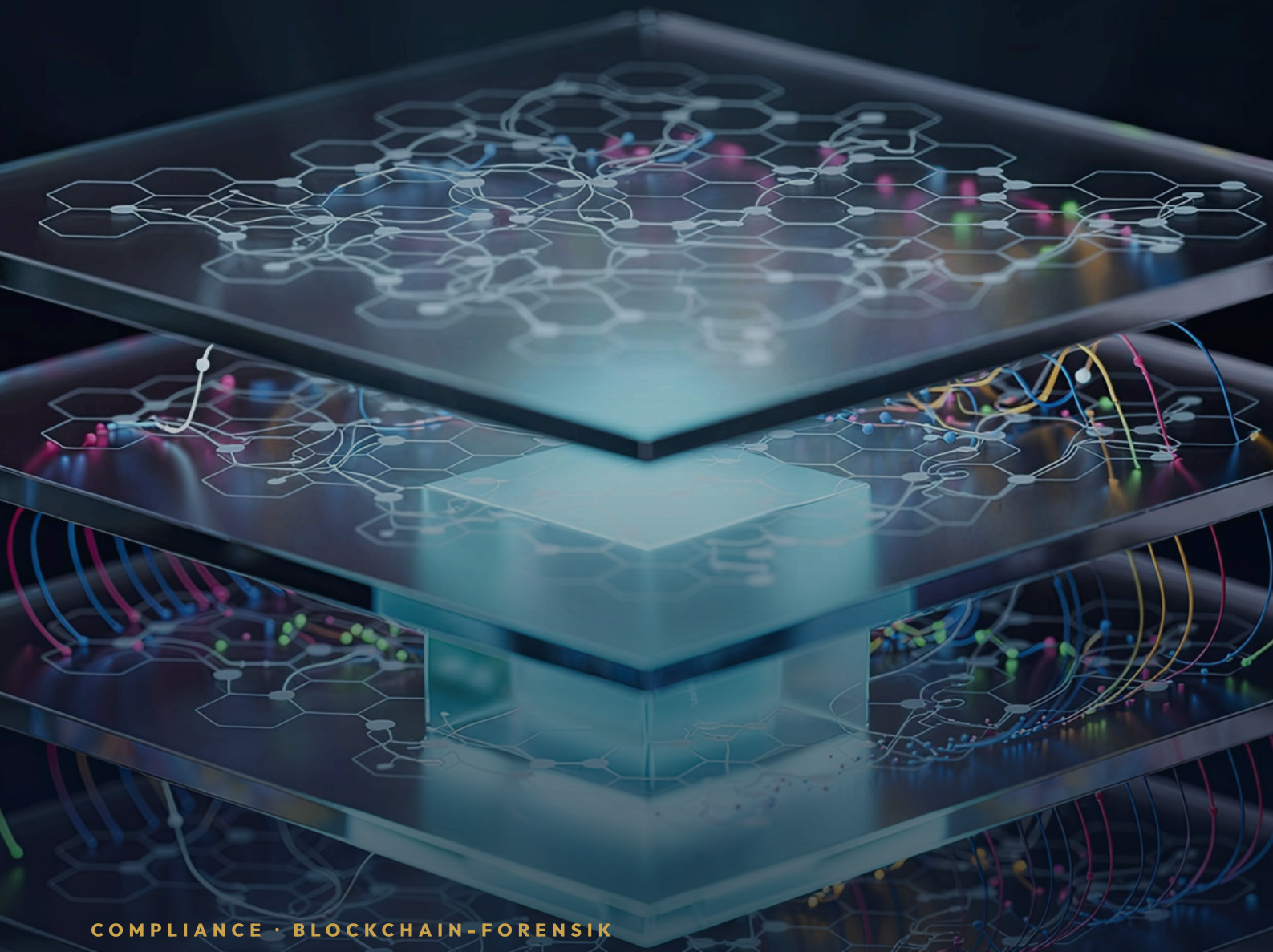
DIGITAL ASSET
INTELLIGENCE

RESEARCH REPORT
NR. 19 · 2026



COMPLIANCE · BLOCKCHAIN-FORENSIK

Nested Services im Kryptomarkt

Verdeckte Intermediäre, Compliance-Lücken und neue Ansätze der Blockchain-Forensik

FORSCHUNGSFOKUS

Warum die sichtbare Kryptobörse nicht zwingend der tatsächliche wirtschaftliche Transaktionsdienstleister ist – und welche Folgen dies für Ermittlungen, Sanktionskontrollen, Compliance und die Bewertung von Zahlungsflüssen hat.

WHITEPAPER · STAND: 15. OKTOBER 2026

FINANZ FORENSIK GMBH · FINANCIAL INTELLIGENCE

WHITEPAPER · OKTOBER 2026

Nested Services im Kryptomarkt

Verdeckte Intermediäre, Compliance-Lücken und neue Ansätze der Blockchain-Forensik

FINANZ·FORENSIK · FINANCIAL INTELLIGENCE & BLOCKCHAIN FORENSICS RESEARCH REPORT 19 / 2026

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

Eigenständiges Research-Whitepaper · Stand: 15. Oktober 2026

FORSCHUNGSFOKUS

Warum die sichtbare Kryptobörse nicht zwingend der tatsächliche wirtschaftliche Transaktionsdienstleister ist – und welche Folgen dies für Ermittlungen, Sanktionskontrollen, Compliance und die Bewertung von Zahlungsflüssen hat.

Quellenbasis: Originalanalyse von Crystal Intelligence (August 2026), FATF, EBA, EU-Recht, BaFin und US-Finanzministerium. Eigene Leistung: unabhängiger Quellenabgleich, methodische Prüfung, Risikoeinordnung und forensisches Prüfmodell.

INHALT

— Executive Summary
01 Begriff und technische Funktionsweise
02 Marktumfang: Was die Zahlen tatsächlich belegen
03 Kritischer Quellencheck und Grenzen
04 Regulatorische Entwicklung und eigenständiger Abgleich
05 Eigene forensische Typologie
06 Praktischer Ermittlungsworkflow
07 Fallkonstellationen und Ermittlungsnutzen
08 Risikobewertung für Verpflichtete
09 Empfehlungen mit Umsetzungspriorität
10 Konfidenz- und Evidenzstandard
— Fazit
— Methodik und Quellennachweise

Executive Summary

Nested Services sind Krypto-Dienstleister, die ihre Kunden über Konten, Wallets oder Liquiditäts- und Zahlungsinfrastruktur anderer Anbieter bedienen. Eine On-Chain-Transaktion lässt deshalb häufig die Host-Börse erkennen, nicht aber den tatsächlich kundenführenden Zwischenanbieter oder dessen Endkunden. Diese Unschärfe kann sowohl reguläre Geschäftsmodelle als auch Hochrisikoaktivitäten betreffen. [1]

7,97 Mrd. USD
Bruttotransaktionsvolumen 2017–2025
Crystal Intelligence

2.275.270
erfasste Transaktionen
Crystal Intelligence

39
Host-Börsen, 2.052 zugeschriebene Wallet-Adressen
Crystal Intelligence

87,4 %
des erfassten Volumens entfallen auf einen Host
Crystal Intelligence

Crystal Intelligence erfasst in einem Datensatz für 2017 bis 2025 etwa 7,97 Mrd. USD Bruttotransaktionsvolumen, 2.275.270 Transaktionen, 2.052 zugeschriebene Wallet-Adressen und 39 Host-Börsen. 87,4 % des erfassten Volumens entfallen laut Studie auf einen Host. Diese Zahlen beschreiben die von Crystal identifizierte Teilmenge – weder den gesamten Markt noch nachgewiesene illegale Geldflüsse. [1]

Die eigene Recherche zeigt, dass das Thema inzwischen ausdrücklich in internationalen Standards und europäischen Aufsichtsleitlinien adressiert wird. Die FATF behandelt regulatorische Lücken bei Offshore-VASPs und der indirekten Nutzung regulierter Plattformen; die EBA-Leitlinien und die EU-Travel-Rule verlangen risikoadäquate Sorgfalt und den Umgang mit fehlenden Transferinformationen. [2–6]

ZENTRALE ERKENNTNISSE

- Ein regulierter Host ist kein Beleg dafür, dass alle dahinterliegenden Endkunden gleichwertig überprüft wurden.
- „Nested“ ist eine Infrastruktur- und Geschäftsmodellbeschreibung, keine strafrechtliche Bewertung.
- On-Chain-Cluster, Zahlungsrhythmen und Sweep-Muster sind Indikatoren; belastbare Zuschreibung erfordert zusätzliche Bestätigung.
- Die Ermittlungsfrage lautet nicht allein „Zu welcher Börse floss das Geld?“, sondern „Welcher Dienstleister kontrollierte die Kundenbeziehung und wer initiierte den Transfer?“.
- Ein belastbares Prüfverfahren muss Attribution, rechtliche Einordnung und Sicherung der Belege strikt trennen.

01 Begriff und technische Funktionsweise

Ein Nested Service kann als Broker, OTC-Desk, Swap-Service, Zahlungsabwickler oder informelle Wechselstelle tätig sein und für Einzahlungen oder Auszahlungen Infrastruktur eines größeren Virtual Asset Service Provider (VASP) beziehungsweise Crypto-Asset Service Provider (CASP) nutzen. Für Nutzer tritt der kleinere Anbieter als unmittelbarer Vertragspartner auf, während die Blockchain an einer relevanten Stelle nur ein Konto oder eine Hot-Wallet des Hosts zeigt. [1]

MODELL	KENNZEICHEN	HAUPTPROBLEM
Offengelegtes Hosting	Formale Geschäftskundenbeziehung zwischen Nested Service und Host	Host kennt die Geschäftsbeziehung, aber nicht zwangsläufig jeden Endkunden
Nicht offengelegtes Hosting	Als Privat- oder Normalkonto geführte Infrastruktur für Drittgeschäfte	Kundenvolumen und tatsächliche Dienstleisterrolle können verschleiert werden
Hybrides / mehrstufiges Hosting	Eigene Wallets und fremde Börsenkonten werden kombiniert	Zurechnung und Zuständigkeiten über mehrere Ebenen erschwert

Wesentlich ist die Unterscheidung von drei Identitätsebenen: Kontoinhaber beim Host, operativer Betreiber der kundenorientierten Plattform und wirtschaftlich handelnder Endkunde. Keine dieser Ebenen darf ohne Beleg mit einer anderen gleichgesetzt werden.



Abbildung 1: Drei Identitätsebenen bei Nested Services. *Die Blockchain zeigt in der Regel nur die äußere Ebene. Eigene Darstellung.*

02 Marktumfang: Was die Zahlen tatsächlich belegen

KENNZAHL	CRYSTAL-AUSWERTUNG 2017–2025	EINORDNUNG
Bruttovolumen	**7,97 Mrd. USD**	Kumulierte Zu- und Abflüsse; kein Nettoschaden
Transaktionen	**2.275.270**	Erfasster Analysebestand, keine Vollerhebung
Wallet-Adressen	**2.052**	Attributionsgrundlage des Datensatzes
Host-Börsen	**39**	Als Host genutzte Börsen laut Crystal
Host-A-Konzentration	**87,4 % (ca. 6,97 Mrd. USD)**	Starke Konzentration im Datensatz; Ergebnisse maßgeblich von einem Host geprägt
Historischer SUEX-Fall	**1,86 Mrd. USD separat**	Aus Crystal-Gesamtsumme ausgenommen

Zahlen und Methodik: *Crystal Intelligence, August 2026, S. 9–16, 23, 30. [1]*

Die Verteilung über die Jahre zeigt, warum neben dem Volumen auch die Transaktionsanzahl betrachtet werden muss: Crystal meldet für 2021 einen Volumengipfel von 2,64 Mrd. USD und 236.558 Transaktionen; 2025 hingegen 1.090.185 Transaktionen bei 941 Mio. USD. Der rechnerische

Durchschnittsbetrag je Transaktion ist damit von rund 11.200 USD auf rund 860 USD gefallen. Für Monitoring-Systeme kann deshalb eine reine Konzentration auf Großbeträge unzureichend sein. [1]

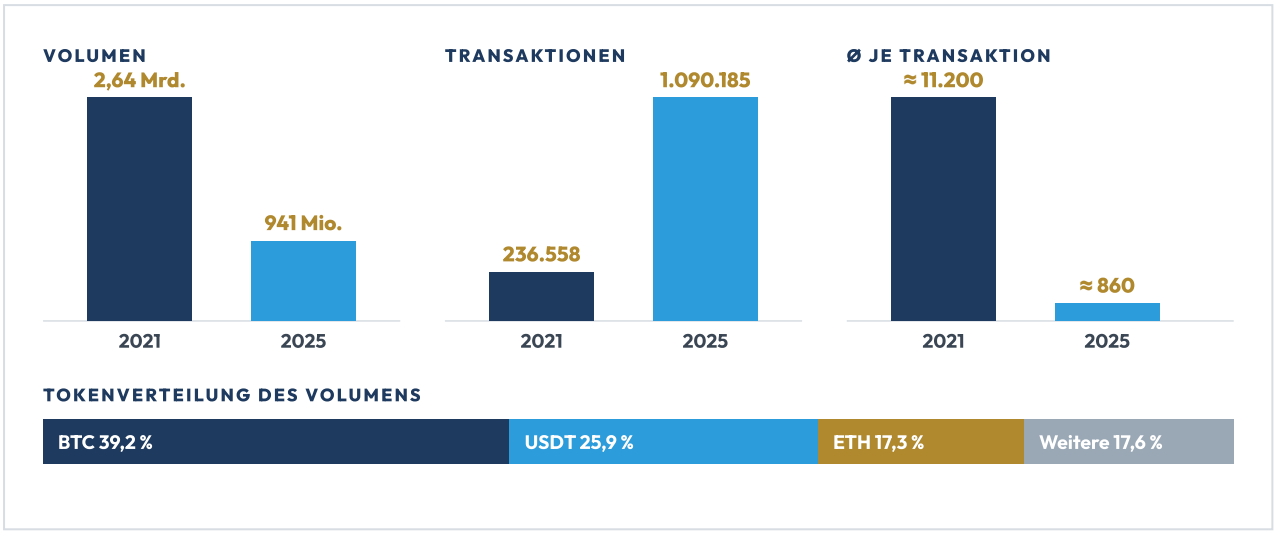
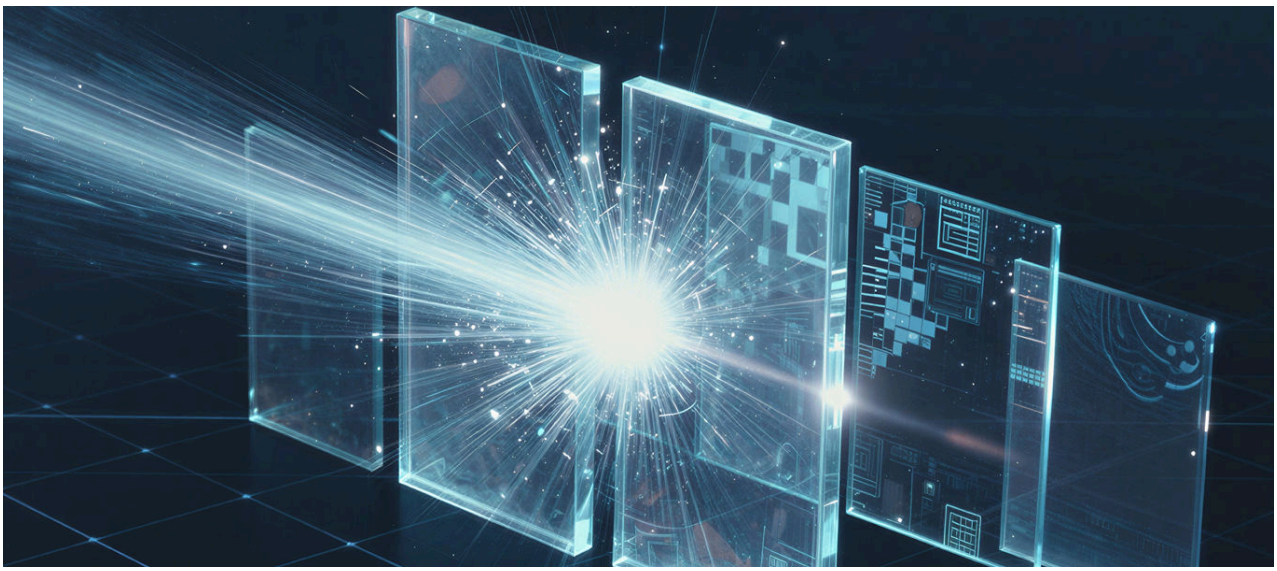


Abbildung 2: Mehr Transaktionen, kleinere Beträge. *Volumen in USD, Transaktionsanzahl und rechnerischer Durchschnittsbetrag je Transaktion 2021 und 2025 sowie Tokenverteilung des Volumens. Daten: Crystal Intelligence, August 2026 [1]; eigene Darstellung.*

Crystal ordnet etwa 39,2 % des Volumens BTC, 25,9 % USDT und 17,3 % ETH zu; die übrigen 17,6 % entfallen auf weitere Token. Diese Tokenverteilung kann auf unterschiedliche Geschäftsmodelle und Transferkosten hindeuten, sagt aber nichts über die Legalität eines einzelnen Transfers aus. [1]

03 Kritischer Quellencheck und Grenzen

Die Crystal-Zahlen beruhen auf einer proprietären Attributionsdatenbank. Eine unabhängige Replikation der 2.052 Adressen, der vollständigen Entity-Liste und sämtlicher Transfers ist ohne zugrunde liegende Adress- und Transaktionsdaten nicht möglich. Die hier vorliegende Recherche bestätigt daher die Konsistenz zentraler öffentlich prüfbarer Regulierungs- und Sanktionsaussagen, nicht die Vollständigkeit des proprietären Datensatzes.



VERÖFFENTLICHUNGS- UND ZITIERHINWEIS

Der Crystal-Report wird als Drittquelle mit Titel, Erscheinungsmonat und Seitenstellen ausgewiesen. Aus ihm werden keine Originalgrafiken und keine umfangreichen Passagen übernommen.

PRÜFPUNKT 1 – BRUTTOZÄHLUNG

Gemäß Crystal werden absolute Zu- und Abflüsse an zugeschriebenen Adressen summiert. Daraus kann eine Doppelzählung wirtschaftlich derselben Gelder in Ketten oder wiederholten Transfers entstehen. Das Ergebnis ist weder eine Schätzung der kriminellen Erträge noch des tatsächlichen wirtschaftlichen Nettovolumens. [1]

PRÜFPUNKT 2 – ZÄHL- UND ZUORDNUNGSGRENZEN

Der Report nennt 17 dem Iran zugeordnete Entitäten, während die sichtbare Kennzeichnung NS-04 bis NS-19 nur 16 Codes umfasst; der Anhang verweist auf eine weitere, nicht vollständig einzeln ausgewiesene Entität. Außerdem bleiben die Host-Kürzel anonymisiert. Diese Punkte sind als Transparenzgrenzen und nicht als eigenständig verifizierte Sachverhalte zu behandeln. [1]

PRÜFPUNKT 3 – JURISDIKTION UND SANKTIONEN

Eine geografische Iran-Zuordnung allein erlaubt keine pauschale Aussage, jede Person oder jede Transaktion sei weltweit verboten. Konkrete Rechtsfolgen hängen unter anderem von beteiligten Personen, Gütern, zuständigem Recht, US-Bezug, Ausnahmen und Listenstatus ab. Die weitreichende Formulierung des Ausgangsreports wird hier deshalb nicht übernommen.

PRÜFPUNKT 4 – VERHALTENSSIGNALE

Sweeps, Sammelwallets und geringe Restbestände sind auch bei legitimen Custody-, Payment- oder Treasury-Systemen üblich. Sie begründen einen Prüfauftrag, für sich genommen jedoch keinen Tatnachweis.

04 Regulatorische Entwicklung und eigenständiger Abgleich

4.1 FATF: internationale Mindeststandards

Die FATF veröffentlichte am 11. März 2026 einen Bericht zu Offshore-VASPs und am 16. Juli 2026 ihr siebtes Targeted Update zu Virtual Assets. Der Offshore-Bericht beschreibt ausdrücklich nicht lizenzierte Offshore-Dienstleister, die als vermeintliche Privatkunden Konten bei lizenzierten VASPs nutzen; dies entspricht dem Muster des nicht offengelegten Hostings. Im Targeted Update meldeten 91 von 109 hierzu befragten Jurisdiktionen (83 %) eine gesetzliche Umsetzung der Travel Rule (Absatz 24). Davon hatten 55 von 91 Jurisdiktionen (60 %) noch keine Feststellungen, Anordnungen oder sonstigen ausdrücklich auf die Travel Rule bezogenen Aufsichts- bzw. Durchsetzungsmaßnahmen gemeldet (Absatz 25). Diese Angabe betrifft nicht die gesamte VASP-Aufsicht. Die FATF-Selbstauskünfte sind keine unabhängige Wirkungsprüfung. [2, 3]

4.2 Europäische Union: MiCAR, Geldwäscheprävention, Travel Rule

Seit dem 30. Dezember 2024 gelten die Zulassungs- und Aufsichtsanforderungen von Titel V MiCAR (Verordnung (EU) 2023/1114) für CASPs. [7] Dies schafft einen definierten Regelungsrahmen, verhindert aber nicht automatisch, dass nicht offengelegte Drittgeschäfte über fremde Infrastruktur laufen. Die EBA-Risikofaktorenleitlinien verlangen einen risikobasierten Umgang mit Kunden, Produkten, Vertriebskanälen und Geografie; sie adressieren auch Beziehungen von Finanzinstituten zu Kryptodienstleistern. [4]

Die Transfer-of-Funds-Verordnung (EU) 2023/1113 und die seit 30. Dezember 2024 geltenden EBA-Travel-Rule-Leitlinien regeln begleitende Angaben zu Absendern und Empfängern sowie die Behandlung fehlender und unvollständiger Informationen. Bei Nested Services bleibt zusätzlich die

Frage, ob das formell übermittelte Datenset die tatsächliche Intermediärrolle sachgerecht abbildet. [5, 6]

Die Höchstfrist nach Art. 143 Abs. 3 MiCAR endete EU-weit am 1. Juli 2026, sofern Mitgliedstaaten nicht kürzere Übergangsfristen vorsahen. Für die in § 50 Abs. 1 KMAG bestimmten Unternehmen endete die Fortgeltung ihrer bisherigen Erlaubnis nach § 50 Abs. 2 Nr. 3 KMAG spätestens mit Ablauf des 31. Dezember 2025; sie konnte nach Nr. 1 oder 2 auch früher entfallen. § 50 KMAG enthält unterschiedliche Konstellationen, insbesondere für ehemals erlaubnisfreie Tätigkeiten. Deshalb darf diese Frist nicht pauschal auf jeden Anbieter übertragen werden. Maßgeblich bleiben Geschäftsmodell, einschlägiger Erlaubnistatbestand und individuelle Zulassungslage. [8, 11]

4.3 Sanktionen: der dokumentierte Fall SUEX

OFAC sanktionierte SUEX OTC, S.R.O. am 21. September 2021. Das US-Finanzministerium führte an, dass mehr als 40 % der bekannten Transaktionshistorie mit illegalen Akteuren in Verbindung standen und Transaktionen zu mindestens acht Ransomware-Varianten gehörten. Das ist ein unabhängig belegtes Beispiel für Sanktionsrisiken bei vermittelnden Kryptodienstleistern. Die zusätzlich von Crystal für SUEX genannten 1,86 Mrd. USD Nested-Volumen sind demgegenüber Crystal-eigene Auswertungsdaten. [1, 9, 10]

05 Eigene forensische Typologie: Erkennen ohne vorschnelle Zuschreibung

Das nachfolgende Prüfmodell wurde für die praktische Fallarbeit strukturiert. Es unterscheidet technische Wahrscheinlichkeit, geschäftliche Identität und belastbare Tatsachenfeststellung.

SIGNAL	MÖGLICHE ERKLÄRUNG	ERFORDERLICHE GEGENPROBE
Automatisierter Sweep	Host-basierte Einzahlungskonten oder reguläres Treasury	Zeitserie, mehrere unabhängige Einzahlungsvorgänge, Clusterzuordnung
Viele Zahler, ein Zielcluster	Broker-/Payment-Sammelkonto oder Kundenaggregation	Transaktionszweck, Einzahlungsanweisungen, Off-Chain-Belege
Hot-Wallet-Auszahlung	Custody durch Börse	Kontoauszüge oder Börsenauskunft zur initiierenden Partei
Interne ID / UID / Pay-ID	Nutzung börseninterner Transfers	Authentizität der Zahlungsinstruktion und Plattformzuordnung
Mehrere Host-Börsen	Redundanz, Liquidität oder Verschleierung	Separate Nachweise für jede Geschäftsbeziehung
Fehlende Lizenzangaben	Informationsdefizit oder tatsächliche Erlaubnislücke	Registerabfrage mit Zeitstempel und Rechtsträgerabgleich

Bei Bitcoin sind Common-Input-Heuristiken nur unter Berücksichtigung von CoinJoin- und UTXO-Ausnahmen belastbar. Auf accountbasierten Chains können Sweep-Verhalten und Gas-Funding Hinweise liefern, aber Smart Contracts und Exchange-interne Buchungen erschweren Eigentumszuordnungen. Clusterlabels externer Analyseanbieter sind Hypothesen, deren Belastbarkeit von Quelle und Aktualität abhängt.

06 Praktischer Ermittlungsworkflow

1. **Belegaufnahme:** ursprüngliche Plattform-URL, App-Screenshots, Chatverlauf, Zahlungsanweisungen und Zeitstempel beweissicher erfassen, einschließlich Hashwerten der gesicherten Dateien.
2. **On-Chain-Mapping:** exakte Chain, Transaktionshashes, Tokenkontrakt, Sender-/Empfängeradresse und Blockzeit feststellen.
3. **Attributionskontrolle:** Host-Cluster prüfen; Quelle und Versionsstand jeder Zuordnung dokumentieren.
4. **Nested-Hypothese:** prüfen, ob die Kundenoberfläche Wallets oder IDs eines Hosts nutzt und Einzahlungen regelmäßig in Host-Cluster gelangen.
5. **Unabhängige Bestätigung:** wiederholte technische Beobachtung, belastbare OSINT-Nachweise oder rechtmäßig durchgeführte Testinteraktion; rechtliche Freigabe vor Testzahlungen.
6. **Gegenhypothesen:** normale Custody, White-Label-Anbieter, Zahlungsdienstleister, Broker und interne Exchange-Transfers aktiv prüfen und, soweit möglich, ausschließen.
7. **Auskunfts- und Sicherungsersuchen:** getrennt an Host und Nested-Betreiber richten, soweit rechtlich und praktisch möglich.
8. **Bewertung:** Sicherheit der Host-Zuordnung, Sicherheit der Betreiberzuordnung und Identität des Endkunden jeweils separat ausweisen.

07 Fallkonstellationen und Ermittlungsnutzen

7.1 Betrugsfall mit Einzahlungsadresse einer Großbörse

Wenn ein angebliches Investmentportal eine Deposit-Adresse nutzt, die zu einer bekannten Börse gehört, folgt daraus nicht, dass die Betrugsplattform mit dieser Börse identisch ist. Denkbar sind ein Kundenkonto der Betreiber beim Host oder ein zwischengeschalteter Dienstleister. Ermittlungsrelevant sind der Zeitraum, in dem die Deposit-Adresse eindeutig einem Konto zugeordnet war, die Konto-/Subkonto-Zuordnung und die Weiterverfügung über die Mittel. Ohne Auskunft des Hosts bleibt der wirtschaftliche Initiator häufig unbekannt.

7.2 OTC- und Cash-Desk-Modell

Bei Bargeld- oder P2P-basierten Wechselstellen können viele Zahlungen über wenige Host-Konten konzentriert werden. Auffällig ist weniger die Existenz der Börsenanbindung als die Kombination aus ungeklärtem Endkunden-KYC, ungewöhnlichen Volumina, fehlender Unternehmensidentität und inkonsistenten Herkunftsnachweisen.

7.3 Sanktionsexponierte Intermediäre

Entscheidend sind aktuelle Listen- und Länderprüfungen, Kontrollbeziehungen und die konkrete Rechtshoheit. Ein technischer Host-Match löst eine vertiefte Prüfung aus, ersetzt jedoch keine sanktionsrechtliche Subsumtion.

08 Risikobewertung für Verpflichtete

RISIKO	PRÜFFRAGE	KONTROLLMASSNAHME
Attribution	Ist der sichtbare Host tatsächlich der Kundenanbieter?	Entity-Level-Mapping und Herkunft des Labels
KYC/KYB	Wer kennt und prüft den Endkunden?	Vertragliche Offenlegung der Drittgeschäftstätigkeit
Sanktionen	Wer initiiert und kontrolliert die Verfügung?	Listenabgleich, Geografie und Ownership-/Control-Analyse
Regulierung	Ist die Tätigkeit im Zielmarkt erlaubnisgedeckt?	CASP-/VASP-Register, Zeitraum, Rechtsform
Dokumentation	Ist der Befund reproduzierbar?	Beweismittelkette, Hashes, Versionsarchiv

09 Empfehlungen mit Umsetzungspriorität

Für Börsen und Zahlungsdienstleister

- Geschäftskonten und volumenstarke Privatkonten auf faktische Drittgeschäftstätigkeit prüfen.
- Nested-Service-Offenlegung mit Angaben zu Unterkunden, Jurisdiktionen und weiteren Hosts vertraglich verankern.
- Verhaltensbasierte Regeln nicht auf Transaktionshöhe beschränken; auch Sweep-Zeiten, Adressaggregation und viele Kleinbeträge beobachten.
- Treffer zu Sanktionen oder Hochrisikojurisdiktionen stets durch menschliche Fachprüfung validieren.

Für Ermittlungsbehörden und forensische Gutachter

- „Börsen-Cluster erreicht“ und „Betreiber identifiziert“ als zwei unterschiedliche Ergebnisstufen führen.
- Konto- und Subkontoinformationen zeitnah beim Host sichern; Blockchain allein bildet interne Bücher nicht ab.
- Jede Aussage mit Transaktions-/Adressbeleg und Konfidenzgrad versehen.
- Anbieterlabels und Trefferlisten zum Analysezeitpunkt archivieren; spätere Änderungen sind möglich.

Für Aufsicht und Kreditinstitute

- Intermediärbeziehungen bei CASP-Geschäftsbeziehungen ausdrücklich in Risikoanalysen berücksichtigen.
- Herkunft der Endkundendaten und Eskalationsprozesse auch bei White-Label- und API-Geschäftsmodellen prüfen.
- Informationsaustausch zwischen Aufsicht, FIU und Marktteilnehmern rechtssicher operationalisieren.

10 Konfidenz- und Evidenzstandard von Finanz Forensik

STUFE	MINDESTGRUNDLAGE	ZULÄSSIGE FORMULIERUNG
A – belegt	Originärbeleg und unabhängige Bestätigung	„Nachgewiesen ist …“
B – stark gestützt	Mehrere konsistente On-/Off-Chain-Indizien	„Mit hoher Wahrscheinlichkeit …“
C – plausible Hypothese	Einzelne passende Verhaltensmuster	„Es bestehen Hinweise …“
D – unbestätigt	Nur Plattformbehauptung, Screenshot oder einzelnes Label	„Nicht verifiziert …“

Diese Matrix ist ein vorgeschlagener interner Prüfstandard, keine gesetzliche Klassifikation. Technischer Nachweis einer Host-Verbindung, strafrechtliche Verantwortlichkeit und wirtschaftlich Berechtigte sind voneinander abzugrenzen.

Fazit

Nested Services sind keine Randerscheinung der Blockchain-Forensik, sondern eine strukturelle Grenze der rein adressbasierten Interpretation. Das entscheidende Risiko entsteht dort, wo eine regulierte Infrastruktur als Vertrauenssignal gelesen wird, obwohl der eigentliche Kundenkontakt über einen weniger transparenten Intermediär läuft. Die konsequente Trennung von Host, Intermediär und Endkunde kann die Qualität von Ermittlungen, Compliance-Entscheidungen und Sanktionsprüfungen deutlich verbessern.

Das Whitepaper benennt keine zusätzlichen, eigenständig identifizierten Täter, Hosts oder Transaktionen. Sein eigenständiger Forschungsbeitrag liegt im Primärquellenabgleich, der kritischen Interpretation einer proprietären Datengrundlage und der Entwicklung eines praktisch überprüfbaren Ermittlungsrasters. ■

Methodik und Quellennachweise

Recherchezeitpunkt: 15. Oktober 2026. Die Ausgangsstudie wurde inhaltlich ausgewertet; öffentlich zugängliche Primärquellen von Aufsichten und Behörden wurden separat abgeglichen. Alle Zahlen aus der proprietären Analyse sind ausdrücklich Crystal Intelligence zugerechnet. Eigene Empfehlungen sind als fachliche Ableitungen zu verstehen. Es wurde kein unabhängiges On-Chain-Sample neu berechnet und kein Zugriff auf Crystal-Rohdaten behauptet.

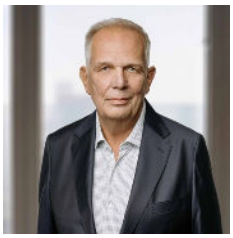
1. Crystal Intelligence (August 2026): Nested Services – The $8 billion compliance blindspot. PDF-Fassung, 31 Seiten. Insbesondere S. 9–16, 19–25, 27–30.
2. FATF (16.07.2026): Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, insbesondere Abs. 24–25 und Abb. 1.10. – fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html
3. FATF (11.03.2026): Understanding and Mitigating the Risks of Offshore Virtual Asset Service Providers. – fatf-gafi.org/en/publications/Virtualassets/Understanding-Mitigating-Risks-Offshore-VASPs.html
4. European Banking Authority (16.01.2024): EBA issues guidance to crypto-asset service providers to effectively manage their exposure to ML/TF risks. – eba.europa.eu/publications-and-media/press-releases/eba-issues-guidance-crypto-asset-service-providers
5. Verordnung (EU) 2023/1113 (Transfer of Funds Regulation). – eur-lex.europa.eu/eli/reg/2023/1113/oj
6. EBA (2024): Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 (Anwendung ab 30.12.2024). – eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-terrorism/guidelines-information-requirements-relation-transfers-funds-and-certain-crypto-assets-transfers
7. BaFin (22.01.2025): Kryptowerte-Dienstleister: Welche Vereinfachungen und Herausforderungen es jetzt gibt. – bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2025/fa_250122_MiCAR_Vereinfachungen_Herausforderungen.html

8. Kryptomärkteaufsichtsgesetz (KMAG), § 50, insbesondere Abs. 1–4 (amtlicher Gesetzestext). – gesetze-im-internet.de/kmag/__50.html
9. OFAC (21.09.2021): Publication of Updated Ransomware Advisory; Cyber-related Designation (SUEX). – ofac.treasury.gov/recent-actions/20210921
10. U.S. Department of the Treasury (21.09.2021): Treasury Takes Robust Actions to Counter Ransomware. – home.treasury.gov/news/press-releases/jy0364
11. ESMA (04.07.2024): Q&A 2220 – Entities not authorised as CASPs by the end of the transition period. – esma.europa.eu/publications-data/questions-answers/2220

PUBLIKATIONSHINWEIS

Diese Publikation dient der fachlichen Information. Sie ersetzt weder eine fallbezogene Blockchain-Untersuchung noch eine rechtliche, aufsichtsrechtliche oder sanktionsrechtliche Beratung. Alle Aussagen zu konkreten Marktteilnehmern sind an den angegebenen Stichtag und die jeweiligen Quellen gebunden.

AUTOR



David Lüdtke

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

David Lüdtke 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.

ÜBER FINANZ FORENSIK

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.

KONTAKT

Finanz Forensik GmbH · finanz-forensik.de · postfach@finanz-forensik.de · +49 6057 9189145 · Stand: 15. Oktober 2026

Herausgeber: Finanz Forensik GmbH · Würzburger Str. 59, 63639 Flörsbachtal · HRB 100521, Amtsgericht Hanau · USt-IdNr. DE454473675 · Geschäftsführung: Lydia Bonhard-Lüdtke, David Lüdtke. Stand: 15. Oktober 2026. Zitiervorschlag: Finanz Forensik GmbH, Nested Services im Kryptomarkt, 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.