



Financial
Intelligence Unit



ALTERNATIVE ZAHLUNGSMETHODEN UND NEUE TECHNOLOGIEN

Anhaltspunkte, Typologien sowie besondere
Hinweise zur Geldwäschebekämpfung

Inhaltsverzeichnis

Vorwort der Leitung	- 1 -
Verwendung des Dokuments	- 2 -
Einführung und Begriffsabgrenzung: Alternative Zahlungsmethoden und neue Technologien	- 4 -
ALTERNATIVE FORMEN VON VERMÖGENSGEGENSTÄNDEN	- 5 -
Kryptowerte	- 6 -
NFT	- 8 -
Sonstige digitale Werte (Gaming-Bereich)	- 10 -
DIGITALISIERUNG VON ZAHLUNGSMÖGLICHKEITEN/ZAHLUNGSPLATTFORMEN	- 10 -
E-Wallets / Digitale Wallets von Online-Zahlungsdienstleistern	- 11 -
Social-Media- und Streaming-Plattformen	- 12 -
Crowdfunding-Plattformen	- 13 -
Modi Operandi	- 15 -
... IM ZUSAMMENHANG MIT KRYPTOWERTEN	- 15 -
Nutzung von Mixer/Tumbler/Blender	- 15 -
Nutzung von Bridges/Chain-Hopping/-Swapping	- 20 -
ICO – Initial Coin Offering	- 22 -
Marktmanipulation zu Zwecken der Geldwäsche	- 24 -
Nutzung von nicht-lizenzierten Krypto-Handelsplattformen und Kryptobörsen in Hochrisikostaat	- 26 -
Nutzung von Online-Glücksspielseiten mit Kryptowerten	- 31 -
Nutzung von Krypto-Automaten (Krypto-ATM)	- 33 -
Allgemeine, nicht einer speziellen Typologie zuordenbare Anhaltspunkte	- 35 -
... IM ZUSAMMENHANG MIT NFT	- 36 -
Über-/ Unterfakturierung bei NFT	- 38 -
Ausgabe von NFT/Handel mit NFT	- 38 -
... IM ZUSAMMENHANG MIT SONSTIGEN DIGITALEN WERTEN (GAMING-BEREICH)	- 40 -
Handel mit sonstigen digitalen Werten zur Verschleierung	- 40 -
Gaming-Karten	- 43 -
... IM ZUSAMMENHANG MIT E-WALLETS / DIGITALEN WALLETS	- 45 -
... IM ZUSAMMENHANG MIT SOCIAL-MEDIA- UND STREAMING-PLATTFORMEN	- 49 -
... IM ZUSAMMENHANG MIT CROWDFUNDING	- 53 -
Anlage A – Allgemeine Anhaltspunkte für Geldwäsche	- 58 -
Literaturverzeichnis	- 65 -
Dokumenteninformation	- 66 -

Vorwort der Leitung

Liebe Leserinnen und Leser,

die Abwicklung von Zahlungen hat sich in den vergangenen Jahren stark gewandelt. Mit Kryptowerten entstand ein neues Phänomen, das besondere Missbrauchsrisiken aufweist. Die FIU beobachtet über die letzten Jahre eine kontinuierlich steigende Zahl an Meldungen, die hiermit in Verbindung stehen. Für die erfolgreiche Bekämpfung der Finanzkriminalität ist es von herausragender Bedeutung, Verpflichtete hinsichtlich der neusten Methoden der Geldwäsche zu sensibilisieren sowie sie bei der Identifizierung von auffälligen Transaktionsmustern zu unterstützen.

Neben dem Aufkommen von Kryptowerten sind Geldwäsche-Risiken aber auch von anderen Trends beeinflusst. Neue Technologien und ein geändertes Zahlungsverhalten schlagen sich auch im Bereich der Geldwäsche nieder. Heute gibt es deutlich mehr verschiedene Zahlungsmöglichkeiten als noch vor wenigen Jahren. Wurden Zahlungen früher überwiegend bar oder durch Überweisungen und Lastschriften abgewickelt, erfolgen Zahlungen heute häufiger unbar, mit mobilen Endgeräten und kontaktlos, und oft unter Einbindung von zwischengeschalteten Zahlungsdienstleistern - im Bereich des E-Commerce, aber auch im Handel vor Ort. Geldwäscher nutzen die sich ihnen bietenden Möglichkeiten ebenfalls aus und haben

neue Wege identifiziert, Transaktionen im Zusammenhang mit illegalen Aktivitäten zu verschleiern.



Das vorliegende Papier gibt einen Überblick über die neuen Zahlungsmethoden und stellt anhand von Beispielen und Anhaltspunkten dar, wie diese typischerweise zur Geldwäsche eingesetzt werden.

Das Papier möge Sie und uns bei unserem gemeinsamen Kampf gegen Finanzkriminalität und Geldwäsche unterstützen.

Daniel Thelesklaf
Leiter FIU

Die FIU wertet Finanzinformationen zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung aus, reichert diese an und übermittelt qualitativ hochwertige Analyseberichte an die wichtigsten Akteure. Damit trägt die FIU zum Schutz der Integrität des deutschen Finanzsystems bei, indem der Missbrauch durch Kriminelle verhindert wird.

Verwendung des Dokuments

Ziel dieses Dokuments ist es, Verpflichtete in Deutschland dabei zu unterstützen, verdächtige Transaktionen oder Aktivitäten zu identifizieren, die einen Bezug zu Geldwäsche mit alternativen Zahlungsmethoden und neuen Technologien haben. Darüber hinaus sollen die im Folgenden beschriebenen Anhaltspunkte dazu beitragen, das Verständnis zu den Hintergründen und Abläufen von Geldwäsche bei der Verwendung dieser Technologien zu vertiefen.

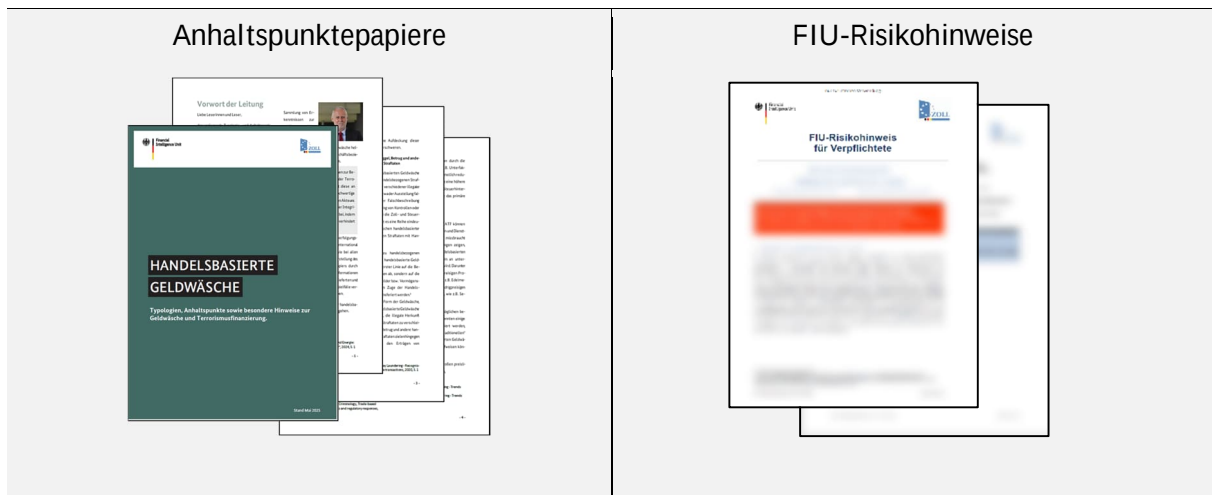
Ein grundlegendes Verständnis ist essentiell, um Risiken zu erkennen und entsprechend zu bewerten. Die Bewertung soll nach einem risikobasierten Ansatz erfolgen. Der gesamte vorliegende Sachverhalt muss dabei im Kontext betrachtet und in seiner Gesamtheit bewertet werden. Der Fokus im Rahmen einer Untersuchung bzw. Bewertung sollte dabei auf den beteiligten Parteien, den Zahlungsströmen und allen weiteren Rahmenbedingungen zum jeweiligen Sachverhalt liegen, um potenzielle Geldwäscheaktivitäten zu identifizieren.

Die Ausführungen in diesem Anhaltspunktepapier berücksichtigen neben eigenen Erkenntnissen der FIU aus Analysen und Austausch mit anderen nationalen und internationalen Stellen auch Informationen und Erkenntnisse aus einschlägigen Veröffentlichungen und Berichten.

Die nachfolgend aufgeführten Anhaltspunkte sind nicht abschließend. Ein Verdacht auf Geldwäsche kann sich im Einzelfall auch aus weiteren Anhaltspunkten ergeben. In der Regel reicht das Vorliegen eines einzelnen Anhaltspunktes nicht aus, um einen relevanten Verdacht im Sinne von § 43 Abs. 1 GwG zu begründen. Die Notwendigkeit zur Abgabe einer Verdachtsmeldung kann insbesondere bei Vorliegen mehrerer der in diesem Papier oder in weiteren Anhaltspunktepapieren der FIU beschriebenen Anhaltspunkte für Geldwäsche bestehen - ggf. auch zusätzlich in Verbindung mit FIU-Risikohinweisen. Während das hier vorliegende Papier insb. Anhaltspunkte im Zusammenhang mit der Nutzung von alternativen Zahlungsmethoden und neuen Technologien darstellt, sind bei der Gesamtwürdigung zusätzlich auch die im Anhang aufgeführten allgemeinen Anhaltspunkte für Geldwäsche zu berücksichtigen.

Etwaige Anmerkungen oder Vorschläge zur Verbesserung dieses Papiers richten Sie bitte
gerne per E-Mail an
Anhaltspunktepapiere.gzd@fiu.bund.de.

Das Dokument einschließlich aller seiner Teile ist urheberrechtlich geschützt. Mit Ausnahme der Nutzung ausschließlich für interne Zwecke ist jede Verwertung und Vervielfältigung ohne ausdrückliche Zustimmung der FIU Deutschland unzulässig. Dies gilt medienunabhängig insbesondere für Wiedergaben, Kopien, Mikroverfilmung, Übersetzungen sowie die Speicherung und Verarbeitung in elektronischen Systemen.



Anhaltspunktepapiere und FIU-Risikohinweise sind im Verbund zu sehen. Beide Produkte geben Hinweise, die zur Abgabe einer Geldwäsche-Verdachtsmeldung führen können.

Anhaltspunktepapiere geben allgemeine und grundlegende Informationen zu spezifischen geldwäscherelevanten bzw. für die Terrorismusfinanzierung relevanten Themen.

FIU-Risikohinweise geben konkrete Hinweise zu spezifischen aktuellen Auffälligkeiten im Kontext der Geldwäsche oder Terrorismusfinanzierung („Red Flags“).

Anhaltspunktepapiere können u.a. für die Grundkonfiguration von AML-Prozessen und AML-Systemen bei Verpflichteten und Dienstleistern verwendet werden. Zudem dienen sie als Material für Schulungen und Sensibilisierungen.

FIU-Risikohinweise werden aus aktuellem Anlass zielgruppenspezifisch verteilt. Sie sollen zu einer zielgerichteten Adaption von AML-Prozessen und Transaktionsüberwachungen genutzt werden.

Anhaltspunktepapiere sind grundsätzlich auf eine längere Gültigkeitsdauer ausgerichtet. Sie gelten bis auf Widerruf oder bis zu einer Aktualisierung.

FIU-Risikohinweise haben eine begrenzte zeitliche Gültigkeit.

Die FIU bedankt sich bei allen Strafverfolgungs- und Partnerbehörden sowie bei allen weiteren Beteiligten, die bei der Erstellung des Typologie- und Anhaltspunktepapiers unterstützt haben, für die Zulieferung von wertvollen Informationen, Hinweisen und Beispielfällen.

Einführung und Begriffsabgrenzung: Alternative Zahlungsmethoden und neue Technologien

Alternative Zahlungsmethoden, einschließlich der Kryptowerte, sind technologische Entwicklungen, aber auch neue Angebote im Bereich der Zahlungsdienstleistungen. Sie haben den Zahlungsverkehr nachhaltig verändert. Kryptowerte ermöglichen unmittelbare Transaktionen zwischen Transaktionsbeteiligten ohne die Einbindung von Finanzintermediären, wenngleich in der Praxis häufig zentrale Kryptohandelsplattformen oder andere Dienstleister genutzt werden. Dazu kommt, dass die Transaktionen pseudonym erfolgen können, sie schnell und grenzüberschreitend sein können. Kriminelle, die Zahlungen im Zusammenhang mit ihren Aktivitäten abwickeln möchten, wurden bereits sehr früh auf die Potenziale aufmerksam, die ihnen Kryptowerte bieten. Für Geldwäsche und Terrorismusfinanzierung gehen von ihnen besondere Risiken aus. Dies kann die FIU auch anhand des zahlenmäßigen Aufkommens an Verdachtsmeldungen feststellen.

Es sind nicht nur alternative Methoden entstanden, die sich für Geldwäsche und zur Terrorismusfinanzierung eignen, sondern auch die Art und Weise, wie Zahlungen erfolgen, hat sich stark verändert. Digitale Zahlungsplattformen und E-Wallets spielen insb. im Onlinehandel eine bedeutende Rolle. Große IT-Anbieter sind in den Markt eingetreten und bieten Milliarden von Nutzenden Möglichkeiten Zahlungen zu tätigen. Darüber hinaus bieten Social-Media-Plattformen oder Online-Spiele neue

Optionen, monetäre Werte zu transferieren. Allgemein ist die Digitalisierung im Finanzsektor vorangeschritten. Zahlungen erfolgen heute in höherem Maße mobil mithilfe von Apps oder Wearables. Sie erfolgen öfter unbearbeitet, kontaktlos oder zeitlich unmittelbar (z.B. durch Echtzeitüberweisungen). Einige Anbieter von Bankdienstleistungen und Zahlungsplattformen, die konsequent auf Innovationen setzten, haben in kürzester Zeit ein enormes Kundenzuwachstum erfahren, insb. sogenannte Neo-Banken. Innerhalb weniger Jahre haben einige Start-ups im Finanzsektor ihren Kundenstamm deutlich vergrößern können. Während sich hierdurch die Effizienz des Zahlungsverkehrs erhöht hat, gehen mit diesen Entwicklungen auch verschiedene Risiken einher, die die FIU im Blick hält.

In den nachfolgenden Abschnitten wird zunächst ein Überblick über Entwicklungen im Bereich der alternativen Zahlungsmethoden gegeben. Es wird hierbei nicht das Ziel verfolgt eine vollständige und detaillierte Beschreibung zu geben. Ziel ist es dafür zu sensibilisieren, wie neue digitale Vermögensgegenstände (im Weiteren auch als Assets bezeichnet) und neue Zahlungsmöglichkeiten für Zwecke der Geldwäsche und Terrorismusfinanzierung genutzt werden. In dem darauffolgenden Abschnitt werden konkrete Modi Operandi der Geldwäsche mit digitalen Vermögensgegenständen und alternativen Zahlungsmethoden erläutert

und anhand praktischer Fallbeispiele dargestellt.

Alternative Formen von Vermögensgegenständen

Wurden traditionell von Zentralbanken ausgegebene Währungen (bar und unbar) neben hochwertigen Gütern zur Geldwäsche genutzt, so haben sich inzwischen neue digitale Formen im Bereich der Geldwäsche- und Terrorismusfinanzierung fest etabliert. Der vergleichsweise einfache Zugang, eine hohe Akzeptanz bzw. einfache Handelbarkeit als Vermögenswert, die Möglichkeit, sie Peer-to-Peer sicher und grenzüberschreitend zu übertragen, macht sie auch für den illegalen Einsatz sehr attraktiv. Kryptowerte basieren auf der sogenannten Distributed-Ledger-Technologie, welche ihre Funktionsweise sicherstellt.

Hinzu kommt, dass im Bereich der digitalen Vermögenswerte nicht mehr nur traditionelle Banken einen Zugang zum Zahlungsverkehr und Finanzdienstleistungen bieten, sondern auch eine Vielzahl anderer Akteure. Für die Bekämpfung von Geldwäsche bringen diese Zahlungsmethoden und -möglichkeiten neue Herausforderungen und eine neue Komplexität.

Die nachfolgenden Abschnitte beschreiben diese neuen Formen von Vermögenswerten näher.

Distributed-Ledger-Technologie (DLT)

Bei der Distributed-Ledger-Technologie (DLT) handelt es sich um eine spezielle Form der elektronischen Datenverarbeitung und -speicherung. Als Distributed-Ledger oder „Verteiltes Kontenbuch“ wird eine dezentrale Datenbank bezeichnet, die Teilnehmenden eines Netzwerks eine gemeinsame Schreib- und Leseberechtigung erlaubt. Im Gegensatz zu einer zentral verwalteten Datenbank bedarf es in diesem Netzwerk keiner zentralen Instanz, die neue Einträge in der Datenbank vornimmt. Neue Datensätze können jederzeit von den Teilnehmern selbst hinzugefügt werden. Ein anschließender Aktualisierungsprozess sorgt dafür, dass alle Teilnehmenden jeweils über den neuesten Stand der Datenbank verfügen. Eine besondere Ausprägung der DLT ist die Blockchain. (Gabler Wirtschaftslexikon, 2018)

Kryptowerte

Kryptowerte haben sich über die vergangenen Jahre enorm weiterentwickelt. Es gibt sie inzwischen in einer großen Anzahl und verschiedensten Ausprägungen. Einige von ihnen haben unter hohen Schwankungen enorme Wertsteigerungen erfahren. Stablecoins, die meist traditionelle Währungen digital abbilden, weisen sehr hohe Handelsvolumina auf. Da sie an andere Währungen „gekoppelt“ sind, unterliegen sie den gleichen Preis- bzw. Wechselkursschwankungen, denen auch die zugrundeliegenden Währungen unterliegen. Nach den Erkenntnissen von Blockchainanalytics-Unternehmen werden sie in großem Umfang für Transaktionen im Zusammenhang mit Straftaten genutzt.

Gründe für die Nutzung von Kryptowerten für illegale Zwecke sind einige grundlegende Eigenschaften wie Pseudonymität, Zuverlässigkeit, eine hohe Transaktionsgeschwindigkeit, eine gute Handelbarkeit, und die Möglichkeit grenzüberschreitende Transaktionen zu tätigen.

In den letzten Jahren hat es verschiedene regulatorische Maßnahmen gegeben, die auch den Risiken, die mit Kryptowerten einhergehen, etwas entgegensetzen sollen. Sie wurden in Deutschland bereits früh regulatorisch als Finanzinstrumente eingestuft, zum 1. Januar 2020 wurde das Kryptoverwahrgeschäft als erlaubnispflichtige Finanzdienstleistung

Definitionen:

Artikel 3 Absatz 1 Nummer 5 der Verordnung (EU) 2023/1114:

„Kryptowert“: eine digitale Darstellung eines Werts oder eines Rechts, der bzw. das unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden kann.

Vormalige Definition im KWG (§ 1 Abs. 11 Satz 4 und 5 KWG):

„Digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann.“

eingeführt. Auch auf internationaler Ebene sind wesentliche regulatorische Maßnahmen erfolgt.

Die Verordnung (EU) 2023/1114 (Markets in Crypto Assets Regulation; kurz MiCAR)¹ trat am 29. Juni 2023 in Kraft und schuf eine europaweit einheitliche Regulierung des Marktes für

¹ Verordnung (EU) 2023/1114 (<https://eur-lex.europa.eu/legal->

[content/DE/TXT/?uri=CELEX:32023R1114](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023R1114), Abruf: 23. April 2025.)

Kryptowerte. Sie regelt Transparenz- und Offenlegungspflichten für die Emission und den Handel von Kryptowerten, die Zulassungspflicht von und die Aufsicht über Kryptowerte-Dienstleister sowie Emittenten von Kryptowerten, die ordnungsgemäße Geschäftsorganisation von Kryptowerte-Emittenten sowie Kryptowerte-Dienstleistern, Investoren- und Verbraucherschutzvorschriften für die Emission, den Handel und die Verwahrung von Kryptowerten sowie Vorschriften zur Bekämpfung von Marktmissbrauch auf Kryptohandelsplätzen.

Die Geldtransferverordnung (EU) 2023/1113 (Transfer of Funds Regulation) trat im Juni 2023 in Kraft und erfasst auch Kryptowertetransfers. Sie enthält Vorschriften zu den Angaben, die bei Durchführung eines Geld- bzw. Kryptowertetransfers zu übermitteln sind. Die Angaben dienen der Prävention von Geldwäsche und Terrorismusfinanzierung und sollen die Rückverfolgbarkeit von Transaktionen gewährleisten. Sie setzte die FATF Travel Rule im europäischen um. Die Travel Rule verpflichtet Crypto Assets Service Provider (CASPs) Herkunfts- und Empfängerdaten transaktionsbegleitend zu übermitteln und zu prüfen. Mit der Kryptowertetransferverordnung (KryptoWTransferV) wurde die Travel Rule der FATF bereits zuvor in deutsches Recht umgesetzt.

Die FIU beobachtete bis weit in das Jahr 2022 hinein, dass eingegangene Meldungen, die Auffälligkeiten im Zusammenhang mit Kryptowerten aufwiesen, vorrangig von Kreditinstituten übermittelt wurden. Seit dem dritten Quartal

2022 lässt sich im längeren Trend feststellen, dass die Anzahl der Meldungen, die von CASPs (Crypto Asset Service Providern) stammen, ansteigt. Dazu ist anzumerken, dass zunehmend verpflichtete Institute, insb. Kreditinstitute und Finanzdienstleistungsinstitute, über eine Erlaubnis zur Erbringung von Kryptowerte-Dienstleistungen verfügen. Die entsprechenden Meldungen beruhen regelmäßig auf automatisiert generierten Risikoindikationen der eingesetzten Blockchain-Analyse-Tools.

Grundlage dieser Systeme sind Risikoscores, die auf Basis von Datenbanken und Analysen generiert werden. Eine erhöhte Risikoeinstufung kann insbesondere dann erfolgen, wenn Wallet-Adressen im Zusammenhang mit Darknet-Marktplätzen, bekannten

Decentralized Finance (DeFi):

Sogenannte Dezentralisierte Finanzdienstleistungen, auch bezeichnet als DeFi, sind neue Arten von Anwendungen, die auf der Basis von Blockchains mittels Smart Contract-Funktionalitäten ausgeführt werden. Voraussetzungen dafür ist, dass eine Blockchain die Ausführung von Programmecode ermöglicht. Die Programme, die dann auf Basis von Smart Contracts ausgeführt werden, bieten verschiedene Finanzdienstleistungen im Kryptobereich bzw. auf Basis von Kryptowerten an. Dazu gehören der Tausch in verschiedene Kryptowerte über dezentrale Handelsplattformen („DEXes“) aber auch dezentrale Formen der Kreditvergabe oder dezentral erzeugte Stablecoins.

Betrugssachverhalten, sanktionierten Entitäten oder sonstigen potenziell geldwäscherelevanten Aktivitäten identifiziert wurden. Gleiches gilt für Adressen mit Bezügen zu nicht regulierten oder als risikobehaftet eingestuften Kryptobörsen, Mixing- oder Anonymisierungsdiensten oder sonstigen Diensten, die geeignet sein könnten, die Nachvollziehbarkeit von Transaktionsströmen erheblich zu erschweren.

Informationen zu den jeweils verdächtigen Faktoren, den zugrunde liegenden Risikoindikatoren sowie zur konkreten Transaktionsstruktur sind für die FIU von erheblicher Relevanz und sollten im Rahmen der Verdachtsmeldung möglichst vollständig, nachvollziehbar und strukturiert übermittelt werden.

Quelle	URL (Stand Juli 2026)
Gesamtüberblick, unter anderem über Kryptowerte und Kryptobörsen	https://coinmarketcap.com/
Überblick zu Kryptoautomaten	https://coinautmradar.com/
BaFin-Unternehmensdatenbank: Überblick über in Deutschland registrierte Entitäten aus dem Finanzsektor einschl. MiCAR-Emittenten, Kryptowertpapierregisterführer, Kryptoverwahrer und Kryptowerte-Dienstleister ²	https://portal.mvp.bafin.de/database/InstInfo/
Nützliche Informationsquellen für die Überprüfung von Wallet-Adressen	Blockchain-Explorer z.B. für Bitcoin (BTC): https://www.walletexplorer.com/ , für Ethereum (ETH): https://etherscan.io/ Abgleich mit Wallet-Blacklists (z.B. https://btcbblack.it/bitcoin)

NFT

NFT, Non-Fungible Token (nicht austauschbare Token), haben sich zu einer neuartigen digitalen Asset-Klasse entwickelt, die über den

Markt für digitale Kunstwerke hinausreicht. „Nicht austauschbar“ ist hierbei mit „einzartig“ gleichzusetzen, vergleichbar mit einer

² Auswahl über die Suchoption „Kategorie“ in der Datenbank.

einzelnen bestimmten Sammelkarte. Aus diesem Grund werden NFT auch rechtlich nicht immer mit anderen „fungiblen“ Kryptowerten gleichgesetzt (vgl. EU-GeldtransferVO (Art.2 Abs.14)). Sie werden hier daher gesondert betrachtet.

Aus den unterschiedlichen Beschreibungen von NFT lassen sich folgende zentrale Merkmale ableiten.

- NFT sind auf einer (Smart Contract fähigen) Blockchain tokenisierte digitale Dateien. Sie sind einzigartig und nicht wie bspw. bei Bitcoin durch ein anderes Token der gleichen Art (Bitcoin) ersetzbar (d.h. nicht fungibel).
- Die Dateien können dabei alles Mögliche sein: Bilddateien, Videos, Musik, Spiele, digitale Sammelkarten, In-Game-Items, Texte, Ausbildungszertifikate, es kann sich auch um einen programmierten Software- bzw. Programmcode handeln. In der Regel wird das NFT mit einer Datei verknüpft.
- Durch das NFT wird die Datei in der Blockchain als Original verifiziert und zertifiziert. Der Prozess der Erstellung eines NFT wird als „Minting“ bezeichnet.
- NFT ermöglichen digitales Eigentum an einem einzigartigen (digitalen) Gegenstand. Der Eigentumsnachweis ist unmittelbar verifizierbar, ohne dass Intermediäre benötigt werden.
- NFT sind beliebig übertragbar.

NFT hatten zeitweilig eine hohe Aufmerksamkeit erfahren. Es hatte sich Anfang der 2020er

Jahre zeitweise ein regelrechter Hype gebildet, der jedoch stark abgeebbt ist. Der Grund für den Hype waren die enormen Summen, die teilweise für die einzigartigen Token gezahlt wurden.

Ähnlich wie Kunstgegenstände stellen NFT

Token:

Als Krypto-Token bezeichnet man eine digitalisierte, auf einer Blockchain dezentral gespeicherte Abbildung von Vermögenswerten. Ihnen wird eine bestimmte Funktion oder ein bestimmter Wert zugesprochen. Diese Werte können unterschiedlichste Eigenschaften, Funktionalitäten oder Rechte darstellen. Die Werte können den Krypto-Token selbst innewohnen oder die Werthaltigkeit wird den Krypto-Token von den beteiligten Verkehrskreisen zugesprochen. (Quelle: BaFin)

Werte dar, deren Preis nicht an objektive Wertmaßstäbe gebunden ist, die damit schwierig bewertbar und potenziell leicht manipulationsanfällig sind. Es gibt Beispiele, in denen NFT z.B. zum Smurfing von Beträgen eingesetzt werden. Dazu gibt es wie bei anderen Vermögenswerten auch Möglichkeiten durch die Manipulation von Handelsaktivitäten.

Der zwischenzeitliche Hype um NFT hat sich inzwischen deutlich abgeschwächt. Dies ist insbesondere darauf zurückzuführen, dass viele Projekte keinen nachhaltigen wirtschaftlichen oder praktischen Nutzen aufweisen und der Markt in der Hochphase vor allem durch spekulative Nachfrage sowie teils stark überhöhte Bewertungen geprägt war. In der Folge hat das

allgemeine Interesse an NFT spürbar nachgelassen, sodass sich der Markt heute stärker auf einzelne Anwendungsbereiche (u.a. In-Game-

Sonstige digitale Werte (Gaming-Bereich)

Neben den zuvor beschriebenen, auf Basis der Distributed-Ledger-Technologie basierenden Vermögenswerte, gibt es weitere, die ebenfalls an Bedeutung gewonnen haben. Es handelt sich hierbei um zumeist von Plattformen oder Spieleentwicklern zentralisiert ausgegebene Währungen oder virtuelle Gegenstände, die auch außerhalb der Plattform bzw. des Spiels nachgefragt und handelbar sind.

In-Game-Währungen (z.B. Gold, Credits, Token) und virtuelle Gegenstände (z.B. seltene Ausrüstung, Sammelkarten) sind zentrale Elemente vieler Videospiele, insbesondere in Online-Titeln. In-Game-Währungen sind dabei digitale Zahlungsmittel, die Spielende gegen reales Geld kaufen können oder innerhalb eines Spiels verdienen können, um damit besondere Inhalte freizuschalten. Sie dienen oft als Ersatz für echtes Geld und ermöglichen den Erwerb von Spielfortschritten, kosmetischen Anpassungen oder praktischen Vorteilen. Virtuelle

Währungen, Digitale Identitäten) mit tatsächlichem Mehrwert konzentriert.

Gegenstände umfassen hingegen alle Objekte, die innerhalb einer Spielwelt existieren. Sie haben oft einen klaren Nutzwert im Spiel und können über In-Game-Marktplätze gegen In-Game-Währungen gekauft oder auch innerhalb des Spiels verschenkt werden. Über Drittanbieter ist es möglich In-Game-Währungen, Gegenstände oder gar ganze Gaming-Accounts für reales Geld zu kaufen oder gegen solches zu verkaufen. Ein solcher Tausch gegen echtes Geld ist in vielen Fällen nicht von den Spieleentwicklern vorgesehen oder sogar verboten, sodass hier auf Zweitmärkte ausgewichen wird. Da die Spieleentwickler zudem keine Kontrolle über die Zweitmärkte haben, lassen sich diese Geschäfte nur schwer verhindern. Risiken entstehen in diesem Bereich vor allem dadurch, dass in der Regel weder Spieleentwickler noch die Zweitmärkte geldwäscherechtlichen Sorgfaltspflichten unterliegen.

Digitalisierung von Zahlungsmöglichkeiten/Zahlungsplattformen

Die Digitalisierung hat zahlreiche neue Zahlungsmöglichkeiten und Zahlungsplattformen hervorgebracht. Insbesondere im stark gewachsenen Internethandel und im Bereich des E-Commerce haben sich neue Formen der Zahlungsabwicklung verbreitet. Diese werden häufig zwischen kaufender und verkaufender Partei eingesetzt bzw. zwischengeschaltet. Nutzende von Zahlungsdienstleistungen finden

eine Vielzahl von Anbietern verschiedener Apps und Plattformen, bei denen sie ihre Zahlungsdetails hinterlegen können und mit denen sie Zahlungen ausführen können.

In Anbetracht ihrer Vielzahl dürften Nutzende heute nur noch selten über nur eine Zahlungsoption oder eine einzige Kontoverbindung verfügen. Eine Kontoeröffnung erfolgt

nur noch selten im Wege einer persönlichen Vorsprache beim Institut, sondern zumeist online per Video-Identifizierungsverfahren. Die Hürden und der Aufwand für die Eröffnung digitaler Konten sind gering, was sie für die Verschleierung und Verlagerung von Vermögenswerten zu Zwecken der Geldwäsche anfällig macht. Die erweiterte Vielfalt und die Anzahl an Zahlungsmöglichkeiten bietet ihnen neue Optionen, die in diesem Abschnitt vorgestellt werden.

Dazu zählen auch Möglichkeiten, Werte zwischen den Usern von Sozialen Medien zu transferieren. Social-Media-Plattformen bieten

ihren Nutzenden vermehrt solche Möglichkeiten an.

Die Plattformökonomie bringt auch Kapitalgebende und Kapitalnehmende noch einfacher und enger zusammen. Crowdfunding-Plattformen im Internet, die in den vergangenen Jahren stark gewachsen sind, bieten Finanzierungsmöglichkeiten außerhalb der klassischen Finanzierungsquellen.

Die mit diesen Optionen einhergehenden Möglichkeiten lassen sich zur Geldwäsche ausnutzen, weshalb in diesem Papier hierfür besonders sensibilisiert werden soll.

E-Wallets / Digitale Wallets von Online-Zahlungsdienstleistern

Über die letzten Dekaden haben sich mit der fortschreitenden Digitalisierung und der Verbreitung des Onlinehandels alternative unbare Zahlungsformen fest etabliert. Transaktionen im Zusammenhang mit Käufen werden hierbei nicht unmittelbar über die Bankverbindungen der Transaktionsbeteiligten abgewickelt. Stattdessen wird eine digitale Wallet, die von einem Zahlungsdienstleister oder einem E-Geldinstitut bereitgestellt wird, zwischengeschaltet. Einige dieser Zahlungsdienstleister verfügen inzwischen über marktbeherrschende Stellungen. Der Marktführer in Deutschland hat nach eigenen Angaben 35 Millionen aktive Kundenkonten. Durch die Zwischenschaltung eines Zahlungsdienstleisters oder E-Geld-Instituts muss man dem jeweils anderen Transaktionspartner nicht seine Konto-/Kreditkartennummern offenbaren oder für jede Transaktion

Bankdaten eingeben. Dies erzeugt für die Nutzenden oftmals ein höheres Gefühl der Sicherheit, geht aber auch mit einem höheren Maß an Vertraulichkeit einher, weil man der Gegenpartei der Transaktion keine sensiblen Informationen wie Bankdaten übermitteln muss oder sich nicht klar mit persönlichen Angaben offenbaren muss, sondern z.B. Alias-Namen angeben kann. Die Nutzenden verknüpfen die Accounts bzw. ihre digitalen Wallets mit Zahlungsdaten, über die dann auch die Transaktionen abgerechnet werden. Inzwischen ist die Auswahl an Zahlungsdienstleistern sehr groß, da weitere Anbieter in diesen Markt eingetreten sind. Dazu gehören nicht nur traditionelle Finanzdienstleister, sondern auch große IT-Anbieter (Google Pay, Apple Pay), die schon seit längerer Zeit eigene Zahlungsdienste anbieten (z.B. für App-, In-App-Käufe aber auch darüber hinaus).

Aber auch große Onlinehändler haben eigene Zahlungsdienste etabliert und ermöglichen eine komfortable Nutzung des Dienstes auch bei anderen Unternehmen. Der Kunde oder die Kundin kann im Onlinehandel heute in der Regel zwischen einer größeren Zahl unterschiedlicher Anbieter und Bezahlmethoden wählen. Die Zahlungsdienstleister bieten den Nutzenden weitere unterschiedliche Services an, wie Zahlung aus Rechnung oder Ratenzahlung.

Social-Media- und Streaming-Plattformen

Content-Provider erlangen durch die Plattform unmittelbar eine potenzielle Reichweite von Mrd. von Nutzenden. Vor zwei Jahrzehnten fast noch gänzlich unbekannt, haben sich Social-Media- und Streaming-Plattformen zu einem riesigen Markt entwickelt mit einer Nutzerbasis im Milliardenbereich. Es gibt so gut wie keine Person, die nicht mindestens einen Account auf einer der führenden Plattformen hat. Die weiterwachsende Anzahl der Nutzenden führt in diesem Bereich auch zu einem deutlichen Anstieg der verbundenen Geldflüsse. Allein im Jahr 2024 wurden weltweit etwa 32,2 Milliarden Euro für Content-Provider-Werbung ausgegeben.³ Die Gage für einen einzelnen Post oder für ein einzelnes Video orientiert sich dabei in der Regel sehr stark an der Reichweite der Content-Provider und liegt je nach Plattform in etwa zwischen 1.000 und 10.000 US-Dollar. In seltenen Fällen können jedoch Gagen von bis zu 1 Million US-Dollar für einen einzigen Post verdient werden.⁴

Auch geben sie zum Teil eigene Zahlungskarten heraus, die für Einkäufe in lokalen Geschäften genutzt werden können. Doch nicht nur die Zahlungen im Onlinehandel wickeln die Anbieter ab, sondern häufig auch Zahlungen und Transaktionen zwischen den Nutzenden des Zahlungsdienstleisters untereinander.

Neben den bestehenden typischen Vergütungssystemen für die Anzahl der Aufrufe, die Zahl der Follower und Followerinnen und den anteiligen Werbeeinnahmen, ermöglichen viele Plattformen auch den direkten Transfer von monetären Werten in Form von Coins/Geschenken/Donations zwischen den Nutzenden der Plattformen. Gelder lassen sich so zwischen den Nutzenden versenden und anschließend in Form von Fiat-Währungen auszahlen. Anreiz für Plattformen ist die Schaffung eines zusätzlichen und differenzierten Wegs zur Monetarisierung angebotener Inhalte. Dabei ist dieses Prinzip vergleichbar mit einem virtuellen Trinkgeldglas. Gefällt der gezeigte Inhalt, bietet die Plattform den Nutzenden die Möglichkeit den Content-Providern Geld als Donations zukommen zu lassen. Diese Donations können in Form einer eigenen Plattform-Währung (wie beispielsweise „TikTok-Coin“), mehreren einmaligen Abonnements (beispielsweise „Subs“

³ (Statista, 2024)

⁴ (Influencer Marketing Hub, 2025)

auf Twitch) oder virtuellen Geschenken erfolgen.

Bei Donations erfolgen in der Regel zunächst Einzahlungen über die von der Social-Media- oder Streaming-Plattform zur Verfügung gestellten Kanäle (bspw. bei Twitch: Paypal, Amazon Pay, Kredit Karte, Kryptowerte, Paysafe Karte, Apple Pay u.v.m.). Je nach Plattform wird die Einzahlung entweder gezielt einer bestimmten Verwendung zugeordnet und

unmittelbar damit ausgelöst, oder sie fließt auf eine Art Wallet (entweder in Fiat oder der Plattform-Währung), die als Prepaidkonto für die Nutzung auf der Plattform dient.

Eine Person, die die Donations erhält kann diese dann entweder – sofern es sich um eine Plattform-Währung handelt – weiterreichen oder aber über die Plattform in Fiat auszahlen lassen.

Crowdfunding-Plattformen

Crowdfunding wird genutzt, um für die Finanzierung von Projekten, Immobilien, Startups und etablierten Unternehmen finanzielle Mittel zu beschaffen. Diese Art der Finanzierung erfreut sich in den letzten Jahren einer zunehmenden Beliebtheit. Laut einer Markterhebung der ESMA (European Securities and Markets Authority) betrug die aggregierte Summe der über EU-Crowdfunding-Anbieter abgewickelten Projekte im Jahr 2024 über 4 Mrd. Euro und somit deutlich mehr als die 1 Mrd. Euro im Jahr 2023. Im selben Zeitraum stieg die Anzahl der in der EU niedergelassenen Anbieter von 98 (in 17 Ländern) auf 181 (in 21 Ländern).⁵ Verschiedene Plattformen bieten Möglichkeiten ein Projekt oder eine Idee einer Vielzahl von Menschen vorzustellen und finanzielle Mittel für die Verwirklichung des Projekts zur Verfügung zu sammeln (Schwarmfinanzierung). Crowdfunding kann über eine eigens dafür erstellte Crowdfunding-Plattform oder über diverse andere Medien und somit eigeninitiativ erarbeitet

werden. Über das Internet, Homepages und soziale Medien wird dann dafür geworben, sich an dem Projekt finanziell zu beteiligen. Beteiligte bei einem Crowdfunding sind Projektinitiiierende und deren Unterstützerinnen und Unterstützer.

Auf der jeweiligen Plattform können die Projektinitiiierenden ihr Projekt der Öffentlichkeit vorstellen. Potenzielle Unterstützer und Unterstützerinnen können sich dort über Projekte informieren und sich aussuchen, welches sie finanziell fördern möchten. Wenn sie ein Projekt ausgewählt und einen Beitrag zur Finanzierung geleistet haben (in der Regel durch eine Zahlung an die Crowdfunding-Plattform, die dann die Gelder an die Projektinitiiierenden weitergibt), bekommen sie je nach Art des Crowdfundings hierfür von den Projektinitiiierenden eine Gegenleistung in Aussicht gestellt. Das können z.B. auch Zinszahlungen sein. Die konkrete Gegenleistung für die Investition hängt allerdings von dem gewählten Crowdfunding-Modell ab.

⁵ (ESMA)

Es lassen sich dabei vier mögliche Modelle unterscheiden: Spendenbasiertes Crowdfunding (donation based), Gegenleistungsbasiertes Crowdfunding (reward-based), Kreditbasiertes

Crowdfunding (lending-based) und Crowdfunding (equity-based).⁶ Schätzungen über die Größe des Crowdfunding-Marktes belaufen sich auf rund 1,8 Mrd. US-Dollar im Jahr 2025.⁷

⁶ (Arten von Crowdfunding)

⁷ <https://www.fortunebusinessinsights.com/de/crowdfunding-markt-107129> (Abruf 23.10.2025).

Modi Operandi...

In den nachfolgenden Abschnitten werden typische Nutzungsformen der zuvor beschriebenen (alternativen) Zahlungsmethoden und

... im Zusammenhang mit Kryptowerten

Für Geldwäsche mit Kryptowerten ist zunächst danach zu differenzieren, ob der aus einer Straftat stammende Ertrag, der gewaschen werden soll, bereits in Form von Kryptowerten vorliegt oder nicht. Sofern dies nicht der Fall ist, erfolgt zuvor eine Konvertierung in Kryptowerte. Diese Phase der Konvertierung von Fiatgeld in Kryptowerte stellt dann eine erste Phase bzw. Stufe der Geldwäsche dar, auf die hier aber nicht vertiefend eingegangen wird, da die anschließenden Verschleierungsmöglichkeiten mit Kryptowerten im Vordergrund der Betrachtung stehen.

Viele Kryptowerte, wie beispielsweise Bitcoin, können durch die Nutzenden nur pseudonym (d.h. nicht vollständig anonym) gehandelt werden. Da bei gängigen Kryptowerten sämtliche

neuen Technologien im Zusammenhang mit Geldwäscheaktivitäten dargestellt.

Transaktionen auf der Blockchain dauerhaft öffentlich gespeichert sind und Wallet-Adressen zumindest mittelbar mit natürlichen oder juristischen Personen in Verbindung stehen, sind Transaktionen und Wallets unter Nutzung zusätzlicher Informationen und Analyseverfahren grundsätzlich einer konkreten Person zuzuordnen. Aus diesem Grund werden zur Geldwäsche diverse Tools und Möglichkeiten genutzt um diese Nachvollziehbarkeit zu erschweren und um auf diese Weise inkriminierte Gelder zu verschleiern. Die gängigsten und bisher bekannten Modi Operandi werden in den folgenden Abschnitten dargestellt.

Die FIU bittet die Verpflichteten bei Abgabe einer Verdachtsmeldung zu den hier genannten Phänomenen und Typologien in der Verdachtsmeldung den Indikator

C1011 - Auffälligkeiten i.Z.m. Kryptowährungen (z.B. Bitcoin)

zu setzen. Dies entbindet die Verpflichteten aber nicht von einer aussagekräftigen Sachverhaltschilderung.

Nutzung von Mixer/Tumbler/Blender

Ein Mixer (oder auch Tumbler oder Blender genannt) ist ein Dienst, der Kryptowerte von verschiedenen Nutzenden miteinander vermischt und so dazu dient die Herkunft zu verschleiern. Die Nutzung von Mixern ist nicht per se illegal.

Neben legitimen Gründen zur legalen Nutzung von Mixern, wie beispielsweise den Schutz der finanziellen Privatsphäre, bietet diese Art der Vermischung von Kryptowerten im Fall des Betriebens von Geldwäsche die Chance das

Nachverfolgen inkriminierter Gelder zu erschweren oder teils unmöglich zu machen.

Die Nutzung eines Mixers läuft im Wesentlichen in vier Schritten ab:

1. Einzahlung

Nutzende erhalten eine einzigartige Einzahlungsadresse vom Mixer-Dienst. So können mehrere Zahlungen einer einzelnen Person nicht direkt miteinander in Verbindung gebracht werden.

Auf diese einzigartige Adresse zahlen die Nutzenden die zu mixenden Kryptowerte ein. In der Regel handelt es sich hierbei um selbstverwaltete bzw. unhosted Wallets.

2. Poolbildung

Die eingezahlten Kryptowerte werden in einen Pool übertragen, in dem auch die Kryptowerte anderer Nutzender übertragen werden. Dieser Pool beinhaltet viele verschiedene unhosted Wallets und ermöglicht es die Einzahlungen durch mehrfache Transaktionen zwischen diesen Wallets zu vermischen. Um das Vermischen effizienter und damit die Nachverfolgbarkeit schwieriger zu machen, erfolgen die Transaktionen innerhalb dieses Pools nicht in der Höhe der Einzahlungen. Die Beträge werden gestückelt durch den Pool transferiert. Eine Nachverfolgbarkeit auf Basis der Transaktionshöhe ist somit praktisch nicht mehr möglich.

3. Verzögerte Auszahlung

Viele Mixer bieten die Option von unterschiedlichen verzögerten Auszahlungen an, dabei kann es sein, dass die Auszahlung in einem

zufälligen Abstand von einigen Stunden oder Tagen nach der Einzahlung erfolgt oder, dass die Auszahlung zunächst an eine Zwischenwallet geleistet wird und die Nutzenden diese nach Belieben von dieser an die eigene Wallet übertragen kann.

Zweck dieser verzögerten Auszahlungsmethoden ist das Einbinden einer weiteren Hürde der Nachverfolgbarkeit.

4. Auszahlung an neue Adresse

Die Auszahlung erfolgt schließlich an eine von dem oder der Nutzenden angegebene Wallet-Adresse. Diese hat/sollte in der Regel keine Verbindung zu der Wallet haben von der die Einzahlung erfolgt ist.

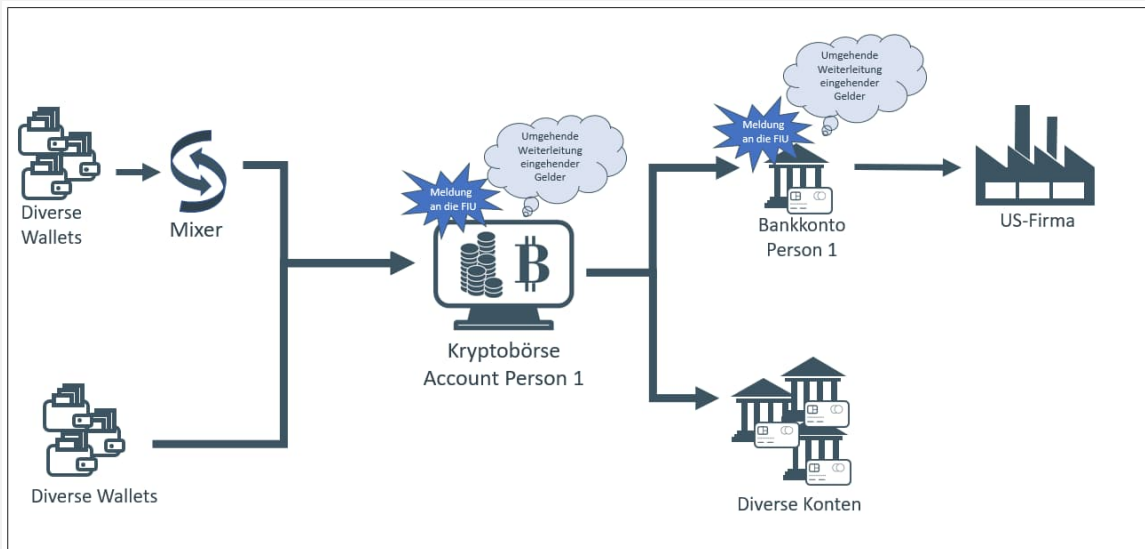
Zum jetzigen Zeitpunkt bieten einige Blockchain-Analyse-Tools die Möglichkeit zur teilweisen Rückverfolgung der aus bekannten Mixern ausgehenden Kryptowerte. Diese Rückverfolgung ist jedoch nur in solchen Fällen möglich, in denen die Wallet aufgrund von Informationen oder anhand bestimmter Kriterien einem Mixer zugeordnet werden konnte und basiert auf dem Follow-the-Money-Ansatz – in diesem Fall von den vom Mixer ausgezahlten Kryptowerten hin zu den eingezahlten Kryptowerten.

Anhaltspunkte, die auf die Nutzung von Mixern zur Geldwäsche hindeuten könnten:

- Der Zufluss von Kryptowerten auf eine Wallet erfolgt zuvor über eine Vielzahl zwischengeschalteter Adressen, die typischerweise eine erhöhte Transaktionskomplexität aufweisen.
- Ein Blockchain-Analyse-Tool oder ein vergleichbares Monitoring-System weist auf eine mögliche oder wahrscheinliche Verbindung der Herkunfts- oder Zieladresse zu Mixing-Services, Coin-Join-Transaktionen oder sonstigen Anonymisierungs- bzw. Verschleierungsmechanismen hin.
- Es liegen strukturierte Zahlungseingänge vor, beispielsweise:
 - o Regelmäßige oder gleiche Abstände der Zahlungseingänge
 - o Multi-Input/Multi-Output-Transaktionen
 - o Transaktionen lassen sich an Pool-Adressen zurückverfolgen
- Zahlreiche Nutzende senden Werte an dieselbe Wallet-Adresse ohne, dass es einen legitimen Grund (Geschäftszweck, Adresse ist einer Börse zugehörig etc.) dafür gibt.

Beispielfall

Bei einer Handelsplattform wurde Person 1 auffällig, da sie in 67 Transaktionen Bitcoins und USDC im Wert von über 400.000 Euro von diversen Wallets erhalten hatte. Hinzu kam, dass ein Teil der Gelder von einer Wallet kam, die in Verbindung zu einem Mixing Service steht. Person 1 leitete einen Großteil der Gelder (394.000 Euro) umgehend weiter. In 60 Transaktionen wurden 107.000 Euro an diverse Bankkonten gezahlt und in 6 Transaktionen wurden 287.000 Euro an ein Bankkonto mit Person 1 als Kontoinhaber gezahlt.

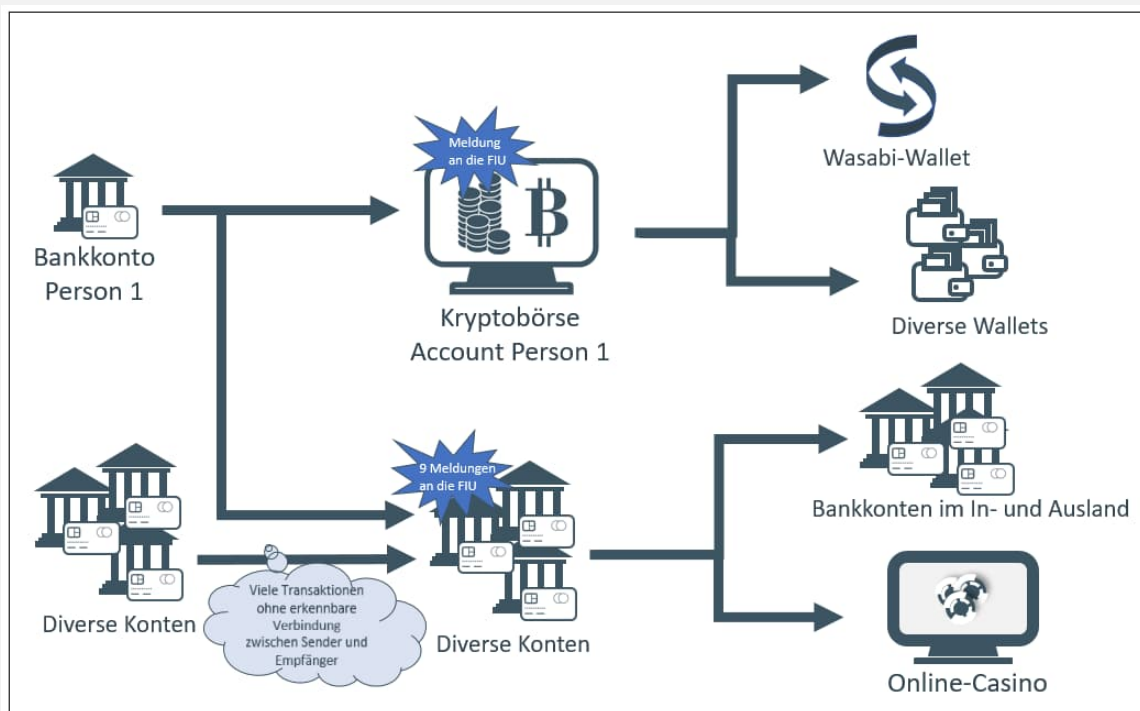


Die kontoführende Bank meldete wiederum, dass die Gelder umgehend an eine US-Firma weitergeleitet wurden. Eine Verbindung zwischen Person 1 und der Firma bestand nicht. Außerdem sei Person 1 Student und besitze kein geregeltes Einkommen, sodass die Umsätze nicht mit den wirtschaftlichen Verhältnissen der Person 1 übereinstimmen.

Beispielfall

Bei einer Kryptobörse wurde Person 1 auffällig, da sie Kryptowerte im Wert von ca. 920.000 Euro an eine Wallet-Adresse versendet hat, die dem Mixing Service Wasabi-Wallet zugeordnet wurde. Darüber hinaus versendete die Person in 37 Transaktionen ca. 1 Mio. Euro an andere Wallet-Adressen.

Das zugehörige Referenzkonto wurde zeitgleich in 9 weiteren Verdachtsmeldungen bei der FIU gemeldet. Dieses ist auffällig geworden, da vierstellige Beträge an weitere Konten der meldenden Institutionen gingen, ohne dass eine ersichtliche Verbindung zwischen Empfänger- und Senderkonten bestand. Darüber hinaus wurden die Gelder anschließend an andere Konten im In- und Ausland sowie in einem Fall an Glücksspielseiten weitergeleitet.



Nutzung von Bridges/Chain-Hopping/-Swapping

Mechanismen, die eine Nutzung von Vermögenswerten in Form von Kryptowerten oder aber auch Informationen zwischen verschiedenen Blockchains ermöglichen, nennen sich Bridges. Sie sind aber auch unter diversen anderen Namen bekannt. Zu den bekanntesten Bezeichnungen zählen Blockchain- oder Cross-Chain-Bridges, deren Nutzung dann als Chain-Hopping oder Chain Swapping bezeichnet wird. Bridges dienen dazu, Interoperabilität zwischen unterschiedlichen Blockchain-Netzwerken herzustellen, da diese grundsätzlich nicht miteinander kompatibel sind. Im groben lassen sie sich in die beiden Kategorien vertrauensbasiert (Abwicklung wird von einer unabhängigen Instanz durchgeführt) und vertrauenslos (Abwicklung ohne unabhängige Instanz – meist über Smart Contracts) einordnen.

Das Geldwäscherisiko bei der Nutzung von Bridges liegt in der Möglichkeit

Vermögenswerte in Form von Kryptowerten zwischen verschiedenen Blockchain-Netzwerken zu verschieben und die Nachvollziehbarkeit der Geldflüsse zu erschweren. Besonders die Formen der Bridges, die keine nachvollziehbaren Protokolle in Form von Smart Contracts zugrunde liegen haben, sind für Ermittlungsbehörden schwer nachzuvollziehen. Hinzu kommt, dass aufgrund der Entwicklungen die Kosten für Sprünge zwischen den Netzwerken immer geringer werden, sodass ein häufigeres, hintereinandergeschaltetes Nutzen von Bridges ohne große Verluste möglich ist. Dies wiederum nutzen Geldwäschetreiber um das Nachvollziehen der Geldbewegungen weiter zu erschweren.

Anhaltspunkte, die auf die Nutzung von Bridges zur Geldwäsche hindeuten könnten:

Der Kunde oder die Kundin...

- ...veranlasst in kurzer Zeit zahlreiche wirtschaftlich nicht plausible Handels- und Umtauschgeschäfte bzw. Konvertierung zwischen verschiedenen Kryptowerten ohne erkennbaren Hintergrund, mit dem mutmaßlichen Ziel die Nachvollziehbarkeit der Transaktionskette zu erschweren.
- ...einer zentralisierten Börse erhält häufig Kryptowerte-Einzahlungen von Adressen, die mit Bridges verbunden sind und kann diese Transaktionen nicht erklären. Zugleich zeigt eine Blockchain-Analyse, dass einige dieser Gelder auf illegale Quellen wie bspw. Wallets mit Verbindung zu Ransomware oder dem Darknet zurückgeführt werden können.

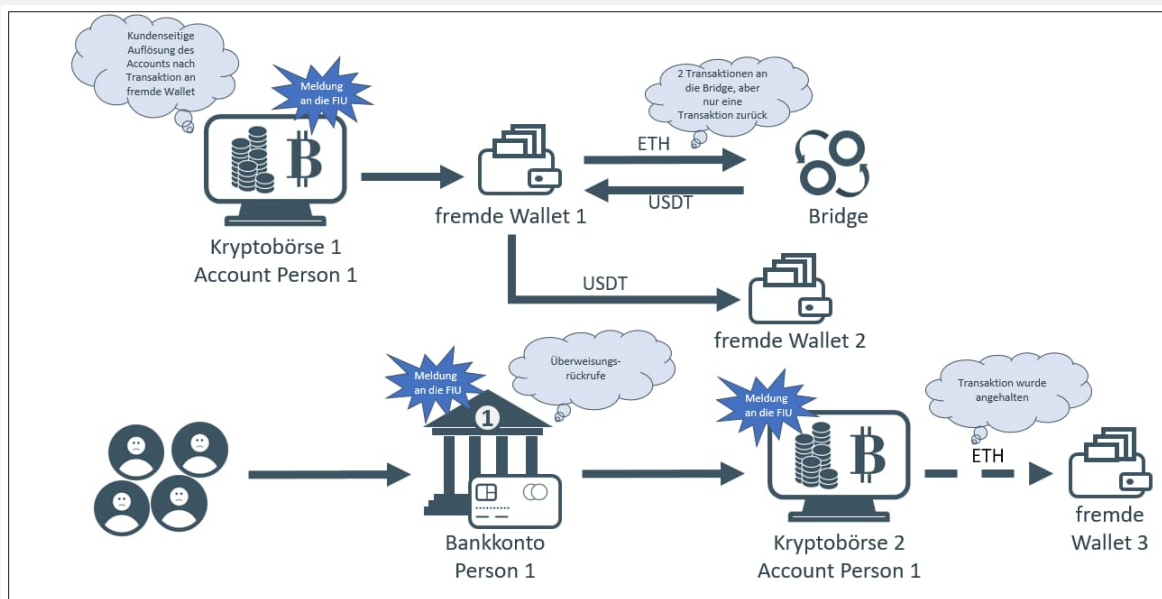
Beispielfall

Von einer Kryptobörse 1 wurde eine Person gemeldet, die kurz vor kundenseitiger Auflösung des Kontos ihre Kryptowerte (Ethereum) auf eine fremde Wallet transferiert hatte. Von dieser Wallet wurden die Kryptowerte in zwei Transaktionen zu einem Bridging-Service versendet. Für eine Transaktion wurde der entsprechende Betrag in USDT zurückversendet, der Verbleib der restlichen Kryptowerte ist unklar. Die USDT wurden daraufhin an eine andere Wallet-Adresse transferiert.

Bei einer weiteren Kryptobörse 2 wurde eine Kryptowertetransaktion des gleichen Kunden an eine fremde Wallet angehalten. Die Bank von der die dazugehörigen Fiat-Einzahlungen stammen, gab auch eine Verdachtsmeldung zu dieser Person ab. Aus dieser geht hervor, dass die Gelder ihm kurz vor Einzahlung in einer Transaktion überwiesen wurden. Für diese Transaktion erreichte die Bank ein Überweisungsrückruf, dem der Kunde aber nicht zugestimmt hat.

Aus mitgelieferten Screenshots eines Chats des Kunden mit einem vermeintlichen Investmentberater geht hervor, dass der Kunde Opfer eines Anlagebetrugs geworden sein könnte. Er hatte aufgrund einer Werbung ein Konto bei einer Handelsplattform eröffnet, was zur Kontaktaufnahme des erwähnten Beraters führte. Bereits nach wenigen Tagen simulierte die Handelsplattform eine große Wertsteigerung des Portfolios, sodass der Kunde mithilfe des Beraters sein Konto bei der Kryptobörse 1 auflöste und die Gelder wie beschrieben weiterleitete. Es ist zu vermuten, dass die Kontrolle über die Kryptowerte danach nicht mehr bei ihm lag.

Durch ein gefälschtes Schreiben einer ausländischen Finanzaufsichtsbehörde eröffnete er gemeinsam mit dem Berater ein Konto bei der Kryptobörse 2, um sich dort seine angeblichen Gewinne auszahlen zu lassen. Dieses musste daraufhin mit 25.000 Euro für die Auszahlung legitimiert werden, dabei bat der Berater dem Kunden an ihm die Summe zu leihen bis die Auszahlung erfolgt ist. Daraufhin erhielt der Kunde die Fiatgelder, für die die Bank kurz darauf ein Überweisungsrückruf erhielt.



Die Nutzung des Bridging-Service erschwert hierbei die Nachverfolgung der Transaktionen und dient den Tatbeteiligten sowohl zur Umwandlung der Taterträge in Stablecoins und zur Verschleierung.

ICO – Initial Coin Offering

Ein Initial Coin Offering (ICO) ist die Verbindung von Crowdfunding (Schwarmfinanzierung durch Spenden) beziehungsweise Crowdinvesting (Schwarmfinanzierung durch Investitionen) mit der Blockchain. Begrifflich ist es angelehnt an Initial Public Offering (IPO), dem englischen Wort für Börsengang. Bei einem ICO werden allerdings im Gegensatz zum IPO keine Unternehmensanteile verkauft, sondern Einheiten eines Kryptowertes – auch Token genannt. Der ICO ermöglicht es in Token zu investieren, die noch nicht öffentlich gehandelt werden und diese zu erwerben.

Diese Token können entweder mit anderen Kryptowerten oder mit Fiat-Währungen erworben werden. In der Regel dient der Verkauf der Token der Finanzierung eines Projekts, meist eines Software-Projekts welches auf der Blockchain-Technologie basiert.

Im Anschluss an das ICO können die Token auf Börsen gehandelt werden. Dies ermöglicht einen Erwerb der Token auch nach der Markteinführung.

ICO werden von Startups aus dem Technologiesektor genutzt, um strikte Regulierungen im Finanzmarkt zu umgehen. Vergleichbar mit Crowdfunding/-investing Projekten beschreiben Anbieter in einer Art Broschüre was der Hintergrund ihres Projektes ist und welche

Probleme damit gelöst oder welche neuen Entwicklungen damit einhergehen sollen. Ebenfalls in dieser Phase wird ein Finanzierungsziel festgelegt, welches benötigt wird um das Projekt umzusetzen. In der Regel ist die Menge der offerierten Token begrenzt und die Herausgebenden behalten, genau wie beim Crowdinvesting auch, einen Teil der Token für sich. Dies fördert den eigenen Anreiz, das Projekt erfolgreich umzusetzen. Verfehlt ein ICO das gesetzte Finanzierungsziel, gilt das Projekt als gescheitert. In diesem Fall würden alle, die investiert haben, ihr Geld zurückerhalten.

Aufgrund prominenter Betrugsfälle wie „OneCoin“ werden in ICO vor allem Risiken für Vortaten zur Geldwäsche gesehen (insb. im Zusammenhang mit Betrug: „Fake-ICO“, „rug pulls“). Auf den zweiten Blick bieten sie allerdings auch die Möglichkeit zur Geldwäsche an sich. Geldwäschebetreibende könnten ein ICO-Projekt starten und mit inkriminierten Geldern in dieses Projekt investieren. Nach Abschluss des Projektes würde die Herkunft des Geldes als Auszahlung aus dem Investment ausgewiesen.

Grundsätzlich kann zwischen zwei Arten von angebotenen Token unterschieden werden:

Utility Token

Mit dem Besitz eines Tokens gehen keinerlei Rechte am Projekt einher. Vielmehr sollen die Token am Ende des Projektes als Zahlungsmittel genutzt werden. Mit einem erfolgreichen Projekt steigt der Wert des Tokens und ermöglicht das Erzielen von Kursgewinnen.

Revenue Share Token / Security Token / Equity Token

Ein Revenue Share Token, oder auch Security oder Equity Token genannt, lässt sich eher mit einer Aktie vergleichen. Der Besitzer eines Tokens ist zum Empfang von Gewinnausschüttungen berechtigt. Der Token fungiert in diesem Fall nicht zur Zielerfüllung des Projektes, sondern eher zum Auszahlen der Gewinne.

Je nachdem, wie der Token technisch implementiert ist, kann es sein, dass die Ausschüttung automatisiert über Smart Contracts erfolgt. Ein Beispiel könnte sein, dass ein Projekt Gewinne in Form von Ethereum generiert. Investierenden, die den eigenen Ethereum-basierten Token aus dem ICO halten, wird ein entsprechender Anteil des Gewinns auf ihre Ethereum-Wallet gutgeschrieben.⁸

Prominentes Beispiel eines Revenue Share Tokens:

Das bekannteste Beispiel für einen erfolgreichen ICO ist Ethereum. Ethereum ist ein Blockchain-Netzwerk zur Implementierung sogenannter Smart Contracts. Unter Smart Contracts werden auf der Blockchain hinterlegte Verträge verstanden, die ausgeführt werden, sobald alle in dem Vertrag definierten Bedingungen erfüllt sind.

Die nativen Token von Ethereum heißen Ether.

Der ICO für Ethereum war im Jahr 2014. Zu einem Preis von 40 US-Cents konnten Ether erworben werden und führten zu Einnahmen in Höhe von ca. 18 Mio. US-Dollar. Am 15. Juli 2025 lag der Wert eines Ether bei ca. 3.000 US-Dollar.

Bereits im Jahr 2016 nutzen erste Unternehmen in einem Pilotprojekt das Ethereum-Netzwerk für den täglichen Gebrauch. Damals wurde der erste Getreidehandel zwischen einem Landwirt und einem Großunternehmen abgewickelt. Die neue Technologie wurde dafür genutzt, dass der Landwirt sein Getreide über eine Plattform an das Unternehmen verkaufen konnte und bei der Lieferung direkt über die Plattform bezahlt wurde. (Hall, 2017)

⁸ (BTC-Echo)

Anhaltspunkte, die auf die Nutzung von ICO zur Geldwäsche hindeuten könnten:

- Es werden Kryptowerte oder Token genutzt, deren Ausgestaltung, Emissionsstruktur oder wirtschaftlicher Hintergrund nicht hinreichend transparent oder dokumentiert ist oder die im Zusammenhang mit potenziellen Betrugsdelikten stehen. Dies betrifft insbesondere Konstellationen, die auf betrügerische Kapitalbeschaffungsmodelle wie Schneeballsysteme oder nicht existierende bzw. betrügerische Token-Emissionen (sogenannte „Scam-ICOs“) abzielen.
- Eingehende Zahlungen weisen auf eine Mittelherkunft aus der Teilnahme an einem ICO hin. Weitere Transaktionen oder sonstige Aktivitäten, die auf eine tatsächliche Projektumsetzung schließen lassen, sind jedoch nicht erkennbar.
- Die Projekterstellenden wirken unseriös oder sind nicht ermittelbar.
- Das Projektziel ist nicht nachvollziehbar.

Marktmanipulation zu Zwecken der Geldwäsche

Es gibt verschiedene Formen der Marktmanipulation des Krypto-Finanzmarktes. Durch Marktmanipulation können inkriminierte Gelder nicht nur in den Finanz- und Wirtschaftskreislauf eingeschleust werden, sondern lassen sich auch noch vermehren. Durch den erfolgreichen Handel am Markt können sie im Anschluss einen Teil der Gelder als Gewinn ausweisen und sauber nutzen. Das inkriminierte

Geld stellt somit eine Art Startkapital dar, welches bei jeder der im folgenden aufgeführten Marktmanipulation zu Investitionszwecken benötigt wird. Im Rahmen der Geldwäsche stellen diese Manipulationsformen daher lediglich ein Vehikel dar, das es ermöglicht einen Nachweis für die Herkunft der Gelder zu generieren.

Wash Trading

Beim Wash Trading werden Vermögenswerte bzw. Assets gleichzeitig ge- und verkauft, um die Illusion hoher Markttätigkeiten zu erzeugen. Prinzipiell ist bei dieser Aktivität das Ziel andere Marktteilnehmende zu täuschen. Grundsätzlich weisen ungewöhnliche Handelsvolumina, die Preisstabilität bei hohem Handelsvolumen und ein (fast) gleichzeitiger Kauf und Verkauf eines Assets in identischer Höhe auf Wash Trading hin.

Zum Zwecke der Geldwäsche kann sich das Wash Trading anbieten, um mit dem Verkauf von Assets die Herkunft des Vermögens auszuweisen. Ein Nebeneffekt wären die „günstigen“ Verluste, die lediglich in Form von Trading-Gebühren entstehen würden. Ein über mehrere Etappen durchgeführtes Wash Trading könnte somit die Verfolgbarkeit zur ursprünglichen Herkunft des Geldes erschweren.

Pump-and-Dump & Poop-and-Scoop

Beim Pump-and-Dump (auf Deutsch aufpumpen und abstoßen) handelt es sich um eine potenzielle Betrugsmasche im Bereich der Handelsmärkte. Bei dieser Form der Marktmanipulation wird zunächst für einen günstigen Kurs ein Asset gekauft. Dann werden Informationen gestreut, dass ein bestimmter Vermögenswert sprichwörtlich "durch die Decke geht". In Folge der falschen Informationen steigt das Asset im Wert, da immer mehr Investierende auf das Asset aufmerksam werden und den Informationen glauben. Dies ist die Phase des „Pump“. Sobald der Assetkurs für hoch genug erscheint, werden alle Anteile deutlich über dem Wert des Einkaufspreises verkauft. Dieses Abstoßen des Assets stellt den „Dump“ dar. In Folge des Abverkaufs sinkt der Preis des Assets wieder rapide ab und die Investierenden, die erst spät investiert haben verlieren einen Teil ihrer Investitionen.

Layering & Spoofing & Shilling

Sowohl das Layering als auch das Spoofing sind Arten der Marktmanipulation, bei der eine Person Kauf- oder Verkaufsaufträge platziert, die ein Signal für andere Marktteilnehmende darstellen soll und diese zum Handeln verleiten soll. Die Aufträge werden dabei jedoch noch vor Ausführung wieder storniert, sodass am Ende Einfluss auf den Assetkurs genommen wurde, ohne aktiv am Markt gehandelt zu haben.

Der Unterschied zwischen Layering und Spoofing liegt lediglich in der Zielgruppe. Während sich das Spoofing an einzelne

Poop-and-Scoop ist im Prinzip das Gegenteil von Pump-and-Dump. Die Marktmanipulierenden streuen Falschinformationen, um den Assetkurs fallen zu lassen (Poop). Ist der Assetkurs niedrig genug, fangen sie an das Asset zu einem niedrigen Kurs zu erwerben (Scoop). Diese Käufe gepaart mit dem Fakt, dass sich auf Dauer herausstellen wird, dass die Informationen nicht der Wahrheit entsprechen, lassen den Kurs wieder steigen. An diesem Punkt können die Manipulierenden ihr Asset gewinnbringend veräußern. Bei einem Pump-and-Dump oder Poop-and-Scoop beispielsweise dient die hohe Fluktuation des Assets und der erreichten Gewinne möglicherweise zu einer geringeren Skepsis als eine Investition in ein Asset mit stabilen Kurswerten bei denen sich zeitlich kurz hintereinander stattfindende Ein- und Auszahlung zu sehr ähneln.

Marktteilnehmende richtet, soll das Layering den breiten Markt beeinflussen.

Shilling ist eine Manipulationsform, bei der Personen des öffentlichen Lebens (Prominente, Content-Provider etc.) ein Asset bewerben, da sie selbst davon profitieren. Entweder, weil sie selbst bereits in das Asset investiert haben, oder weil sie für das Bewerben bezahlt werden. Ziel ist es den Preis des Assets hochzutreiben und von den Steigerungen zu profitieren.

Beim Layering, Spoofing und Shilling werden inkriminierte Gelder in Form vieler kleinerer

Transaktionen in den Markt gebracht. Dabei könnten diese vielen kleineren Investitionen unter dem Deckmantel einer „tollen Investition“ versteckt werden. Die Investition scheint auch nach außen vertretbar, da entweder auf die Marktbewegungen oder die Werbung

verwiesen werden. In dem Wissen, wann der Kurs wieder sinken wird, können die Gelder aus dem Markt gezogen werden und die „tolle Investition“ bleibt inklusive einer möglichen Rendite ausweisbar.

Anhaltspunkte, die auf die Nutzung von Marktmanipulation hindeuten könnten:

- Käufe und Verkäufe werden gleichzeitig durch denselben Marktteilnehmenden ausgeführt.
- Der Kunde oder die Kundin führt innerhalb eines kurzen Zeitraums viele kleine Käufe durch.

Nutzung von nicht-lizenzierten Krypto-Handelsplattformen und Kryptobörsen in Hochrisikostaa- ten

Zu Hochrisikobörsen zählen zum einen Kryptobörsen, die nicht lizenziert und von der BaFin oder anderen ausländischen Finanzaufsichtsbehörden beaufsichtigt werden. Die Funktion von nicht-lizenzierten Krypto-Handelsplattformen ist identisch zu den lizenzierten, sie ermöglichen den Handel und Austausch von Kryptowerten und auch den Austausch zwischen Krypto und Fiat. Nicht-lizenzierte Börsen werden aber nicht von einer Aufsichtsbehörde reguliert, d.h. sie besitzen keine offizielle Lizenz zum Handel und zur Verwahrung von Kryptowerten. Durch die uneingeschränkte Funktion verbunden mit der fehlenden Regulierung in Form von niedrigen Registrierungsschwellen und einer hohen Anonymität (fehlende KYC-Prozesse u.ä.) geht ein besonders hohes Risikopotenzial von diesen Handelsplattformen aus. Geldwäschetreibende melden sich mit illegal erwirtschafteten Kryptowerten an und tauschen ihre Assets gegen andere Kryptowerte oder wandeln diese in Fiatgeld um. Die fehlenden oder unzureichenden KYC-Standards

ermöglichen es den Geldwäschetreibenden anonym zu bleiben und nach dem Wechsel der inkriminierten Kryptowerte entweder „saubere“ Kryptowerte oder sogar Fiatgeld zu erhalten. Für den Fall, dass Nutzende nun „saubere“ Kryptowerte halten, können sie diese auch über eine lizenzierte Handelsplattform in Fiat-Währung umtauschen.

Die zweite Kategorie der Hochrisikobörsen sind die Kryptobörsen in Hochrisikostaa-
ten. Schwachstellen in der Bekämpfung von Geldwäsche in bestimmten Jurisdiktionen werden oft gezielt ausgenutzt. Diese Staaten befinden sich oftmals in den Regionen Afrika und Osteuropa sowie im mittleren Osten. Eine Einstufung des Geldwäsche- und Terrorismusfinanzierungs-Risikos der Staaten wird beispielsweise von der FATF (Financial Action Task Force)

vorgenommen und ist öffentlich über deren Internetauftritt zugänglich.⁹

Darüber hinaus stellen auch solche Staaten ein potenziell höheres Risiko dar, die eine hohe finanzielle Anonymität aufweisen und/oder sich als unkooperativ mit anderen Jurisdiktionen zeigen, da nur rudimentäre oder keine Informationen im Rahmen von Strafverfolgungsmaßnahmen geteilt werden. Gleiches gilt auch für sanktionierte Staaten, die darüber hinaus vermutlich sogar ein Interesse daran haben könnten, dass Gelder aus dem Ausland in ihr Hoheitsgebiet überführt und in den dortigen regulären Wirtschaftskreislauf eingebracht werden.

Ein weiterer Bereich, der sich im Zusammenhang mit risikobehafteten Staaten eröffnet, sind solche Jurisdiktionen, in denen keine Regulatorik in Bezug auf Kryptowerte besteht. Es ist durchaus möglich, dass Staaten zwar im Allgemeinen gut gegen Geldwäsche und Terrorismusfinanzierung aufgestellt sind, sich kooperativ im Umgang mit anderen Jurisdiktionen zeigen und auch nicht auf einer Sanktionsliste wiederzufinden sind, sie aber aufgrund von fehlenden Krypto-Regularien ein potenziell hohes Risiko darstellen.

Das Vorgehen der Geldwäschetreibenden auf Handelsplattformen in Hochrisikostaaten unterscheidet sich in der Regel nicht zu dem Vorgehen bei der Nutzung nicht-lizenzierter Handelsplattformen.

FATF (Financial Action Task Force)

Die FATF ist ein im Jahr 1989 gegründetes internationales Gremium zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung mit Sitz in Paris. Es besteht aus 40 Mitglieder (38 Mitgliedstaaten und 2 regionale Organisation).

Die FATF legt internationale Standards fest, die darauf abzielen, diese illegalen Aktivitäten und die daraus für die Gesellschaft entstehenden Schäden zu verhindern. Sie setzt sich dafür ein, den notwendigen politischen Willen zu schaffen, um nationale gesetzgeberische und regulatorische Reformen in diesem Bereich herbeizuführen.

Die etablierten Standards sollen sicherstellen, dass nationale Behörden effektiv gegen illegale Gelder, die mit Straftaten in Verbindung stehen, vorgehen können. Mehr als 200 Ländern und Hoheitsgebiete haben sich dazu verpflichtet, die Standards umzusetzen. Sie werden durch regelmäßig stattfindende Evaluierungen hinsichtlich der Um-

⁹ <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>.

Anhaltspunkte, die auf die Nutzung von nicht-lizenzierten Krypto-Handelsplattformen zur Geldwäsche hindeuten könnten:

- Der genutzte Handelsplatz oder der für diesen tätige ausländische Zahlungsdienstleister...
 - o ...hat seinen Unternehmenssitz in einem Hochrisikostaat (bspw. gemäß Liste der EU oder der FATF¹⁰) mit fehlender oder unzureichender Anti-Geldwäsche- und/oder Anti-Terrorismusfinanzierungsregelung für Geschäfte mit Kryptowerten.
 - o ...hat seinen Unternehmenssitz in einer sanktionierten Jurisdiktion.
 - o ...besitzt eine Lizenz in einer sanktionierten Jurisdiktion.
 - o ...gibt keine oder nur unzureichende Informationen zum Unternehmenssitz preis.
 - o ...ist nicht als solcher registriert (z.B. in den Registern und Datenbanken der Aufsichtsbehörden – in Deutschland: BaFin¹¹), handelt aber so, dass er erlaubnispflichtige Finanzdienstleistungen betreibt (bspw. weil er diese bewirbt).
 - o ...führt nur ein sehr niedrigschwelliges On-Boarding seiner Kundschaft durch (bspw. kein KYC (Know-Your-Customer) oder CDD (Customer Due Dilligence), Anmeldung nur mit Passwort und E-Mailadresse).
 - o ...setzt seiner Kundschaft keine Restriktionen (bspw. keine Limits hinsichtlich des Handelsvolumens, kein Stopp der Ein- und Auszahlungen bei direkter Verbindung zu inkriminierten Geldern).
 - o ...weist eine hohe Quote eingehender und/oder ausgehender Kryptowertetransaktionen mit (möglichen) Hinweisen zu kriminellen Aktivitäten auf (bspw. Ransomware, Darknet-Bezug etc.).
 - o ...weist seine Kundschaft daraufhin den stattfindenden Kryptohandel nicht gegenüber Dritten (bspw. Banken) zu erwähnen und bei Ein- und Auszahlungen irreführende oder uneindeutige Angaben im Verwendungszweck anzugeben.
 - o ...wurde erst vor kurzem eröffnet.
 - o ...wird in Chats im Darknet zur Abwicklung von Geschäften benannt/beworben.
 - o ...bietet On-/Off-Ramping mit wirtschaftlich nicht nachvollziehbaren Fiat-Währungen an (bspw. ein Handelsplatz mit Sitz auf Zypern bietet Ein-/Auszahlungen in russischen Rubel an).
 - o ...bietet den Handel mit sanktionierten Kryptowerten oder Kryptowerten, die von einer sanktionierten Jurisdiktion herausgegeben werden, an.
 - o ...gibt eine Kontakt-Telefonnummer aus einem Hochrisikostaat an.
 - o ...ändert in regelmäßigen Abständen und ohne nachvollziehbaren Grund die Kontaktinformationen (bspw. Adresse, Telefonnummer).

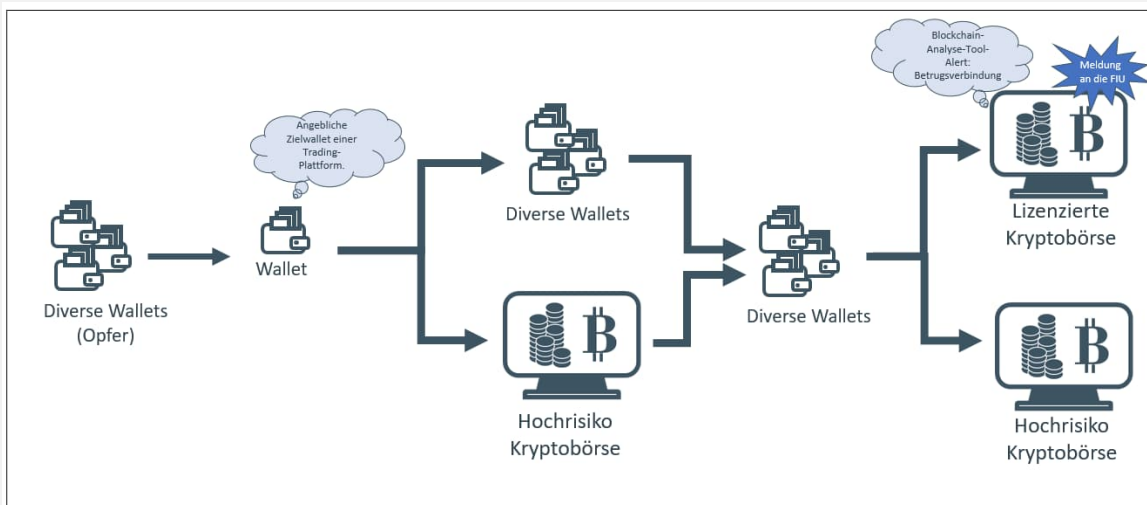
¹⁰ <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>.

¹¹ <https://portal.mvp.bafin.de/database/InstInfo/start.do>

- o ...hat eine undurchsichtige oder unbekannte Eigentümerstruktur und es gibt Hinweise auf das Vorhandensein einer Briefkastenfirma.
 - o ...hat eine Person als Geschäftsführer, die aus einem Hochrisikostaat stammt oder die in den Medien in Verbindung mit kriminellen Aktivitäten gebracht wird
- Es erfolgen auffallend viele Transaktionen mit bisher weitgehend unbekannten Handelsplätzen für Kryptowerte, die darüber hinaus noch besonders exponiert im Hinblick auf die Einbindung von DeFi-Anwendungen oder DEXes (Decentralized Exchanges) sind.
- Der Kunde oder die Kundin nutzt auffällig oft Kryptowerte mit erweitertem Anonymisierungsgrad (z.B. Zcash, Dash, Monero) oder leitet Kryptowerte mit geringerem Anonymisierungsgrad an Handelsplätze weiter und konvertiert sie unmittelbar in Kryptowerte mit erweitertem Anonymisierungsgrad. Es werden Kryptowerte oder andere Instrumente genutzt, deren Ausgestaltung nicht hinreichend dokumentiert ist, die in Verbindung mit möglichem Betrug stehen oder die auf die Realisierung von Betrugsmaschinen wie Schneeballsysteme oder Fake-Coins bzw. Fake ICO abzielen.
- Es finden Kryptowertetransaktionen statt, bei denen die IP-Adresse der sendenden Person und der Zieladresse unterschiedlichen Jurisdiktionen zugeordnet werden können.
- Es finden ohne wirtschaftlichen Grund Kryptowertetransaktionen an einen ausländischen Crypto Asset Service Provider (CASP) statt.
- Es werden Fiat-Überweisungen von CASPs an Bankkonten getätigt, die einer anderen Jurisdiktion zugeordnet werden als die der sendenden Person.

Beispielfall

Bei einer lizenzierten Krypto-Handelsplattform wurde ein Kunde aufgrund hoher Einzahlungen auffällig. Das Blockchain-Analyse-Tool gab an, dass die Einzahlungen indirekte Verbindungen zu Betrugsfällen aufweisen. In einer tiefergehenden Analyse konnte ein Netzwerk ausgemacht werden, bei dem die Täter mehrere Schein-Trading-Plattformen vertrieben und deren Opfer Gelder an eine Ziel-Wallet einzahlen ließen. Von diesem Wallet wurden die Gelder entweder an Hochrisikobörsen oder andere Wallets transferiert. Im Anschluss wurden die Gelder wiederum an zahlreiche weitere Wallets weitergeleitet und anschließend entweder über eine lizenzierte Handelsplattform oder eine weitere Hochrisiko-Börse ausgedasht.



Über das gesamte Netzwerk wurden innerhalb weniger Monate mindestens 5 Mio. Euro an die Betrüger transferiert. Bei den verwendeten Kryptowerten handelte es sich größtenteils um Ethereum, Ripple und Solana.

Nutzung von Online-Glücksspielseiten mit Kryptowerten

Ein wachsender Bereich potenzieller Geldwäscheaktivitäten sind Online-Glücksspielseiten, die Kryptowerte als Zahlungsmittel akzeptieren. Solche Plattformen operieren in der Regel im Ausland und unterliegen damit nicht den gleichen regulatorischen Anforderungen wie in Deutschland lizenzierte Anbieter. In Deutschland sind durch den Glücksspielstaatsvertrag bei lizenzierten Anbietern Einzahlungen in Form von Kryptowerten nicht erlaubt. Der mögliche Missbrauch des Glücksspiels zur Verschleierung von Mittelherkünften der nicht-lizenzierten Anbieter, die eine Einzahlung von

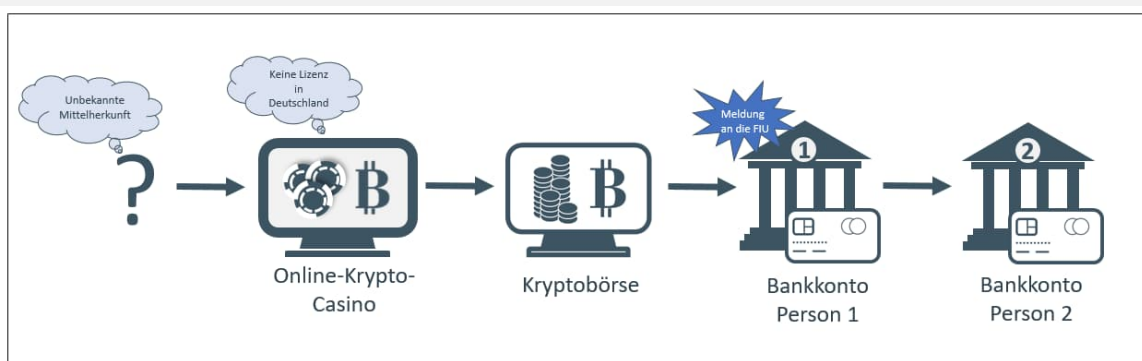
Kryptowerten ermöglichen, ähneln sich nach Einzahlung denen der herkömmlichen Anbieter. Allerdings entstehen durch die zusätzliche Einzahlungsmöglichkeit von Kryptowerten weitere Risiken. So können diese Casinos auch zum reinen Umtausch von Kryptowerten zu Fiat-Währungen oder andersrum genutzt werden, ohne dass eine Überprüfung der Mittelherkunft vorgenommen wird. Zudem ist auch ein gemeinsames Glücksspiel mehrerer Personen denkbar, um sich gegenseitig Kryptowerte zu übertragen, ohne dass dies eindeutig auf der Blockchain zu sehen ist.

Anhaltspunkte, die auf eine Nutzung von Online-Glücksspiel zur Geldwäsche hindeuten können

- Der Kunde oder die Kundin...
 - o ...erhält oder sendet Gelder an Online-Casinos, die nicht auf der Whitelist der Gemeinsamen Glücksspielbehörde der Länder steht.
 - o ...nutzt Online-Casinos, die Kryptowerte als Zahlungsmittel akzeptieren.
 - o ...nimmt kaum am Glücksspiel teil, sondern nutzt das Glücksspielkonto vielmehr als Durchlaufkonto. Die Ein- und Auszahlungen finden daher in (nahezu) identischer Höhe statt.
- Das Bankkonto der Kundschaft weist lediglich Eingänge eines Casinos und keine Ausgänge an das Casino auf.

Beispielfall

Bei Bank 1 wurde eine Person durch hohe Zahlungseingänge einer Kryptobörse und der teilweise zeitnahen Weiterleitung an ein Bankkonto einer dritten Person bei einer anderen Bank auffällig. Auf Nachfrage der Bank, woher diese Gelder stammen, gab der Kunde die Information, dass er regelmäßig Glücksspiel in einem Online-Casino spielt und dort eine hohe Summe gewonnen hat. Dieses Casino ist allerdings kein lizenzierter Anbieter in Deutschland und ermöglicht zudem das Glücksspiel mit Kryptowerten. Die Weiterleitung der Gelder mit 6-stelligem Betrag begründete die Person damit, dass er die Gefahr sah, seinen Gewinn wieder zu verspielen und ihn daher zur Aufbewahrung an eine Person aus ihrem Familienkreis übersendete.



Neben der grundsätzlich strafbaren Ausführung des illegalen Glücksspiels ist in diesem Fallbeispiel zudem denkbar, dass das Glücksspiel als ein Schritt zur Verschleierung eines anderen kriminellen Ursprungs der Gelder genutzt wurde.

Nutzung von Krypto-Automaten (Krypto-ATM)

Krypto-Automaten ermöglichen einen Erwerb von Kryptowerten mit eingezahltem Bargeld. Ein Verkauf von Kryptowerten und eine Barauszahlung des Gegenwerts war an den in Deutschland ursprünglich und legal aufgestellten Automaten nicht möglich. Das legale Betreiben von Automaten, ohne dass eine Erlaubnis der BaFin vorliegt, ist in der Bundesrepublik nicht möglich. Die Betreiber unterliegen geldwäscherechtlichen Sorgfaltspflichten. Gleichwohl kam es in der Vergangenheit vor, dass Automaten ohne vorliegende Erlaubnis aufgestellt und betrieben wurden. Die Automaten, u.a. in Kiosken oder in der Nähe von Glücksspiel-Anbietern platziert, wurden zeitnah nach ihrer Entdeckung beschlagnahmt. Im Zusammenhang mit Geldwäscheaktivitäten stammt

das an Krypto-Automaten eingezahlte Bargeld aus Straftaten und soll durch den Umtausch in Kryptowerte dem Zugriff der Strafverfolgungsbehörden entzogen oder an weitere Tatbeteiligte weitertransferiert werden. Unter Umständen können Krypto-Automaten auch gezielt zum Zweck der Geldwäsche aufgestellt werden. In bekannten Fällen wurden sie gezielt damit beworben, dass keine Kundenidentifizierung erfolgt.

Der FIU sind darüber hinaus Fallkonstellationen bekannt, bei denen sehr wahrscheinlich auch Einzahlungen an legal aufgestellten Automaten zum Zwecke der Geldwäsche erfolgten.

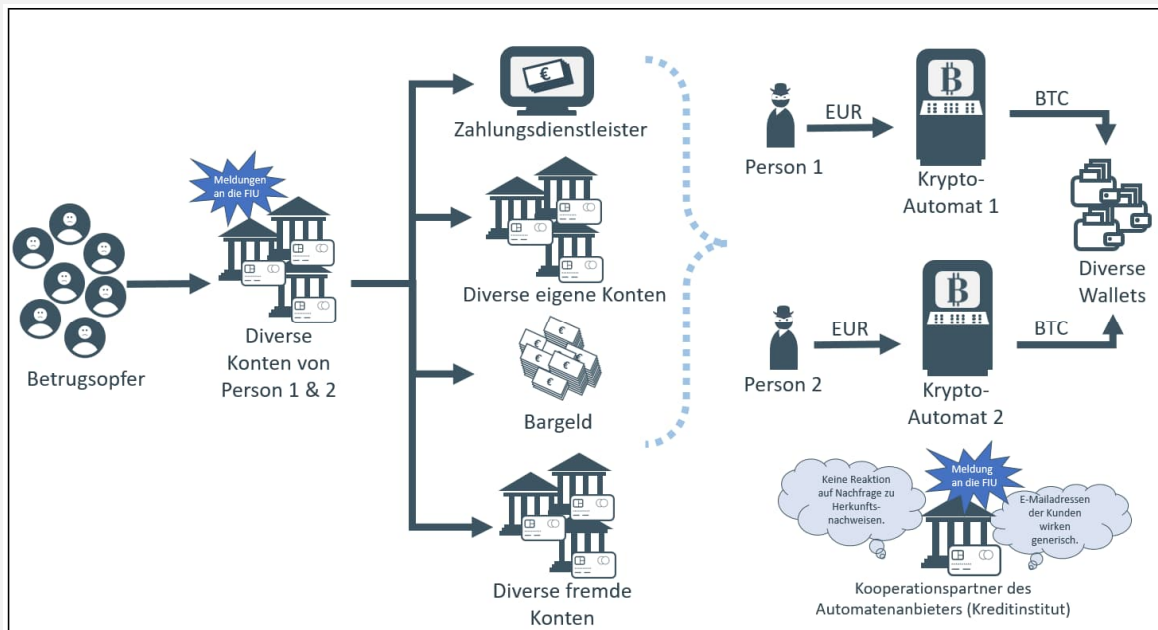
Anhaltspunkte für Geldwäsche im Zusammenhang mit Krypto-ATM

- Es werden Automaten für Kryptowerte an risikobehafteten Orten mit erhöhter Kriminalität genutzt.
- Es werden Automaten für Kryptowerte trotz sehr hoher Transaktionsgebühren genutzt.
- Nutzende weisen eine ungewöhnlich hohe Zahl an Transaktionen oder Transaktionen mit hohen Beträgen an Automaten für Kryptowerte auf.
- Ein- und Auszahlungen an Krypto-Automaten erfolgen zu ungewöhnlichen Zeitpunkten oder finden an auffälligen Orten statt (z.B. fernab der Wohnanschrift).
- Der (Geschäfts-)Kunde oder die (Geschäfts-)Kundin betreibt zahlreiche Automaten/Geschäftsstellen für Kryptowerte an Standorten mit erhöhter Kriminalitätsrate.

Beispielfall

Die gemeldeten Personen registrierten sich mit ihren Zugangsdaten bei dem Betreiber von Krypto-Automaten und durchliefen erfolgreich die Kundenidentifizierung.

Die beiden gemeldeten Personen erwerben an zwei unterschiedlichen Krypto-Automaten über einen Zeitraum von knapp zwei bzw. drei Monaten in acht bzw. zehn Transaktionen für jeweils über 17.000 Euro Bitcoin und transferieren diese an unterschiedliche Wallet-Adressen. Den angefragten Nachweis über die Herkunft der eingezahlten Gelder bleiben die Kundinnen schuldig. Die E-Mailadressen wirken generisch, es erscheint zweifelhaft, ob tatsächlich die registrierten Personen der Bank Rückmeldungen gaben.



Zu den Personen liegen weitere Verdachtsmeldungen von unterschiedlichen Banken vor. Einige davon berufen sich auch auf Auskunftersuchen von Strafverfolgungsbehörden, die sich wiederum auf Geschädigte beziehen, die Zahlungen an mehrere Konten tätigten. Die eingehenden Zahlungen wurden entweder an Paypal verfügt, am Tag der Einzahlung bar abgehoben oder an andere (eigene) Konten oder Konten weiterer Personen transferiert. Bei Betrachtung der Gesamtheit der Konten werden weitere auffällige Zahlungseingänge ersichtlich, die möglicherweise betrügerisch erfolgten. Sie enthalten Verwendungszwecke wie sie typischerweise im Zusammenhang mit Love-Scams auftreten.

Allgemeine, nicht einer speziellen Typologie zuordenbare Anhaltspunkte

Während die zuvor dargestellten Modi Operandi typischer Weise in vielen Geldwäsche-Fällen und Verdachtsmeldungen mit Bezug zu Kryptowerten, auch in Kombination, auftreten, gibt es daneben noch weitere Anhaltspunkte, die häufig im Zusammenhang mit Geldwäsche-Aktivitäten identifizierbar sind.

Es handelt sich hierbei um einzelne Auffälligkeiten, die in Verbindung mit anderen Handlungen einen Verdacht auf kriminelle Aktivitäten unterstreichen können. Diese Anhaltspunkte werden daher der Vollständigkeit halber im Folgenden aufgeführt.

Weitere allgemeine Anhaltspunkte, die auf eine Nutzung von Kryptowerten zur Geldwäsche hindeuten können:

- Der Kunde oder die Kundin...
 - o ...nutzt Domain-Registare (Domain Name Registrars, DNS) oder Domain-Adressen, die bei Proxy-Servern registriert sind, sodass der Inhaber/ die Inhaberin der Domain ausgeblendet oder angepasst wird (auf diese Weise wird der Anonymisierungsgrad des Nutzenden erhöht).
 - o ...führt Kryptowertetransaktionen aus, die in Umfang und Häufigkeit nicht zu seinem/ihrem Finanzprofil passen.
 - o ...leitet erhaltene Gutschriften in Form von Kryptowerten unmittelbar an andere Wallets (vor allem non-custodial-Wallets) weiter.
 - o ...transferiert Mittel in Kryptowerte auf sein/ihr Nutzerkonto bei einem Handelsplatz und leitet diese unmittelbar weiter. Sein/ Ihr Nutzerkonto (einschließlich dort angelegter Wallet-Adressen) dient nur zur Durchleitung der Mittel. Da bei jeder Transaktion Gebühren anfallen, ergibt die Transaktion wirtschaftlich keinen Sinn.
 - o ...nutzt auffällig häufig dezentrale DeFi-Handelsplätze (z.B. decentralized exchanges – DEX), Gaming-Token oder Handelsplätze für NFTs.
 - o ...nutzt eine oder mehrere Kredit- oder Debitkarten, die mit Wallets verknüpft sind, zur Abverfügung großer bzw. auffälliger Beträge in gesetzlichen Zahlungsmitteln (z.B. Euro, USD) – „crypto-to-plastic“.
 - o ...erhält Gelder von Wallet-Adressen, in denen gestohlene Vermögenswerte aufbewahrt wurden (z.B. aus Hacking-Attacken).
 - o ...tätigt Transaktionen von/an Wallet-Adressen, die mit Erpressung, Ransomware, sanktionierten Adressen oder anderen Formen illegaler Aktivitäten in Verbindung stehen (z.B. Kinderpornographie bzw. Child Sexual Abuse Material (CSAM)).
 - o ...transferiert Kryptowerte an auffällige Zieladressen, die mit möglicherweise unseriösen oder betrügerischen Anlagen stehen könnten.

- o ...führt viele Transaktionen durch, die eine Nachvollziehbarkeit der Mittelflüsse erschwert, wie z.B. zahlreiche „multiple input“-„multiple output“-Transaktionen oder zahlreiche Transaktionen über unterschiedliche Wallet-Adresen, bei denen jeweils ein kleinerer Teilbetrag an eine bestimmte, häufig dieselbe Wallet-Adresse gesendet wird, solange bis der Restbetrag aufgebraucht ist (sog. „Peel Chains“).
- Es gibt Hinweise von Geschädigten auf eine bestimmte Zieladresse.
- Es lassen sich Transaktionen von/an Wallet-Adressen mit Darknet-Bezug feststellen (z.B. ehemalige und aktuelle Darknet-Märkte wie AlphaBay, Chemical Revolution, Empire Market, HansaMarket, Hydra Market, Silkroad, Wallstreet Market etc.).
- Es gibt Hinweise, dass die Herkunfts- oder Zielwallet in Verbindung zu Mixing- oder Tumbler-Services stehen.
- Es gibt Hinweise, dass die Herkunft oder das Ziel von Kryptowerten Wallet-Adressen sind, die sich Wallet-Providern mit erhöhten Anonymisierungsgraden (z.B. Wasabi, Samourai) zuordnen lassen.
- Es lassen sich zahlreiche Transaktionen an/von neu-generierten Wallet-Adressen ohne bisherigen Umsatz feststellen.
- Es gibt Hinweise auf die Verbindung einer Wallet-Adresse zu illegalen Aktivitäten (bspw. als Adresse für das Sammeln von Spendengeldern für Vereinigungen, die terroristische Aktivitäten unterstützen).

... im Zusammenhang mit NFT

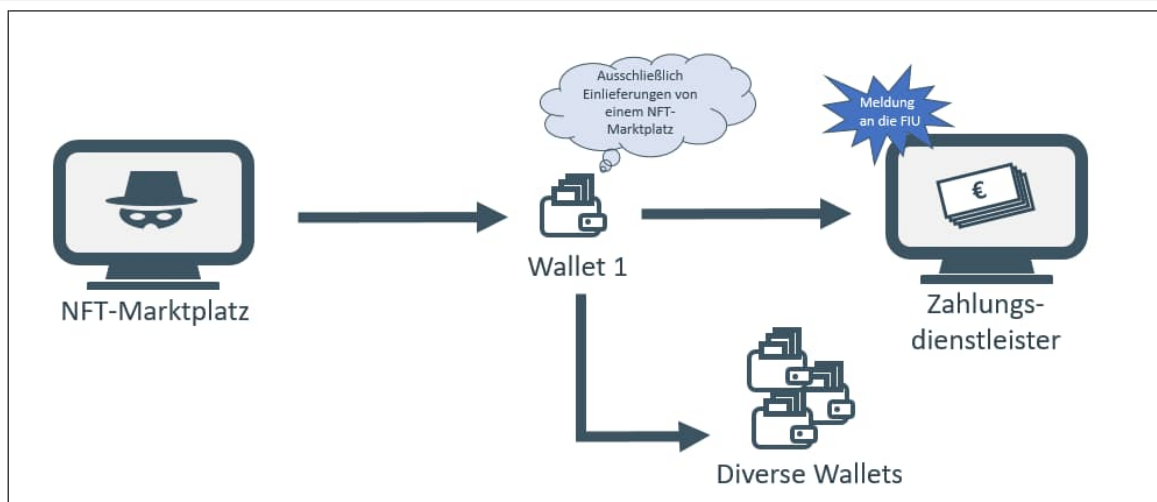
NFT lassen sich ähnlich wie Kryptowerte zum Zwecke der Geldwäsche und anderer illegaler Aktivitäten einsetzen. Die begünstigenden Faktoren sind ähnlich gelagert wie bei Kryptowerten (Pseudonymität, Konvertier-, Übertrag- und Handelbarkeit). Dazu kommt die Möglichkeit höhere Werte zu transferieren sowie insgesamt intransparente Preissetzungsprozesse.

Markt- und Preismanipulation lässt sich mit NFT einfach durchführen, ebenso wie Geschäfte mit sich selbst. Sie lassen sich aufgrund ihrer Merkmale daher vergleichbar mit Kryptowerten zur Verschleierung einer illegalen Herkunft von Geldern einsetzen.

Die FIU bittet die Verpflichteten bei Abgabe einer Verdachtsmeldung mit Bezügen zu NFT um einen ausdrücklichen Hinweis in der Sachverhaltsdarstellung durch Nennung des konkreten Stichworts. Dies entbindet die Verpflichteten aber nicht von einer aussagekräftigen Sachverhaltsschilderung.

Fallbeispiel

Im Rahmen des Transaktions-Monitorings fiel dem Verpflichteten auf, dass die Senderwallet eine sehr hohe Anzahl an ein- und ausgehenden Transaktionen aufweist. Die Einlieferungen stammen dabei fast ausschließlich vom einem NFT Marktplatz. Waren auf der Senderwallet lediglich ca. 3 ETH enthalten, gingen innerhalb von 10 Tagen ca. 18 ETH ein. Die Einlieferungen konnten auf einen NFT Marktplatz zurückgeführt werden. Die Verpflichtete konnte nicht ausschließen, dass die durchgeführten Transaktionen in Verbindung mit einer Straftat stehen und meldete daher an die FIU.



Über- / Unterfakturierung bei NFT

Der Gegenwert von NFT lässt sich, wie oben beschrieben, nicht oder nur sehr schwierig anhand objektiver Parameter bestimmen, sondern richtet sich ganz nach dem Geschmack bzw. der subjektiven Zahlungsbereitschaft einer an dem NFT interessierten Person. Dies ermöglicht Spielräume, Preise willkürlich festzusetzen. So kommt es im Handel mit NFT durchaus vor, dass diese unter Angabe eines falschen Preises verkauft werden. Mit Hilfe einer Rechnung, die entsprechende falsche Angaben enthält, sollen die Zahlungen legitimiert werden.

Im Falle einer Überfakturierung werden NFT angeboten, deren Preis (deutlich) oberhalb des marktüblichen Preises liegen. Durch die Überfakturierung ist der Käufer in der Lage, zusätzliche Vermögenswerte auf die verkaufende

Partei zu übertragen, da die Zahlung durch die kaufende Partei höher ist als der Wert, den man erhalten hätte, wenn man das NFT auf dem freien Markt verkauft/angeboten hätte.

Bei der Unterfakturierung werden NFT angeboten, deren Preise (deutlich) unterhalb des marktüblichen Preises liegen. Das zu Grunde liegende NFT hat in der Regel einen deutlich höheren Wert. Durch die Unterfakturierung sind verkaufende Parteien in der Lage, zusätzliche Vermögenswerte auf die kaufenden Parteien zu übertragen, da die Zahlung niedriger ist als der Wert den die kaufende Partei hätte zahlen müssen, wenn sie die Ware auf dem freien Markt erworben hätte.

Ausgabe von NFT/Handel mit NFT

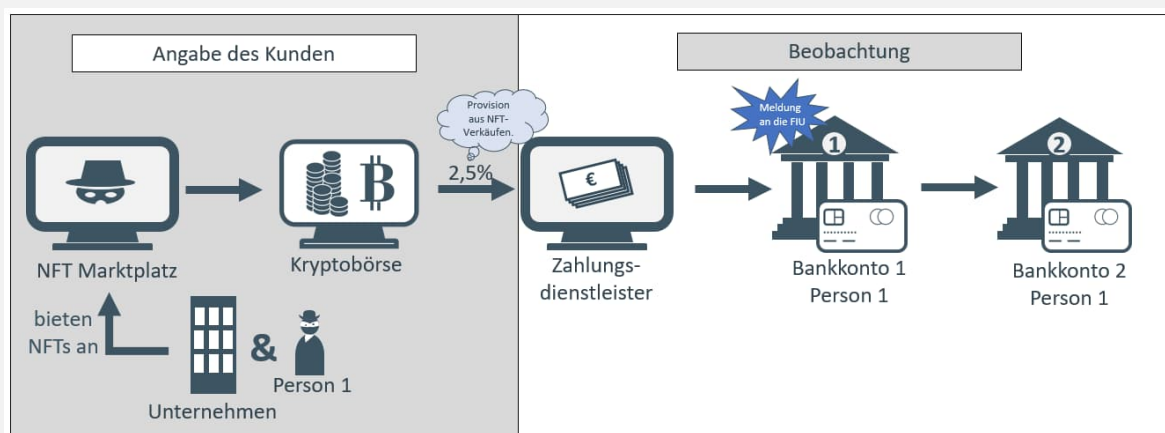
Wie bereits zuvor beschrieben, lassen sich NFT selbst erstellen und über Plattformen einem breiten Publikum anbieten. Die erzielten Erlöse können dann mit Hilfe von inkriminierten Geldern erzielt worden sein. Das macht es attraktiv, NFT-Kollektionen gezielt etwa mit dem primären Ziel der Geldwäsche oder zur Terrorisfinanzierung aufzulegen. Die NFT lassen sich dann gegen inkriminierte Mittel veräußern. Die Tatbeteiligten können ihre Umsätze mit

der Nachfrage nach ihren NFT begründen. Diese Variante erscheint dann vorteilhaft, wenn der Tatertrag bereits in Form von Kryptowerten vorliegt oder Erträge aus kriminellen Off-Chain-Aktivitäten in Kryptowerte getauscht wurden.

Fallbeispiel

Auf dem Privatgirokonto einer Person erfolgten an innerhalb von zwei Tagen Gutschriften von einem Zahlungsdienstleister mit Bezug zu einer Kryptobörse über insgesamt ca. 53 TEUR. Ein vorheriger Erwerb der Kryptowerte war anhand der bekannten Kontoführung nicht erkennbar. Der Gegenwert wurde anschließend überwiegend auf ein Konto der Person bei einer anderen Bank weitergeleitet.

Auf Nachfrage zum wirtschaftlichen Hintergrund gab die Person an, dass sie in Kooperation mit einer Firma eine NFT-Collection erstellt habe. Von jedem verkauften Exemplar erhielt sie dabei eine Provision in Höhe von 2,5%. Die Transaktionen seien über einen mitgelieferten Link einsehbar. Die Einnahmen würden dann bei der Kryptobörse umgewandelt und auf das Konto ausbezahlt.



Anhaltspunkte, die auf eine Nutzung von NFT zur Geldwäsche hindeuten können:

- Das Transaktionsverhalten der Kundschaft ist in Bezug auf die umfangreiche Nutzung bzw. hohe Nutzungsanteile für den Handel mit „Non fungible token“ (NFT) auffällig.
- Inaktive Wallets werden plötzlich für Transaktionen mit einer begrenzten Auswahl von NFT oder bestimmten NFT-Sammlungen genutzt.
- Aus verkauften NFT erlöste Kryptowerte werden nicht in den NFT- oder den Kryptowertemarkt investiert, sondern werden entweder nicht genutzt oder in Fiat-Währungen konvertiert.
- NFT werden zwischen einer begrenzten Zahl von Wallets gehandelt.
- Der Wert eines NFT erscheint zum Zeitpunkt des Verkaufs ungewöhnlich tief (im Hinblick auf bestimmte Indikatoren/Parameter wie Floor Price, Handelsvolumen etc.).
- Mehrere NFT, die zu einer Wallet oder eine Gruppe von Wallets gehören, werden über einen bestimmten Zeitraum mit Verlust verkauft.
- Der Verkauf von NFT erfolgt zwischen miteinander verbundenen Wallets, die daher wahrscheinlich unter Kontrolle desselben Nutzenden stehen.

... im Zusammenhang mit sonstigen digitalen Werten (Gaming-Bereich)

In-Game-Währungen und virtuelle Gegenstände sind für Geldwäsche attraktiv, da solche Gegenstände nicht pauschal im Sinne von Geld regulatorisch erfasst sind. Ihre regulatorische Relevanz ist aber einzelfallabhängig. Sie hängt beispielsweise von Handelbarkeit, Echtgeldbezug oder Tokenisierung ab.

Nutzende können sich unter bestimmten Umständen anonym als im Finanzbereich bewegen. Eine Identifizierung der Gamerinnen und Gamer ist in aller Regel nicht vorgesehen.

Die FIU bittet die Verpflichteten bei Abgabe einer Verdachtsmeldung mit Bezügen zu sonstigen digitalen Werten um einen ausdrücklichen Hinweis in der Sachverhaltsdarstellung durch Nennung einschlägiger Stichworte. Dies entbindet die Verpflichteten aber nicht von einer aussagekräftigen Sachverhaltsschilderung.

Handel mit sonstigen digitalen Werten zur Verschleierung

Zur Geldwäsche erwerben Tatbeteiligte mit inkriminierten Geldern direkt oder über Zweitmärkte oder Gutscheinkarten In-Game-

Währungen oder virtuelle Gegenstände. Gaming-Karten bieten dabei zusätzlich den Vorteil, dass diese bis zu einer bestimmten

Grenze vollkommen anonym besorgt werden können.

Vor allem seltene Ausrüstung oder seltene Skins erfolgreicher Spiele können dabei sehr preisstabil sein und auch über einen längeren Zeitraum gehalten werden. Zur weiteren Verschleierung können sowohl In-Game-Währungen, als auch Ausrüstungen innerhalb des Spiels mehrmals weitergegeben werden. Daraufhin werden die virtuellen Güter – entweder

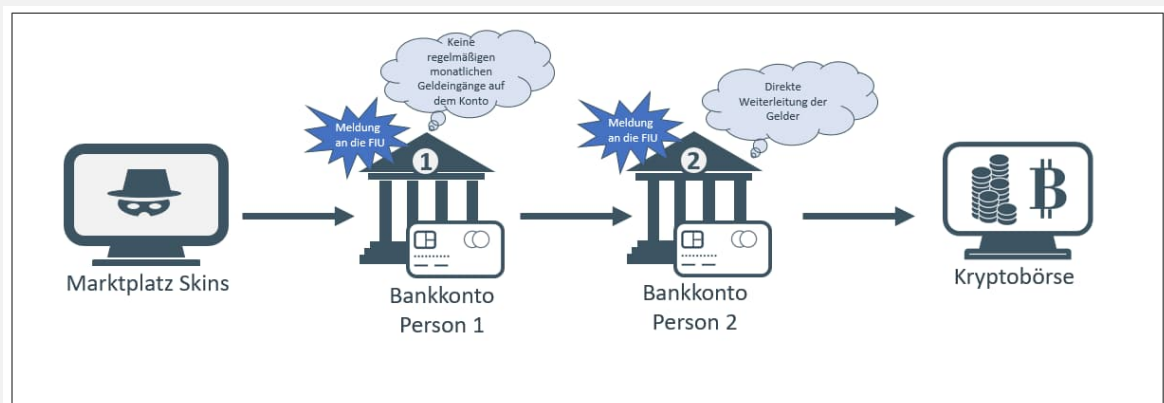
in Form der In-Game-Währung, einzelner Gegenstände oder ganzer Accounts - wieder über einen Zweitmarkt verkauft und der resultierende Geldeingang bei einem Finanzinstitut durch den Verkauf legitimiert. Ob die auf dem Zweitmarkt verkauften virtuellen Güter legal erspielt oder zuvor mit inkriminierten Geldern erworben wurden, ist dann nicht mehr ersichtlich.

Anhaltspunkte für die Nutzung von sonstigen digitalen Werten zur Geldwäsche:

- Häufige Käufe oder Verkäufe von In-Game-Items mit hohen Werten und daraus resultierende hohe Anzahl an Zu- und Abgängen im Zusammenhang mit Marktplätzen für virtuelle Gegenstände auf dem Bankkonto der Kundschaft.
- Kurze Haltedauer von virtuellen Gegenständen.
- Dieselben Gegenstände oder der gleiche Betrag an Währungen wird zwischen mehreren Gaming-Accounts hin und hergeschoben.
- Auffällig häufige Nutzung von Guthabekarten zur Aufladung des Gaming-Accounts.

Beispielfall

Bei der Bank 2 wurde ein Konto einer Person auffällig, das als Durchlaufkonto fungiert und ausschließlich Gelder von einem Konto derselben Person bei Bank 1 erhält. Diese Gelder wurden umgehend nach Erhalt vor allem an Kryptobörsen weitergeleitet. Das Konto bei Bank 1 weist keine regelmäßigen monatlichen Geldeingänge auf, sondern nur Bargeldeinzahlungen und hohe Erträge eines Marktplatzes für Skins.



Gaming-Karten

Allgemein sind Guthabekarten im Handel weit verbreitete Zahlungsmittel, die mit einem festen Betrag aufgeladen werden können. Sie werden in physischen Läden oder online verkauft und erlauben Nutzenden, Waren und Dienstleistungen oft auch ohne Bankkonto zu bezahlen. Ihre Einfachheit, sehr verbreitete Akzeptanz und die Möglichkeit sie bis zu einem gewissen Betrag anonym zu erwerben oder weiterzuverkaufen, machen sie für Geldwäsche attraktiv. Während der Einkauf der Karten anonym vollzogen wird, können Rechnungen bei Weiterverkäufen der Karten als Legitimierung

der Geldeingänge bei Banken vorgelegt werden.

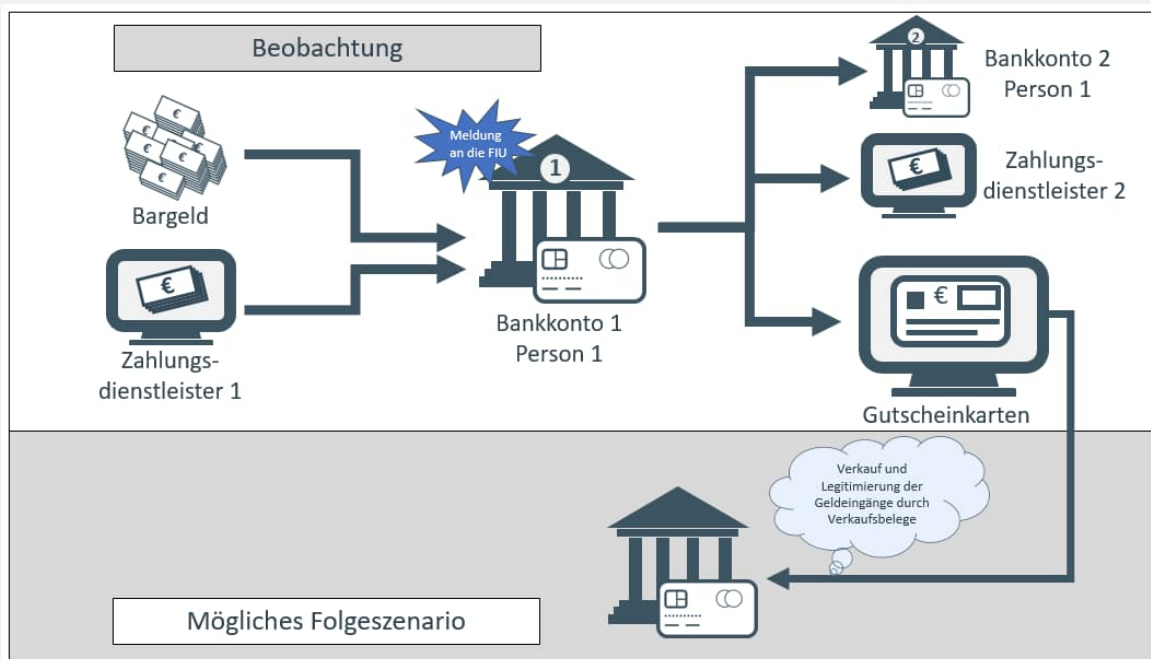
Im Bereich Gaming spielen Guthabekarten eine wichtige Rolle. Sie dienen dem Erwerb von In-Game-Währungen, die dann im Spiel eingelöst werden können und zum Teil an andere Spielende übertragbar sind. Aufgrund der hohen Nachfrage lassen sich Karten bzw. Einlöse-codes allerdings auch gut auf Zweitmärkten weiterveräußern und handeln (siehe vorheriger Abschnitt).

Anhaltspunkte, die auf eine Nutzung von Guthabekarten zur Geldwäsche hindeuten können:

- Der Kauf von Guthabekarten mit einem hohen Betrag an Bargeld.
- Wiederholte Käufe von Guthabekarten unterhalb von erlaubten Schwellenwerten um Identifikation zu vermeiden (siehe hierzu das Merkblatt – Hinweise zum Zahlungsdiensteaufsichtsgesetz (ZAG), abrufbar https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html).
- Das Transaktionsverhalten der Kundschaft weist wiederholte Zahlungen eines identischen und glatten Betrags im gleichen oder auch in verschiedenen Läden auf.
- Häufige Geldeingänge von spezialisierten Plattformen, die den Verkauf von Gaming-/Guthabekarten anbieten.

Beispielfall

Bei Bank 1 wurde ein Kunde durch eine Vielzahl an Bargeldeinzahlungen auffällig. In Summe wurde so über mehrere Monate ein 6-stelliger Betrag auf das Bankkonto 1 eingezahlt, wobei die Einzelbeträge meist unter 1.000 Euro lagen und häufig mehrere Einzahlungen pro Tag stattfanden. Die Bargeldeingänge wurden bei der Bank als Ertrag aus Verkäufen von privaten Vermögensgegenständen deklariert, wobei der Wahrheitsgehalt dieser Aussage nicht beurteilt werden konnte. Weitere nicht unerhebliche Eingänge kamen von einem Zahlungsdienstleister. Genutzt wurden die Gelder hauptsächlich zur Weiterleitung auf ein weiteres Bankkonto der gleichen Person bei einer anderen Bank und über einen Zahlungsdienstleister oder aber als Zahlungsmittel bei zwei Anbietern diverser Guthabenkarten.



Ein mögliches Folgeszenario wäre dabei der Weiterverkauf der Guthabenkarten und eine Legitimierung der Geldeingänge bei einer anderen Bank durch die Verkaufsbelege. Auch eine eigene Nutzung der Karten zum Erwerb von In-Game-Währung eines Onlinespiels zur weiteren Verschleierung ist denkbar.

... im Zusammenhang mit E-Wallets / Digitalen Wallets

Die Zwischenschaltung von Zahlungsdienstleistern und E-Geld-Instituten im Zahlungsverkehr kann eine zusätzliche Ebene der Verschleierung von Transaktionsbeteiligten bieten, da man für die Abwicklung von Zahlungen nicht mehr die originäre Herkunft der Gelder im Sinne einer Kontoverbindung offenbaren muss. Zahlungsempfangenden sind dann häufig nur die Informationen über den Namen des zwischengeschalteten Wallet-Anbieters bekannt. Hintergründe zu den erfolgten Transaktionen, z.B. zu welchem Zweck sie dienten, sind ebenfalls nicht immer ohne Weiteres ersichtlich. Dies ist auch ein Motiv, um z.B. Zahlungen an Glückspielanbieter oder Zahlungen im

Zusammenhang mit Adult Entertainment über Finanzdienstleister und nicht über die Bank, bei der ein Hauptkonto geführt wird, abzuwickeln. Durch die vergrößerte Anonymität und die Verschleierungsmöglichkeiten bezüglich der Herkunft von Geldern und des Zwecks von Transaktionen eignen sich E-Wallets auch um Gelder aus Straftaten zu empfangen oder weiterzuleiten. Im Zusammenhang mit mutmaßlichen Geldwäschehandlungen ist die Nutzung von Finanzdienstleistern im Ausland ohne erkennbaren Grund in besonderem Maße auffällig, da hier eine Identifikation von Beteiligten u.U. besonders erschwert ist.

Die FIU bittet die Verpflichteten bei Abgabe einer Verdachtsmeldung mit Bezügen zu E-Wallets / Digitalen Wallets um einen ausdrücklichen Hinweis in der Sachverhaltsdarstellung durch Nennung einschlägiger Stichworte. Dies entbindet die Verpflichteten aber nicht von einer aussagekräftigen Sachverhaltsschilderung.

Anhaltspunkte, die auf eine Nutzung von digitalen Wallets und E-Wallets zur Geldwäsche hindeuten können:

- Der Kunde oder die Kundin erhält ungewöhnlich häufig Zahlungen über Online-Bezahlsysteme, ohne dass diese sich z.B. durch seine Geschäftstätigkeiten plausibilisieren lassen.
- Der Kunde oder die Kundin leitet eingehende Gelder unmittelbar an Finanzdienstleister und E-Wallet-Anbieter weiter.
- Es liegen Hinweise vor, dass der Kunde oder die Kundin mehrere Banken und Konten nutzt, um auffällige Transaktionen zu splitten und diese auf Konten sowie unterschiedliche Zahlungsdienstleister und E-Wallet-Anbieter zu verteilen.
- Es sind zahlreiche Transaktionen an Anbieter von E-Geld feststellbar, ohne dass ein plausibler wirtschaftlicher Grund dafür erkennbar wäre. Auf dem Konto lässt sich zudem keine kunden- und kontotypischen Transaktionen feststellen.
- Ein Konto weist viele und hohe Gutschriften von E-Geld-Instituten und E-Wallets auf, deren wirtschaftlicher Hintergrund unklar ist. Die Gelder werden im Anschluss unmittelbar und auffällig verwendet. Sie werden z.B. an Handelsplattformen für Kryptowerte weitergeleitet, sofort bar verfügt oder an andere Konten (von Dritten, ins Ausland) oder Zahlungsdienste weitertransferiert.

Fallbeispiel

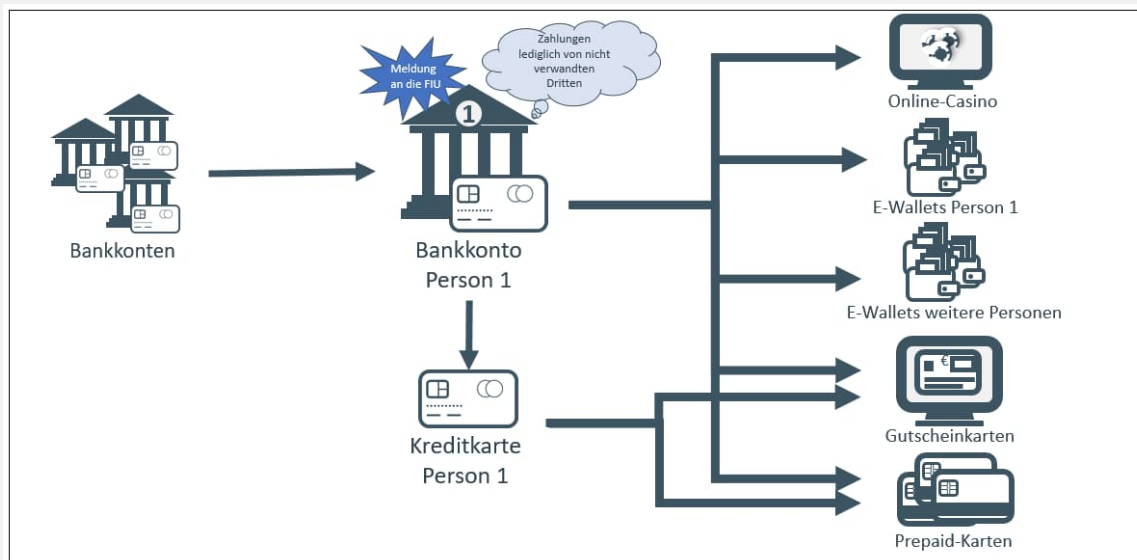
Der gemeldete Kunde hält ein Girokonto bei der Verpflichteten, hat eine Debit Card sowie ein Tagesgeldkonto. Auch besitzt er eine Kreditkarte.

In einem Zeitraum vom 20 Monaten erhielt der Kunde rund 200 Gutschriften in Höhe von fast 34.000 EUR, in erheblichem Umfang von nicht verwandten Dritten, ohne dass hierfür ein nachvollziehbarer Grund erkennbar ist. Zu den größten Einzahlern gehören insbesondere ein Betreiber eines Online-Casinos sowie diverse Dritte und Zahlungsdienstleister.

Die eingehenden Gelder wurden regelmäßig zeitnah weiterverwendet.

Ein Großteil der Weiterleitungen entfiel auf Kartenzahlungen bei Prepaid- und Gutscheinanbietern sowie E-Wallets: 186 Zahlungen an Anbieter A (ca. 11.300 Euro), über 40 Zahlungen an zwei Plattformen für den Erwerb von Guthabekarten. Hinzu kamen 250 Transaktionen an einen E-Wallet-Anbieter mit Bezug zum Namen des Kunden sowie weitere Zahlungen an Händlerkonten, die bei dem E-Wallet-Betreiber geführt werden, darunter Plattformen für den Erwerb von Guthabekarten sowie Plattformen für digitale Güter. Ferner wurden Zahlungen an Glücksspiel- und Gaming-Anbieter festgestellt. Auch auffällige Peer-to-Peer-Transfers an unterschiedliche Nutzer eines E-Wallet-Anbieters konnten beobachtet werden.

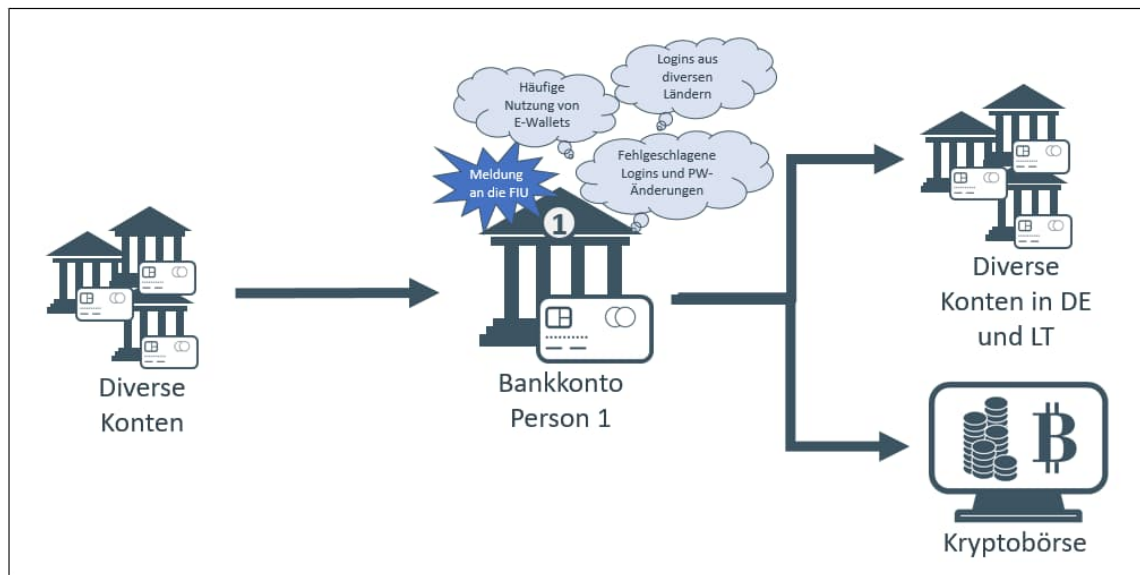
Auch bei der Überprüfung der Kreditkartenumsätze ist aufgefallen, dass der Kunde seine Kreditkarte zwischen innerhalb eines Zeitraums von zwei Jahren wiederholt für den Erwerb von Prepaid-Karten und Geschenkgutscheinen genutzt hat.



Das Transaktionsverhalten des Kunden erschien dem Verpflichteten insgesamt wirtschaftlich nicht plausibel. Herkunft und Zweck der Mittel sind weitgehend unklar. Auffällig sind insbesondere die hohen Drittmittelzuflüsse, die unmittelbare Weiterleitung der Gelder an Prepaid- und Gutscheinanbieter, Peer-to-Peer-Transfers sowie Glücksspielzahlungen.

Fallbeispiel

Ausgelöst wurde die Untersuchung bezüglich des Kunden bei dem meldenden Verpflichteten aufgrund interner Betrugswarnungen. Die Ergebnisse der Untersuchung deuten darauf hin, dass hinreichende Beweise für einen begründeten Verdacht auf Geldwäsche vorlagen.



Die Überprüfung der Transaktionen auf dem Konto des Hauptverdächtigen ergab ein insgesamt auffälliges und ungewöhnliches Verhalten. Das Konto weist keine typischen, unkomplizierten täglichen Ausgabenmuster auf. Es wurden dagegen mehrere grenzüberschreitende Transaktionen, die häufige Nutzung von E-Wallets und verschiedene Gerätelogins aus Ländern fern des deklarierten Wohnsitzes des Kunden festgestellt. Des Weiteren gab es mehrere fehlgeschlagene Anmeldeversuche und Passwortänderungen. Insbesondere konnten bestimmte Geldflüsse zu Krypto- und E-Wallet-Plattformen nicht vollständig geklärt werden, da die vom Kunden angegebene Tätigkeit und der erklärte Zweck solche Transaktionen nicht rechtfertigen.

Auf dem Konto erfolgten Einzahlungen von verschiedenen Privatpersonen und Entitäten aus mehreren europäischen Ländern. Diese Gelder wurden anschließend zügig über ausgehende Banküberweisungen an Dritte in Litauen und Deutschland transferiert.

Aufgrund der Warnmeldungen wurde der Hauptverdächtige kontaktiert. Obwohl der Nutzer auf die Informationsanfrage reagierte, legte er keine Dokumente vor. Das Konto des Nutzers zeigt ein transitorisches Muster, bei dem Herkunft und Ziel der Gelder vage sind, was auf APP-Betrug und Geldwäsche schließen lässt. Das schnelle Bewegungsmuster der Gelder deutet auch auf potenzielle Finanzagententätigkeit hin, da Gelder ohne plausible Begründung an Dritte weitergeleitet werden.

... im Zusammenhang mit Social-Media- und Streaming-Plattformen

Im Social-Media- und Streaming-Bereich erfolgen Zahlungen an Content-Provider nicht immer anhand nachvollziehbarer Kenngrößen (Anzahl Follower und Followerinnen, Aufrufzahlen etc.). Sowohl die Einnahmen aus Werbung als auch die eingenommenen Donations von anderer Nutzenden unterliegen keinen festen Regelungen. Geleisteten Zahlungen können zwar erbrachte Leistungen gegenüberstehen, ob diese aber dem Wert der Zahlungen entsprechen, ist trotz der oben genannten Kenngrößen nicht eindeutig ermittelbar. Diese Intransparenz angemessener Zahlungen birgt die Gefahr, dass inkriminierte Gelder über die

Content-Provider gewaschen werden. Dabei werden die Gelder entweder in Form eines (vermeintlichen) Werbedeals oder als Donation an die Provider gezahlt und können von diesen als Einnahmen aus geleisteten Social-Media- oder Streaming-Dienstleistungen ausgewiesen werden. Inwiefern Content-Provider tatsächlich eine Leistung erbracht haben und ob diese Leistung dem übertragenen Wert entspricht, kann nicht oder nur mittels aufwendiger Recherche nachvollzogen werden.

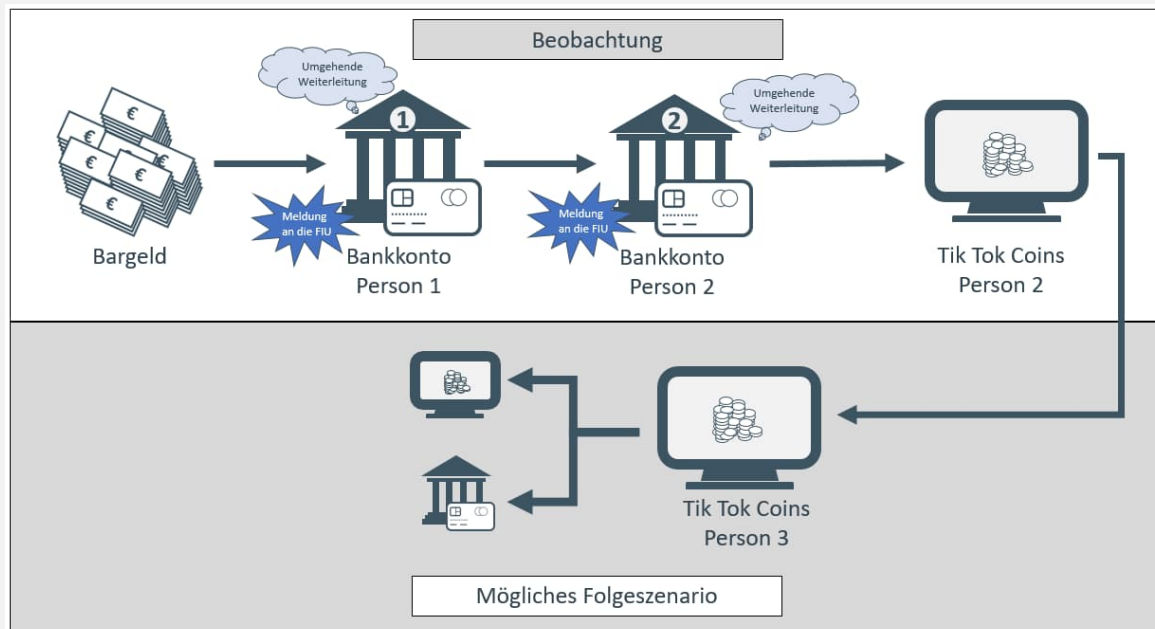
Die FIU bittet die Verpflichteten bei Abgabe einer Verdachtsmeldung mit Bezügen zu Social-Media- und Streaming-Plattformen um einen ausdrücklichen Hinweis in der Sachverhaltsdarstellung durch Nennung einschlägiger Stichworte. Dies entbindet die Verpflichteten aber nicht von einer aussagekräftigen Sachverhaltsschilderung.

Anhaltspunkte, die auf eine Nutzung von Social-Media- und Streaming-Plattformen zur Geldwäsche hindeuten können:

- Content-Provider (z.B. Influencer, Streamer) mit geringer Reichweite hat ein hohes Einkommen aus seiner/ihrer Tätigkeit.
- Sie/Er erhält Zahlungen von Firmen und Payment Service Providern (für Social-Media-Plattformen), die keine Produkte oder Dienstleistungen anbieten.
- Content-Provider kann keine Werbeverträge oder Rechnungen vorlegen.
- Es haben auffällig viele kleine Content-Provider denselben Sponsor.

Beispielfall – Bareinzahlungen über Konten an Plattform

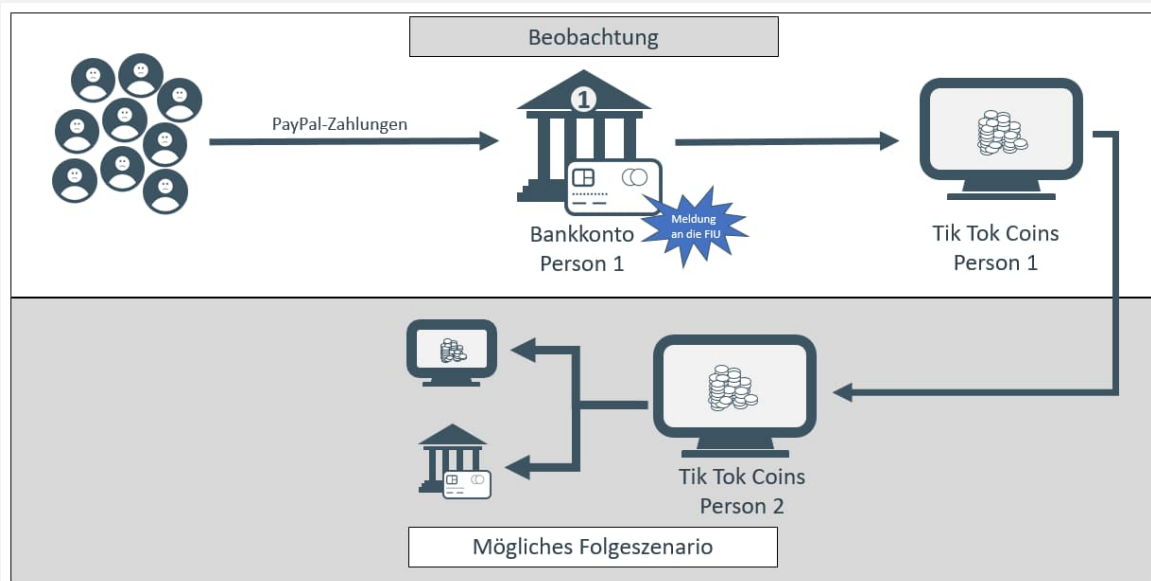
Bei der Bank 1 wurde ein Konto auffällig, da ihr Kunde Person 1 zahlreiche Bareinzahlungen zeitnah an Person 2 weiterleitete. Bei der Bank 2 wurde das Konto der Person 2 ebenfalls auffällig, da die eingehenden Gelder der Person 1 umgehend an die Plattform weitergeleitet wurden. Dabei berichtet die Bank 2 von einer mittleren dreistelligen Anzahl Transaktionen in fünfstelliger Höhe.



Aus Recherchen ist das Phänomen bekannt, dass die eingezahlten Gelder in Form der Plattform-Währung über einen oder mehrere Nutzer weitergeleitet und anschließend ausgezahlt werden. So ist es möglich die ausgezahlten Gelder als sogenannte Donations und entsprechend als Einnahmen aus den Social Media Tätigkeiten auszuweisen.

Beispielfall – Weiterleitung von Paypal-Zahlungen an Plattform

Bei der Bank 1 wurde ein Konto auffällig, da ihr Kunde zahlreiche Paypal-Gutschriften zeitnah an TikTok weiterleitete.



Aus Recherchen ist das Phänomen bekannt, dass die eingezahlten Gelder in Form der Plattform-Währung über einen oder mehrere Nutzer weitergeleitet und anschließend ausgezahlt werden. So ist es möglich die ausgezahlten Gelder als sogenannte Donations und entsprechend als Einnahmen aus den Social Media Tätigkeiten auszuweisen.

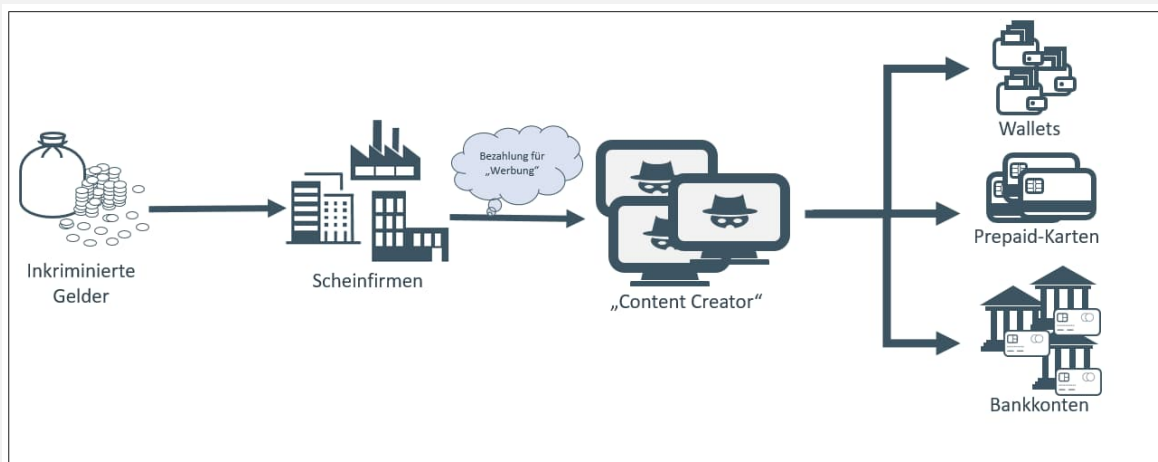
Schematische Darstellung – Legitimierung durch Werbeeinnahmen (veröffentlichter Fall aus den Vereinigten Arabischen Emiraten)

Im Jahr 2025 wurden in den Vereinigten Arabischen Emiraten ein Content-Provider mit 12.000 Followern auffällig. Dieser wurde innerhalb von 6 Monaten mit über 900.000 AED von osteuropäischen und südostasiatischen Unternehmen für Werbung bezahlt.

Ermittlungen ergaben, dass die Firmen weder Produkte noch Webseiten aufwiesen und so lediglich als Scheinfirmen zur Geldwäsche fungierten. Außerdem handelte es sich in diesem Fall um ein ganzes Geldwäschenetzwerk aus mehreren Scheinfirmen und Content-Providern.

Zum Aufbau des Netzwerkes wurden zunächst Content-Provider mit geringer Reichweite engagiert. Ihre Reichweite wurde im Anschluss mit Bots und gekauften Likes erhöht, sodass größere Werbeeinnahmen legitimiert werden konnten. Dann wurden Werbeaufträge erteilt und inkriminierte Gelder getarnt als Werbezahllungen über Krypto-fähige Debitkarten und Online-Überweisungen getätigt.

Die Content-Provider wiederum zahlten die Gelder über Wallets, Prepaid-Karten oder Bankkonten aus.



... im Zusammenhang mit Crowdfunding

Crowdfunding lässt sich für verschiedene illegale Zwecke missbrauchen. Gelder, die für bestimmte Projekte eingesammelt werden, werden u.U. nicht für den intendierten Zweck eingesetzt. Ziel des Sammelns von Spenden oder finanziellen Zuwendungen ist dann nicht, mit den Geldern ein Projekt zu finanzieren, sondern sie zur persönlichen Bereicherung einzusetzen (Spendenbetrug). Darüber hinaus könnten Projekte nur zu dem Zweck aufgesetzt werden, Transaktionen zu plausibilisieren, während die Zahlungen an das Projekt tatsächlich dem Erwerb von illegalen Gütern dienen (z.B. Drogen/Betäubungsmitteln, Waffen).

Zudem bietet Crowdfunding Möglichkeiten, Transaktionen mit illegalem Hintergrund zu verschleiern und Geldwäsche zu betreiben.

Hierbei werden Gelder aus kriminellen Aktivitäten zur Finanzierung von Projekten verwendet, die nur zum Schein ins Leben gerufen wurden. Die Projekte können z.B. von Strohpersonen aufgesetzt werden. Ein Vorteil der Nutzung einer Crowdfunding-Plattform für Tatbeteiligte besteht darin, dass Gelder in aller Regel unbar transferiert werden. Insofern kann Crowdfunding insb. für die Geldwäsche von Geldern dienen, die bereits in Form von Giralgeld vorliegen.

Für Verpflichtete empfiehlt es sich daher, die Verwendung von Geldern, die aus Crowdfunding stammen, genau in den Blick zu nehmen.

Die FIU bittet die Verpflichteten bei Abgabe einer Verdachtsmeldung mit Bezügen zu Crowdfunding um einen ausdrücklichen Hinweis in der Sachverhaltsdarstellung durch Nennung des konkreten Stichworts. Dies entbindet die Verpflichteten aber nicht von einer aussagekräftigen Sachverhaltsschilderung.

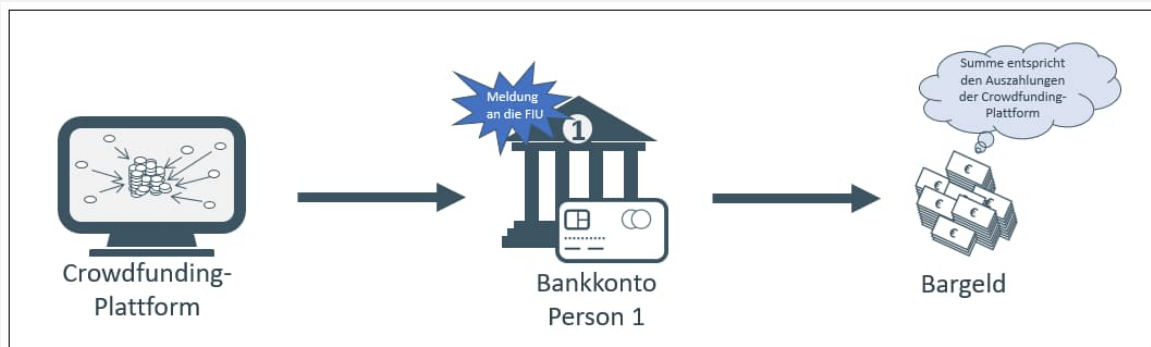
Anhaltspunkte, die auf eine Nutzung von Crowdfunding zur Geldwäsche hindeuten können:

- Hinweise auf die Strukturierung von Zahlungen: Auf Einzahlungen von Crowdfunding-Webseiten folgen strukturierte Bargeldabhebungen.
- Durchlaufcharakter von Zahlungen: Es gehen Einzahlungen von mehreren Konten ein oder es wird Bargeld eingezahlt und die Gelder werden dann sofort an Crowdfunding-Plattformen weitergeleitet. Gelder von verschiedenen Konten gehen bei einem Kunden oder einer Kundin ein und werden anschließend an dieselbe Crowdfunding-Plattform überwiesen.
- Privatkonten erhalten Zahlungen von nicht bekannten Personen und (ausländischen) Unternehmen, wobei die Gelder dann an Crowdfunding-Plattformen überwiesen werden.

- Es gibt eine auffällige Häufung bei verschiedenen Projekten, bei denen jeweils die identischen Investierenden und Kapitalsuchenden in Erscheinung treten.
- Eine Vielzahl von Investierenden sind unter der gleichen Adresse registriert oder geben gleiche Daten an.
- Einzelne Personen investieren auffallend hohe Beträge in ein Projekt, unmittelbar nachdem die Investitionsmöglichkeit publiziert wird.
- Die Finanzierungsziele von einzelnen Kapitalsuchenden werden häufig bereits nach auffällig kurzer Zeit erreicht.
- Ein Projekt erreicht sein Finanzierungsziel trotz auffallend unattraktiver Konditionen.
- Für ein Projekt gehen auffällig viele Geldeingänge oder ein hoher Einmalbetrag von einem ausländischen Konto ein.
- Kapitalsuchende starten ungewöhnlich häufig oder zeitnah neue, ähnlich gelagerte Projekte.
- Kapitalsuchende zahlen ungewöhnlich häufig aufgenommene Mittel, auch mit hohem Volumen, vorzeitig zurück.
- Die Höhe des Finanzierungsprojektes ist ungewöhnlich hoch bzw. niedrig im Vergleich zu ähnlichen Projekten.

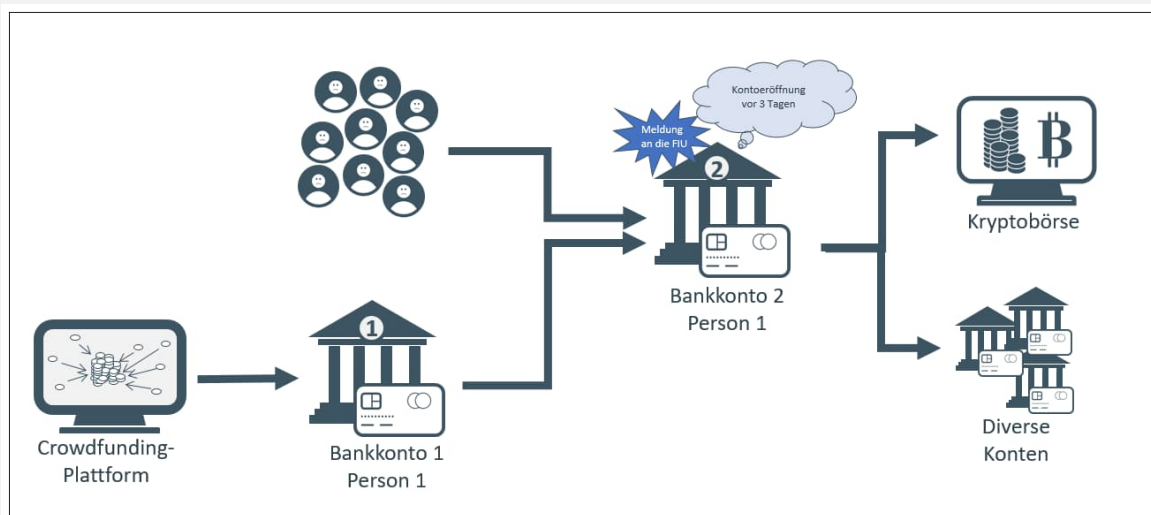
Fallbeispiel

Auf dem Konto der Person fanden in einem Zeitraum von eineinhalb Monaten diverse Gutschriften in Höhe von insgesamt über 4.500 Euro von einer Crowdfunding-Plattform sowie anschließende Barauszahlungen in etwa gleicher Höhe statt.



Fallbeispiel

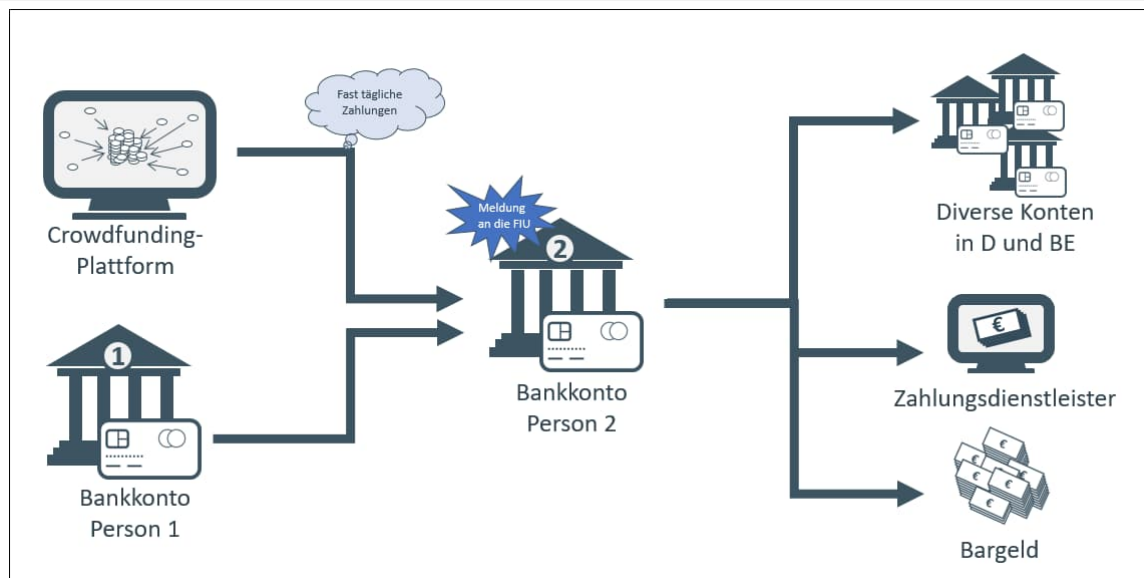
Das Konto des Kunden wurde durch einen internen Hinweis auffällig. Nach Durchsicht des Kontos fiel auf, dass es sich um ein erst drei Tage altes Konto handelte. Auf dem Konto werden regelmäßig Eigenüberträge getätigt, die nach Erhalt an weitere Fremdkonten, bzw. einem weiteren Referenzkonto weitergeleitet werden. Nach Mittelherkunfts-anfrage, sendete der Kunde uns einen Screenshot auf dem eine Überweisung über mehr als 5.800 Euro von einer Spendenplattform auf ein anderes Konto der Kundin eingehen. Die Kundin teilte mit, dass sie Organisator einer Spendenkampagne für eine Familie mit krankem Kind sei. Die Kundin leitet die Kundin Teilbeträge der Spenden erst auf das Konto beim Verpflichteten und daraufhin nochmals einen Teilbetrag auf ein weiteres Referenzkonto bei einer Kryptobörse weiter. Dieses Transaktionsverhalten stimmt nicht mit der Aussage des Kunden, die Gelder der Familie zukommen zu lassen überein. Auf dem Konto gibt es mehrere Zahlungseingänge von verschiedenen Personen und Konten zu finden u.a. von



Eingehende Transaktionen wurden innerhalb von Minuten weitergeleitet, zumeist auf weitere Konten der gemeldeten Person bei anderen Banken. Aufgrund des beschriebenen Sachverhalts vermutet die Verpflichtete den Verdacht auf Finanzagent-Tätigkeit, Spendenbetrug und Geldwäsche.

Fallbeispiel

Das aufgefallene Privatkonto weist innerhalb von zwölf Monaten diverse Überweisungseingänge von einem Zahlungsdienstleister in Höhe von über 32.000 Euro mit Bezug auf eine Crowdfunding-Plattform (fast tägliche Zahlungen) sowie von einer Drittperson in Höhe von mehr als 34.000 Euro auf. Die meisten Gelder verbleiben auf dem Konto, jedoch wird ein Teil dieser Gelder an Dritte in Deutschland und Belgien sowie via Zahlungsdienstleister transferiert oder in bar verfügt. Laut Internetrecherchen sammelt der Kontoinhaber über eine Plattform Gelder, um Hilfe für Menschen in Gaza zu mobilisieren.



Die originäre Mittelherkunft der oben genannten Transaktionen ist unbekannt. Zudem erscheint dem Verpflichteten die jeweils zeitnahe Verfügung dieser Gelder basierend auf den vorliegenden Informationen ungewöhnlich und zweifelhaft.

Anlage A – Allgemeine Anhaltspunkte für Geldwäsche

Die folgenden Punkte versammeln allgemeine branchen- oder sektorenübergreifende Auffälligkeiten, die Anhaltspunkte für Geldwäscheaktivitäten sein können. Allen Auffälligkeiten ist gemein, dass sie Anzeichen für eine Verschleierung von kriminellen Erträgen sein können. Typische Erscheinungsformen werden beispielhaft aufgeführt.

Hinweis auf Vortaten der Geldwäsche – Kriminelle Erträge

Klar vorliegende Hinweise auf kriminelle Erträge sind in der Natur der Sache liegend auch besonders starke Hinweise auf sich anschließende Geldwäschehandlungen.

Anhaltspunkte (beispielhaft):

- Hinweise auf eine Vortat der Geldwäsche (z.B. Betrug, illegales Glücksspiel, Marktmanipulation), auch aus öffentlichen Informationsquellen
- Zahlungsverhalten entspricht bekannten (anderweitig beschriebenen) Vortaten-Typologien (z.B. Korruption, Cybercrime, Menschenhandel, Kauf von Darstellungen sex. Ausbeutung von Kindern)
- Mitteilungen von Geschädigten (z.B. Überweisungen an Fakeshops)
- Auffällige Überweisungsrückrufe, Hinweise auf Missbrauch von Lastschriftverfahren u.Ä.
- Hinweise auf Steuerstraftaten wegen Auffälligkeiten in der Buchführung bspw. Nicht-Erklären von Einnahmen

Unklarer Auslandsbezug

Grenzüberschreitende Transaktionen oder Geschäftsbeziehungen bieten Möglichkeiten, Zahlungsflüsse und Transaktionspartner zu verschleiern. Zudem kann die Strafverfolgung durch die Betroffenheit mehrerer Jurisdiktionen erschwert werden. Insbesondere dann, wenn kein plausibler Grund für einen Auslandsbezug erkennbar ist, können Auslandsbezüge Hinweise auf Verschleierungshandlungen bieten.

Anhaltspunkte (beispielhaft):

- Grenzüberschreitende Transaktionen ohne plausiblen Grund, Schleusen von Geldern durch Vielzahl von Jurisdiktionen
- Häufiges Senden von Zahlungen an unterschiedliche Zahlungsempfänger in verschiedenen Ländern
- Weiterleiten von Geldern ins Ausland ohne plausiblen Grund
- Auf dem Konto mit einer deutschen Bankverbindung werden Bareinzahlungen getätigt, obwohl der Wohnsitz und der übliche Aufenthalt der Kundschaft im Ausland ist

Bezug zu Hochrisiko-Ort oder Hochrisiko-Finanzplatz

Bestimmte Länder sind aufgrund der dort bestehenden Lücken bezüglich Geldwäschebekämpfung attraktiv für Geldwäsche. Durch verschiedene Institutionen (z.B. EU, FATF, MONEYVAL) werden Bewertungen und Einstufungen von Jurisdiktionen veröffentlicht, die in ihren Systemen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung strategische Mängel aufweisen („graue“ und „schwarze“ Listen). Bezüge können sich ergeben im Hinblick auf die Kundschaft, das Konto beziehungsweise die Transaktion (z.B. Herkunft von Kaufpreiszahlungen, Zugriffe von IP-Adressen), den Sitz von Unternehmen oder Geschäftskontakten.

Anhaltspunkte (beispielhaft):

- Listen und Einstufungen der FATF
- EU-Sanktionslisten
- Schwarze Liste des IWF
- Citizenship-by-Investment (CBI)-Staatenliste der OECD
- EU-Liste nicht kooperativer Länder und Gebiete für Steuerzwecke
- Bezug zu Typologie- oder vortatenbezogenen Hochrisikoländern

Nicht nachvollziehbarer Einbezug Dritter – Hinweise auf Strohpersonen

Durch den Einbezug unbeteiligter Dritter als Vermittelnde oder als Geschäftspartnerin oder Geschäftspartner (Strohpersonen) wird bei der Geldwäsche das Ziel verfolgt, die Rückverfolgbarkeit zu den an Vortaten Beteiligten und den kriminellen Ursprüngen von Geldern zu verhindern. Gegebenenfalls werden zum Zwecke der Verschleierung auch wirtschaftlich unplausible Provisionen und Gebühren in Kauf genommen.

Anhaltspunkte (beispielhaft):

- Unplausibler Einbezug von Dritten (Strohpersonen) in Transaktion oder Geschäft, z.B. Kauf, Kontoführung durch andere Personen (auch Familienmitglieder)
 - ggf. unter Akzeptanz von unüblich hohen Gebühren (Provisionen, Gebühren)
- Eine dolmetschende Person übernimmt Wortführerschaft ohne (eentlichen) geschäftlichen Kontakt einzubinden
- Einbindung von juristischen Personen, deren Transaktionen nicht zum Geschäftszweck passen

Allgemeine oder branchenspezifische Auffälligkeiten der Kundschaft

Verschiedene Merkmale des Kundenverhaltens können darauf hindeuten, dass die Person versucht, eine illegale Unternehmung zu verbergen oder zu verschleiern. Hierzu zählen auch das Eingehen von unnötigen Risiken, die bei einem legitimen Geschäft unplausibel wären. Konkrete Auffälligkeiten können sich hier auch aus Verhaltensweisen ergeben, die bezogen auf die gegenwärtige Branche beziehungsweise für den vorliegenden Kontext (geschäfts-)untypisch sind.

Anhaltspunkte (beispielhaft):

- Mangelnde Kooperationsbereitschaft, keine Reaktion auf Rückfragen
- Auffällige Vermeidung des direkten Kontaktes, Aggressivität oder Nervosität
- Widersprüchliche Kundenangaben zur Herkunft und Verwendung von Mitteln
- Ausüben von hohem Zeitdruck (z.B. bei Vertragsabwicklung)
- Unübliches Eingehen von Risiken (z.B. persönlicher Transport von Wertgegenständen im gewerblichen o. geschäftlichen Umfeld)

Diskrepanz zwischen Kundenprofil und Transaktion oder Geschäft

Hierunter werden Transaktionen und Geschäfte verstanden, die in einem auffallenden Missverhältnis zu den wirtschaftlichen Verhältnissen, zum Geschäftszweck oder zu legalen Einkünften der handelnden Personen stehen. Eine bestehende Diskrepanz zu den Mitteln, über die verfügt werden soll, und den Mitteln, die legitim oder zum Geschäftszweck passend wären, kann auf eine illegale Geldquelle hindeuten beziehungsweise auf Versuche, den tatsächlichen Transaktionshintergrund zu verschleiern.

Anhaltspunkte (beispielhaft):

- Kundschaft hat keine geschäftsspezifischen Kenntnisse oder gewerblichen Hintergründe, die der Transaktion bzw. der Geschäftsbeziehung angemessen wären (z.B. hochpreisige Güter werden durch Branchenfremde gehandelt, Investitionen in Anlageprodukte ohne entsprechende Kenntnisse)
- Bezogen auf Kundenprofil unplausibles Vermögen, unplausible Einkünfte
- Transaktion widerspricht Geschäftszweck der Kundschaft
- Luxusgüter, Edelmetalle oder Wertpapiere werden unter ungewöhnlich erscheinenden Umständen zum Ankauf angeboten (z.B. Behauptung, diese nach dem Tod der besitzhabenden Person gefunden zu haben)
- Örtlich nicht plausible Geschäftsbeziehung zwischen Kundschaft und Verpflichteten oder zwischen den beteiligten Transaktionsparteien

Verschleierung von Identität und Faktoren, die Anonymität begünstigen

Hierzu zählen Maßnahmen, die es erschweren sollen, die tatsächlichen wirtschaftlichen Berechtigten bei einer Transaktion zu identifizieren. Die Verwendung falscher Identitätsdokumente zur Eröffnung von Konten oder zur Durchführung von Transaktionen entkoppelt die Verbindung zwischen Vermögenswerten und Kriminellen. Auch mittels verschachtelter Gesellschaftskonstruktionen (auch: in- oder ausländische Briefkastenfirmen) soll mitunter die Identität der dahinterstehenden Personen und Gelder verborgen werden.

Anhaltspunkte (beispielhaft):

- Probleme bei der Identifizierung der Kundschaft oder der wirtschaftlich Berechtigten
- Verweigerung der Identifizierung oder Offenlegung der wirtschaftlich Berechtigten
- Vorlegen falscher oder gestohlener Identifikationsunterlagen
- Angabe auffälliger Kontaktdaten (z.B. generische Emailadresse, ausländische Telefonnummer, Sammeladresse/-postfächer)
- Konstruktion bzw. Einbezug undurchsichtiger Firmenkonstrukte
- Auffällige Verwendung von technischen Verfahren, die eine Verschleierung der Identität ermöglichen können (z.B. Tor-Browser, VPN, Proxy-Server)

Unplausible Umtauschgeschäfte

Bei der Geldwäsche wird versucht, die Herkunft von Geldern zu verschleiern, indem diese über verschiedene Konten, Zahlungsmittel oder Wirtschaftsgüter verschoben, umgetauscht oder weitergeleitet werden. Bei legitimen Geschäften würde man im Regelfall versuchen, bürokratischen Aufwand und ggf. Bankgebühren zu minimieren.

Anhaltspunkte (beispielhaft):

- Kundschaft veranlasst zahlreiche Handels- und Umtauschgeschäfte ohne erkennbaren Hintergrund
- Hoher oder ungewöhnlicher Umtausch von Bargeld in andere Stückelungen der gleichen Währung oder in andere Währungen
- Wirtschaftsgüter wechseln in einer Serie von aufeinanderfolgenden Transaktionen mehrfach den Eigentümer, unter Umständen mit nicht nachvollziehbaren Preissteigerungen oder -minderungen

Forcierte Rückabwicklungen, Erstattungen oder Rückzahlungen

Bei forcierten Rückabwicklungen, Erstattungen oder Rückzahlungen ist es das Ziel, eine legitime Erklärung für Geldeingänge auf einem Konto zu erhalten. In der Regel wird versucht, die Rückabwicklung über ein anderes Zahlungsmittel oder ein anderes Konto abzuwickeln als das, welches für die ursprüngliche Zahlung verwendet wurde. Gegebenenfalls werden Kosten für Rückabwicklungen oder Vorfälligkeitsentschädigungen akzeptiert.

Anhaltspunkte (beispielhaft):

- Vorzeitige Rückzahlung von Darlehen unter Hinnahme von Strafzinsen oder Gebühren
- Kaufverträge oder diesbezügliche Anzahlungen sollen rückabgewickelt werden, wobei veränderte Rückzahlungsmodalitäten verlangt werden; deswegen u.U. anfallende Vertragsstrafen werden widerspruchslos akzeptiert
- Überzahlung eines geforderten Betrags durch Schuldnerin oder Schuldner, anschließend wird Rückzahlung verlangt (ggf. auf ein anderes Konto oder auf das Konto von Dritten)

Transaktion liegt deutlich über oder unter einem angekündigten oder typischen Wert

Liegt eine Transaktion deutlich über oder unter einem zuvor angekündigten oder einem üblichen Wert, kann das ein Hinweis auf eine Verschleierung von Geldflüssen illegaler Herkunft sein. Ein Erwerb von Gütern zu überhöhten Preisen kann ein Hinweis darauf sein, dass für die kaufende Person andere Kriterien entscheidungsrelevant sind als die, ein wirtschaftlich sinnvolles Geschäft zu machen. Deutliche überhöhte oder zu niedrige Rechnungen oder Kaufpreise können zudem als Vorwand dienen, um Gelder aus illegalen Quellen zu den empfangenden Personen zu transferieren.

Anhaltspunkte (beispielhaft):

- Unstimmigkeiten i.Z.m. Wert einer Ware und Verkaufspreis
- Über- oder Unterfakturierung von Kaufpreisen
- Angebotene Objekte oder Dienstleistungen werden auffallend oberhalb oder unterhalb ihres tatsächlichen Marktwertes vertrieben bzw. in Rechnung gestellt
- Dasselbe Objekt wird im Vergleich zu vorherigen Verkäufen zu einem ungewöhnlich hohen oder niedrigen Kaufpreis erworben bzw. veräußert

Hohe Geldsummen ohne erkennbare legale Quellen – Unklare Mittelherkunft

Eine erfolgreiche Geldwäschehandlung setzt voraus, dass die inkriminierte Herkunft von Geldern verborgen bleibt. Geldflüsse mit unklarer, unplausibler Mittelherkunft oder eine Weigerung einer Person, die Herkunft von Mitteln zu erklären, können daher Hinweise auf Geldwäsche sein.

Anhaltspunkte (beispielhaft):

- Kundschaft ist involviert in auffällig hohe Transaktionen ohne wirtschaftliche Erklärung
- Vorzeitige Tilgung eines Darlehens in signifikanter Höhe ohne plausible Darlegung der Mittelherkunft
- Zugunsten Dritter gestellte Sicherheiten werden zurückgegeben, ohne dass bekannt ist, wie Geld-/Kreditgebende abgelöst wurden
- Kundschaft kann oder will keine Nachweise für (möglicherweise nur vorgetäuschte) hohe Schenkungen / Erbschaften bringen

(Branchen-)unübliche Transaktionen mit Bargeld

Branchenunübliche hochvolumige Barzahlungen können aufgrund der Anonymität von Bargeld einen Versuch darstellen, illegal erworbene Gelder in den Wirtschaftskreislauf einzuspeisen.

Anhaltspunkte (beispielhaft):

- Barkauf sehr hochpreisiger Güter oder Edelmetalle
- Hohe Barzahlung in unüblich kleiner Stückelung
- Zahlung mit beschädigten oder alten Banknoten

Sonstige wirtschaftlich nicht plausible Transaktionen

Hierzu zählen jegliche Transaktionen, die kostenintensiv und wirtschaftlich sinnlos erscheinen. Geldbewegungen, die einen Verlust (auch durch eigentlich unnötige Gebühren oder Provisionen) oder eine geringere Rendite mit sich bringen, ohne dass ein sichtbarer kompensierender Nutzen für Kunden erkennbar ist, können darauf hindeuten, dass es bei der Unternehmung eher darum geht, die Nachvollziehbarkeit der Transaktionskette zu erschweren, anstatt um Rentabilität.

Anhaltspunkte (beispielhaft):

- Inkaufnahme von Verlusten bei Gewerbetreibenden
- Beteiligte zeigen kein oder nur ein geringes Kostenbewusstsein
- Nutzung von Bezahlservices außerhalb des üblichen Bankensektors

Unübliche Geschäftsgestaltung bei Unternehmen

Der Versuch, inkriminierte Werte in das Wirtschaftssystem einzuspeisen, indem sie mit den Transaktionen eines durch Geldwäscher kontrollierten bestehenden Unternehmens vermischt werden, hat für Zwecke der Geldwäsche mehrere Vorteile. Hierzu zählen bessere Kontrollmöglichkeiten durch wirtschaftliches Eigentum, welches zugleich durch eine komplexe Eigentumsstruktur des Unternehmens nach außen verschleiert werden kann. Branchenabhängig können illegal erworbene Barmittel mit Geschäftsumsätzen vermischt werden, vor allem in bargeldintensiven Wirtschaftsbranchen. Zudem erregen hochvolumige Transaktionen, größere Schwankungen bei Transaktionen oder Auslandsbezüge bei Unternehmen in der Regel weniger Misstrauen als bei Privatpersonen. An dieser Stelle werden verschiedene Geldwäsche-Auffälligkeiten aufgeführt, bei denen eine unternehmerische Tätigkeit im Vordergrund steht. Eine ausführliche Übersicht und Erläuterung zu Anhaltspunkten für handelsbasierte Geldwäsche bietet das entsprechende Anhaltspunktepapier.

Anhaltspunkte (beispielhaft):

- Hinweise auf verdeckte Verbindungen zwischen kaufender und verkaufender Partei („Scheingeschäfte“)
- Gründung von lediglich dem Kapitaldurchlauf dienenden Gesellschaften, insbesondere bei Mittelzufluss aus dem Ausland
- Gehandelte Ware passt nicht zum Unternehmenszweck
- Die Bestandsdauer bzw. der wirtschaftliche Hintergrund eines Unternehmens passen nicht zum Kaufgeschäft (z. B. eine Firma kauft ohne diesbezüglichen Geschäftszweck über die Zeit wiederholt hochpreisige Fahrzeuge)
- Viele Unternehmen befinden sich im Besitz einer Person oder eine Person beabsichtigt, in kurzer Zeit verschiedene Unternehmen gründen zu wollen, ohne dass eine nachvollziehbare steuerliche, rechtliche oder wirtschaftliche Notwendigkeit dafür besteht

- Bestehende Unternehmen werden von Dritten übernommen und Geschäfte außerhalb des bisher üblichen Rahmens getätigt (der Geschäftszweck des Unternehmens ausgeweitet). Transaktionen selbst sind anschließend i.d.R. unauffällig, weil sie sich in das bestehende Geschäft eingliedern
- Unrealistische Geschäftsumsätze
- Ein nicht rentables Geschäft wird ohne Erklärung lange aufrechterhalten
- Ein Sicherheiten-Geber zahlt, ohne hierzu unmittelbar verpflichtet zu sein
- Verträge mit unüblichen Konditionen (z.B. ohne Sicherungsinstrumente oder Garantien, unübliche Zahlungskonditionen)
- Marktunübliche Finanzierungen (z.B. Einbindung von Privatarlehen, Verzinsungen, Sicherheiten)
- Ungewöhnlich viele Verträge mit dem gleichen geschäftlichen Kontakt
- Kurz vor Abschluss eines Vertrags werden neue Beteiligte oder Vereinbarungen eingeführt

Literaturverzeichnis

BTC-Echo. (kein Datum). Abgerufen am 24. November 2025 von [btc-echo.de](https://www.btc-echo.de/academy/bibliothek/initial-coin-offering-ico/): <https://www.btc-echo.de/academy/bibliothek/initial-coin-offering-ico/>

ChainPort. (06. Januar 2025). *Hackernoon*. Abgerufen am 24. November 2025 von [Hackernoon.com](https://hackernoon.com/lang/de/Cross-Chain-Br%C3%BCcken-erkl%C3%A4rten,-wie-sie-funktionieren-und-warum-Sicherheit-so-wichtig-ist): <https://hackernoon.com/lang/de/Cross-Chain-Br%C3%BCcken-erkl%C3%A4rten,-wie-sie-funktionieren-und-warum-Sicherheit-so-wichtig-ist>

ESMA. (kein Datum). *ESMA (European Securities and Markets Authority)*. Abgerufen am 28. Mai 2026 von <https://www.esma.europa.eu/sites/default/files/2026-01/ReadMe.html>

FATF. (2020). *Trade-Based Money Laundering - Trends & Developments*. FATF.

Hall, J. (02. Februar 2017). *S&P Global*. Abgerufen am 27. November 2025 von <https://www.spglobal.com/commodity-insights/en/news-research/blog/agriculture/020217-agridigital-pioneers-blockchain-use-with-first-farmer-buyer-agriculture-settlement>

Handelskammer Hamburg. (kein Datum). Abgerufen am 27. November 2025 von <https://www.handelskammer-hamburg.de/>: <https://www.handelskammer-hamburg.de/gruendung-sicherung-nachfolge/finanzierung-foerderung/crowdfunding2/arten-6723724>

Influencer Marketing Hub. (21. März 2025). *Influencer Marketing Hub*. Abgerufen am 24. November 2025 von [influencermarketinghub.com](https://influencermarketinghub.com/influencer-rates/#toc-1): <https://influencermarketinghub.com/influencer-rates/#toc-1>

Jasch, A. (05. Juli 2017). *Companisto*. Abgerufen am 24. November 2025 von [Companisto.com](https://www.companisto.com/de/academy/recht-steuern-und-hilfsthemen/ico-funding-wenn-crowdfunding-auf-die-blockchain-trifft?ic_adwords=yes&gad_source=5&gad_campaignid=21449656257&gclid=EAIaIQobChMI06jj0PWajgMVTZmDBx1mYy35EAAYASAAEgI_G_D_BwE): https://www.companisto.com/de/academy/recht-steuern-und-hilfsthemen/ico-funding-wenn-crowdfunding-auf-die-blockchain-trifft?ic_adwords=yes&gad_source=5&gad_campaignid=21449656257&gclid=EAIaIQobChMI06jj0PWajgMVTZmDBx1mYy35EAAYASAAEgI_G_D_BwE

Plisio. (27. November 2023). Abgerufen am 24. November 2025 von [Plisio.net](https://plisio.net/de/blog/what-are-cross-chain-bridges-a-detailed-guide): <https://plisio.net/de/blog/what-are-cross-chain-bridges-a-detailed-guide>

Sistig, S. (09. Januar 2025). *UBS Steuerberatung*. Abgerufen am 24. November 2025 von <https://ubs-tax.de/donations-im-steuerrecht/>

Statista. (01. Oktober 2024). *statista.com*. Abgerufen am 24. November 2025 von Statista: <https://de.statista.com/themen/1842/social-media/>

Twitch. (24. November 2025). Von [Twitch.tv](https://help.twitch.tv/s/article/how-to-subscribe?language=de): <https://help.twitch.tv/s/article/how-to-subscribe?language=de> abgerufen

Dokumenteninformation

Informationen zum Dokument

Dokumententitel: Alternative Zahlungsmethoden und neue Technologien - Anhaltspunkte, Typologien sowie besondere Hinweise zur Geldwäschebekämpfung

Versionsnummer: 01.00

Informationsübersicht

Klassifizierung	offen
Veröffentlichungsort	FIU Homepage
Kontakt-E-Mailadresse	Anhaltspunktepapiere.gzd@fiu.bund.de

Änderungshistorie

Version	Datum	Beschreibung/Änderung
01.00	22.06.2026	Initiale Erstellung des Dokuments



Financial
Intelligence Unit

