



Model United Nations
Schleswig-Holstein 2026
**Fachkommission für
Suchtstoffe**

**Missbrauchsrisiko von
Kryptowährungen im
internationalen
Drogenhandel**

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Inhaltswarnung	2
Zusammenfassung	3
Punkte zur Diskussion	4
Einleitung	5
Hintergrund und Grundsätzliches	5
Was sind Kryptowährungen?	5
Handel mit Kryptowährungen	6
Missbrauch durch Geldwäsche	7
Internationale Bemühungen	8
Kernkonflikt:	8
Aktuelles	8
Aktuelle Resolutionen zu Kryptowährungen	8
Regionale Regularien	10
Probleme	10
Umsetzung der Travel Rule:	10
Aufsichtsarbitrage:	10
Dezentrale Börsen (DEX) und Mixer:	10
Cash-out-Transaktionen:	11
Verhältnismäßigkeit der Regulierung:	11
Lösungsansätze	11
Harmonisierung der Regulierung	12
Verbot der Privacy Coins	12
Schließung regulatorischer Schlupflöcher	12
Stärkung der Strafverfolgung	13
Konkurrierende Perspektiven	13
Hinweise zur Recherche	13
Glossar/Lexikon	14
Quellen	17

Inhaltswarnung

Dieser Gremientext benennt unter anderem die Themen Drogenhandel und kriminelle Organisationen. Bei manchen Personen lösen diese Themen starke Emotionen aus. Falls Sie zu den betroffenen Personen gehören, entscheiden Sie bitte selbst, ob Sie gerade in der Lage sind,

sich mit dem Thema / diesen Themen zu beschäftigen, ob Sie das lieber zu einem späteren Zeitpunkt tun oder vorher bestimmte Maßnahmen ergreifen wollen.

Zusammenfassung

Kryptowährungen wie *Monero* und *Bitcoin* haben den internationalen Drogenhandel grundlegend verändert. Ihre Eigenschaften - schnelle grenzüberschreitende Transaktionen und relative Anonymität - machen sie für kriminelle Organisationen besonders attraktiv. Der Fall des Archetyp Market, einer Darknet-Plattform mit 250 Millionen Euro Umsatz, zeigt das Ausmaß des Problems.

Die technische Grundlage bildet die *Blockchain*-Technologie, ein dezentrales Transaktionsregister. Während *zentrale Börsen (CEX)* Nutzeridentitäten überprüfen müssen, umgehen *dezentrale Plattformen (DEX)* und sogenannte *Privacy Coins* diese Kontrollen weitgehend. Kriminelle nutzen *Mixer*, um Transaktionen zu verschleiern, bevor sie Kryptowährungen wieder in Bargeld umwandeln.

Internationale Organisationen wie die *Financial Action Task Force (FATF)* entwickeln Empfehlungen zur Geldwäschebekämpfung, und UN-Resolutionen fordern verstärkte Maßnahmen gegen den Missbrauch digitaler Währungen. Die EU hat Privacy Coins bereits verboten, und verschiedene Staaten verschärfen ihre Regulierung.

Die zentralen Herausforderungen liegen in der uneinheitlichen Umsetzung internationaler Standards, der technischen Schwierigkeit, dezentrale Systeme zu regulieren, und dem Fehlen koordinierter *Cash-Out*-Kontrollen. Besonders problematisch ist, dass Kryptobörsen in schwach regulierte Länder ausweichen können. Die Debatte kreist um die fundamentale Frage: Wie lässt sich effektive Strafverfolgung mit dem Schutz finanzieller Privatsphäre vereinbaren? Lösungsansätze umfassen harmonisierte *KYC*-Pflichten, schwarze Listen nicht-kooperativer Staaten und verbesserte Blockchain-*Forensik*. Dabei muss berücksichtigt werden, dass

dezentrale Finanzprodukte in autoritären Staaten legitime Alternativen zum staatlich kontrollierten Finanzsystem darstellen können.

Punkte zur Diskussion

- Balance zwischen Privatsphäre und Strafverfolgung
 - Wie kann ein Gleichgewicht zwischen dem Schutz der finanziellen Privatsphäre legitimer Nutzer*innen und den Anforderungen der Strafverfolgung gefunden werden?
 - Welche Schwellenwerte und Überwachungsmechanismen sind verhältnismäßig, ohne zu übergreifende Überwachungsmechanismen zu etablieren?
- Technische Durchsetzbarkeit von Regulierungen bei dezentralen Systemen
 - Welche technischen und rechtlichen Instrumente können eingesetzt werden, um *Compliance*-Anforderungen bei Services wie *DEXs* durchzusetzen, die keinen zentralen und damit adressierbaren Betreiber*innen haben?
 - Sollten Entwickler*innen und Infrastrukturanbieter*innen rechtlich haftbar gemacht werden können?
- Menschenrechtsschutz in der Regulierung
 - Wie lässt sich sicherstellen, dass staatliche Regulierungsrahmen für *Kryptowährungen* nicht missbraucht werden, um die Versammlungsfreiheit oder legitime Opposition finanziell zu isolieren oder zu unterdrücken?
 - Welche menschenrechtlichen Mindeststandards müssen in internationalen Abkommen verankert werden?
- Wissenstransfer und Standardisierung von *Blockchain*-Analyse-Kompetenzen
 - Wie kann ein systematischer internationaler Wissenstransfer etabliert werden, um Strafverfolgungsbehörden weltweit mit den notwendigen Fähigkeiten zur Blockchain-Analyse und *Kryptowährungsforensik* auszustatten?

- Welche Rolle sollten internationale Organisationen bei der Entwicklung standardisierter Schulungsprogramme und der Zertifizierung von Blockchain-Ermittler*innen spielen?

Einleitung

Im Juni 2025 gelang durch die Zusammenarbeit europäischer und US-amerikanischer Ermittler*innen ein spektakulärer Schlag gegen den „Archetyp Market“ - eine der weltweit größten *Darknet*-Plattformen für Drogenhandel mit einem geschätzten Umsatz von 250 Millionen Euro. Die Plattform, auf der ausschließlich mit der anonymen *Kryptowährung Monero* bezahlt wurde, wickelte über 612.000 Kund*innenkonten Geschäfte mit verschiedensten Drogen ab. Dieser Fall verdeutlicht, wie digitale Währungen den internationalen Drogenhandel vereinfacht haben: Sie ermöglichen grenzüberschreitende Transaktionen mit hoher Geschwindigkeit und relativer Anonymität; Eigenschaften, die kriminelle Organisationen systematisch ausnutzen.

Für die Vereinten Nationen stellt diese Entwicklung eine fundamentale Herausforderung dar, da die etablierten Mechanismen zur Bekämpfung der Drogenfinanzierung untergraben werden. Die zentrale Frage lautet: Wie können Staaten effektiv gegen den Missbrauch vorgehen, ohne dabei die finanzielle Privatsphäre legitimer Nutzer*innen unverhältnismäßig einzuschränken?

Hintergrund und Grundsätzliches

Was sind Kryptowährungen?

Kryptowährungen sind digitale Zahlungsmittel, die auf *Blockchain*-Technologie basieren - einem dezentralen, öffentlich einsehbaren Transaktionsregister. Anders als traditionelle Währungen

werden sie nicht von Zentralbanken kontrolliert und ermöglichen grenzüberschreitende Transaktionen mit hoher Geschwindigkeit und relativer Anonymität. Diese Eigenschaften machen sie sowohl für legitime Nutzer*innen als auch für kriminelle Organisationen attraktiv.



Quelle: Pexels, Wordspectrum

Privacy Coins sind Kryptowährungen, die speziell für maximale Transaktionsanonymität entwickelt wurden. Anders als *Bitcoin* verschleiern sie kryptographisch Absender*in, Empfänger*in und Beträge. Diese Technologien machen forensische Blockchain-Analysen in der Theorie fast unmöglich, praktisch ist es Ermittler*innen teilweise möglich, Implementierungsfehler zu Nachverfolgungszwecken auszunutzen.

Handel mit Kryptowährungen

Der Handel erfolgt über *zentralisierte Börsen (CEX)* oder *dezentralisierte Plattformen (DEX)*. Während CEX wie beispielsweise Coinbase "*Know Your Customer*"-Verfahren (*KYC*) implementieren müssen (also die Identität ihrer Nutzer*innen verifizieren), umgehen DEX diese Kontrollen durch ihre dezentrale Struktur ohne zentrale Aufsicht. Privacy Coins wie Monero nutzen zusätzliche Verschlüsselungstechniken, um Transaktionen praktisch unauffindbar zu machen. *Stablecoins* wie *Tether (USDT)*, deren Wert meist an

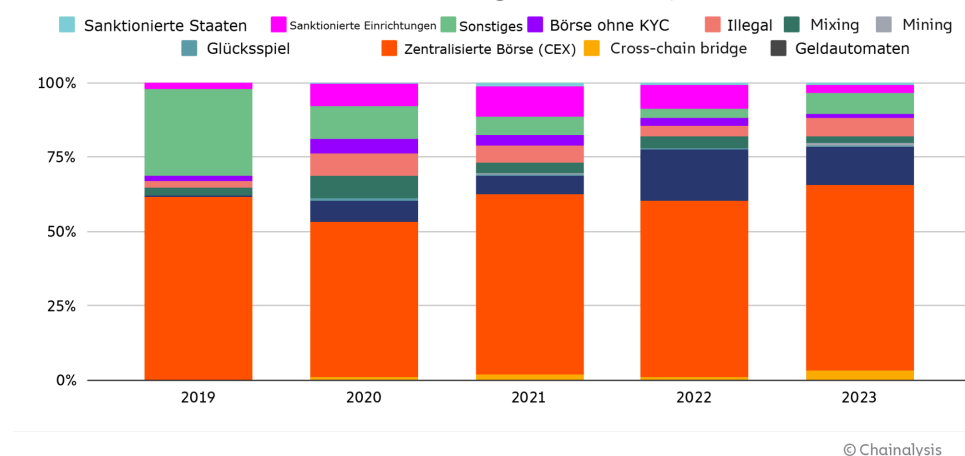
herkömmliche Währungen gekoppelt ist, dienen Kriminellen als Brücke zwischen Kryptowährungen und traditionellem Geld.

Missbrauch durch Geldwäsche

Unter Geldwäsche versteht man finanzielle Transaktionen, die darauf ausgelegt sind, die Herkunft und die Existenz von Geld oder anderen Vermögenswerten aus illegalen Transaktionen zu verstecken, um es dann wieder in den regulären Wirtschaftskreislauf einfließen zu lassen. Das Ziel der Geldwäsche ist es also, die Herkunft illegal erworbenen Geldes zu verschleiern. Das illegale Geld kann neben dem Handel mit Drogen auch aus Erpressung, dem illegalen Waffenhandel oder aus der illegalen Prostitution stammen.

Der typische Geldwäschezyklus unter Verwendung von Kryptowährungen verläuft wie folgt: Bargeld aus Drogengeschäften wird in Kryptowährungen konvertiert (*Cash-In*) und anschließend durch mehrere *Wallets* und sogenannte *Mixer* geschleust. Anschließend wird die digitale Währung wieder in Bargeld oder reguläre Bankkonten umgewandelt (*Cash-Out*). *Vendor Shops* auf Darknet-Plattformen verzeichneten 2024 einen Anstieg von über 600 Millionen US-Dollar an Kryptowährungstransaktionen.

Ziele von Geldern aus illegalen Wallets, 2019 - 2023



Ziele von Geldern aus illegalen Wallets, 2019 - 2023 | Quelle: Chainalysis, Originalgrafik ist auf Englisch, hier sinngemäß ins Deutsche übersetzt.

Internationale Bemühungen

Mit der *Financial Action Task Force on Money Laundering (FATF)* gibt es ein - von der UN abgekoppeltes - internationales Gremium, welches Standards zur Bekämpfung von Geldwäsche entwickelt. Die 1989 von der *G7* gegründete Organisation erstellt Empfehlungen, die als globale Referenz für nationale Gesetzgebungen dienen. Besonders relevant ist Empfehlung 15, die seit 2019 Kryptobörsen einschließt. Die FATF veröffentlicht *Grey- und Blacklists* von Staaten mit Regulierungsdefiziten - Länder auf diesen Listen erleiden Reputationsschäden und haben erschwerte Zugänge zu internationalen Finanzmärkten.

Kernkonflikt:

Während Befürworter*innen Datenschutzrechte und finanzielle Freiheit hervorheben, argumentieren Strafverfolgungsbehörden, dass mangelnde Transparenz organisierte Kriminalität begünstigt. Regulierungsmöglichkeiten liegen primär bei KYC-Pflichten für Börsen, Verboten anonymer Dienste (beispielsweise die EU verbietet ab 2027 Privacy Coins und anonyme Wallets), Sanktionen gegen Mixer sowie internationaler Kooperation bei der Blockchain-Analyse.

Aktuelles

Aktuelle Resolutionen zu Kryptowährungen

Resolution 9/3 (2018):

https://www.unodc.org/documents/treaties/Resolutions_and_Decisions/COP9/Resolution_9-3.pdf empfiehlt den Mitgliedstaaten der *UN*

Convention against Transnational Organized Crime (UNTOC)

ausdrücklich, rechtliche Maßnahmen zur Verhinderung der Nutzung von Kryptowährungen zur Geldwäsche zu ergreifen. Konkret sollen Unternehmen, die mit Kryptowährungen handeln, verpflichtet werden, Geldwäsche-Bekämpfungsvorschriften einzuhalten, einschließlich Kundensorgfaltspflichten (Customer Due Diligence) und der Offenlegung von Quelle, Ziel und Zweck von Transaktionen.

Die Resolution 63/1 der Fachkommission für Suchtstoffe (FfS) von 2020 betont die Bedeutung der Zusammenarbeit zwischen Behörden und dem Privatsektor zur Identifizierung verdächtiger Transaktionen. Sie ruft insbesondere dazu auf, die Nutzung von Kryptowährungen im illegalen Drogenhandel zu verhindern und fordert Partnerschaften mit Finanzinstituten und Anbieter*innen von Geldtransferdienstleistungen.

Besonders hervorzuheben ist die im Dezember 2024 von der UN-Generalversammlung verabschiedete Konvention gegen Cyberkriminalität, deren Schaffung 2017 von Russland initiiert wurde: <https://docs.un.org/ot/A/RES/79/243>. Die Konvention zielt darauf ab, internationale Kooperation bei der Bekämpfung von Cyberkriminalität zu stärken, einschließlich des Austauschs elektronischer Beweise und technischer Unterstützung, insbesondere für Entwicklungsländer. Die Konvention ist durchaus umstritten. Menschenrechtsorganisationen und der UN-Sonderberichterstatter für Menschenrechte kritisieren unter anderem ihre breite Definition von Cyberkriminalität und potenzielle Überwachungsmöglichkeiten. Nach einer Unterzeichnungszeremonie im Oktober 2025 haben bereits 65 Staaten ihre Unterstützung durch eine Unterschrift angezeigt; sie wird aber erst nach *Ratifizierung* durch 40 Staaten in Kraft treten.



Generalsekretär António Guterres (links) und Vietnams Premierminister Pham Minh Chinh bei der gemeinsamen Unterzeichnungszeremonie zur Konvention gegen Cyberkriminalität | Quelle: UN Photo, Vibhu Mishra

Regionale Regularien

Parallel zur UN-Arbeit haben einzelne Staaten und Regionen Maßnahmen ergriffen: Japan verbot Privacy-Coins bereits 2018, gefolgt von Südkorea und Australien. Die [EU-MiCA-Verordnung \(Markets in Crypto-Assets\) 2023/1114](#), die ab Dezember 2024 vollständig in Kraft trat, führte zur [Delisting](#) von Privacy Coins wie Monero und Zcash von europäischen Börsen. Die USA verhängten Sanktionen gegen Krypto-Mixer.

Probleme

Obwohl die Internationale Staatengemeinschaft bei der Bekämpfung der Finanzierung von Drogenhandel über Kryptowährungen große Fortschritte gemacht hat, gibt es immer noch große Lücken in der Vorbeugung, Aufdeckung und Verfolgung.

Umsetzung der Travel Rule:

Die "[Travel Rule](#)" besagt, dass [Dienstleister*innen für Kryptowährungen \(sogenannte VASPs\)](#) bei Transaktionen bestimmte Informationen über Absender*in und Empfänger*in weitergeben müssen. Aber nur wenige Länder setzen diese Regel komplett um. Es fehlen gemeinsame technische Standards und eine gegenseitige Anerkennung zwischen den Dienstleister*innen.

Aufsichtsarbitrage:

Kryptobörsen und andere Dienstleister*innen können sich in Länder zurückziehen, wo die Regularien und Kontrollen schwächer sind. Es gibt kein stark koordiniertes Rahmenwerk zur Geldwäscheprävention.

Dezentrale Börsen (DEX) und Mixer:

Bei diesen Systemen gibt es keine klaren Verantwortlichen, was Eingriffe erheblich erschwert. Hierbei handelt es sich um ein grundlegendes technisches Problem bei dezentralen Finanzprodukten.

Zu einem gewissen Grad können Zugangspunkte (wie Webseiten oder Server) reguliert werden, dafür fehlt allerdings auch eine einheitliche Regelung.

Cash-out-Transaktionen:

Wenn Kryptowährungen in *Fiatwährungen* umgewandelt werden, sind das extrem wichtige Datenpunkte für die Ermittler*innen. Diese Transaktionen werden aber nicht systematisch erfasst, und unterschiedliche KYC-Pflichten in verschiedenen Ländern machen die Verfolgung weniger effektiv.

links: Eine schwer nachzuverfolgende Möglichkeit, Kryptowährungen in reguläre Währungen umzutauschen, sind sogenannte Crypto-ATMs. | Quelle: Wikimedia Commons, Benoît Prieur



Verhältnismäßigkeit der Regulierung:

Wenn Kryptowährungen reguliert werden, wird oft auch die Möglichkeit eingeschränkt, sie anonym zu nutzen. Gerade in Ländern, wo Grundrechte eingeschränkt sind, können DEX eine wichtige Alternative zu einem staatlich kontrollierten Finanzsystem sein.

Lösungsansätze

Um die Risiken von Kryptowährungen im Drogenhandel einzudämmen, gibt es verschiedene Ansätze, die sich teils ergänzen, teils aber auch im Spannungsfeld zwischen Strafverfolgung und dem Schutz der Privatsphäre stehen. Diese sollten bei MUN-SH durch die Fachkommission für Suchtstoffe zunächst in Form einer *Resolution* vorgebracht werden. Diese wäre zwar nicht rechtlich bindend, würde aber politischen Druck ausüben und die Grundlage für konkrete Maßnahmen schaffen.

Harmonisierung der Regulierung

Ein zentraler Ansatz besteht darin, internationale Standards für VASPs zu schaffen. Diese Standards könnten auf den bestehenden Empfehlungen der FATF aufbauen. Konkret würde dies umfassendere KYC-Regelungen bedeuten.

Für die oben genannte Travel Rule könnten gegenseitige Anerkennungsabkommen geschaffen werden, bei denen sich Länder auf gemeinsame technische Standards einigen. Vorbild könnten hier die Mechanismen der FATF sein: Länder, die diese Standards nicht umsetzen, würden zwar nicht formal vom Finanzmarkt ausgeschlossen, würden aber faktisch mit dem Verlust von Korrespondenzbankbeziehungen und verringertem Investorenvertrauen rechnen müssen - was bereits heute bei der FATF-Grey-List zu beobachten ist.

Verbot der Privacy Coins

Ein weitergehender Vorschlag wäre das koordinierte Verbot der Privacy Coins. Praktisch würde ein Verbot durch ein Delisting dieser Finanzprodukte an öffentlichen Börsen ablaufen, wie es derzeit in der EU passiert. Dadurch würde ihre Liquidität stark eingeschränkt, auch wenn ein Handel über DEX weiterhin möglich wäre. Ähnlich könnten Mixer sanktioniert werden, indem man primär bei deren *Hosts* ansetzt.

Schließung regulatorischer Schlupflöcher

Um zu verhindern, dass sich Kryptobörsen in schwach regulierte Länder zurückziehen, könnte eine internationale "schwarze Liste" nicht-kooperativer *Jurisdiktionen* erstellt werden, analog zur bereits existierenden FATF-Greylist. Für Transaktionen mit Dienstleister*innen aus diesen Ländern würden dann erweiterte Sorgfaltspflichten gelten, was den regulatorischen Aufwand erhöht und diese Jurisdiktionen weniger attraktiv macht.

Stärkung der Strafverfolgung

Ein weiterer Ansatz liegt in der Verbesserung der Ermittlungsfähigkeiten. Das *UN-Büro für Drogen- und Verbrechensbekämpfung (UNODC)* könnte seine Trainingsprogramme für Blockchain-Forensik und Krypto-Tracing ausweiten, um Ermittler*innen weltweit besser zu schulen. Zudem könnte der grenzüberschreitende Informationsaustausch vereinfacht werden, wobei hier besonders auf Verhältnismäßigkeit, Menschenrechte und eine geteilte Definition von Verbrechen zu achten ist. An dieser Stelle sei nochmal auf die oben genannte Konvention gegen Cyberkriminalität verwiesen, bei welcher sehr ähnliche Probleme auftreten.

Konkurrierende Perspektiven

Bei all diesen Ansätzen bleibt die Grundfrage bestehen: Wie viel Privatsphäre soll zugunsten effektiverer Strafverfolgung eingeschränkt werden? Während strengere Regulierung die Kriminalitätsbekämpfung erleichtert, können DEX gerade in autoritären Staaten eine wichtige Alternative zum staatlich kontrollierten Finanzsystem sein. Diese unterschiedlichen Länderpositionen müssen in einer Resolution berücksichtigt werden.

Hinweise zur Recherche

Ein guter erster Anhaltspunkt für die Recherche Ihrer Länderposition zu diesem Thema könnte die Position zur Konvention gegen Cyberkriminalität sein: <https://docs.un.org/ot/A/RES/79/243>

Eine Liste der unterzeichnenden Staaten findet sich hier: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_n=XXVIII-16&chapter=18

Teilweise gibt es auch öffentliche Positionsaussagen zu der Konvention (z.B., USA, UK, Human Rights Watch). Generell enthalten offizielle Websites von Staaten häufig Positionsaussagen. Zusätzlich ist

es auch empfehlenswert, sich die Resolution selbst anzuschauen:

<https://docs.un.org/ot/A/RES/79/243>

Weiterhin ist interessant, ob der zu vertretende Staat Mitglied in der FATF ist, eine Liste der Mitglieder ist hier zu finden:

<https://www.fatf-gafi.org/en/the-fatf/who-we-are.html>

Glossar/Lexikon

Aufsichtsarbitrage: strategisches Ausweichen von Unternehmen in Länder mit lockerer Regulierung, um strengerer Vorschriften zu entgehen.

Bitcoin: erste und bekannteste digitale Währung (seit 2009). Anders als Privacy Coins lassen sich Bitcoin-Transaktionen grundsätzlich zurückverfolgen, auch wenn die Nutzer*innen dabei pseudonym bleiben.

Blockchain: verteiltes digitales Kontenbuch, das Transaktionen dauerhaft und für alle einsehbar speichert. Nachträgliche Änderungen sind praktisch unmöglich.

Cash-In: Bargeld wird in Kryptowährungen konvertiert

Cash-Out: Rückumwandlung digitaler Währungen in herkömmliches Geld. Dieser Vorgang ist für Ermittler*innen besonders relevant, da hier oft Identitäten aufgedeckt werden können.

CEX (Centralized Exchange): Börsenplattformen wie Coinbase mit zentraler Verwaltung, die verpflichtet sind, ihre Kund*innen zu identifizieren.

Compliance: Befolgung rechtlicher Vorgaben und Regulierungsstandards durch Organisationen.

Darknet: abgeschirmte Internetbereiche, die nur über Spezialsoftware erreichbar sind und Anonymität gewährleisten. Genutzt sowohl für legale Zwecke als auch für illegale Märkte.

Delisting: Ausschluss einer digitalen Währung vom Handel an einer Börse, was deren Handelbarkeit massiv einschränkt.

DEX (Decentralized Exchange): Handelsplattformen ohne zentrale Betreiber*innenstruktur, die deshalb kaum regulierbar sind und oft keine Identitätsprüfungen vornehmen.

FATF (Financial Action Task Force): 1989 etabliertes internationales Gremium, das Richtlinien gegen Geldwäsche und Terrorfinanzierung erarbeitet.

Fiatwährungen: traditionelle staatliche Währungen wie Euro oder Dollar, die von Zentralbanken herausgegeben werden.

Forensik: wissenschaftliche Untersuchungsmethoden zur Verbrechensaufklärung. Bei digitalen Währungen werden Transaktionsmuster analysiert, um illegale Aktivitäten zu identifizieren.

G7: Zusammenschluss der sieben führenden Industriestaaten, der sich mit globalen Wirtschafts- und Politikfragen befasst. Seine Mitglieder sind Deutschland, Frankreich, Italien, Japan, Kanada, das Vereinigte Königreich und die Vereinigten Staaten.

Grey-/Blacklists: FATF-Verzeichnisse von Staaten mit unzureichender Geldwäschebekämpfung. Die Listung führt zu Vertrauensverlust und eingeschränktem Zugang zu globalen Finanzströmen.

Host: Als Host wird ein wichtiger Bestandteil eines Rechnernetzes bezeichnet, der im Normalfall rund um die Uhr läuft und Dienstleistungen für andere Systeme erbringt. Mittels seines Betriebssystems stellt er Dienste wie die Speicherung und Bereitstellung von Daten, Websites, Anwendungen und andere Ressourcen bereit und stellt die dafür notwendige Infrastruktur zur Verfügung. So kann ein Host Informationen und Inhalte für Benutzer*innen zugänglich machen – sei es über das Internet oder über ein internes Netzwerk.

Jurisdiktion: Geltungsbereich staatlicher Gesetze und behördlicher Zuständigkeiten.

KYC (Know Your Customer): Identifikationsprozesse, mit denen Finanzdienstleister ihre Kund*innen verifizieren müssen, um Geldwäsche vorzubeugen.

Kryptowährungen: digitale Zahlungssysteme auf *Blockchain*-Basis, die ohne staatliche Kontrolle auskommen und internationale Überweisungen in Echtzeit ermöglichen.

MiCA-Verordnung (Markets in Crypto-Assets): seit Ende 2024 gültiges EU-Regelwerk für digitale Vermögenswerte, das erstmals umfassende Standards für den europäischen Kryptomarkt setzt.

Mixer: Programme, die Transaktionen verschiedener Nutzer*innen miteinander vermischen und dadurch ihren Ursprung verschleiern. Werden für Datenschutz wie für kriminelle Zwecke eingesetzt.

Monero: auf Anonymität spezialisierte digitale Währung, die durch fortgeschrittene Verschlüsselung alle Transaktionsdetails verbirgt.

Privacy Coins: digitale Währungen mit eingebauten Anonymisierungsfunktionen, die eine Nachverfolgung von Zahlungsströmen extrem erschweren.

Ratifizierung: bedeutet, dass Rechtsnormen in nationales Recht übernommen werden, indem das Parlament oder die Bevölkerung durch Volksabstimmung zustimmen und ggf. das Staatsoberhaupt dies mit seiner*ihrer Unterschrift bestätigt. Erst so wird der von der Regierung geschlossene völkerrechtliche Vertrag wirksam.

Resolution: formelle Beschlüsse internationaler Organisationen. Meist rechtlich unverbindlich, entfalten sie dennoch politische Wirkung durch öffentlichen Druck.

Stablecoins: digitale Währungen mit stabilem Wert durch Kopplung an traditionelle Währungen, was starke Wertschwankungen verhindert.

Tether (USDT): wertgebundener Token, der den US-Dollar im Verhältnis 1:1 abbildet und häufig als Verbindungsglied zwischen Krypto- und traditionellem Finanzmarkt dient.

Travel Rule: internationale Vorgabe, nach der bei Krypto-Überweisungen Absender*innen- und Empfänger*innendaten weitergegeben werden müssen - analog zu klassischen Banküberweisungen.

UNODC (UN Office on Drugs and Crime): UN-Behörde, die Staaten im Kampf gegen Drogenkriminalität und organisiertes Verbrechen berät und unterstützt.

UNTOC (UN Convention against Transnational Organized Crime): internationales Übereinkommen gegen grenzüberschreitende organisierte Kriminalität, das Verbrechen wie Menschenhandel und Geldwäsche bekämpft.

VASPs (Virtual Asset Service Providers): Unternehmen, die Dienstleistungen rund um digitale Vermögenswerte anbieten, etwa Börsen oder digitale Geldbörsen-Anbieter*innen.

Vendor Shops: individuelle Verkaufsseiten im Darknet, über die einzelne Händler*innen ihre illegalen Waren anbieten.

Wallets: digitale Aufbewahrungsorte für Kryptowährungen, entweder als Software-Anwendung oder als physisches Speichergerät.

Quellen

- UN-Generalversammlung: Konvention gegen Cyberkriminalität. A/RES/79/243, 2024. <https://docs.un.org/ot/A/RES/79/243>
Dieses Dokument ist die aktuellste und umfassendste Konvention zum Thema Cyberkriminalität, die auch den Missbrauch von Kryptowährungen einschließt. Sie ist besonders relevant für die internationale Zusammenarbeit.
(Englisch)

- UNODC: Resolution 9/3. 2018
https://www.unodc.org/documents/treaties/Resolutions_and_Decisions/COP9/Resolution_9-3.pdf - Diese Resolution empfiehlt den UNTOC-Mitgliedstaaten rechtliche Maßnahmen zur Verhinderung der Nutzung von Kryptowährungen zur Geldwäsche. Sie legt den Grundstein für nationale Gesetzgebungen. (Englisch)
- Fachkommission für Suchtstoffe: Resolution 63/1. 2020.
<https://www.unodc.org/unodc/en/commissions/CND/index.html> - Betont die Bedeutung der Zusammenarbeit zwischen Behörden und dem Privatsektor zur Identifizierung verdächtiger Transaktionen im Zusammenhang mit illegalem Drogenhandel und Kryptowährungen. (Englisch)
- Asia Times: South Korea Bans Privacy Coins. 2020.
<https://asiatimes.com/2020/11/south-korea-bans-privacy-coins> - Berichtet über das Verbot von Privacy Coins in Südkorea. (Englisch)
- CoinCodex: Australian Exchanges Are Delisting Privacy Coins as They Succumb to Regulatory Pressure.
<https://coincodex.com/article/9325/australian-exchanges-are-delisting-privacy-coins-as-they-succumb-to-regulatory-pressure> - Berichtet über die Delistung von Privacy Coins in Australien aufgrund regulatorischen Drucks. (Englisch)
- EBA: EU-MiCA-Verordnung 2023/1114
<https://www.eba.europa.eu/sites/default/files/2024-12/25bb6d67-4bd1-4e54-805c-269d9657e7fb/Preventing%20ML%20TF%20in%20the%20EU%27s%20crypto%20assets%20sector.pdf> - Das EU-Regelwerk setzt umfassende Standards für den europäischen Kryptomarkt und hat bereits zur Delistung von Privacy Coins geführt. Es ist ein konkretes Beispiel für regionale Regulierung. (Englisch)
 - Hier finden Sie eine Zusammenfassung auf Deutsch:
<<https://eur-lex.europa.eu/DE/legal-content/summary/european-crypto-assets-regulation-mica.html>

- GOV.UK: UK National Statement on Signing the UN Convention Against Cybercrime.
<https://www.gov.uk/government/speeches/uk-national-statement-on-signing-the-un-convention-against-cybercrime> - Enthält die nationale Stellungnahme des Vereinigten Königreichs zur Unterzeichnung der UN-Konvention gegen Cyberkriminalität. (Englisch)
- Human Rights Watch:
 - Upcoming Cybercrime Treaty Will Be Nothing But Trouble. 2024.
<https://www.hrw.org/news/2024/08/07/upcoming-cybercrime-treaty-will-be-nothing-trouble> - Eine kritische Perspektive auf die UN-Konvention gegen Cyberkriminalität, die menschenrechtliche Bedenken äußert. (Englisch)
 - Joint Statement on the Signing of the UN Convention on Cybercrime. 2025.
<https://www.hrw.org/news/2025/10/24/joint-statement-on-the-signing-of-the-un-convention-on-cybercrime> - Eine gemeinsame Erklärung von Menschenrechtsorganisationen zur Unterzeichnung der UN-Konvention über Cyberkriminalität. (Englisch)
- OHCHR: Statement by the UN Special Rapporteur on Human Rights. 2024.
<https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2024-07-25-stm-SR-CT-Cybercrime-Convention.pdf> - Eine weitere kritische Stellungnahme zur UN-Konvention gegen Cyberkriminalität, die die potenziellen Auswirkungen auf die Menschenrechte beleuchtet. (Englisch)
- UNODC:
 - UN Convention against Transnational Organized Crime (UNTOC).
<https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html> - Das Übereinkommen ist die Grundlage für die Bekämpfung grenzüberschreitender organisierter Kriminalität, zu der auch der Drogenhandel gehört. (Englisch)

- UNODC: Cybercrime and Online Trafficking.
<https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/onlinetrafficking/payment/regulation.html> -
Bietet Informationen zu Cyberkriminalität und
Online-Handel, einschließlich der Regulierung von
Zahlungen. (Englisch)
- UN Treaties: Status of the UN Convention against Cybercrime.
https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18 - Zeigt den aktuellen Status
der Unterzeichnungen und Ratifizierungen der UN-Konvention
gegen Cyberkriminalität. (Englisch)
- U.S. Department of the Treasury: Press Release.
<https://home.treasury.gov/news/press-releases/jy1933>
Informiert über die Sanktionen der USA gegen Krypto-Mixer.
(Englisch)
- USUN: Explanation of Position of the United States on the
Adoption of the Resolution on the UN Convention against
Cybercrime.
<https://usun.usmission.gov/explanation-of-position-of-the-united-states-on-the-adoption-of-the-resolution-on-the-un-convention-against-cybercrime-in-ungas-third-committee/> - Erläutert
die Position der Vereinigten Staaten zur UN-Konvention gegen
Cyberkriminalität. (Englisch)