DIGITAL ASSET
INTELLIGENCE

RESEARCH REPORT
NR. 04 · 2026

STUDIE · MARKTANALYSE

Krypto-Betrug in Deutschland

Schäden von bis zu 1,3 Milliarden Euro pro Jahr — eine datenbasierte Schätzung aus Polizei-, Aufsichts- und internationalen Beschwerdedaten.

7 KAPITEL · CHARTS · QUELLEN

FINANZ FORENSIK GMBH · FINANCIAL INTELLIGENCE

EXECUTIVE SUMMARY

Krypto-Betrug kostet Deutschland bis zu 1,3 Milliarden Euro pro Jahr

Die belastbarste deutsche Evidenz spricht für einen von Investment- und Cybertrading-Betrug dominierten Markt — mit hohem Einzelschaden, starker oberer Schiefe und erheblicher Dunkelziffer.

FINANZ·FORENSIK · FINANCIAL INTELLIGENCE & BLOCKCHAIN FORENSICS RESEARCH REPORT 04 / 2026

0,80 Mrd. €	≈ 39.500 €	56 %	0,45–1,30 Mrd. €
Direkter Schaden pro Jahr (Zentralszenario)	Durchschnittlicher Schaden je Fall	Anteil Investment- / Cybertrading-Betrug	Bandbreite direkter Jahresschaden

Für Deutschland insgesamt lässt sich auf Basis staatlicher Teilstatistiken, EU-/Interpol-Typologien und internationaler Krypto-Beschwerdedaten ein jährlicher direkter Schaden aus Krypto-Betrug in einer plausiblen Bandbreite von 0,45 bis 1,30 Mrd. Euro schätzen; das Zentralszenario liegt bei rund 0,80 Mrd. Euro. Rechnet man indirekte Effekte hinzu — Ermittlungs- und Compliancekosten, Opfernebenkosten, Präventions- und Vertrauensverluste — ergibt sich ein gesamtwirtschaftlicher Schaden von plausibel 0,52 bis 2,08 Mrd. Euro pro Jahr.

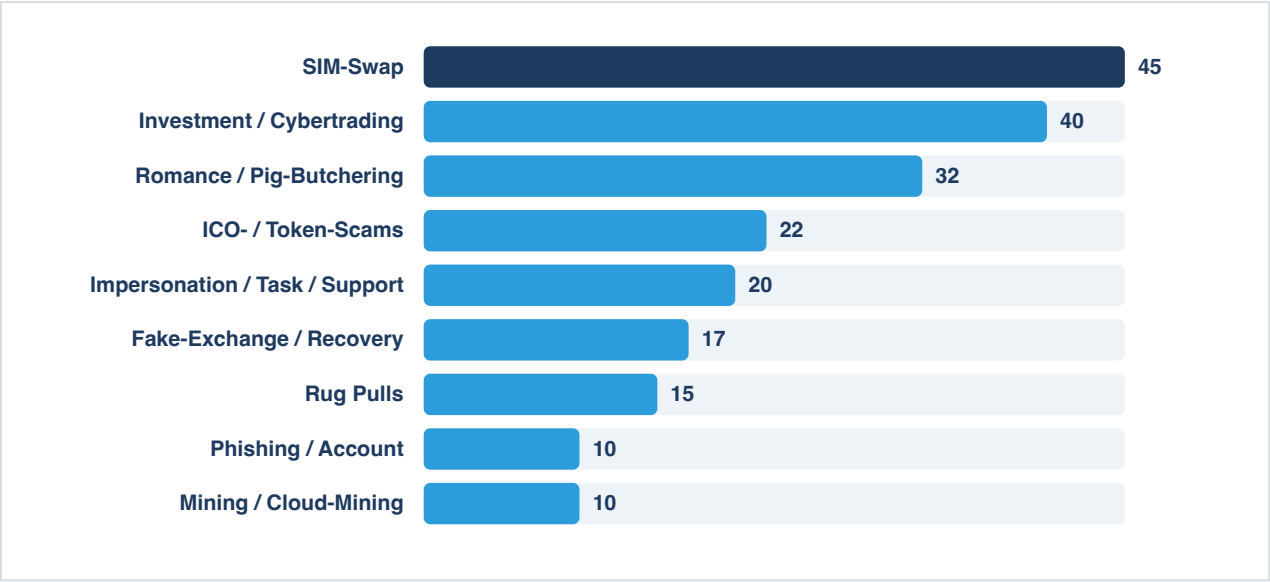
Diese Werte sind keine amtliche Statistik, sondern ein transparentes Szenariomodell auf Basis unvollständiger, heterogener Primärdaten. Wichtigste methodische Schlussfolgerung: Wer nach „der durchschnittlichen Schadenshöhe“ fragt, sollte Mittelwert und Median getrennt berichten.

KERNERGEBNISSE AUF EINEN BLICK

- **Direkter Schaden:** 0,45–1,30 Mrd. € pro Jahr, Zentralszenario rund 0,80 Mrd. €.
- **Volkswirtschaftlich:** 0,52–2,08 Mrd. € pro Jahr inkl. Ermittlungs-, Compliance- und Vertrauenskosten (zentral 1,08 Mrd. €).
- **Pro Fall:** ⌀ rund 39.500 € — der Median liegt aber deutlich darunter (heavy-tailed Verteilung).
- **Dominanz:** Investment-/Ponzi-/Cybertrading-Betrug verursacht rund 56 % der direkten Verluste.
- **Datenlage:** fragmentiert — keine bundesweite Krypto-Betrugsstatistik; belastbar v. a. Sachsen, Rheinland-Pfalz, Bayern.
- **Dunkelziffer:** hoch — jede Schätzung ist eher Untergrenze als Obergrenze.

01 Schadenshöhe und dominierende Betrugsarten

Die arithmetischen Mittelwerte je vollendetem Fall liegen konsistent im mittleren fünfstelligen Bereich: Sachsen registrierte 2019–2024 knapp 4.800 Cybertrading-Fälle mit 190,5 Mio. Euro Schaden (rund 39.700 Euro je Fall); Oberbayern Nord rund 42.000 Euro; Schwaben Süd/West 2024 rund 28.100 Euro je Fall. Große Verfahren zeigen den schweren rechten Rand: 28,6 Mio. Euro bei 235 Geschädigten entsprechen rund 122.000 Euro je Opfer.



Durchschnittlicher Schaden je Fall (Tsd. Euro). *Beobachtete deutsche Massenserien für Investment/Cybertrading; übrige Werte als kalibrierte Schätzbänder. Per-Fall-Mittel ≠ Anteil am Gesamtschaden.*

Der Mittelwert von rund 39.500 Euro treibt die volkswirtschaftliche Summe; der Median liegt — wegen vieler kleiner Anfangseinzahlungen von 250 bis 500 Euro und weniger sechs- bis siebenstelliger Großfälle — modelliert eher bei 8.000 bis 12.000 Euro.

02 Anteile am Gesamtschaden

In der Schadensverteilung dominiert Investment-/Cybertrading-Betrug. Im IC3-Datensatz 2024 entfielen 5,82 von 9,32 Mrd. USD Krypto-Verlusten auf Investment (rund 62 %). Für Deutschland ist der Anteil bewusst konservativ auf 56 % gesetzt, um Pig-Butchering, Fake-Exchange-/Recovery-Maschen und sonstige Krypto-Zahlungsscams separat auszuweisen.

Anteil jeder Betrugsart am direkten Gesamtschaden. *Zentralszenario Deutschland, kalibriert aus deutschen Polizeidaten, Europol-Einschätzung, IC3-Verluststruktur und Chainalysis/TRM-Typologien.*

03 Volkswirtschaftlicher Schaden

Der Gesamtschaden folgt dem Modell *direkte Verluste + Opfernebenkosten + Ermittlungs-/Compliancekosten + Vertrauens- und Friktionskosten*. Da keine offizielle Jahresgesamtrechnung existiert, wird der direkte Schaden aus mehreren Teilankern trianguliert; die indirekten Aufschläge betragen im Zentralszenario rund 35 % der direkten Verluste.

KONSERVATIV

0,52 Mrd. €

0,45 Mrd. € direkt + 0,07 Mrd. € indirekt

Untere Bandkante, geringe Multiplikatoren.

ZENTRAL

1,08 Mrd. €

0,80 Mrd. € direkt + 0,28 Mrd. € indirekt

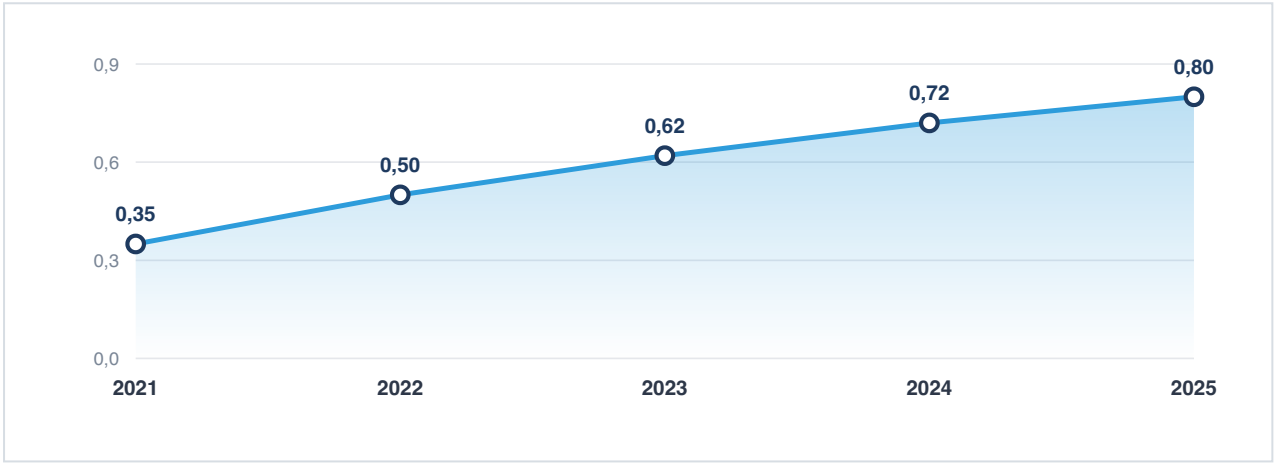
Mittel aus DE-Teilstatistiken, EU-/IC3-Struktur.

HOCH

2,08 Mrd. €

1,30 Mrd. € direkt + 0,78 Mrd. € indirekt

Obere Bandkante, hohe Dunkelziffer.



Modellierter direkter Jahresschaden 2021–2025 (Mrd. Euro). *Illustrative, modellierte Zeitreihe — keine amtliche Statistik. Richtung gestützt durch steigende regionale Schäden, sächsische Falldynamik und EU-Lagebilder.*

Über fünf Jahre ergibt sich ein kumulativer volkswirtschaftlicher Schaden von grob 2,6 bis 9,0 Mrd. Euro, zentraler Orientierungswert rund 5,0 Mrd. Euro — ausdrücklich als Band, nicht als Punktwert.

Geld, das im Dunkeln verschwindet. *Über Wallets, Fake-Plattformen und Off-Ramps fließen die Werte in Täterstrukturen — die forensische Spur entscheidet über Aufklärung und Recovery.*

04 Datengrundlage und Abgrenzung

Die deutsche Primärquellenlage ist fragmentiert. Belastbare Zahlen stammen aus Landeskriminalämtern, Polizeipräsidien und Staatsanwaltschaften — nicht aus einer einheitlichen Bundesstatistik. Die BaFin beschlagnahmte in Operation Herakles 1.406 illegale Domains, BKA und ZIT schalteten 2024 47 in Deutschland gehostete Exchange-Services ab — Belege für die industrielle Infrastruktur hinter dem Betrug.

> ***„Jede aktuelle Schadensschätzung ist eher als Floor denn als Ceiling zu lesen — die Dunkelziffer ist strukturell hoch."***
>
> LIMITATIONEN DER DATENLAGE

---

05 Einordnung durch Finanz Forensik

Warum Cybertrading dominiert: Investment-Maschen skalieren über Fake-Plattformen, bezahlte Werbung und Call-Center industriell. **Warum die Dunkelziffer höher liegt:** Scham, späte Einsicht und verzögerte Mustererkennung führen zu massiver Untererfassung. **Was am stärksten wächst:** Pig-Butchering, Recovery-Ketten und KI-gestützte Personalisierung. **Was das für Betroffene heißt:** Geschwindigkeit schlägt Nachbetrachtung — frühe Wallet-Sicherung, On-Chain-Clustering und Off-Ramp-Analyse entscheiden über die Recovery-Chance.

06 Methodik

Dreistufig: deutsche Primärquellen priorisieren und beobachtete Mittelwerte direkt berechnen; für Lücken sachnahe internationale Benchmarks (IC3 2024, FTC, Europol/Interpol/Chainalysis/TRM); diese an deutsche Massendaten kalibrieren statt US-Werte 1:1 zu übernehmen. Zentraler Referenzanker: rund 39.500 Euro je Fall. Großfälle werden für die Gesamtsumme bewusst nicht getrimmt, für den „typischen" Fall aber separat ausgewiesen; Mediane sind modellierte Bandbreiten.

07 Limitationen und Empfehlungen

Größte Schwäche: fehlende bundesweite Standardisierung. Fünf Schritte würden den Erkenntnisgewinn stark erhöhen:

- Einheitliche Krypto-Betrugs-Taxonomie auf Bundesebene, harmonisiert mit Europol-/Interpol-Kategorien.
- Standardfelder je Polizeifall: Zahlungsweg, Asset, Wallet/Exchange, Erstkontaktkanal, Recovery-Status.
- Geteilter Mindest-Datenstandard zwischen BKA, BaFin, Bundesnetzagentur, BSI, Zahlungsdienstleistern und CASPs.
- Jährliche Lageberichte mit Mittelwert, Median, Quantilen und Streuung nach Betrugsart.
- Monitoring „verhinderter Schäden" zur Wirkungsmessung von Prävention.

QUELLENBASIS

DEUTSCHE PRIMÄRQUELLEN

LKA Sachsen (Cybertrading 2019–2024: 190,5 Mio. € / ≈4.800 Fälle) · Polizei Rheinland-Pfalz (77 Mio. €) · Bayerische Polizei (Oberbayern Nord, Schwaben Süd/West) · Generalstaatsanwaltschaften Sachsen & Bayern.

AUFSICHT & INFRASTRUKTUR

BaFin (betrügerische Handelsplattformen, Operation Herakles: 1.406 Domains) · BKA/ZIT (47 abgeschaltete Exchange-Services) · Bundesnetzagentur (Rufnummernmissbrauch) · BSI (Smishing, SIM-Swapping).

INTERNATIONALE KALIBRIERUNG

Europol IOCTA 2024 · Interpol Global Financial Fraud Assessment 2024 · FBI IC3 Report 2024 · FTC · Chainalysis · TRM Labs · GASA-Report 2025.

Die Werte sind keine amtliche Statistik, sondern ein transparentes Szenariomodell auf Basis unvollständiger, heterogener Primärdaten (Stand 2026).

ÜBER DEN AUTOR

David Lüdtke

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

Gerichtsfeste Kryptotransaktionsanalysen, OSINT-gestützte Vermögensermittlung und gutachterliche Aufbereitung für Strafverteidiger, Insolvenzverwalter und Unternehmen. 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.