Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Januar 2024

National Risk Assessment (NRA)

Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets

Inhaltsverzeichnis

1. Glossar

Blockchain-Technologie	Variante von mehreren möglichen sogenannten Distributed Ledger-Technologien (DLT).
CeFi	Centralized Finance
CEX	Centralized Exchange
DAO	Decentralized Autonomous Organization
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DLT	Distributed Ledger Technology bzw. Technik verteilter elektronischer Register, die es ermöglicht, Daten dezentral auf vielen Computern zu speichern und zu verwalten, wodurch Transaktionen transparent, sicher und fälschungssicher werden.
FATF/GAFI	Financial Action Task Force/Groupe d'action financière
FI	Finanzintermediär
Fiatgeld	Gesetzliches, durch Zentralbanken herausgegebenes Zahlungsmittel, das im Gegensatz zu Warengeld nicht mehr mit physischen Waren oder Rohstoffen gedeckt ist.
FIU	Financial Intelligence Unit
GW/TF	Geldwäscherei/Terrorismusfinanzierung
Hosted / custodial Wallet	Wallet eines Kunden bei einem Finanzintermediär mit VASP-Tätigkeit mit Zugriffsmöglichkeit durch letzteren
KGGT	Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung
KYC	"Know Your Customer" (Kenne deinen Kunden) bezeichnet das Verfahren, das von Finanzintermediären eingesetzt wird, um die Identität von Kunden zu überprüfen, das Kundenrisiko zu bewerten und zu überwachen sowie illegale Aktivitäten wie Geldwäscherei zu verhindern.

Metaverse	Virtuelle Welt, die durch die Verbindung von physischen und digitalen Elementen entsteht und den Benutzern ermöglicht, in einer immersiven Umgebung zu interagieren.
Multisig Wallet	Multisig Wallets (*Multi-signature Wallet)* sind digitale Geldbörsen, bei denen mehrere private Schlüssel notwendig sind (bzw. normalerweise mehrere Personen ihre Zustimmung geben müssen), um Transaktionen durchzuführen, was die Sicherheit erhöht.
NFT	Non-Fungible Token
Off-Chain Transaktion	Nicht auf einer Blockchain registrierte VA-Transaktion
On-Chain Transaktion	Auf einer Blockchain registrierte VA-Transaktion
Peer-to-Peer (P2P)	Netzwerkmodell, bei dem die teilnehmenden Geräte ohne einen zentralen Server direkt miteinander verbunden sind, was in einer dezentralen Interaktion zwischen den Geräten unter gleichgestellten Voraussetzungen resultiert.
PEP	Politisch exponierte Person
Privacy Coin	Kryptowährungen, die darauf abzielen, die Privatsphäre und Anonymität der Benutzer bei Transaktionen zu erhöhen, zum Beispiel Monero oder Zcash.
Rugpull	Wenn ein Entwicklerteam ein Projekt (bspw. eine DeFi-Plattform) plötzlich aufgibt und seine gesamte Liquidität verkauft oder abzieht.
Smurfing	Aufteilung einer einzigen Transaktion mit hohem Gegenwert in kleinere Teilbeträge, um den tatsächlichen Gegenwert der Transaktion zu verschleiern und GW/TF-Abwehrmassnahmen in Zusammenhang mit erlaubten Maximalbeträgen zu umgehen.
Smart Contract	Automatisierter digitaler Vertrag, der die Bedingungen und Ausführung von Transaktionen zwischen Parteien ohne Zwischenhändler oder menschliches Eingreifen regelt.

Stablecoins	VAs, die darauf abzielen, einen stabilen Umrechnungswert zu haben, indem sie an einen Rohstoff (z.B. 1 Gramm Gold = 1 Stablecoin-Einheit) oder eine Währung (z.B. z.B. 1 CHF = 1 Stablecoin-Einheit) gekoppelt werden.
SVB	Strafverfolgungsbehörden
TBML	Trade-based Money Laundering (handelsbasierte Geldwäscherei)
Travel Rule	Auf der FATF-Empfehlung Nr. 16 beruhende Regelung, die Finanzintermediären mit und ohne VASP-Tätigkeit vorschreibt, bei grenzüberschreitenden Transaktionen personenbezogene Daten ihrer Kunden auszutauschen.
Unhosted / non-custodial Wallet	Private Wallet ohne Zugriffsmöglichkeit durch Dritte
VA	Virtual Asset
VA-ATM	Virtual Asset-Bancomat
VASP	Virtual Asset Service Provider
Web3	Weiterentwicklung des Internets, in der dezentrale Anwendungen und Systeme auf der Blockchain-Technologie aufbauen.

2. Executive Summary

Kryptowährungen (*Virtual Assets*, VAs) haben sich in den letzten zehn Jahren von einer Nischenaktivität zu einem Massenphänomen entwickelt, das Auswirkungen auf das traditionelle Finanzsystem hat. Die Verwendung von VAs ist für Privatpersonen wie Unternehmen üblicher geworden. In der Schweiz bieten immer mehr Finanzintermediäre Dienstleistungen im VA-Bereich an; sogenannte Virtual Asset Service Provider (VASP). Allerdings haben auch Kriminelle das Potenzial dieses Zahlungssystems erkannt. VAs werden inzwischen für unterschiedlichste illegale Zwecke missbraucht, von «einfachen» Diebstahls- und Betrugsdelikten bis hin zu schwersten Formen der transnationalen Kriminalität, einschliesslich Geldwäscherei und Terrorismusfinanzierung (GW/TF). Diese Entwicklungen stellen sämtliche Stakeholder, die ins Geldwäschereiabwehrdispositiv eingebunden sind, vor erhebliche Herausforderungen.

Im Jahr 2018 veröffentlichte die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) zum Thema Missbrauch von Kryptowährungen für GW/TF erstmals eine Risikoanalyse und stufte die Gefährdungen und Verwundbarkeiten für die Schweiz als «erheblich» ein. Im Gegensatz dazu hatte die Meldestelle für Geldwäscherei (MROS) zu diesem Zeitpunkt erst einige wenige Verdachtsmeldungen im Zusammenhang mit VAs erhalten.

Der Einfluss und die Bedeutung von VAs haben sich seit 2018 grundlegend geändert. Die Sensibilisierung und das Bewusstsein im Markt sind deutlich gewachsen. Die MROS erhält inzwischen täglich VA-relevante Verdachtsmeldungen – für die Strafverfolgungsbehörden gehören VAs mittlerweile zum Arbeitsalltag. Die MROS konnte vier zentrale Entwicklungen feststellen:

1. In der Schweiz ist die Anzahl Finanzintermediäre mit VASP-Tätigkeit von unter zehn im Jahr 2018 auf über 204 per Ende 2022 deutlich angestiegen. Trotzdem haben mindestens 180 dieser Finanzintermediäre keine Verdachtsmeldung an die MROS ausgelöst.

2. Die Verwendung von VAs hat sich in der Schweiz zwischen 2018 und 2023 vervielfacht.; Immer mehr Privatpersonen und Unternehmen verwenden und akzeptieren VAs für Zahlungen im Handel, für Dienstleistungen und für Investitionen. Die Grenzen zwischen dem traditionellen Finanzsektor und dem VA-Bereich werden immer unschärfer; VAs werden zunehmend in herkömmliche Zahlungsplattformen integriert und die «beiden Welten» verschmelzen.

3. Die kriminelle Verwendung von VAs hat sowohl in der Schweiz als auch global zugenommen. Sie ist zudem deutlich diverser geworden. Strafverfolgungsbehörden sind vermehrt mit Verfahren aus unterschiedlichen Wirtschaftsbereichen konfrontiert, die Bezüge zu VAs aufweisen. So werden immer mehr Strafanzeigen im Zusammenhang mit Diebstahl oder anderweitiger Entwendung (z.B. Betrug, ungetreue Geschäftsbesorgung) von VAs erstattet. Die Schadenssummen, die durch VAs anfallen, sind stark angestiegen und belaufen sich in der Schweiz für das Jahr 2022 mindestens auf einen zweistelligen Millionenbetrag (im Vergleich: 2007 sind es knapp 7 Mio. Franken). Die Verwendung von VAs ist bei gewissen Straftaten (z.B. Investmentbetrug, Ransomeware) zum Standard geworden. VAs haben sich zu einem gängigen Werkzeug der Finanzkriminalität entwickelt.

4. Finanzintermediäre in der Schweiz haben in den vergangenen Jahren immer häufiger mutmasslich GW/TF-relevante Vorgänge mittels VAs auf den von ihnen geführten

Konten festgestellt. Dies führt zu einem starken Anstieg VA-relevanter Verdachtsmeldungen an die MROS: Im Jahr 2022 wiesen bereits fast 14% aller Verdachtsmeldungen einen Konnex zu VAs auf. In diesen konnten unter anderem Verbindungen zu politisch exponierten Personen (PEP), internationalen Korruptionsaffären, transnationalen Gruppen im Bereich der organisierten Kriminalität oder staatlichen Akteuren festgestellt werden.

Die Risikoanalyse kommt zum Schluss, dass die GW/TF-Risiken im VA-Bereich gegenüber 2018 angestiegen sind. Gefährdungen und Verwundbarkeiten, welche bereits 2018 identifiziert wurden, haben sich grösstenteils verschärft und erweitert. Aufgrund ihres höheren Stellenwerts und den mit ihnen verbundenen Risiken erfordern VAs die nötige Aufmerksamkeit sämtlicher Stakeholder.

Nebst den identifizierten Gefährdungen und Verwundbarkeiten der Schweiz gegenüber GW/TF im VA-Bereich tragen verschiedene Faktoren zur Minderung dieser Risiken bei:

- Die internationale Zusammenarbeit bei VA-Ermittlungen zeigt, dass verstärktes Tracing, Sperrungen und Einziehungen von VAs Geldwäscherei und Terrorismusfinanzierung effektiv bekämpfen können.

- Viele kleine VA-Anbieter sind mittlerweile verschwunden oder haben fusioniert. Dies hat dazu beigetragen, dass grosse Kryptobörsen ihre Compliance-Massnahmen verstärkt haben, was das Abwehrdispositiv weltweit stärkt.

- Blockchains sind naturgemäss transparenter als traditionelle Zahlungssysteme. Dies führt zu einer besseren Nachverfolgbarkeit von VAs; Blockchain-Analysetools können verdächtige Aktivitäten leichter identifizieren und verfolgen.

- Schliesslich trägt in der Schweiz die Ausweitung der Definition von Finanzintermediation im VA-Bereich dazu bei, eine breitere Palette von Akteuren in den Anwendungsbereich des Geldwäschereigesetzes zu bringen. Dies schliesst Lücken in den Massnahmen zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung.

Die KGGT schlägt vier Massnahmen vor, um das aktuelle GW/TF-Abwehrdispositiv im VA-Bereich zu stärken:

1. **Verbesserung des Daten- und Kenntnisstands zum VA-Sektor in der Schweiz**
   Informationen zum VA-Sektor und zur kriminellen Verwendung von VAs in der Schweiz sind unerlässlich, um GW/TF-Risiken angemessen zu identifizieren, zu verstehen und zu bewerten.

2. **Förderung eines proaktiven Meldeverhaltens von Finanzintermediären mit VASP-Tätigkeit**
   Finanzintermediäre mit VASP-Tätigkeit sollten künftig ihre GW/TF-Abklärungen verstärken, um besser in der Lage zu sein, verdächtige Vorgänge zu entdecken und diese der MROS zu melden.

3. **Bereitstellung von ausreichenden Kapazitäten und Ressourcen für die GW/TF-Bekämpfung im VA-Bereich**
   Die Zusammenarbeit zwischen sämtlichen zuständigen Stakeholdern muss verstärkt werden, um den Herausforderungen der GW/TF-Bekämpfung im VA-Bereich gerecht zu werden.

4. **Stärkung der internationalen Zusammenarbeit**
   Die Schweiz soll sich auf internationaler Ebene weiterhin für eine wirksame Bekämpfung der Kriminalitätsrisiken im Finanzsektor einsetzen und die Umsetzung der Empfehlung der Financial Action Task Force (FATF) vorantreiben.

Zusammenfassend ist es wichtig, dass die Schweiz die Risiken von VAs ernst nimmt und angemessene Massnahmen ergreift, um Geldwäscherei und Terrorismusfinanzierung wirksam zu bekämpfen. Die Bedeutung von VAs im Finanzsektor nimmt zu; die Schweiz muss sich den Herausforderungen stellen um mit den rasanten Entwicklungen Schritt halten zu können.

3. Einleitung

Die Verwendung von virtuellen Währungen (bzw. Virtual Assets – nachfolgend *VAs*, vgl. Kapitel 4.1) hat in den letzten fünf Jahren deutlich zugenommen. Eingesetzt für legale Zwecke werden sie beispielsweise für Investitionen, die Bezahlung von Waren und Dienstleistungen oder für weltweite Überweisungen. Allerdings besitzen VAs auch Eigenschaften, die sie anfällig machen, für Geldwäscherei- und Terrorismusfinanzierungszwecke (GW/TF) missbraucht zu werden. Ihre zunehmende Verwendung für kriminelle Zwecke im Allgemeinen sowie für GW/TF-Zwecke im Speziellen stellt sowohl Finanzintermediäre als auch Aufsichts- und Strafverfolgungsbehörden vor erhebliche Herausforderungen.

Die erste allgemeine GW/TF-Risikoeinschätzung von VAs mit konkretem Bezug zur Schweiz wurde 2014 publiziert.[1] Zum damaligen Zeitpunkt wurde festgehalten, dass in Europa keine grossen Geldwäscherei- oder Terrorismusfinanzierungsfälle mit Bezug zu VAs bekannt wären, und dass die Meldestelle für Geldwäscherei «wenig Meldungen im Zusammenhang mit Bitcoin» erhielt. Im Jahr 2018 veröffentlichte die Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) ihre erste sektorielle Risikoanalyse zur vorliegenden Thematik.[2] Hierbei wurden die Geldwäscherei- und Terrorismusfinanzierungsrisiken im Zusammenhang mit der Verwendung von virtuellen Währungen für den Finanzplatz Schweiz vertieft untersucht und die damit verbundenen Gefährdungen und Verwundbarkeiten als «erheblich» eingestuft. Im Jahr 2021 veröffentlichte die KGGT nach 2016 die zweite sektorübergreifende Gesamtbeurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz.[3] In diesem Bericht wurde angesichts der wachsenden Gefährdung der Schweiz durch VAs, der schnellen Entwicklung dieses Sektors sowie der Schwierigkeit, die damit verbundenen Risiken zu messen, eine aufmerksame Verfolgung der Lage empfohlen. Nötigenfalls sei der sektorielle Bericht zu VAs von 2018 zu aktualisieren. Der vorliegende Bericht setzt diese Empfehlung um.

Die MROS übernahm diesen Auftrag von der KGGT. Diese ist eine ständige interdepartementale Koordinationsgruppe, die vom Bundesrat Ende 2013 eingesetzt wurde. Sie hat den Auftrag, die Politik zur Bekämpfung der Geldwäscherei (GW) und der Terrorismusfinanzierung (TF) zu koordinieren und die Risiken in diesen Bereichen zu beurteilen.[4] Der vorliegende Bericht ist das Ergebnis dieser sektoriellen Risikoanalyse, die in enger Kooperation mit Aufsichts-, Strafverfolgungs- sowie weiteren Behörden und Ämtern des Bundes durchgeführt wurde.

Die Erfüllung des Auftrags gestaltete sich schwierig, da die meisten Daten, welche für eine genaue Beurteilung der GW/TF-Risiken für die Schweiz im Zusammenhang mit VAs notwendig sind, nicht flächendeckend verfügbar waren. Hierzu gehören einerseits Angaben zur Grössenordnung der im VA-Bereich operierenden juristischen und natürlichen Personen[5] sowie andererseits Angaben zur kriminellen Verwendung von VAs in der Schweiz, wie zum Beispiel konsolidierte Zahlen zur Anzahl Verfahren in der Schweiz, den untersuchten Straftatbeständen und den involvierten Beträgen sowie den daraus resultierenden Entscheiden. Trotz dieser Schwierigkeit sind gewisse Aussagen zur Bedeutung und zum

[1] Bundesrat, *Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwab (13.3687) und Weibel (13.4070) vom 25. Juni 2014*, S. 20f.
[2] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 4.
[3] KGGT, *Zweiter nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung*, Oktober 2021, S. 53.
[4] Zum Mandat und der Zusammensetzung der KGGT, vgl. Staatssekretariat für internationale Finanzfragen (SIF), *Auftrag der Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung*, bewilligt durch den Bundesratsbeschluss vom 17. November 2021.
[5] Z.B. von diesen verwaltete, versteuerte oder abgewickelte Vermögen oder Einkünften in VAs, oder zu den VA-relevanten Finanzflüssen, die auf den Finanzplatz Schweiz gelangen oder diesen verlassen

Wachstum des VA-Sektors und den damit verbundenen Geldwäscherei- und Terrorismusfinanzierungsrisiken beschränkt möglich. Hierfür wurden im Rahmen des vorliegenden Berichts unterschiedliche Erhebungen durchgeführt und Quellen ausgewertet. Sie ersetzen zwar nicht den Bedarf an zuverlässigen Zahlen zwecks Einordnung der Risiken, liefern aber eine fundierte Einschätzung. Diese lässt sich wie folgt zusammenfassen:

Erstens ist der VA-Sektor seit 2018 weltweit und national stark gewachsen. Die gesamte VA-Marktkapitalisierung machte im Jahr 2018 noch weniger als 1% des globalen Bruttoinlandprodukts (BIP) aus – auf ihrem jüngsten Höhepunkt im Jahr 2021 waren es bereits 2.7%.[6] Auch wenn diese Angaben teilweise den sehr volatilen Preisschwankungen geschuldet sind, hat die Verwendung von VAs in den letzten Jahren offensichtlich stark zugenommen. Schätzungen gehen davon aus, dass im Jahr 2023 weltweit inzwischen rund 420 Millionen Menschen, bzw. mehr als 4% der Weltbevölkerung, VAs besassen.[7] Diese starke Zunahme hat auch in der Schweiz stattgefunden. Verschiedene Umfragen in der Schweiz ergaben, dass im Jahr 2020 zwischen 7-10% der Befragten VAs gekauft hatten, während es im Jahr 2022 bereits zwischen 18-20% waren.[8] VA-Finanzflüsse bleiben im Hinblick auf andere Finanzflüsse allerdings immer noch relativ überschaubar. Während das weltweite Transaktionsvolumen sämtlicher VAs mit 15.8 Billionen US-Dollar pro Jahr seinen bisherigen Höchstwert erreichte (2021), bewegt sich beispielsweise das weltweite Handelsvolumen für ausserbörsliche Devisengeschäfte mit 7.5 Billionen US-Dollar *pro Tag* (April 2022) in einer völlig anderen Grössenordnung.[9]

Zweitens hat die kriminelle Verwendung von VAs seit 2018 weltweit zugenommen und sich diversifiziert. Berichte verschiedener Länder, supranationaler Organisationen und auf Blockchainanalyse spezialisierte Unternehmen machen deutlich, dass die kriminelle Verwendung von VAs seit 2018 global zugenommen hat und diverser geworden ist. Geldwäschereigefährdungen gehen längst nicht mehr nur von Vortaten im Bereich der Cyberkriminalität und «kryptospezifischen» Delikte aus.[10] Mittlerweile gehen Gefährdungen auch von den verschiedensten Straftaten im «Offline»-Bereich aus, darunter schwerste Formen der Wirtschaftskriminalität und letztlich auch die Verwendung von VAs durch professionelle Geldwäschereinetzwerke.[11] Zudem ist der Einsatz von VAs bei bestimmten Straftaten, insbesondere bei Ransomware-Attacken sowie im Bereich des Online-Anlagebetrugs, mittlerweile üblich und eher die Regel als die Ausnahme.

Drittens ist die Anzahl Finanzintermediäre mit VASP-Tätigkeit, die in der Schweiz domiziliert sind, seit 2018 stark angewachsen: Damals gab es weniger als zehn Finanzintermediäre mit VASP-Tätigkeit; per Ende 2022 waren es mindestens 204. Darüber hinaus kann beobachtet werden, dass auch Schweizer Finanzintermediäre *ohne* VASP-Tätigkeit immer öfter Berührungspunkte zum VA-Sektor aufweisen – zum

[6] Financial Stability Board (FSB), *FSB Chair's letter to G20 Finance Ministers and Central Bank Governors*, März 2018, S. 2. Gemäss dem Finanzstabilitätsrat wuchs die Marktkapitalisierung von VAs im Jahr 2021 um das 3,5-fache auf 2,6 Billionen US-Dollar; vgl. Financial Stability Board (FSB), *Assessment of Risks to Financial Stability from Crypto-assets*, Februar 2022, S. 1. Laut Berechnungen der Weltbank erreichte das weltweite BIP im Jahr 2021 96.1 Billionen US-Dollar; vgl. World Bank, *GDP (current US$) – World*, zuletzt abgerufen im Mai 2023.
[7] Triple-A, *Global Cryptocurrency Ownership Data*, zuletzt abgerufen im Mai 2023.
[8] Moneyland, *Wie legen Schweizer ihr Geld an?*, 22. April 2020. Moneyland, *So investieren Schweizerinnen und Schweizer ihr Geld*, 19. Juli 2022. Weitere ähnlich gestaltete Umfragen weichen um wenige Prozentpunkte nach oben oder unten ab, aber weisen dieselbe Tendenz auf, z.B.: Migros Bank, *Kryptowährungen bei jüngeren Generationen beliebter als Gold*, 27. Februar 2020. Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, 22. Juni 2021.
[9] Für das weltweite Transaktionsvolumen sämtlicher VAs, vgl. Chainalysis, *The Crypto Crime Report 2022*, Februar 2022, S. 3. Für das weltweite Handelsvolumen für ausserbörsliche Devisengeschäfte, vgl. Bank for International Settlements (BIS), *OTC foreign exchange turnover in April 2022*, Oktober 2022.
[10] Zum Beispiel ICO- und weitere Investorenbetrügereien oder etwa die Verwendung von VAs in unterschiedlichen *Money Mule*-Schemas.
[11] Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, Dezember 2021, S. 2.

Beispiel durch die von ihren Kunden ausgeübten Geschäftstätigkeiten und in Auftrag gegebenen Transaktionen. Im Hinblick auf die allgemeine Zunahme dieser Berührungspunkte sowie der festgestellten Zunahme in der kriminellen Verwendung von VAs hat sich deshalb auch die Verwundbarkeit des Schweizer Finanzplatzes, für GW/TF-Zwecke im Zusammenhang mit der missbräuchlichen Verwendung von VAs, insgesamt erhöht.

Zu bestätigen scheint dies, viertens, die deutliche Zunahme der Verdachtsmeldungen, die bei der Meldestelle für Geldwäscherei (MROS) eingereicht wurden und einen Zusammenhang mit VAs aufweisen: Für die Schweiz wurde in der im Jahr 2018 veröffentlichen Risikoanalyse noch festgestellt, dass Schweizer Behörden bis anhin keinen einzigen Fall von Terrorismusfinanzierung mittels VAs identifiziert hatten und erst wenige Fälle von Geldwäscherei durch die Nutzung dieser neuen Technologien erfasst seien.[12] Diese Schlussfolgerung ist heute überholt. Im Vergleich zu 2018 erhält die Meldestelle für Geldwäscherei (MROS) täglich Verdachtsmeldungen im Zusammenhang mit der Verwendung von VAs für Geldwäscherei- oder Terrorismusfinanzierungszwecke. Knapp 10% aller Verdachtsmeldungen, die zwischen 2020 und 2022 bei der MROS eingereicht wurden, wiesen Bezüge zu VAs auf, wobei dieser Anteil für das Jahr 2022 bereits bei 13.8% lag.

Um den hier zusammengefassten Entwicklungen Rechnung zu tragen, und die GW/TF-Bekämpfung im VA-Bereich zu verstärken, wurde in der Schweiz seit 2018 das materielle Recht an unterschiedlichen Stellen angepasst (vgl. Kapitel 4.4). Einige dieser Anpassungen gehen über die von der Financial Action Task Force (FATF) formulierten Empfehlungen hinaus. Bei der Umsetzung des materiellen Rechts bestehen aber spezifische Herausforderungen, welche die Wirksamkeit des schweizerischen GW/TF-Abwehrdispositivs in diesem Bereich beeinflussen:

Erstens hängt die Entdeckung von Geldwäscherei und Terrorismusfinanzierung mittels VAs in der Schweiz stark vom Meldeverhalten der Finanzintermediäre mit VASP-Tätigkeit ab. Verfügbare Zahlen deuten allerdings darauf hin, dass letztere im Vergleich mit Finanzintermediären *ohne* VASP-Tätigkeit deutlich seltener eine Verdachtsmeldung erstatten. So haben seit 2020 von den mittlerweile über 204 Finanzintermediären mit VASP-Tätigkeit lediglich 24 eine Verdachtsmeldung erstattet, während die MROS in derselben Periode von 118 Finanzintermediären *ohne* VASP-Tätigkeit mindestens eine Verdachtsmeldung erhielt, die einen Zusammenhang mit VAs aufwies.

Zweitens besteht ein spezifisches Merkmal des VA-Bereichs in der Tatsache, dass damit verbundene Dienstleister, Geschäftsaktivitäten, Personen und Transaktionen stark international geprägt sind. Eine der grössten Herausforderungen auf diesem Gebiet besteht in der Tatsache, dass die meisten Länder die Empfehlungen der FATF für den VA-Bereich, darunter insbesondere die Einhaltung der *Travel Rule*, nicht oder noch nicht umgesetzt haben (vgl. Kapitel 4.3.2). Im internationalen Vergleich hat die Schweiz ihre bereits bestehende gesetzliche Regelung sehr früh auch für die *Travel Rule* als anwendbar erklärt. Nichtsdestotrotz sind die im Ausland ansässigen VASPs verwundbar, als Einfallstor für kriminelle Vermögenswerte (in VAs oder Fiatwährung) in den legalen Finanzkreislauf missbraucht zu werden. Zudem ist es wichtig zu betonen, dass diese VAs stets nur eine Transaktion, bzw. eine Sekunde davon entfernt sind, in der Schweiz zu landen. Durch die Nichtumsetzung der FATF-Empfehlungen für den VA-Bereich in Drittländern erhöht sich deshalb auch die Anfälligkeit des Finanzplatzes Schweiz, für Geldwäscherei- und

[12] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 4.

Terrorismusfinanzierungszwecke missbraucht zu werden. Dieser Umstand erfordert von den Finanzintermediären erhöhte Aufmerksamkeit. Sämtliche Finanzintermediäre – mit oder ohne VASP-Tätigkeit – sind verwundbar, mittels Überweisungen auf indirektem Weg als Empfänger inkriminierter Vermögenswerte aus diesen Ländern missbraucht zu werden.

Drittens stehen insbesondere die schweizerischen Strafverfolgungsbehörden – aber auch weitere mit der GW/TF-Abwehr befasste Behörden und Ämter – vor spezifischen Herausforderungen im VA-Bereich. Rund die Hälfte von ihnenhat bereits mit dem Aufbau von Personal, Wissen und technischen Mitteln begonnen, um diesen Herausforderungen zu begegnen.

Viertens birgt die Simultanität (bzw. die gleichzeitige Existenz) verschiedener Zahlungsabwicklungssysteme aus Sicht der GW/TF-Bekämpfung seit jeher ein Risiko in sich. Mit der Simultaneität von Fiat- und VA-Zahlungsabwicklungssystemen, die sich ganz grundsätzlich unterscheiden und Daten und Informationen zu den jeweiligen Systemen deshalb auch unterschiedlich aufgebaut, aufbewahrt und verfügbar sind, hat dieses Risiko eine neue Dimension erreicht. Überdies existieren auch für einzelne VAs simultan verschiedene mögliche Zahlungsströme, die teilweise eine hohe Anonymität bieten.[13] Durch die Simultanität verschiedener Zahlungsabwicklungssysteme wird der Blick aufs Ganze für einzelne Akteure, zum Beispiel für einen Finanzintermediär oder eine Strafverfolgungsbehörde, erheblich erschwert. Kriminelle machen sich diesen Umstand zunutze, um illegal erlangte Vermögenswerte zu waschen und ihre Spuren zu verwischen. Mit den sekundenschnellen elektronischen und weltweiten Wechselmöglichkeiten von Fiatwährung und VAs sowie der Option für Benutzer von VAs, diese ebenfalls innert Sekunden aus dem Bereich der Finanzintermediation abzuziehen und auf privat kontrollierte Wallets zu transferieren, hat sich diese Problematik deutlich akzentuiert. Die Komponenten «Geschwindigkeit» und «elektronische Grenzenlosigkeit» erschweren somit eine ganzheitliche Betrachtung.

Die Risikolandschaft im VA-Sektor hat sich in den letzten Jahren verändert und die Verwendung von Kryptowährungen für Geldwäscherei- und Terrorismusfinanzierungszwecke hat zugenommen. Es ist höchst unwahrscheinlich, dass VAs in naher Zukunft wieder von der Bildfläche verschwinden werden. Gleichzeitig ist es schwierig, die diesbezüglichen Geldwäscherei- und Terrorismusfinanzierungsrisiken zu messen. 15 Jahre nach der Entstehung des ältesten VAs (Bitcoin) existieren keine verlässlichen konsolidierten Daten zur Grösse und Ausgestaltung des VA-Sektors sowohl weltweit wie auch in der Schweiz sowie den mit ihm verbundenen Fiat- und VA-Finanzflüssen. Dementsprechend liegen auch keine Erkenntnisse darüber vor, wie hoch der Anteil an diesen Finanzflüssen ist, die einen kriminellen Ursprung haben könnten. Wie im vorliegenden Bericht ausgeführt wird, gibt es in der Schweiz auch keine Bestimmungen, welche die Zuständigkeit für die Erhebung solcher Zahlen im Sinne eines nationalen Monitorings regeln würden.

Während das Argument des «bald wieder verschwindenden VA-Hypes» für eine gewisse Zeit seine Berechtigung hatte, um auf eine solche Erhebung zu verzichten, hat sich der Mangel eines nationalen Monitorings angesichts der rasanten Entwicklungen im VA-Bereich inzwischen zu einem Risiko an sich entwickelt. Bessere Daten zur tatsächlichen Grösse des VA-Sektors und der kriminellen Verwendung von VAs in der Schweiz würden eine Beurteilung, inwiefern die bereits entdeckten (Verdachts-)Fälle repräsentativ für Vorgänge im schweizerischen VA-Sektor sind und welche Empfehlungen zur Änderung des Dispositivs angemessen scheinen, erleichtern.

[13] Am Beispiel der ältesten Kryptowährung Bitcoin: Transaktionen lassen sich einerseits direkt auf der Blockchain durchführen (*on-chain*), andererseits aber auch ausserhalb der Blockchchain (*off-chain*), namentlich über Zahlungsnetzwerke, die auf der Bitcoin-Blockchain aufbauen (sog. *Second layers*) oder damit verbunden sind, zum Beispiel über das Lightning Network oder mittels CoinSwaps durch Statechains.

Jüngste Erfolge bei der Sperrung und Einziehung von inkriminierten VAs zeigen zugleich auf, dass im VA-Bereich erhebliche Chancen und bisher ungeahnte Möglichkeiten in Bezug auf die GW/TF-Bekämpfung bestehen. Die grundsätzliche Transparenz der meisten VAs kann von den Finanzintermediären und Strafverfolgungsbehörden genutzt werden, um verdächtige Aktivitäten unmittelbar zu entdecken und VA-Finanzflüsse nachzuverfolgen. Damit bietet der VA-Bereich im Kontext der der GW/TF-Bekämpfung einen entscheidenden Vorteil gegenüber dem traditionellen Zahlungsverkehr – sofern denn die dafür notwendigen Mittel und Expertisen zur Verfügung stehen.

4. Rahmen

Dieses Kapitel dient der rechtlichen und wirtschaftlichen Einordnung von Virtual Assets (VAs) im nationalen und internationalen Rahmen. Dabei werden die Begriffe "Virtual Assets" und "Virtual Asset Service Provider" gemäss der Definition der FATF erläutert und mit den ihnen entsprechenden Begriffen in schweizerischen rechtlichen Erlassen und amtlichen Publikationen abgeglichen. Für eine Übersicht, welche Personen und Dienstleistungen unter diese Definitionen fallen, werden die grundlegenden Aspekte und Unterscheidungen des VA-Ökosystems und ihr Zusammenspiel mit dem traditionellen Finanzsektor schematisiert. Ebenfalls werden die relevanten regulatorischen Entwicklungen auf internationaler sowie auf nationaler Ebene seit 2018 näher beleuchtet, darunter insbesondere der aktuelle Stand der Umsetzung der FATF-Empfehlungen bezüglich VAs und VASPs.[14] Abschliessend wird trotz begrenzter Datenlage eine möglichst genaue Beschreibung der aktuellen Ausgestaltung des VA-Sektors und der Verwendung von VAs in der Schweiz angestrebt.

4.1 Virtuelle Währungen, “Virtual Assets” und “Virtual Asset Service Provider”

Der im Juni 2014 veröffentlichte Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab und Weibel definierte den Begriff der Virtuellen Währung folgendermassen: «Eine virtuelle Währung ist eine digitale Darstellung eines Wertes, welche im Internet handelbar ist und zwar Funktionen von Geld übernimmt – sie können als Zahlungsmittel für reale Güter und Dienstleistungen verwendet werden – jedoch nirgendwo als gesetzliches Zahlungsmittel akzeptiert wird. Diese Währungen haben eine eigene Denomination. Sie unterscheiden sich von E-Geld folglich insofern, dass diese Währungen nicht durch ein gesetzliches Zahlungsmittel unterlegt sind. Virtuelle Währungen existieren lediglich als digitaler Code und haben deswegen auch kein materialisiertes Gegenstück beispielsweise in Form von Münzen oder Noten. Aufgrund ihrer Handelbarkeit, sind virtuelle Währungen als Vermögenswert einzuordnen.»[15]

Im Oktober 2018 definierte die Financial Action Task Force (FATF)[16] erstmals «Virtual Assets» (VAs) sowie «Virtual Asset Service Providers» (VASPs) – in Abgrenzung zum bisher von ihr benutzten Begriff «Virtual Currency».[17] Die neuen Definitionen wurden der FATF-Empfehlung Nr. 15 («New technologies») hinzugefügt, um klarzustellen, welche Anforderungen im Zusammenhang mit diesen neuartigen Vermögenswerten und ihren Anbietern gelten:

> «A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.».[18]

[14] Für eine Dokumentation der regulatorischen Entwicklungen im Zusammenhang mit VAs und VASPs in der Schweiz bis und mit 2018, vgl. KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018.
[15] Bundesrat, *Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwab (13.3687) und Weibel (13.4070) vom 25. Juni 2014*, S. 7f.
[16] Die FATF gilt als der internationale Standardsetter im Bereich der Geldwäscherei- und Terrorismusfinanzierungsbekämpfung.
[17] FATF, *Outcomes FATF Plenary, 17-19 October 2018*, Oktober 2018. Weitere wichtige Veröffentlichungen der FATF zur Thematik, die diese Entwicklungen widerspiegeln: FATF, *Guidance for a Risk-Based Approach to Virtual Currencies*, Juni 2015. FATF, *Guidance to a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Juni 2019, S. 4. FATF, *The FATF Recommendations*, Februar 2023, S. 140.
[18] FATF, *The FATF Recommendations*, Februar 2023, S. 135.

Die FATF definierte zudem Anbieter von Finanzdienstleistungen im Bereich der Virtual Assets als sogenannte «Virtual Asset Service Providers» (VASPs):

> "Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
> i. exchange between virtual assets and fiat currencies;
> ii. exchange between one or more forms of virtual assets;
> iii. transfer of virtual assets;
> iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
> v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.".[19]

Mit der Verankerung in der Geldwäschereiverordnung des Bundesrates (GwV) am 1. Januar 2016 wurde in der Schweiz der Begriff der «virtuellen Währung» erstmals in einem rechtlichen Erlass erfasst.[20] Währenddessen verwendete die KGGT in ihrer im Jahr 2018 publizierten Risikoanalyse «virtuelle Währungen» synonym mit «Kryptowährungen» und definierte mit dem Wort «Krypto-Asset» einen zusätzlichen Oberbegriff:

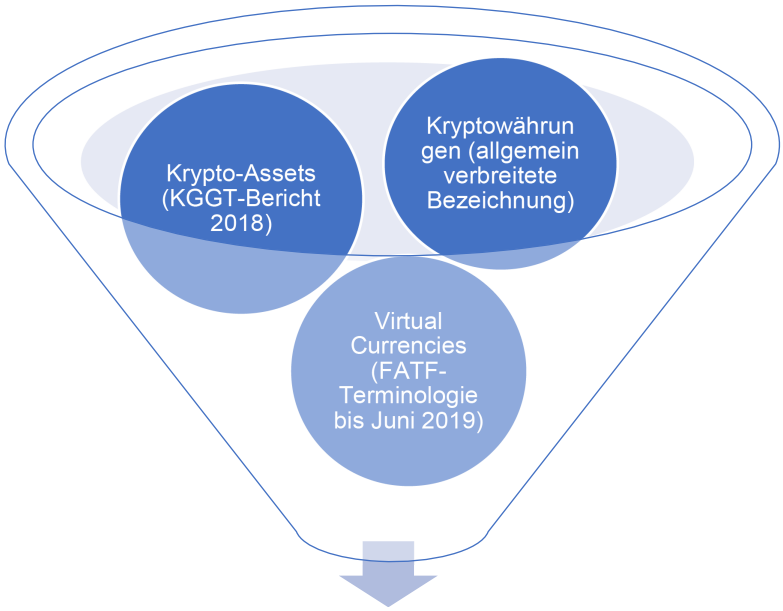
> "Unter einem Krypto-Asset wird gemeinhin eine digitale Repräsentation eines Wertes verstanden, der auf einer Blockchain digital gehandelt werden kann und zum Zweck der Zahlung (Zahlungsfunktion), Nutzung (Nutzungsfunktion) oder Investition (Investitionsfunktion) verwendet werden kann»[21].

Der Einsatz dieses Sammelbegriffs war insofern vorausschauend, als sich unter ihm nicht nur Kryptowährungen im klassischen Sinne, sondern beispielsweise auch neu entstandene Phänomene wie Non-Fungible Tokens (NFTs, vgl. Kapitel 6.2) zusammenfassen lassen – gäbe es in der Definition nicht den Verweis, dass diese auf einer Blockchain gehandelt werden können.[22] Verschiedene Länder verwenden überdies unterschiedliche Begriffe wie beispielsweise «Digital Currencies» oder «Digital Assets», die je nach Land unterschiedlich definiert und verwendet werden.

Aus Sicht der Eidgenössischen Finanzmarktaufsicht (FINMA) ist die in der Schweiz verwendete Terminologie («virtuelle Währungen») mit jener der FATF («Virtual Assets») deckungsgleich. So wird etwa bei der Beurteilung von NFTs durch die FINMA auf die wirtschaftliche Funktion und nicht etwa auf die technische Darstellung abgestellt, wobei die Frage im Vordergrund steht, was für ein Recht das NFT darstellt. Virtuelle Währungen werden im vorliegenden Bericht folglich synonym für *Virtual Assets (VA)* verwendet.

---

[19] FATF, *The FATF Recommendations*, Februar 2023, S. 135.
[20] SR 955.01 – *Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung* (Geldwäschereiverordnung, GwV), Art. 4 Abs. 2 Bst. a., Fassung vom 01.01.2016.
[21] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 8.
[22] Die Blockchain-Technologie ist eine Variante von mehreren möglichen sogenannten Distributed Ledger-Technologien (DLT, bzw. Technik verteilter elektronischer Register, stellt die Oberkategorie für Datenstrukturen dar, die sich über mehrere Computer und Standorte erstrecken). Damit sind theoretisch Kryptowährungen oder NFTs denkbar (und teilweise bereits existent), die auf anderen Distributed Ledger-Technologien als der Blockchain-Technologie beruhen.



Virtuelle Währungen (Schweiz-Terminologie seit 2014)
=
Virtual Assets (FATF-Terminologie ab Juni 2019)

Abbildung 1: Die synonymen Begriffe «Virtuelle Währungen» (CH) und «Virtual Assets» (FATF) sind rechtliche Sammelbegriffe, die beispielsweise auch NFTs umfassen.

4.2 Das VA-Ökosystem

Für die Schematisierung des VA-Ökosystems und die Kategorisierung von Aktivitäten im Zusammenhang mit VAs existieren unterschiedliche Modelle, die sich je nach gewählten Schwerpunkten und eingenommener Perspektive unterscheiden. Das hier präsentierte Modell betrachtet das VA-Ökosystem unter der Perspektive der Wertschöpfung, von der Entstehung eines VAs bis hin zu seiner Nutzung für eine konkrete Dienstleistung. Ebenfalls werden Beispiele für Finanzintermediation gemäss Geldwäschereigesetz innerhalb der Wertschöpfungskette aufgeführt und deren Interaktion mit Akteuren des VA-Ökosystems anhand möglicher Finanzflüsse (in Fiatwährung oder VAs) idealtypisch dargestellt. Aufgrund der rasanten Entwicklungen im VA-Sektor gilt es zu beachten, dass weder die Kategorisierungen noch die aufgeführten Beispiele abschliessend sind. Je nachdem können sich einzelne Kategorien oder Dienstleistungen auch überschneiden.

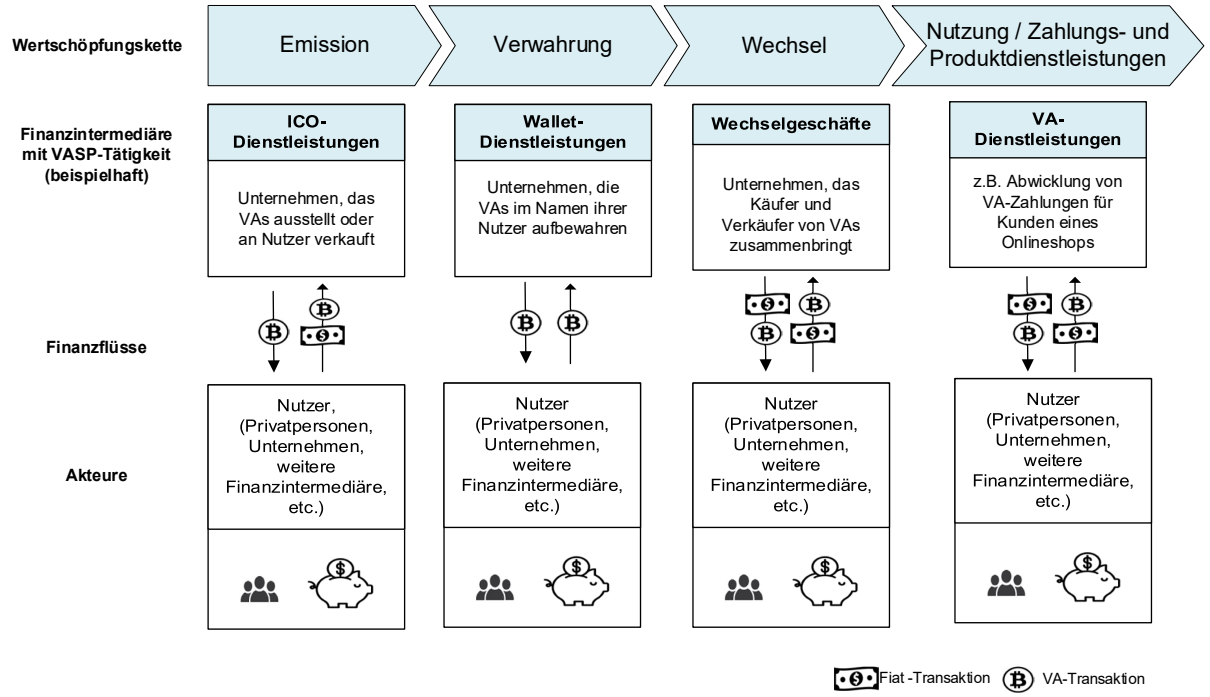


Abbildung 2: Idealtypische Darstellung der VA-Wertschöpfungskette und damit verbundenen Finanzintermediation

Auch für die Kategorisierung von VAs existieren weltweit unterschiedliche Modelle, basierend auf den jeweiligen Merkmalen. Auch hier gilt es zu beachten, dass es Überschneidungen zwischen diesen Kategorien geben kann, und dass die Einteilung von VAs in bestimmte Kategorien oft von verschiedenen Faktoren abhängt, wie beispielsweise technologische Entwicklungen oder den jeweiligen landesspezifischen regulatorische Rahmenbedingungen.

Modell 1: Kategorisierung nach Verwendungszweck und/oder technische Merkmale	Modell 2: Kategorisierung nach rechtlichem Status	Kategorisierung nach Funktion (vgl. Kapitel 4.4.3)
• **Fungible** (z.B. Bitcoin oder Ethereum) vs. **Non-Fungible Token** (z.B. Bored Ape Yacht Club Tokens) • **Ungedeckte VAs** (z.B. Bitcoin oder Ethereum) vs. **unterlegte VAs** (z.B. Stablecoins wie DAI oder USDT) • **Proof-of-Work** (z.B. Bitcoin oder Monero) vs. **Proof-of-Stake** (z.B. Ethereum oder Tezos) • **Pseudonym** (z.B. Bitcoin oder Litecoin) vs. **Anonym** (z.B. Monero oder Zcash) • **Kryptowährungen** (z.B. Bitcoin oder Litecoin) vs. **Smart Contract Plattformen** (z.B. Ethereum oder Binance Smart Chain)	• **Regulierte** vs. **unregulierte** VAs (je nach Jurisdiktion unterschiedlich) • **Verbotene** vs. **erlaubte** VAs (je nach Juristidktion unterschiedlich) • VAs als **offiziell anerkannte Zahlungsmittel** (z.B. Bitcoin in El Salvador) vs. VAs als **inoffiziell verwendete Zahlungsmittel** (z.B. Monero auf Darknetmärkten)	• **Zahlungs-Token** • **Nutzungs-Token** • **Anlage-Token** • **Hybride Token** (Mischformen, z.B: Zahlungs- *und* Nutzungs-Token, oder Anlage-, Nutzungs- *und* Zahlungstoken)

Abbildung 3: Beispiele für mögliche Kategorisierungen von VAs

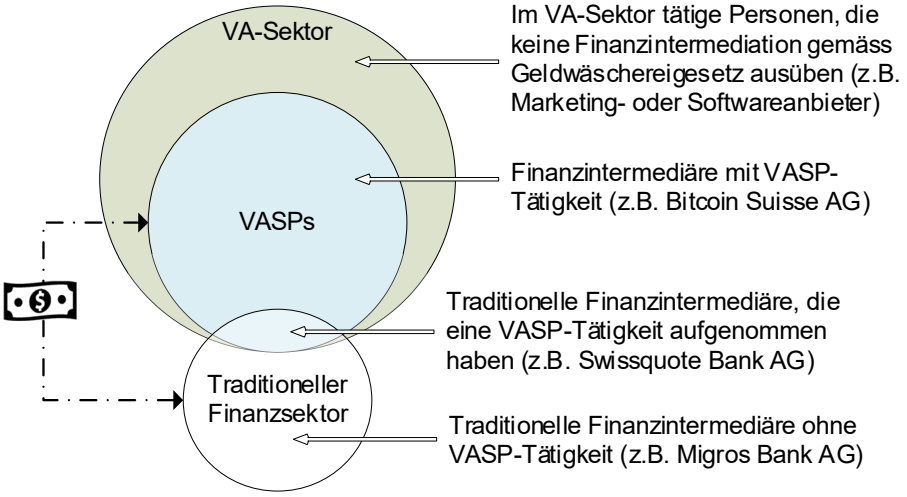


Abbildung 4: Unterscheidung und Interaktion von Finanzintermediären mit und ohne VASP-Tätigkeit

Der VA-Sektor umfasst sämtliche Geschäftstätigkeiten, die eine Verbindung zu VAs aufweisen. Nicht alle fallen in den Bereich der Finanzintermediation gemäss Geldwäschereigesetz (vgl. Kapitel 4.4.1 und 4.4.2). Der vorliegende Bericht fokussiert auf Finanzintermediäre, deren Geschäftstätigkeiten Bezüge zu VAs aufweisen. Solche Bezüge bestehen nicht nur bei den Geschäftstätigkeiten von Finanzintermediären mit VASP-Tätigkeit. Auch die Geschäftstätigkeiten von traditionellen Finanzintermediären ohne VASP-Tätigkeit können VA-Bezüge aufweisen – zum Beispiel, wenn ein traditioneller Finanzintermediär ohne VASP-Tätigkeit für seinen Kunden einen Überweisungsauftrag zu einer VA-Börse durchführt, oder wenn er einem Finanzintermediär mit VASP-Tätigkeit ein Geschäftskonto zu Verfügung stellt. Zu beachten ist zudem, dass nicht sämtliche Geschäftstätigkeiten von Finanzintermediären mit VASP-Tätigkeit eine Verbindung zu VAs aufweisen müssen. So gibt es zum Beispiel Finanzintermediäre mit VASP-Tätigkeit, die darüber hinaus auch herkömmliche Finanzdienstleistungen anbieten, die nicht in Verbindung mit VAs stehen.[23]

Infobox 1

Grenzen zwischen Finanzintermediären mit und ohne VASP-Tätigkeit verschwimmen

Aus der Perspektive der Bekämpfung der Geldwäscherei, deren Vortaten sowie der Terrorismusfinanzierung scheint die Unterscheidung zwischen Finanzintermediären mit und ohne VASP-Tätigkeit mittel- bis langfristig nur noch eine geringe Rolle zu spielen. Hierfür gibt es mehrere Gründe.
Erstens führt die zunehmende Integration von VAs dazu, dass auch traditionelle Finanzintermediäre zunehmend Dienstleistungen im VA-Bereich anbieten. Diese Entwicklung ist bereits jetzt zu beobachten und wird vermutlich anhalten. Zweitens weisen die von traditionellen Finanzintermediären eingereichten Verdachtsmeldungen immer häufiger Berührungspunkte mit dem VA-Sektor auf. Drittens führte das Wachstum des VA-Sektors dazu, dass Finanzintermediäre ohne VASP-Tätigkeit Geschäftsmodelle entwickelten, bei welchen sie selbst zwar keine VASP-Tätigkeit ausüben, das Geschäftsmodell an sich aber explizit auf den VA-Bereich ausgerichtet ist (z.B. die Zurverfügungstellung von Geschäfts- und Zahlungsabwicklungskonten in Fiat für Finanzintermediäre mit VASP-Tätigkeit, welche sodann Zahlungen in VAs auf den Plattformen der Finanzintermediäre mit VASP-Tätigkeit auslösen, vgl. Verwundbarkeit 6 in Kapitel 7.5.1).

[23] Wie z.B. die Zurverfügungstellung eines Aktiendepots.

Bei der Nachverfolgung von verdächtigen Finanzflüssen ist die Unterscheidung zwischen Fiat- und VA-Form letztlich ein technisches Detail. Die Grenze zwischen diesen zwei Kategorien von Finanzintermediären ist bereits heute unscharf. Weiteres Wachstum im VA-Sektor und eine Intensivierung der Geschäftstätigkeiten und Berührungspunkte zwischen Finanzintermediären mit und ohne VASP-Tätigkeit kann dazu führen, dass diese Kategorien zunehmend verschmelzen. Ihre Unterscheidung könnte insbesondere aus Sicht der GW/TF-Bekämpfung nur noch wichtig sein, um herauszufinden, welche Formen von Finanzflüssen (VA oder Fiat) bei der Analyse und Nachverfolgung von verdächtigen Transaktionen berücksichtigt werden müssen.[24]

4.3 Internationale Standards für die GW/TF-Abwehr im VA-Bereich

Seit 2018 war der weltweite VA-Sektor einem starken Wachstum unterworfen. Dieser Wandel drückte sich einerseits durch eine inzwischen breit abgestützte Akzeptanz von VAs, auch im traditionellen Finanzsektor, aus. Andererseits rückte der VA-Sektor verstärkt in den Fokus nationaler und internationale Regulierungsbehörden, Strafverfolgungsbehörden, Financial Intelligence Units (FIUs) sowie des Privatsektors (z.B. Unternehmen im Bereich Blockchainanalyse). Diese begannen sich stärker mit der GW/TF-Problematik im VA-Bereich auseinanderzusetzen und bauten ihre Kapazitäten aus. Gleichzeitig begann die *Financial Action Task Force* (FATF), ihre Empfehlungen systematisch auf den VA-Bereich anzuwenden. Diesbezüglich veröffentlichte die FATF in hoher Frequenz Übersichten und Leitfäden, die nachfolgend näher beleuchtet werden.

[24] Basel Institute On Governance, Europol, *Seizing the Opportunity: 5 recommendations for crypto-assets-related crime and money laundering*, 2022, S. 1f.

2018	2019	2020
• Revision der Empfehlung Nr. 15 (*FATF Recommendations)* und Definition von Virtual Assets und Virtual Asset Service Providers (Oktober)	• Einfügung eines neuen Auslegungsvermerks (*interpretative note*) in die *FATF Recommendations*, in dem die die Anwendung der FATF-Standards auf VAs und VASPs dargelegt wird (Juni) • Guidance for a Risk-Based Approach - Virtual Assets and Virtual Asset Service Providers (Juni)	• 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers (Juli) • Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing report (September)

2021	2022	2023
• Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers (Juli) • Updated Guidance for a Risk-Based Approach - Virtual Assets and Virtual Asset Service Providers (Oktober)	• Targeted Update on Implementation of FATF's Standards on VAs and VASPs (Juni)	• Targeted Update on Implementation of FATF's Standards on VAs and VASPs (Juni)

Abbildung 5: Wichtigste Publikationen der FATF im Zusammenhang mit VAs und VASPs (2018 - 2022)

4.4 Travel Rule, Stablecoins und Decentralized Finance

Die im Oktober 2018 etablierten Definitionen «Virtual Assets» und «Virtual Asset Service Providers», welche der FATF-Empfehlung Nr. 15 («New technologies») hinzugefügt wurden, können als Beginn der intensiven Beschäftigung mit dieser Thematik auf FATF-Ebene angesehen werden.[25] Im Juni 2019 wurden die dazugehörende Interpretativnote verabschiedet. Sie enthält eine Auslegung, wie die Empfehlungen Nr. 10 bis 21 von VASPs umgesetzt werden sollen.[26] Die Implementierung der *Travel Rule*, die im herkömmlichen Zahlungsverkehr bereits seit langer Zeit umgesetzt ist, stellte dabei die wichtigste Auflage dar: Fortan sollen VA-Überweisungen zwischen VASPs – wie bei einer Banküberweisung – Informationen über Absender und Begünstigte enthalten, sodass der empfangende VASP den Namen des Absenders überprüfen sowie die Korrektheit der Empfängerinformationen kontrollieren kann.

[25] FATF, *Outcomes FATF Plenary, 17-19 October 2018*, Oktober 2018.
[26] FATF, *The FATF Recommendations*, Februar 2023, S. 140.

	FATF Travel Rule (R. 16)
Angaben zum Sender	• Name • Kontonummer • Transaktionsreferenznummer • Adresse / Geburtsdatum und Geburtsort / Kundennummer / nationale ID-Nummer
Angaben zum Empfänger	• Name • Kontonummer
Schwellenwert	• EUR 1'000 / USD 1’000

Abbildung 6: Notwendige Angaben, welche beim Zahlungsverkehr – auch bei VA-Zahlungen zwischen VASPs – ausgetauscht werden müssen

Im Juni 2019 veröffentlichte die FATF die «Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers» als Reaktion auf die «drastische Veränderung der Finanzbranche» durch den VA-Sektor.[27] Dieser Leitfaden soll aufzeigen, wie VAs und VASPs in den Anwendungsbereich der FATF-Empfehlungen fallen und wie die Empfehlungen von nationalen Behörden umgesetzt werden können.

Im Juni 2020 verfasste dann die FATF einen Bericht über Stablecoins.[28] Stablecoin-Projekte verfolgen das Ziel, die bislang für VAs typische Preisvolatilität zu begrenzen, indem der Token mit bestimmten Vermögenswerten, etwa Fiat-Währungen, Rohstoffen, Immobilien oder Effekten, unterlegt wird. Ein Token kann zum Beispiel einen Anspruch auf einen Franken, auf ein Gramm Gold, auf einen Anteil an einem Immobilienportfolio oder auf eine bestimmte Menge eines Rohstoffs darstellen. Dabei stellte die FATF fest, dass Stablecoins viele der potenziellen GW/TF-Risiken von VAs im Allgemeinen teilen: Ihre potenzielle Anonymität durch die Übertragung via *non-custodial Wallets*, ihre globale Reichweite sowie ihre Eignung für die Verschleierungsphase im Geldwäschereiprozess.[29] Diese Merkmale würden Verwundbarkeiten bezüglich Geldwäscherei und Terrorismusfinanzierung darstellen. Dementsprechend forderte die FATF ihre Mitgliedsländer auf, die Umsetzung der FATF-Standards für VAs und VASPs zu priorisieren. Ebenso rief die FATF die G20-Länder auf, diesbezüglich mit gutem Beispiel voranzugehen.[30] Darauffolgend veröffentlichte die FATF im September 2020 eine Liste mit *Red Flag Indicators* für Finanzintermediäre mit VASP-Tätigkeit, um diese bei der Identifizierung von verdächtigen Vorgängen und Transaktionen zu unterstützen.[31]

Nach der Verabschiedung des Standards zu den Virtual Assets Service Providern (VASP) im Juni 2019 hat die FATF Ende 2021 den Leitfaden aktualisiert, um offene Fragen zu adressieren und auf neue Entwicklungen im VA-Sektor, insbesondere den neu entstandenen DeFi-Bereich

[27] FATF, *Guidance to a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Juni 2019.
[28] FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, Juni 2020.
[29] Eine *non-custodial* Wallet dient der Selbstverwahrung von VAs durch deren Nutzer, ohne Zugriffsmöglichkeit durch Dritte, vgl. Glossar.
[30] FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, Juni 2020, S. 2 – 4.
[31] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, September 2020.

zu reagieren.[32] Die Definitionen von VAs und VASP sind gemäss FATF sehr breit zu verstehen, sodass auch DeFi-Plattformen darunterfallen können. Dies insbesondere dann, wenn bei solchen Plattformen ein gewisser Grad der Zentralisierung vorliegt, beispielsweise in Form bestimmter Kontroll- oder Eingriffsmöglichkeiten durch die Entwickler der Plattform.[33] Folglich könnten letzteren dieselben Sorgfalts- und Meldepflichten auferlegt werden wie sonstigen Finanzintermediären. Diese Herangehensweise birgt Risiken für die GW/TF-Bekämpfung, insofern als Reaktion auf diesen Ansatz künftige Entwicklungen im VA-Sektor darauf abzielen könnten, VA-Dienstleistungen noch anonymer und dezentraler zu gestalten (vgl. Kapitel 6.2.1). Gleichzeitig stellt der Ansatz jedoch sicher, dass sich natürliche oder juristische Personen, sofern sie tatsächlich die Kontrolle oder genügend Einfluss über eine DeFi-Plattform oder ein DeFi-Protokoll haben, sich nicht mit dem Begriff «DeFi» aus der Verantwortung ziehen und die Einhaltung ihrer Sorgfalts- und Meldepflichten missachten.

Verwundbarkeit 1

Tendenziell abnehmende Bedeutung der Finanzintermediation im VA-Bereich stellt bestehende GW/TF-Regulierungsansätze vor Herausforderungen (2023 identifiziert)

VAs funktionieren aufgrund ihrer technischen Ausgestaltung prinzipiell als transnationales, barrierefreies Netzwerk zur Verschiebung von Vermögenswerten ohne Rücksicht auf territoriale Grenzen oder die Identität der Sender und Empfänger. Die *Peer-to-Peer*-Architektur (P2P) dieser Netzwerke impliziert, dass sie grundsätzlich dezentral organisiert sind und ihre Nutzer in anonymer oder pseudonymer Form daran teilnehmen können. Die Etablierung solcher P2P-Netzwerke scheint ein dauerhafter Trend zu sein. Für die Verschiebung von VAs in diesen Netzwerken sind keine Finanzintermediäre im traditionellen Sinn notwendig. Trotzdem nahmen diese bisher eine wichtige Stellung im VA-Sektor ein, vor allem als On-/Off-Ramps, welche den Wechsel von Fiatwährung und VAs gewährleisten. Verschiedene Szenarien sind vorstellbar, welche die derzeit noch wichtige Rolle von Finanzintermediären beim digitalen Austausch von Vermögenswerten vermindern könnten. So könnte etwa durch die wachsende Popularität von VAs und insbesondere Stablecoins, gepaart mit deren zunehmenden weltweiten Akzeptanz als Zahlungsmittel, mittel- bis langfristig das Bedürfnis abnehmen, VAs bei einem Finanzintermediär zu verwahren oder überhaupt in Fiatwährung umzutauschen. Momentan werden die meisten Stablecoins noch von Unternehmen aus dem VA-Sektor herausgegeben, allerdings existieren bereits Stablecoins, hinter denen sogenannte dezentralisierte autonome Organisationen (DAOs) stehen, deren rechtlicher Status bis dato meistenorts ungeklärt ist. Die GW/TF-Regulierungsansätze der FATF, wie auch spezifisch jene der Schweiz, sind auf die zentrale Rolle von Finanzintermediären und ihrer Einhaltung der Sorgfalts- und Meldepflichten ausgerichtet. Entfällt diese, so wird auch die Regulierung und die damit beabsichtigte Eindämmung der GW/TF-Risiken vor neue Herausforderungen gestellt. [34]

[32] Decentralized Finance (DeFi) ermöglicht es Nutzern, auf verschiedene VA-Finanzinstrumente wie z.B. VA-Handelspaare oder -Derivate zuzugreifen, ohne dass dabei traditionelle Finanzintermediäre eingebunden sind, vgl. Kapitel 6.2.1.
[33] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Oktober 2021, S. 27 – 36.
[34] Vgl. Eidgenössische Finanzmarktaufsicht (FINMA), *Risikomonitor 2022*, November 2022, S. 19. FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Oktober 2021, S. 18f.

4.5 Internationale Umsetzung der Travel Rule stagniert

Sowohl im Juni 2022 als auch im Juni 2023 veröffentlichte die FATF einen Bericht zum weltweiten Stand der Umsetzung der *Travel Rule* mit jeweils ernüchternden Ergebnissen.[35] Für das Jahr 2023 hatte die Mehrheit der befragten Länder (73 von 135[36]) angegeben, bis anhin keine Schritte zur Umsetzung der *Travel Rule* unternommen zu haben. Nur 35 der 135 Länder hätten per März 2023 eine Gesetzgebung zur *Travel Rule* verabschiedet und 27 seien dabei, die entsprechenden Gesetze zu erlassen. Allerdings gab nur rund ein Fünftel dieser Gruppe an, mit der tatsächlichen Durchsetzung und den entsprechenden Aufsichtsmassnahmen begonnen zu haben. Die FATF schlussfolgerte, dass diese Lücke VAs und VASPs anfällig für Missbrauch mache und es dringend notwendig sei und die Umsetzung und Durchsetzung der *Travel Rule* beschleunigt werden müssen.[37] Sowohl das Financial Stability Board der Bank für Internationalen Zahlungsausgleich wie auch die FATF warnten diesbezüglich vor dem Risiko der regulatorischen Arbitrage: Je grösser nationale Unterschiede in der Regulierung des VA-Sektors sind, desto eher können diese Unterschiede von kriminellen Akteuren ausgenutzt werden, indem sie ihre Aktivitäten jeweils in diejenigen Länder verlagern, in denen die Aufsicht weniger entwickelt oder gar ungenügend ist. Zudem werden Finanzintermediäre mit VASP-Tätigkeit in jenen Ländern, welche die *Travel Rule* für VA-Transaktionen nicht umsetzen, bevorteilt, da sie keine Ressourcen zur Abwehr von Geldwäscherei und Terrorismusfinanzierung aufwenden müssen. Die Anstrengungen jener Länder und Finanzintermediäre mit VASP-Tätigkeit, welche die *Travel Rule* einhalten, könnten dadurch unterminiert werden und Teile des Sektors in jene Länder abwandern, welche die *Travel Rule* nicht umsetzen. Dies würde weltweit – auch in der Schweiz – zu einer zusätzlichen Erhöhung der GW/TF-Risiken im VA-Bereich führen.[38]

Seit der Erhebung der FATF im März 2023 haben sich allerdings verschiedene Länder, darunter die EU und Singapur[39], an der Schweizer Umsetzung der *Travel Rule* orientiert, die die Übertragung von VAs auf nicht ermittelte *non-custodial* Wallets untersagt. So enthält die revidierte Geldtransferverordnung der EU (*Transfer of Funds Regulation, TFR*), spezifische Bestimmungen für den Transfer von VAs zwischen VASPs und *non-custodial* Wallets. Demnach gelten die Anforderungen beim Transfer von VAs auch für Transfers an oder von *non-custodial* Wallets, sofern am Transfer ein VASP oder ein anderer Finanzintermediär (also eine *obliged entity*) beteiligt ist (vgl. Erw. (38) TFR). Bei Kryptowertetransfers an oder von *non-custodial* Wallets müssen Finanzintermediäre des Auftraggebers und der begünstigten Person sowohl die erforderlichen Angaben zum Auftraggeber als auch zur begünstigten Person erheben. Bei Zahlungsaufträgen, die EUR 1'000 übersteigen, müssen sie zudem anhand geeigneter Massnahmen überprüfen, ob die *non-custodial* Wallets tatsächlich im Eigentum oder unter der Kontrolle der Kundin oder des Kunden stehen (vgl. Erw. (39) i.V.m. Art. 14 Abs. 5 bzw. Art. 16 Abs. 2 TFR).[40] In Singapur unterliegen Transaktionen mit *non-custodial* Wallets, nicht den Anforderungen der Travel Rule, sondern sollten als mit höheren ML/TF-Risiken behaftet angesehen und behandelt werden. Der Zahlungsdienstleisteranbieter sollte demnach erhöhte risikomindernde Faktoren anwenden.[41]

---

[35] FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, Juni 2022. FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, Juni 2023.

[36] Ohne Länder, die VASPs verbieten.

[37] Ibid. (2023), S.16-17.

[38] Financial Stability Institute, *Supervising cryptoassets for anti-money laundering*, April 2021, S. 19f. FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Juni 2019, S. 9.

[39] Für die Umsetzung der *Travel Rule* in Singapur, vgl. Monetary Authority of Singapore, *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, März 2020.

[40] Amtsblatt der Europäischen Union, *Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849, ABl. L 150*, 9. Juni 2023.

[41] Vgl. *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, März 2020, S. 41 f.

Zudem hat die EU ein Gesetz verabschiedet, welches einen Rechtsrahmen für VASPs schafft und die *Travel Rule* umsetzt. Die MiCa-Verordnung der Europäischen Union (*Markets in Crypto Assets Regulation*), welche die VA-Regulierung innerhalb der EU harmonisiert, tritt voraussichtlich ab 2024 in Kraft.[42] Damit wird die Zahl der Länder, die Gesetze oder Verordnungen zur Umsetzung der *Travel Rule* verabschiedet haben, auf 58 ansteigen.

Verwundbarkeit 2

Ungenügende und ungleiche internationale Um- und Durchsetzung der *Travel Rule* im VA-Bereich (2023 identifiziert)

Während die technologischen und wirtschaftlichen Entwicklungen im VA-Bereich rasch voranschreiten, scheinen regulatorische Entwicklungen nicht Schritt halten zu können. Die Anwendung der *Travel Rule* auf VA-Transaktionen wurde durch die FATF ab 2018 explizit empfohlen, also knapp zehn Jahre nach der weltweit ersten Bitcoin-Transaktion. Zu welchem Zeitpunkt die *Travel Rule* für VA-Transaktionen durch sämtliche FATF-Länder tatsächlich umgesetzt sein wird, ist momentan nicht absehbar. Ihre Nicht-Umsetzung erhöht das Risiko, dass VA-Vermögenswerte krimineller Herkunft durch mangelnde Kontrollen über zahlreiche mögliche Kanäle – in Form von Fiatwährung oder VAs – in den legalen Finanzkreislauf eingespeist werden. Dementsprechend werden grundsätzlich auch sämtliche Finanzintermediäre (mit oder ohne VASP-Tätigkeit) verwundbarer, als Durchgangs- oder Endpunkt von Finanzflüssen mit kriminellem Hintergrund zu fungieren (vgl. Verwundbarkeit 6 in Kapitel 7.5.1). Zudem werden Finanzintermediäre mit VASP-Tätigkeit in jenen Ländern, welche die *Travel Rule* für VA-Transaktionen nicht umsetzen, unfair bevorteilt, da sie keine Ressourcen zur Abwehr von Geldwäscherei und Terrorismusfinanzierung aufwenden müssen. Die Anstrengungen jener Länder und Finanzintermediäre mit VASP-Tätigkeit, welche die *Travel Rule* einhalten, könnten dadurch unterminiert werden und Marktanteile in jene Länder abwandern, welche die *Travel Rule* nicht umsetzen. Dies würde weltweit – auch in der Schweiz – zu einer zusätzlichen Erhöhung der GW/TF-Risiken im VA-Bereich führen.

4.6 Nationaler Rechtsrahmen

Seit 2018 entstanden in der Schweiz neue Regulierungen, die den VA-Bereich betreffende Empfehlungen der FATF umsetzten – teilweise restriktiver als im internationalen Vergleich. In der Schweiz wurde namentlich der bestehende GW/TF-Rechtsrahmen auf virtuelle Währungen (bzw. VAs) und Finanzintermediäre mit VASP-Tätigkeit (bzw. VASPs) ausgedehnt. Sämtliche Finanzvermittlungsaktivitäten im Zusammenhang mit VAs fallen damit in den Anwendungsbereich des Geldwäschereigesetzes (GwG). Die Eidgenössische Finanzmarktaufsicht FINMA hat dabei in mehreren Publikationen ihre Praxis und Auslegungen präzisiert. Das Schweizer Finanzmarktrecht ist prinzipienbasiert und folgt dem Grundsatz der Technologieneutralität. Entscheidend soll alleine sein, dass der Zweck einer Regelung – etwa die Begrenzung des Geldwäschereirisikos – gewahrt bleibt, unabhängig davon, ob die Marktteilnehmer ihre Dienstleistungen in analoger oder digitaler Form anbieten.[43] Die FATF beurteilte im Jahr 2020 im Verlauf des Enhanced Follow-up Prozesses der Schweiz die Umsetzung von Empfehlung Nr. 15 und die dabei angewandten geldwäschereirechtlichen Vorschriften der Schweiz im Zusammenhang mit VAs und VASPs als weitgehend konform.[44]

[42] European Parliament, *Crypto-assets: green light to new rules for tracing transfers in the EU*, April 2023.
[43] Vgl. Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2016*, März 2017, S. 26.
[44] FATF, *Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating*, Januar 2020, S. 7 – 8.

Die folgenden Unterkapitel bieten einen Überblick über den für VAs und VASPs relevanten Schweizer Rechtsrahmen, beurteilen dessen Konformität mit den internationalen Standards und fassen die wichtigsten Änderungen aus Sicht der GW/TF-Bekämpfung zusammen.

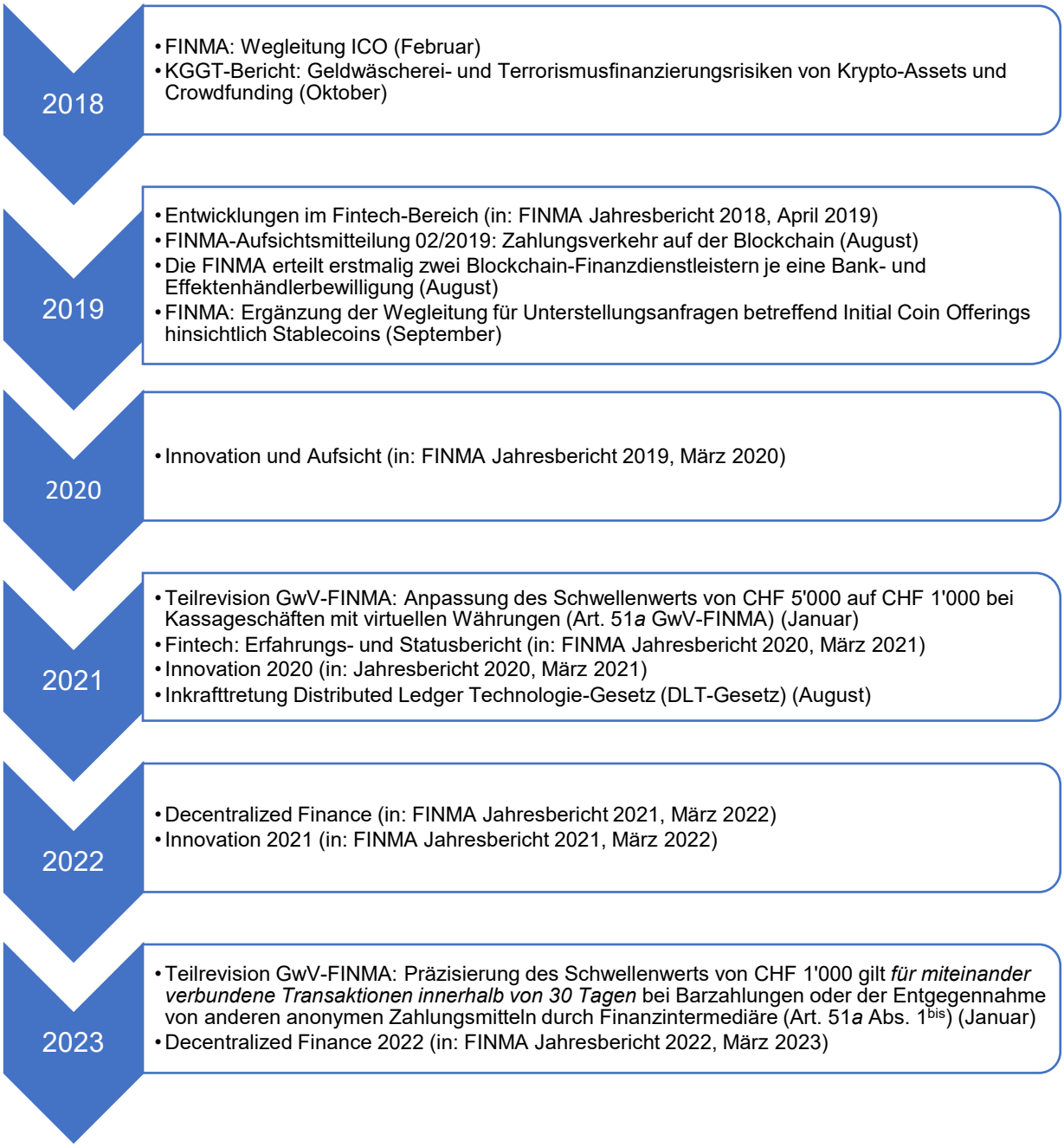


Abbildung 7: Regulatorische Entwicklungen und relevante amtliche Publikationen in der Schweiz im Zusammenhang mit VAs und VASPs (2018 - 2022)

4.6.1 Aufsicht über Finanzintermediäre in der Schweiz im GW/TF-Bereich

Die Regulierung im Bereich der Geldwäscherei beruht auf zwei Säulen: Einerseits ist Geldwäscherei gemäss Artikel 305bis des Schweizerischen Strafgesetzbuches (StGB) ein Delikt und wird von den Strafbehörden geahndet. Andererseits schreibt das Geldwäschereigesetz (GwG) den Finanzintermediären sowie den Händlerinnen und Händlern

bei ihren Kundengeschäften die Einhaltung von Sorgfalts- und Meldepflichten vor. Wer in der Schweiz als Finanzintermediär gilt, wird in Artikel 2 Abs. 2 und 3 GwG definiert.[45]

Bei Banken, Wertpapierhäusern, Versicherungsunternehmen und Instituten nach dem Kollektivanlagengesetz überwacht die FINMA im Rahmen der regulären Aufsicht direkt die Einhaltung dieser Pflichten. Die Einhaltung der Vorschriften wird jedes Jahr vor Ort von den Prüfgesellschaften und vermehrt auch direkt von der FINMA geprüft.

Unabhängige Vermögensverwalter und Trustees unterstehen der Aufsicht durch Aufsichtsorganisationen (AO), welche wiederum durch die FINMA bewilligt und beaufsichtigt werden. Personen und Gesellschaften des Parabankensektors (beispielsweise Kredit- und Leasinggesellschaften, Kreditkartenfirmen, Zahlungsdienstleister oder Geldwechsler) sind ebenfalls der Geldwäschereigesetzgebung unterstellt. Diese zweite Gruppe muss sich zur Überwachung der Einhaltung der Sorgfalts- und Meldepflichten einer Selbstregulierungs-organisation (SRO) anschliessen, die von der FINMA bewilligt und überwacht wird. Die SRO müssen überwachen, ob die ihr angeschlossenen Mitglieder die Geldwäschereipflichten einhalten. Die konkrete Prüfung können die SROs selbst wahrnehmen oder durch beauftragte Prüfgesellschaften durchführen lassen.

Weitere Aufsichtsbehörden beaufsichtigen Finanzintermediäre nach GwG, die in spezifischen Branchen tätig sind: Die Spielbanken nach dem Geldspielgesetz vom 29. September 2017 (BGS)[46] werden von der Eidgenössischem Spielbankenkommission (ESBK) beaufsichtigt, die Handelsprüfer und Gruppengesellschaften nach Artikel 42bis des Edelmetallkontrollgesetzes vom 20. Juni 1933 (EMKG)[47] vom Zentralamt für Edelmetallkontrolle (ZEMK) sowie die Veranstalter von Grossspielen nach dem BGS von der interkantonalen Geldspielaufsicht (GESPA).

4.6.2 Übersicht: VA-Dienstleistungen und ihre Unterstellung unter das Geldwäschereigesetz

Sofern eine VA-Dienstleistung dem GwG unterstellt ist, müssen diese Personen die Sorgfaltspflichten einhalten und unterstehen wie oben dargestellt, der Aufsicht der zuständigen Aufsichtsbehörde.

Kategorie der Dienstleistungen	Unterstellung unter das GwG
Token-Emission (ICOs, Tokenisierung, etc.)	Dem GwG unterstellt, wenn im Rahmen eines ICO Token ausgegeben werden, die mit Zahlungsmitteln gleichgestellt werden können (Zahlungs-Token)
***Custodial* Wallet-Anbieter**	In jedem Fall dem GwG unterstellt

[45] SR 955.0 – *Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung*, (Geldwäschereigesetz, GwG), Fassung vom 23. Januar 2023.

[46] SR 935.51 – *Bundesgesetz über Geldspiele* (Geldspielgesetz, BGS), Fassung vom 1. Januar 2021.

[47] SR 941.31 – *Bundesgesetz über die Kontrolle des Verkehrs mit Edelmetallen und Edelmetallwaren* (Edelmetallkontrollgesetz, EMKG), Fassung vom 1. Januar 2023.

***Non-custodial* Wallet-Anbieter**	Dem GwG unterstellt, sofern die Anbieter bestimmte Kontroll- oder Eingriffsmöglichkeiten besitzen (z.B. *Multi-Signature Wallets*[48] oder Applikationen zur sicheren Aufbewahrung privater Schlüssel, auch wenn diese nur durch den Kunden entschlüsselt werden können, vgl. Kapitel 4.4.6).
Online-Wechselstuben	Ebenso wie herkömmliche Wechselstuben dem GwG unterstellt
Physische Wechselstuben (inkl. VA-ATMs)	Ebenso wie herkömmliche Wechselstuben dem GwG unterstellt
Zentralisierte Handelsplattformen	In jedem Fall dem GwG unterstellt
Dezentralisierte Handelsplattformen & DeFi-Applikationen	Sofern wirtschaftlich betrachtet eine finanzmarktrechtliche Tätigkeit ausgeübt wird, die bewilligungspflichtig wäre, geht die FINMA auch bei neuartiger technischer oder rechtlicher Umsetzung von einer Bewilligungspflicht aus (wirtschaftliche Betrachtungsweise).
Miner	Nicht dem GwG unterstellt

Abbildung 8: VA-Dienstleistungskategorien und ihre Unterstellung unter das Geldwäschereigesetz (regulatorische Änderungen seit der Risikoanalyse von 2018 sind rot markiert)[49]

4.6.3 Wegleitung ICO

2018 veröffentlichte die FINMA einen Leitfaden zu *Initial Coin Offerings* (ICOs).[50] Bei einem ICO überweisen die Anleger finanzielle Mittel an den ICO-Organisator. Im Gegenzug erhalten sie Blockchain-basierte Coins bzw. Token, welche entweder auf einer in diesem Rahmen neu entwickelten Blockchain oder mittels eines sog. *Smart Contract* auf einer bereits bestehenden Blockchain geschaffen und dezentral gespeichert werden.[51] Dabei unterscheidet die FINMA zwischen Zahlungs-Token, Nutzungs-Token und Anlage-Token.[52] Damit wurde Klarheit geschaffen, welche Tätigkeiten von ICOs in den Bereich der Finanzintermediation fallen und somit dem GwG unterstehen; namentlich dann, wenn den bei solchen Fundraising-Operationen ausgegebenen Token eine Zahlungsfunktion zukommt (Zahlungs-Token) gleichgesetzt werden können.[53] Jede natürliche oder juristische Person, die als

[48] Vgl. Glossar.
[49] Vgl. die Tabelle von 2018 in: KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 39f.
[50] Eidgenössische Finanzmarktaufsicht (FINMA), *Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs)*, Februar 2018.
[51] Ibid., S. 1.
[52] Es können auch Mischformen (hybride Token) existieren.
[53] Ibid., S. 6 – 7.

Finanzintermediär tätig und damit dem GwG unterstellt ist, muss für die Ausübung dieser Tätigkeiten in der Schweiz entweder über eine aufsichtsrechtliche Bewilligung der FINMA verfügen (z.B. Bankenbewilligung, Bewilligung als Effektenhändler) oder sich einer Selbstregulierungsorganisation (SRO) anschliessen.

Infobox 2

Token-Kategorisierung gemäss der Eidgenössische Finanzmarktaufsicht FINMA[54]

Zahlungs-Token: Der Kategorie "Zahlungs-Token" (gleichbedeutend mit reinen "Kryptowährungen") werden Token zugeordnet, die tatsächlich oder der Absicht des Organisators nach als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen akzeptiert werden oder der Geld- und Wertübertragung dienen sollen. Kryptowährungen vermitteln keine Ansprüche gegenüber einem Emittenten.

Nutzungs-Token: Als "Nutzungs-Token" bezeichnet die FINMA Token, die Zugang zu einer digitalen Nutzung oder Dienstleistung vermitteln sollen, welche auf oder unter Benutzung einer Blockchain-Infrastruktur erbracht wird.

Anlage-Token: Der Kategorie "Anlage-Token" gehören Token an, die Vermögenswerte repräsentieren. Solche Tokens können insbesondere eine schuldrechtliche Forderung gegenüber dem Emittenten oder ein Mitgliedschaftsrecht im gesellschaftsrechtlichen Sinne darstellen. Bei Anlage-Token werden beispielsweise Anteile an künftigen Unternehmenserträgen oder künftige Kapitalflüsse versprochen. Der Token repräsentiert damit nach der wirtschaftlichen Funktion insbesondere eine Aktie, Obligation oder ein derivatives Finanzinstrument. Unter die Kategorie der Anlage-Token können auch Token fallen, welche physische Wertgegenstände auf der Blockchain handelbar machen sollen.

Die einzelnen Klassifizierungen der Token schliessen sich nicht zwingend gegenseitig aus. Anlage- und Nutzungs-Token können zusätzlich in die Kategorie von Zahlungs-Token fallen (sog. "**hybride Token**"). In diesen Fällen kann der Token kumulativ als Effekte und Zahlungsmittel qualifizieren. Sobald ein Token, zum Beispiel ein NFT, tatsächlich als Zahlungsmittel verwendet wird, handelt es sich dabei um ein Zahlungs-Token (*substance over form*). Dabei finden die Sorgfaltspflichten für Finanzintermediäre bei der Annahme, Aufbewahrung, Anlage oder Übertragung dieser Token Anwendung. Ebenfalls sind Zahlungs-Token von der *Travel Rule*, beziehungsweise von Art. 10 GwV-FINMA erfasst.

4.6.4 Auslegung der Travel Rule in der Schweiz

Eine Herausforderung bei der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung besteht in der wirksamen Überwachung der Vorschriften bei Transaktionen, die auf der Blockchain durchgeführt werden. Auch hier gelten die regulären Überwachungsgrundsätze in Bezug auf die Geldwäschereibekämpfung. In diesem Zusammenhang hielt die FINMA mit der Veröffentlichung der Aufsichtsmitteilung 02/2019 «Zahlungsverkehr auf der Blockchain» fest, dass sie, im Sinne des Grundsatzes der Technologieneutralität, die geltenden Schweizer Vorschriften zur Übermittlung von Angaben im Zahlungsverkehr auch im Blockchain-Bereich anwendet. [55] Mit Bezug auf die Anwendbarkeit der Vorschriften gegen die Geldwäscherei sind keine Erleichterungen gegenüber dem traditionellen Zahlungsverkehr vorgesehen.

[54] Ibid., S. 2 – 3.
[55] Eidgenössische Finanzmarktaufsicht (FINMA), *Aufsichtsmitteilung 02/2019 - Zahlungsverkehr auf der Blockchain*, August 2019.

Artikel 10 GwV-FINMA legt für Finanzintermediäre die Pflicht zur Übermittlung von Daten über den Absender und den Begünstigten fest, wenn ein Überweisungsauftrag – egal, ob in Fiatwährung oder VAs – erteilt wird. Der Finanzintermediär, der die Überweisung erhält, kann dann prüfen, ob der Name des Absenders z. B. auf einer Sanktionsliste steht. Er kann auch prüfen, ob die Angaben des Empfängers korrekt sind oder, falls sie nicht übereinstimmen, ob die Zahlung an den Absender zurückgeschickt werden muss. Die GwV-FINMA erfüllt somit die 2019 überarbeiteten FATF-Standards, welche von VASPs die Einhaltung der FATF-Empfehlungen 10 bis 21 dargelegten Präventionsmassnahmen verlangen, einschliesslich die *Travel Rule*.
Finanzintermediäre mit VASP-Tätigkeit dürfen VAs somit lediglich an externe Wallets ihrer eigenen, bereits identifizierten Kunden senden und VAs nur von solchen Wallets empfangen. Solange die Daten des Senders oder Empfängers im jeweiligen Zahlungssystem nicht zuverlässig übermittelt werden können, dürfen die Finanzintermediäre auch keine VAs von Kunden anderer Institute entgegennehmen oder an Kunden anderer Institute versenden.

	Art. 10 GwV-FINMA& FINMA-Aufsichtsmitteilung 02/2019	FATF Travel Rule INR 15 lit. 7b
Angaben zum Sender	• Name • Kontonummer • Transaktionsreferenznummer • Adresse (oder Geburtsdatum und Geburtsort / Kundennummer oder nationale ID-Nummer)	• Name • Kontonummer • Transaktionsreferenznummer • Adresse / Geburtsdatum und Geburtsort / Kundennummer / nationale ID-Nummer
Angaben zum Empfänger	• Name • Kontonummer (falls keine Kontonummer Transaktionsbezogene Referenznummer.)	• Name • Kontonummer
Schwellenwert	CHF 0.-	EUR 1'000 / USD 1’000
Gültigkeit bei Transaktionen mit *non-custodial* Wallets	Ja, vgl. FINMA Aufsichtsmitteilung 02/2019	Nein

Abbildung 9: Die Umsetzung der *Travel Rule* in der Schweiz

4.6.5 Stablecoins und Decentralized Finance

Die FINMA stellte 2019 eine Zunahme von Projekten zur Schaffung sogenannter Stablecoins fest. Folglich wurde im September 2019 eine Ergänzung zur Wegleitung für Unterstellungsanfragen betreffend ICO publiziert um Anhaltspunkte zu gegeben, wie Stablecoins nach Schweizer Aufsichtsrecht zu beurteilen sind.[56]

Auch bei der aufsichtsrechtlichen Behandlung von Stablecoins wendet die FINMA das Prinzip der Technologieneutralität an. Die FINMA richtet dabei den Fokus auf die wirtschaftliche Funktion und den Zweck eines Tokens (*substance over form*) und berücksichtigt sowohl die bewährten Wertungsentscheide (*same risks, same rules*) als auch die Besonderheiten im Einzelfall. Die Stablecoins sind nach der Art des angebundenen Werts in Fallgruppen eingeteilt. Die Fallgruppen (Anbindung an Währungen, Rohstoffe, Immobilien und Effekten) haben gemeinsam, dass sie aufgrund der üblicherweise bezweckten Eigenschaft als Zahlungsmittel von Stablecoins nahezu immer dem Geldwäschereigesetz unterstellt sind. Bei der Ausgabe von Stablecoins durch beaufsichtigte Institute auf einem Transaktionssystem mit offenem Zugang wie etwa Ethereum, sind insbesondere die erhöhten Geldwäscherei- und Reputationsrisiken zu berücksichtigen. Wegen der Offenheit des Systems hat das herausgebende Institut nach der Ausgabe des Stablecoins nur noch bei der allfälligen Einlösung gegen den unterliegenden Wert eine Kontrollmöglichkeit. Die geldwäschereirechtlichen Sorgfaltspflichten können so nur gegenüber der ersten und der letzten Person, die über den Stablecoin verfügt, wahrgenommen werden. Personen, die dazwischen den Stablecoin auf der offenen Plattform kaufen oder verkaufen, liegen ausserhalb der Kontrolle des herausgebenden Instituts. Wie die FINMA feststellte, würde es sich bei den Stablecoins in diesem Fall um aus Sicht der Geldwäschereibekämpfung problematische Inhaberinstrumente handeln und weiter kann dies zu Reputationsschäden für das betroffene Institut und für den gesamten Schweizer Finanzmarkt führen.

Um diese Risiken zu adressieren, drängen sich bei der Ausgabe von Stablecoins durch beaufsichtigte Institute vertragliche und, soweit angebracht, technologische Übertragungsbeschränkungen auf. Entsprechend müssen sämtliche über die Stablecoins verfügenden Personen vom herausgebenden Institut oder von angemessen beaufsichtigten Vertriebspartnerinnen und Vertriebspartnern hinreichend identifiziert werden, um die Sorgfaltspflichten des Geldwäschereigesetzes bei sämtlichen Transaktionen mit Stablecoins einzuhalten. Dies entspricht einer technologieneutralen Anwendung des Verbots von Inhabersparheften (Art. 5 VSB 20).[57]

Bei DeFi-Applikationen wendet die FINMA die bestehenden Finanzmarktregeln an und abstrahiert dabei von der Verwendung bestimmter Technologien oder Verfahren. Bietet eine DeFi-Applikation dieselbe Dienstleistung und birgt sie dieselben Risiken wie Intermediäre im traditionellen Finanzmarkt, wendet die FINMA auch dieselben Regeln an. Übt eine DeFi-Applikation wirtschaftlich betrachtet eine finanzmarktrechtliche Tätigkeit aus, die bewilligungspflichtig wäre, geht die FINMA auch bei neuartiger technischer oder rechtlicher Umsetzung von einer Bewilligungspflicht aus. Entsprechend sind auch die Vorgaben zur Bekämpfung der Geldwäscherei einzuhalten.[58] Die FINMA beobachtet den Trend hin zur vermehrten Entwicklung und Nutzung von DeFi-Applikationen eng. Dies gilt besonders, wenn FINMA-Beaufsichtigte DeFi-Applikationen nutzen oder nutzen wollen. Sie wendet bei entsprechenden Fragen die bewährten Grundsätze «*substance over form*» und «*same risks,*

[56] Eidgenössische Finanzmarktaufsicht (FINMA), *Ergänzung der Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs)*, September 2019.
[57] Schweizerische Bankiervereinigung (SBVg), *Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken*, 2020.
[58] Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2021*, März 2022, S. 20.

same rules» an und entscheidet stets aufgrund der tatsächlichen wirtschaftlichen Begebenheiten.[59]

4.6.6 DLT-Gesetz

Am 25. September 2020 hat das Parlament das Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register verabschiedet.[60] Damit wurden zehn bestehende Bundesgesetze, unter anderem das Geldwäschereigesetz (GwG) angepasst. Eine wichtige Änderung betrifft die Ausweitung des Geltungsbereichs des Geldwäschereigesetzes. So fallen auf der Stufe des Geldwäschereigesetzes unter Art. 2 Abs. 2 Bst. d^{quater} DLT-Handelssysteme als Finanzintermediäre (Handelssysteme für DLT-Effekten nach Art. 73a des FinfraG[61]) in den Geltungsbereich des GwG. Hierbei wird zusätzlich in der Finanzinfrastrukturverordnung (FinfraV[62]) festgelegt, dass ein DLT-Handelssystem DLT-Effekten und weitere Vermögenswerte nicht zulassen kann, welche die Umsetzung der Anforderungen des GwG erheblich erschweren (beispielsweise Privacy Coins, vgl. Glossar) oder die Stabilität und die Integrität des Finanzsystems beeinträchtigen könnten.

Ebenfalls definiert die Geldwäschereiverordnung (GwV), dass eine Dienstleistung für den Zahlungsverkehr vorliegt, wenn der Finanzintermediär «hilft, virtuelle Währungen an eine Drittperson zu übertragen, sofern er mit der Vertragspartei eine dauernde Geschäftsbeziehung unterhält oder sofern er für die Vertragspartei Verfügungsmacht über virtuelle Währungen ausübt, und er die Dienstleistung nicht ausschliesslich gegenüber angemessen beaufsichtigten Finanzintermediären erbringt».[63] Damit wurden neu auch Wallet-Anbieter und dezentrale Handelsplattformen als Finanzintermediäre dem Geldwäschereigesetz unterstellt, sofern die Anbieter – analog zur Auslegung der FATF – bei solchen Plattformen oder Wallets bestimmte Kontroll- oder Eingriffsmöglichkeiten besitzen.

Dies betrifft beispielsweise Handelsplattformen, die nicht im Besitz des privaten Schlüssels der Kunden sind, die Übertragung der virtuellen Währungen jedoch mittels *Smart Contract* ermöglichen und dabei die Aufträge bestätigen, freigeben oder sperren können oder anderweitig Kontrolle über den *Smart Contract* haben. Ebenfalls fallen zum Beispiel solche Wallet-Anbieter darunter, die über einen Schlüssel verfügen, zu welchem sie Zugang haben und mit dem eine Signierung der Transaktion notwendig ist, bevor diese erfolgreich durchgeführt werden kann (*Multisig Wallet*). Auch erfasst werden können Dienstleistungen zur sicheren Aufbewahrung privater Schlüssel, auch wenn Letztere verschlüsselt sind und grundsätzlich von der Kundin oder dem Kunden entschlüsselt werden müssen. Die Risiken bei derartigen Wallets, welche weder reine *custodial* noch reine *non-custodial* Wallets seien, bestünden darin, dass der Ursprung der virtuellen Währungen durch die Verschiebung zwischen derartigen Wallets und innerhalb von Adressstrukturen verschleiert werden kann. Gerechtfertigt wurden diese Änderungen dadurch, dass der Finanzintermediär bei diesen immer dezentraleren Modellen der Vermögensübertragung nicht mehr in allen

[59] Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2022*, März 2023, S. 21.
[60] BBl 2020 7801, *Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register*, Oktober 2020.
[61] SR 958.1 – *Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel* (Finanzmarktinfrastrukturgesetz, FinfraG).
[62] SR 958.11 – *Verordnung über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel* (Finanzmarktinfrastrukturverordnung, FinfraV).
[63] Geldwäschereiverordnung, GwV, Art. 4 Abs. 1 und 1bis, Fassung vom 01.08.2021. Zitat: Eidgenössisches Finanzdepartement (EFD): *Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens*, Oktober 2020, S. 15.

Geschäftsmodellen die alleinige Verfügungsmacht über Vermögenswerte hat.[64] Anbieter von reinen *non-custodial* Wallets, welche bloss einmalig eine Software zur Verfügung stellen, sollten weiterhin nicht dem Geldwäschereigesetz unterstellt werden. Beim Begriff einmalig geht es beispielsweise um Entwickler, die bloss eine Software zum Download anbieten, ohne mit dem Nutzer irgendeine Geschäftsbeziehung einzugehen. Weiterhin nicht unterstellt sind Handelsplattformen, die lediglich Käufer und Verkäufer zusammenführen und die Abwicklung der Transaktion ohne *Smart Contract* mit Zugriffsmöglichkeit der Handelsplattform erfolgt. Dabei handle es sich um eine reine Vermittlungstätigkeit ohne Eingriff in die Übertragung der virtuellen Währungen.

In der GwV wurde zudem ergänzt, dass die berufsmässige Ausgabe eines Zahlungsmittels eine finanzintermediäre Tätigkeit sei und hierbei auch virtuelle Währungen, die tatsächlich oder nach Absicht des Organisators oder Herausgebers als digitale Zahlungsmittel eingesetzt werden, unter das Geldwäschereigesetz fallen.[65] Diese Formulierung schuf zudem auch mehr Klarheit im Zusammenhang mit der GwG-Unterstellung bei der Emission von VAs im Rahmen von Initial Coin Offerings (ICOs). Mit der Ausdehnung des Begriffs des Finanzintermediärs setzte die Schweiz um, was die FATF in ihrer «Updated guidance on a risk-based approach to virtual assets and virtual asset service providers» den einzelnen Ländern empfiehlt nämlich den VASP-Begriff möglichst breit zu interpretieren.[66]

4.6.7 Geldwäschereiaufsicht durch die FINMA und Änderungen der Geldwäschereiverordnung-FINMA

Ende August 2019 erteilte die FINMA zum ersten Mal zwei Blockchain-Finanzdienstleistern je eine Bewilligung als Bank und als Effektenhändler. Wie bei anderen Finanzintermediären üblich wurde die Aufnahme der Geschäftstätigkeit mit verschiedenen Bedingungen und Auflagen verknüpft, die einen geordneten Geschäftsaufbau sicherstellen sollen. Bereits während des Bewilligungsverfahrens schenkte die FINMA unter anderem den kryptospezifischen Risiken besondere Aufmerksamkeit. Im Zusammenhang mit den operationellen Risiken mussten strenge Kriterien und Kontrollprozesse definiert werden. Im Hinblick auf die sichere Verwahrung von Token wurde, auch mit Unterstützung der zuständigen Bewilligungsprüfer, die Technologieinfrastruktur der beiden Antragsteller gründlich getestet, um die erhöhten Risiken bei Informationstechnologien (IT) und Cyberrisiken hinreichend zu adressieren. Auch im Rahmen der geltenden regulären Überwachungsgrundsätze in Bezug auf die Geldwäschereibekämpfung müssen die gängigen KYC-Vorschriften eingehalten und die vorgeschriebenen Abklärungen der Transaktionen durchgeführt werden.

In den letzten Jahren boten die von der FINMA beaufsichtigten Institute vermehrt Dienstleistungen im Kryptobereich an oder planten entsprechende Angebote. Aufgrund dieser Feststellung hat die FINMA im Jahr 2021 bei Banken verschiedene geplante Geschäftsaktivitäten in diesem Bereich analysiert und auf die geldwäschereirechtlichen Vorgaben hin überprüft.[67] Zudem hat die FINMA ihre Erwartungen an die Prüfgesellschaften für die Prüfung von Instituten, die im Kryptobereich tätig sind, präzisiert. Die fünf existierenden Module,[68] die risikoorientiert für die Prüfung nach Geldwäschereigesetz eingesetzt werden,

[64] Ibid., S. 7.
[65] Geldwäschereiverordnung, GwV, Art. 2 Abs. 3 Bst. b GwG i. V. m. Art. 4 Abs, 1 Bst. c GwV i.V.m. Art. 4 Abs. 1bis Bst. c GwV, Fassung vom 01.08.2021.
[66] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Oktober 2021, S. 24 – 36, insb. Para. 91, S. 35.
[67] Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2021*, März 2022, S. 32.
[68] Booking Centers, Regeln zur Identifikation, komplexe Strukturen, vertiefte Behandlung von politisch exponierten Personen und Trade Finance.

wurde im Sommer 2021 mit einem sechsten Modul zu den Virtual Assets (VA) und Virtual Asset Service Providers (VASP) ergänzt.[69]

Per 1. Januar 2021 wurde zudem der Schwellenwert für die Identifizierung der Vertragspartei bei einer Wechseltransaktion und somit bei einer nicht-dauerhaften Geschäftsbeziehung in Erfüllung der Anforderungen der Empfehlung 15 der FATF von CHF 5 000 auf CHF 1 000 gesenkt (Art. 51*a* GwV-FINMA).[70] Der angepasste Schwellenwert entspricht den Anforderungen der FATF-Empfehlungen und berücksichtigt die erhöhten Risiken in diesem Bereich.[71] Diese Schwelle gilt nicht nur für einzelne Transaktionen, sondern auch für Transaktionen, die als miteinander verbunden aufzufassen sind. Der Hauptanwendungsfall für die Grenze von CHF 1000 ist der Geldwechsel an Automaten für VAs. Diese Regelung wurde von den Selbstregulierungsorganisationen (SRO) übernommen, denen Finanzintermediäre mit VASP-Tätigkeit angeschlossen sind. Die teilrevidierte Geldwäschereiverordnung der FINMA, welche per 1.1.2023 in Kraft trat, präzisierte zudem, dass der Schwellenwert von CHF 1000 für Barzahlungen oder die Entgegennahme von anderen anonymen Zahlungsmitteln (wie beispielsweise Kryptowährungen oder bestimmte Prepaid Karten) für den Verkauf oder Kauf von virtuellen Währungen gilt (Art. 51*a* Abs. 1bis GwV-FINMA).[72] Finanzintermediäre müssen zudem technische Vorkehrungen treffen, um zu verhindern, dass die Schwelle von CHF 1000 mittels miteinander verbundener Transaktionen innerhalb von 30 Tagen überschritten wird.

4.7 VAs und VASPs in der Schweiz

Ein wichtiger methodologischer Aspekt bei Durchführung dieser Risikoanalyse ist die Verschaffung einer Übersicht, in welcher Weise und Intensität VAs in der Schweiz verwendet werden. Zentral hierfür sind Informationen zu den spezifischen Dienstleistungen im VA-Bereich, die in der Schweiz angeboten und dort sowie weltweit genutzt werden. Ebenfalls erforderlich sind Angaben zur Intensität der Interaktion des schweizerischen VA-Sektors mit dem traditionellen Wirtschafts- und Finanzbereich in der Schweiz.[73]

Seit der letzten sektoriellen Risikoanalyse zur vorliegenden Thematik im Jahr 2018 hat einerseits die allgemeine Verwendung von VAs in der Schweiz deutlich zugenommen, andererseits ist der schweizerische VA-Sektor stark gewachsen. Präzise Angaben zur konkreten Ausgestaltung des schweizerischen VA-Sektors fehlen aber weitgehend. Trotzdem gibt es konkrete Hinweise, dass die Schweiz zur Gruppe der Länder gehört, die in diesem Bereich führend sind.

Traditionell spielt der Finanzplatz Schweiz weltweit eine wichtige Rolle als Knotenpunkt für internationale Finanzgeschäfte, insbesondere in den Bereichen der grenzüberschreitenden Vermögensverwaltung, des weltweiten Rückversicherungsgeschäfts, als Rohstoffhandels- und Rohstoffhandelsfinanzierungsplatz sowie als Standort der drittgrössten Börse Europas.[74] Auch im VA-Bereich zählt die Schweiz zu den führenden Standorten.[75] Namentlich im

[69] Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2021*, März 2022, S. 32.
[70] SR 955.033.0 – *Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor* (Geldwäschereiverordnung-FINMA, GwV-FINMA), Art. 51*a*, Fassung vom 01.01.2021.
[71] Es gab zudem konkrete Fälle, in welchen Automaten für VAs (VA-ATMs) in der Schweiz von bestimmten kriminellen Netzwerken im Drogenhandel für die Abwicklung des Zahlungsverkehrs missbraucht wurden. Vgl. z.B. Tages Anzeiger, *Schweizer Online-Drogenversand – «Hippe Kleider, Typ Studentin, und das Täschli voller Drogen»*, 18. März 2021.
[72] Geldwäschereiverordnung-FINMA, GwV-FINMA, Art. 51*a* Abs. 1bis, Fassung vom 01.01.2023.
[73] World Bank, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, Juni 2022, S. 14f.
[74] Bundesrat, *Weltweit führend, verankert in der Schweiz: Politik für einen zukunftsfähigen Finanzplatz Schweiz*, Dezember 2020, S. 5.
[75] Staatssekretariat für internationale Finanzfragen (SIF), *Faktenblatt Krypto*, Januar 2022.

Finanzbereich hat sich ein wachsendes VA-Ökosystem in der Schweiz entwickelt, zu dem gemäss Zahlen des Staatssekretariats für Internationale Finanzfragen bereits über 1000 Firmen zählen.[76]

Die überwiegende Mehrheit dieser im VA-Sektor tätigen Firmen sind allerdings keine Finanzintermediäre gemäss Geldwäschereigesetz. Vielmehr bieten sie Software, Rechts- oder Technologieberatungen oder ähnlich gelagerte Dienstleistungen an, die wiederum von anderen Firmen (darunter auch Finanzintermediäre) im VA-Ökosystem nachgefragt werden (vgl. Abbildung 4 in Kapitel 4.2). Ebenfalls existieren mehrere Branchenverbände, die auf den Ausbau und die Weiterentwicklung der schweizerischen VA-Branche abzielen. Zusätzlich haben viele der weltweit wichtigsten VAs (gemäss ihrer Marktkapitalisierung) in der Schweiz eine Stiftung gegründet.[77] Die meisten dieser Stiftungen befinden sich im Kanton Zug. Im Jahr 2022 wies der Kanton Zug ein Nettowachstum von 25 Stiftungen auf, wobei 20 der Neugründungen auf Krypto-Stiftungen entfielen.[78] Durch die zahlreichen Gründungen von Krypto-Stiftungen weist der Kanton Zug schweizweit die zweithöchste Dichte an Stiftungen pro Kantonsbewohner auf (nach dem Kanton Basel-Stadt).[79] Krypto-Stiftungen – oft stark kapitalisiert durch die Kursgewinne der von ihnen gehaltenen VAs – finanzieren natürliche und juristische Personen sowie Projekte, die an der Weiterentwicklung der zugrundeliegenden Blockchain arbeiten. Im Rahmen des vorliegenden Berichts konnte die Eidgenössische Stiftungsaufsicht (ESA) keine konkreten Angaben zur tatsächlichen Anzahl Krypto-Stiftungen und deren Bilanzen liefern.

4.7.1 Angaben zu Finanzintermediären mit VASP-Tätigkeit in der Schweiz

Im Fokus dieser Risikoanalyse stehen die Finanzintermediäre gemäss Geldwäschereigesetz. Je nach Tätigkeit werden sie als unterstellte Institute direkt von der Eidgenössischen Finanzmarktaufsicht FINMA beaufsichtigt (zum Beispiel Banken), oder sie müssen sich einer von der FINMA anerkannten und beaufsichtigten Selbstregulierungsorganisation (SRO) anschliessen (vgl. Kapitel 4.4.1).

	2018	2020	2022
Anzahl Finanzintermediäre mit VASP-Tätigkeit (FINMA-unterstellte Institute und SRO-Mitglieder)[80]	Mindestens 5[81]	Mindestens 89	Mindestens 204

Abbildung 10: Zunahme von Finanzintermediären mit VASP-Tätigkeit in der Schweiz 2018 - 2022

[76] Staatssekretariat für internationale Finanzfragen (SIF), *Blockchain/DLT*, zuletzt abgerufen im Mai 2023. Staatssekretariat für internationale Finanzfragen (SIF), *Finanzstandort Schweiz, Kennzahlen 2023*, April 2023, S. 13.
[77] Zum Beispiel: Ethereum Foundation, Cardano Foundation, Tezos Foundation, Solana Foundation, Polkadot Foundation, etc.
[78] Center for Philanthropy Studies (CEPS), Universität Basel SwissFoundations, Verband der Schweizer Förderstiftungen Zentrum für Stiftungsrecht, Universität Zürich, *Der Schweizer Stiftungsreport 2023*, Juni 2023.
[79] 30,7 Stiftungen pro 10'000 Einwohner, vgl. Center for Philanthropy Studies (CEPS), Universität Basel SwissFoundations, Verband der Schweizer Förderstiftungen Zentrum für Stiftungsrecht, Universität Zürich, *Der Schweizer Stiftungsreport 2022*, Mai 2022, S. 8.
[80] Die Angaben beruhen auf Informationen der Eidgenössischen Finanzmarktaufsicht FINMA und wurden anhand von Informationen, die der MROS vorliegen, ergänzt.
[81] Im Rahmen der vorliegenden Risikoanalyse wurden Informationen eingeholt, die zeigen, dass im Jahr 2018 bereits mindestens fünf Finanzintermediäre mit VASP-Tätigkeit in der Schweiz existierten. Im zweiten nationalen Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung von 2021 wurde die Anzahl Finanzintermediäre mit VASP-Tätigkeit für das Jahr 2018 mit lediglich zwei beziffert, vgl. KGGT, *Zweiter nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung*, Oktober 2021, S. 51.

Laut Angaben der FINMA existierten per Ende 2022 mindestens 204 Finanzintermediäre mit VASP-Tätigkeit. Davon waren 174 Finanzintermediäre einer SRO angeschlossen sowie 30 Institute der FINMA unterstellt.[82]

Die FINMA beobachtete, dass sich generell die meisten Banken vermehrt mit dem Thema Digitalisierung beschäftigen. Im Zusammenhang mit der Anpassung oder Erweiterung der Geschäftsmodelle ist eine gewisse Dynamik im Geschäft mit VAs, bei der Öffnung von Schnittstellen (*Open Banking*) und in Form einer vermehrten Zusammenarbeit mit Versicherungsgesellschaften erkennbar. Dennoch ist insgesamt noch Zurückhaltung betreffend die strategische Anpassung von Geschäftsmodellen festzustellen. Die von der FINMA beaufsichtigten Institute bieten vermehrt Dienstleistungen im Zusammenhang mit virtuellen Vermögenswerten an oder planen entsprechende Angebote in ihren Dienstleistungskatalog aufzunehmen. Von den Banken und Wertpapierhäusern, die gegenwärtig in der Schweiz Tätigkeiten im Zusammenhang mit VAs ausüben, wird primär die Verwahrung von Token für Kunden und der Kunden- und Eigenhandel betrieben, gefolgt von der Ausgabe von Produkten sowie gesicherten Darlehen.

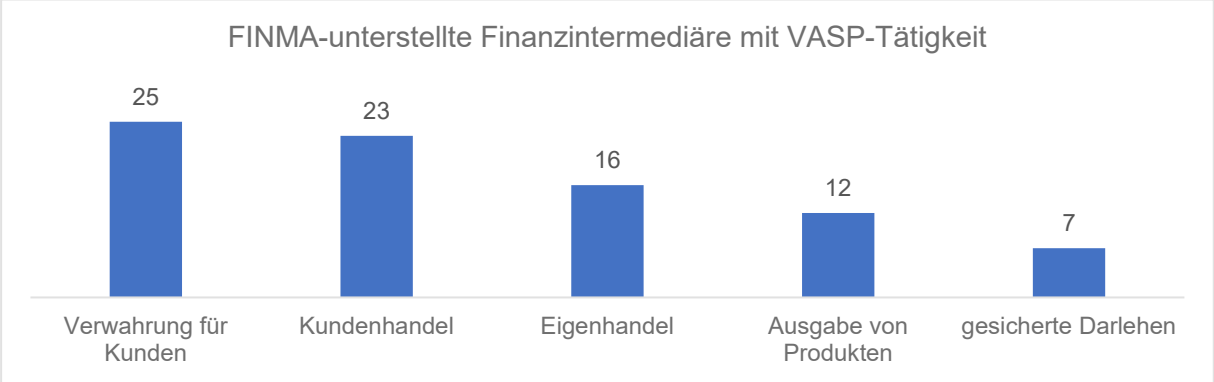


Abbildung 11: Angebotene VASP-Dienstleistungen von 30 FINMA-unterstellten Banken und Wertpapierhäusern mit Kryptoaktivitäten (Stand Ende 2022)[83]

Die überwiegende Mehrheit der Schweizer Finanzintermediäre mit VASP-Tätigkeit ist einer SRO angeschlossen. Gemäss Auskunft der Eidgenössischen Finanzmarktaufsicht FINMA sind Wechselgeschäfte (Fiat-VA sowie VA-VA) sowie Transaktionen von VAs die wichtigsten und meistausgeübten Dienstleistungen dieser Finanzintermediäre.

Die bisher umfassendsten Daten zu den Geschäftstätigkeiten von schweizerischen Finanzintermediären mit VASP-Tätigkeit sind in einer von diversen privaten Akteuren sowie einer Hochschule veröffentlichten Studie «Swiss Digital Asset Market Report 2022» enthalten. Für diese Studie wurden insgesamt 81 Unternehmen mit Sitz in der Schweiz angefragt, von denen 47 an der Erhebung teilnahmen.[84] Für das Jahr 2021 belief sich das Handelsvolumen derjenigen 17 teilnehmenden Unternehmen, welche VA-Handelsgeschäfte anbieten, auf 41.2 Milliarden Schweizerfranken.[85] 16 befragte Unternehmen boten ihren Kunden die Verwahrung von VAs an. Davon stellten 11 Unternehmen ihre Zahlen zur Verfügung, aus denen hervorgeht, dass diese per Ende 2021 VAs im Wert von über 13.2 Milliarden Schweizerfranken für ihre Kunden verwahrten.[86] Da nur ein Bruchteil der Finanzintermediäre mit VASP-Tätigkeit in der Schweiz an der Studie teilnahm, kann davon ausgegangen werden, dass das tatsächliche Handelsvolumen sowie die verwahrten VAs sämtlicher Finanzintermediäre mit

[82] Gemäss Angaben der FINMA übten per Ende September 2023 bereits 38 FINMA-unterstellte Institute eine VASP-Tätigkeit aus.
[83] Vgl. Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2022*, März 2023, S. 23.
[84] Home of Blockchain, *Swiss Digital Asset Market Report 2022*, Mai 2022, S. 16.
[85] Ibid., S. 25.
[86] Ibid., S. 20.

VASP-Tätigkeit in der Schweiz höher liegt. Indessen bleibt unklar, inwiefern die Angaben dieser einzelnen Finanzintermediäre mit VASP-Tätigkeit repräsentativ für die Geschäftstätigkeiten von Finanzintermediären mit VASP-Tätigkeit in der Schweiz sind.

4.7.2 Angaben zur Verwendung von VAs in der Schweiz

Weitere Studien versuchten, grenzüberschreitende VA-Finanzflüsse in oder aus der Schweiz mittels unterschiedlichen Berechnungsmethoden zu beziffern. Das Blockchainanalyse-Unternehmen Chainalysis platzierte die Schweiz für das Jahr 2021 auf dem «DeFi Adoption Index» auf Platz 14 von 154.[87] Auf der europäischen Liste des «Global Crypto Adoption Index» lag die Schweiz für das Jahr 2021 auf Platz 6 sowie für 2022 auf Platz 7 von 30.[88] Gemäss den Verfassern der Studie wurden zwischen Juli 2020 und Juni 2021 VAs im Wert von über 60 Milliarden Dollar aus der Schweiz an DeFi- und CeFi-Plattformen transferiert.[89]
Diese Angaben bewegen sich ungefähr in derselben Grössenordnung wie die Ergebnisse einer jährlich durchgeführten Studie der Hochschule Luzern, die jeweils weltweit das Handelsvolumen für die von der Schweiz aus getätigten Handelsgeschäften auf VA-Plattformen schätzte:[90]

	2020	2021	2022
Zentralisierte VA-Börsen (CHF)	92.6 Mia.	81.2 Mia	50.3 Mia.
Dezentralisierte VA-Börsen (CHF)	4 Mia.	5.1 Mia.	1.5 Mia.
Total (CHF)	**96.6 Mia.**	**86.3 Mia.**	**51.8 Mia.**

Abbildung 12: Geschätztes Volumen für von der Schweiz aus getätigten Handelsgeschäften auf weltweiten VA-Plattformen (CeFi und DeFi) 2020 – 2022

Der berechnete Anteil der Schweiz am weltweiten VA-Handelsvolumen lag in diesen Jahren allerdings immer unter 1%. Auch verglichen mit Finanzflüssen in anderen Sektoren scheinen diese Zahlen immer noch überschaubar: So belief sich das jährliche Handelsvolumen an der Schweizer Börse SIX im Jahr 2022 auf CHF 1208 Milliarden.[91] Es wäre jedoch falsch, aufgrund der seit 2020 jährlich sinkenden und letztlich immer noch überschaubaren Zahlen auch von sinkenden und überschaubaren GW/TF-Risiken im VA-Bereich in der Schweiz auszugehen. In denselben Jahren ist nämlich die Anzahl Geldwäschereiverdachtsmeldungen in der Schweiz sowie die Summe der durch Diebstahl oder Betrügereien entwendeten VAs deutlich angestiegen (vgl. Kapitel 7.2).

[87] Chainalysis, *The 2021 Geography of Cryptocurrency Report*, Oktober 2021, S. 55.
[88] Ibid., S. 55. Chainalysis, *The 2022 Geography of Cryptocurrency Report*, September 2022, S. 29.
[89] Chainalysis, *The 2021 Geography of Cryptocurrency Report*, Oktober 2021, S. 55.
[90] Für 2020 (Erhebungszeitraum: 01.10.2020-01.09.2021), vgl. Institute of Financial Services Zug IFZ (Hochschule Luzern), *Crypto Assets Study 2021*, S. 17 – 20. Für 2021 (Erhebungszeitraum: 01.05.2021-30.04.2022), vgl. Institute of Financial Services Zug IFZ (Hochschule Luzern), *Crypto Assets Study 2022*, S. 12. Für 2022 (Erhebungszeitraum: 01.01.2022-31.12.2022), vgl. Institute of Financial Services Zug IFZ (Hochschule Luzern), *Fintech Study 2023*, S. 63.
[91] Cash, *Handelsvolumen an der SIX 2022 rückläufig*, 3. Januar 2023.

Aufgrund der Berechnungsmethoden in den genannten Studien liegen die tatsächlichen Zahlen vermutlich deutlich höher.[92] Zudem sind in diesen Berechnungen Fiat-Finanzflüsse, die im Zusammenhang mit VA-Handelsgeschäften stehen, nicht berücksichtigt. Hierzu liegen auch keine Schätzungen vor. Ebenfalls geht aus den Zahlen nicht hervor, welchen Akteuren (Privatpersonen, Unternehmen oder Finanzintermediäre mit VASP-Tätigkeit) diese Finanzflüsse zuzuordnen sind, beziehungsweise wie hoch ihre jeweiligen Anteile daran sind. Letztlich geben sämtliche der zuvor genannten Studien lediglich eine ungefähre Vorstellung der Grössenordnung des schweizerischen VA-Sektors und zeigen auf, dass die Verwendung von VAs in der Schweiz heute kein Nischendasein mehr hat.

Für einen Anstieg der Finanzflüsse im Zusammenhang mit der Verwendung von VAs sorgten vermutlich auch die zahlreichen in der Schweiz lancierten ICOs. Die mit ihnen zusammenhängenden Finanzflüsse können allerdings, abhängig vom jeweiligen Projekt, in VAs oder Fiatwährung erfolgen. Die Eidgenössische Finanzmarktaufsicht (FINMA) erhielt seit 2019 über 400 Unterstellungsanfragen im Zusammenhang der Lancierung von ICOs in der Schweiz. Die tatsächliche Anzahl der durchgeführten ICOs liegt vermutlich deutlich höher, da es sich dabei nicht um zwingende Meldungen, sondern um Anfragen bezüglich einer allfälligen Unterstellung unter das Finanzmarktrecht handelt (vgl. Kapitel. 4.4.3).

Aus verschiedenen in der Schweiz durchgeführte Umfragen ist zu entnehmen, dass die Verwendung von VAs in den letzten Jahren klar zugenommen hat. Eine im Jahr 2018 durchgeführte Umfrage zum Schweizer Anlageverhalten ergab, dass 8% der befragten Personen einmal VAs gekauft hatten. Im Jahr 2022 waren es bei derselben Umfrage bereits 18%.[93] Auch wenn einzelne solcher Erhebungen grundsätzlich mit Vorsicht zu geniessen sind, zeigen sie zusammengenommen die gesteigerte Nutzung von VAs in der Schweiz deutlich auf.[94] Die Ergebnisse geben allerdings keinen Aufschluss darüber, wie oft diese VA-Käufe über schweizerische oder ausländische Finanzintermediäre getätigt wurden. Eindeutig sind die Umfrageergebnisse allerdings in Bezug auf die Korrelation von bereits getätigten VA-Käufen und dem Alter der Befragten: Personen zwischen 18 und 49 Jahren gaben besonders häufig an, bereits VAs gekauft zu haben oder beabsichtigen, dies in naher Zukunft zu tun.[95] Dies ist ein starker Hinweis, dass sich der in den letzten Jahren beobachtete Trend hin zu einer vermehrten Verwendung von VAs fortsetzen wird.

Die älteste Kryptowährung Bitcoin lässt sich bereits seit dem Jahr 2016 an sämtlichen SBB-Ticketautomaten in der Schweiz kaufen.[96] Schon Ende 2017 wurde dieser Dienst von mindestens 6000 Personen benutzt, von der Hälfte sogar regelmässig.[97] Der Kauf und teilweise sogar der Verkauf von Monero, des wichtigsten und ältesten Privacy Coins (vgl. Glossar), ist an über 60 in der Schweiz stehenden VA-ATMs, die von unterschiedlichen schweizerischen Finanzintermediären mit VASP-Tätigkeit betrieben werden, möglich.[98] Mittlerweile können Steuerabgaben in gewissen Kantonen auch mit VAs bezahlt werden.[99] Im März 2022 kündigte die Stadt Lugano eine Partnerschaft mit dem Stablecoin-Anbieter Tether an, die darauf abzielt, die Nutzung der Blockchain-Technologie zu beschleunigen und diese als Grundlage für die Transformation der Finanzinfrastruktur der Stadt zu nutzen. Das Projekt

---

[92] Chainalysis sowie die Hochschule Luzern betonen, dass es sich bei den von ihnen berechneten Summen um Mindestangaben handelt, vgl. Institute of Financial Services Zug IFZ (Hochschule Luzern), *Crypto Assets Study 2021*, S. 17. Chainalysis, *The 2021 Geography of Cryptocurrency Report*, Oktober 2021, S. 5.

[93] Moneyland, *Wie legen Schweizer ihr Geld an?*, 22. April 2020. Moneyland, *So investieren Schweizerinnen und Schweizer ihr Geld*, 19. Juli 2022.

[94] Weitere ähnlich gestaltete Umfragen weichen um wenige Prozentpunkte nach oben oder unten ab, aber weisen dieselbe Tendenz auf, z.B.: Migros Bank, *Kryptowährungen bei jüngeren Generationen beliebter als Gold*, Februar 2020. Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, Juni 2021.

[95] Ibid.

[96] Handelszeitung, *6000 Kunden kaufen bei der SBB Bitcoins | Handelszeitung*, 1. November 2017. Schweizerische Bundesbahnen (SBB), *Mit Bitcoin bequem und einfach einkaufen | SBB*, zuletzt abgerufen im Mai 2023.

[97] Ibid.

[98] Coin ATM Radar, *Bitcoin ATM Map*, zuletzt abgerufen im Mai 2023.

[99] Finews, *Tessiner dürfen ihre Steuern jetzt in Bitcoin zahlen*, 7. Juli 2022. Kanton Zug, *Kanton Zug akzeptiert ab 2021 Kryptowährungen für Steuerzahlungen* (Medienmitteilung), 3. September 2020.

sieht vor, dass in der Stadt über 10'000 Geschäfte und Warenverkäufer Bitcoin als Zahlungsmittel akzeptieren, während städtische Dienstleistungen in Bitcoin, Tether und dem eigens kreierten VA LVGA bezahlt werden können.[100]

Wie die nicht abschliessende Liste dieser Beispiele aufzeigt, haben in den letzten Jahren die Möglichkeiten, in der Schweiz VAs zu erwerben, zu verkaufen oder sie als Zahlungsmittel für diverse Dienstleistungen einzusetzen, deutlich zugenommen. Weitere Beispiele illustrieren, dass diese Zunahme auch bei Branchen stattgefunden hat, die mit spezifischen Geldwäschereirisiken behaftet sind. So gibt es in zahlreichen Geschäften – darunter auch Geschäfte für Schmuck und weitere Luxusgüter, Antiquariate, Kunstgalerien und Hotellerie- und Gastronomiestätten – die Möglichkeit, mit VAs zu bezahlen.[101]

Ebenfalls können in der Schweiz Gesellschaften sowie Anteile davon mit VAs erworben werden.[102] Des Weiteren können Gesellschaften mit VAs als Sacheinlage (Gründungskapital) gegründet werden. Bis Anfang 2023 wurde in der Schweiz eine mittlere dreistellige Anzahl Gesellschaften auf diese Weise gegründet, die in den unterschiedlichsten Branchen tätig sind und nicht unbedingt mit VAs oder Finanzdienstleistungen in Verbindung stehen.

Auch Immobilien können in der Schweiz mit VAs erworben werden.[103] Sowohl das Eidgenössische Amt für Grundbuch- und Bodenrecht (EGBA) als auch verschiedene im Zuge dieser Analyse angefragte kantonale Grundbuchämter, Amtsnotariate und Notariatsinspektorate geben an, dass Immobilien in der Schweiz mit VAs gekauft werden.[104] Allerdings gibt es hierzu keine Daten und mit der heutigen rechtlichen Grundlage auch keine Möglichkeit, diese Daten zu erheben, da nur die einzelnen Notariate Einblick in die Vertragsregelungen bezüglich die Art und Weise der Bezahlung von Immobilienkäufen haben. Was die Verwendung von VAs in den 21 konzessionierten Schweizer Casinos sowie deren allfällige Online-Spielangebote betrifft, so kann die Eidgenössische Spielbankenkommission (ESBK) nach Art. 80 Abs. 3 der Geldspielverordnung bestimmte Zahlungsmittel wie VAs verbieten, wenn deren Verwendung mit den Zielen des Bundesgesetzes über Geldspiele unvereinbar ist.[105] Bisher zeigten zwei Spielbanken Interesse an der Verwendung von VAs. Gemäss der ESBK waren sie jedoch nicht in der Lage, ein Verfahren vorzuschlagen, mit welchem sie die Anforderungen der Geldwäschereigesetzgebung erfüllt hätten. Im Laufe des Jahres 2023 wird die ESBK prüfen, ob und unter welchen Bedingungen die Verwendung von VAs als Zahlungsmittel in den Schweizer Casinos mit den Zielen des Gesetzes vereinbar ist. Zum gegenwärtigen Zeitpunkt werden VAs in Spielbanken und Casinos jedoch nicht als Zahlungsmittel akzeptiert.

Da die Schweiz den grössten Goldhandelsplatz der Welt beherbergt, wurde zuletzt auch geprüft, ob die Verwendung von VAs bei Geschäftsabwicklungen rund um den Handel und die Verarbeitung von Gold in der Schweiz gängig ist.[106] Das im Rahmen des vorliegenden Berichts angefragte Eidgenössische Zentralamt für Edelmetallkontrolle (ZEMK) verfügt über keine konkreten Hinweise zur Verwendung von VAs durch die von ihm beaufsichtigten Handelsprüfer, Schmelzer und Ankäufer von Schmelzgut (Stand Mai 2023). Bislang sei nicht

[100] City of Lugano, Tether, *Lugano's Plan B*, zuletzt abgerufen im Mai 2023.
[101] Handelszeitung, *85'000 Händler in der Schweiz können nun Zahlungen mit Bitcoin und Ether annehmen*, 19. August 2021. Für eine geographische Übersicht, vgl. Coinmap, *Crypto ATMs & merchants of the world*, zuletzt abgerufen im Mai 2023.
[102] Vgl. z.B. Aktionariat, *Create a market for your shares*, zuletzt abgerufen im Mai 2023.
[103] Vgl. z.B. Bithome, *Buy and Sell Real Estate with Bitcoin or Cryptos*, zuletzt abgerufen im Mai 2023.
[104] Nebst dem EGBA wurden das Grundbuch- und Vermessungsamt des Kantons Basel-Stadt, das Grundbuchtamt des Kantons Genf, das Amt für Grundbuch und Geoinformation des Kantons Zug, das Notariat der Stadt Zug sowie das Notariatsinspektorat des Kantons Zürich angefragt.
[105] Vgl. SR 935.511 – *Verordnung über Geldspiele* (Geldspielverordnung, VGS), Fassung vom 01.01.2021.
[106] Die Schweiz nimmt im Edelmetallhandel weltweit eine zentrale Rolle ein, vorrangig mit einem Anteil von bis zu zwei Drittel am weltweiten Goldhandel. Beim Schmelzen macht der Anteil der Schweiz rund 40 Prozent der weltweiten Kapazität aus. Von den globalen Branchenführern konzentriert ein Grossteil die Aktivitäten in der Schweiz. Vgl. KGGT, *Erster nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung*, Juni 2015, S. 99.

bekannt, ob einzelne Transaktionen in der internationalen Lieferkette von Edelmetallen in Rohform, die an die grossen Raffinerien (Handelsprüfer) eingehen, mit VAs erfolgen. Es könne nicht ausgeschlossen werden, dass einzelne der rund 800-1'000 in der Schweiz aktiven Ankäufer von Schmelzgut VAs bei der Abwicklung ihrer Geschäfte verwenden.

5. Akteure, Methodologie und verwendete Daten

In diesem Kapitel wird die Methodologie der vorliegende Risikoanalyse zum VA-Bereich erläutert sowie eine Einordnung der teilnehmenden Akteure und der dafür verwendeten Daten und Informationen vorgenommen.

5.1 Methodologie

Risikoanalysen sind iterative Prozesse, die auf einer kontinuierlichen Überprüfung der Risikolandschaft basieren. Durch die wiederholte Durchführung von Risikoanalysen und dem Abgleich mit früheren Ergebnissen und Einschätzungen können neue Erkenntnisse gewonnen und genauere Bewertungen vorgenommen werden, die wiederum in die nächste Analyse einfliessen können. Durch diese Iteration kann die Genauigkeit und Relevanz der Ergebnisse erhöht werden.

Die im vorliegenden Bericht verwendete Methode zur Analyse von GW/TF-Risiken steht im Einklang mit den internationalen Empfehlungen zur Durchführung nationaler Risikoanalysen.[107] Die Beurteilung des Risikos erfolgt über die Identifizierung von Gefährdungen und Verwundbarkeiten sowie risikomindernder Faktoren.

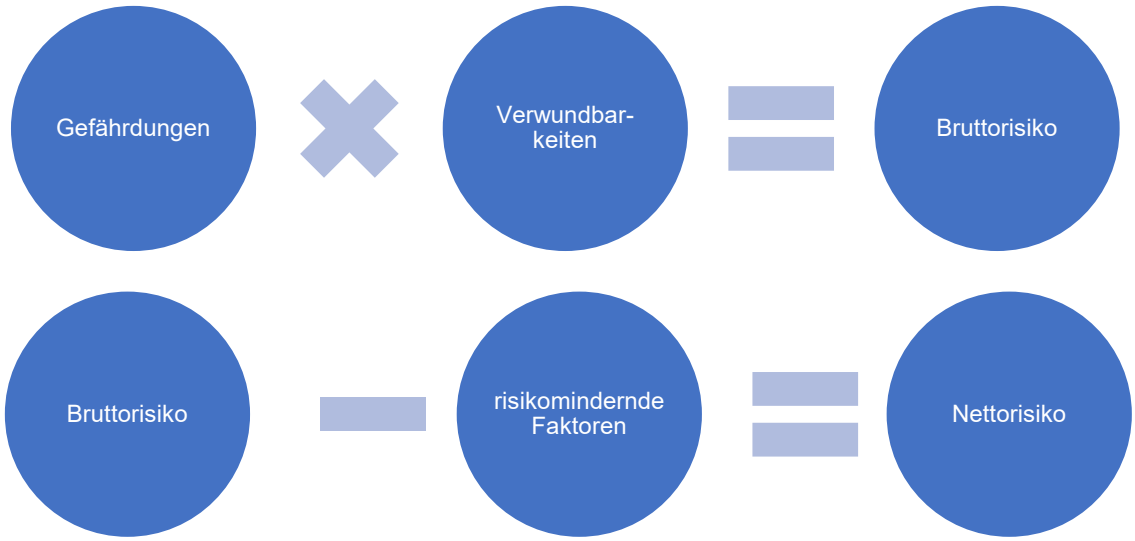


Abbildung 13: Schematische Darstellung der Methodologie zur Bewertung von GW/TF-Risiken

Gefährdungen bezeichnen spezifische Risiken und Bedrohungen, die mit Geldwäscherei- und Terrorismusfinanzierungsaktivitäten verbunden sind. Diese Risiken können sowohl durch konkrete Produkte oder Dienstleistungen entstehen als auch auf Vortaten zur Geldwäscherei zurückzuführen sein. Ein Beispiel für eine Gefährdung, die sich aus konkreten Produkten oder Dienstleistungen ergibt, ist die Ermöglichung von anonymen Zahlungsabwicklungen. Dies kann es Kriminellen erleichtern, Gelder aus illegalen Aktivitäten zu waschen. Ein Beispiel für eine Gefährdung, die auf Vortaten zur Geldwäscherei zurückzuführen ist, ist der illegale

[107] Vgl. FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Oktober 2021. World Bank, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, Juni 2022.

Waffenhandel. Wenn eine kriminelle Organisation illegal Waffen verkauft, bestehen erhöhte Geldwäscherei- und Terrorismusfinanzierungsrisiken, da die kriminelle Organisation durch den Verkauf dieser Waffen illegal erlangte Erlöse waschen oder diese zur Finanzierung von Terroranschlägen einsetzen kann.

Verwundbarkeiten hingegen beziehen sich auf Schwachstellen in einer Organisation oder einem System, die von Kriminellen ausgenutzt werden können, um Geldwäscherei- oder Terrorismusfinanzierungsaktivitäten durchzuführen. Eine solche Verwundbarkeit könnte beispielsweise die unzureichende Gesetzeslage zur Aufsicht über Finanzintermediäre sein, oder unzureichend geregelte, interne Geschäftsprozesse von Finanzintermediären (zum Beispiel zur Identifizierung ihrer Kunden und deren Aktivitäten).

Insgesamt können Gefährdungen und Verwundbarkeiten beide dazu beitragen, das Risiko von Geldwäscherei und Terrorismusfinanzierung zu erhöhen.

Risikomindernde Faktoren sind jene Faktoren, die das Risiko von Geldwäscherei und Terrorismusfinanzierung minimieren, wie zum Beispiel die Ausarbeitung von internen Kontrollprozessen bei Finanzintermediären zur genauen Prüfung ihrer Kunden und deren Aktivitäten.

Brutto- und Nettorisiko: Das Bruttorisiko bezieht sich auf das Risiko, das ohne Berücksichtigung der Effektivität der risikomindernden Faktoren besteht. Das Nettorisiko hingegen bezieht sich auf das verbleibende Risiko, nachdem Risikominderungsmassnahmen ergriffen wurden. Das Ziel besteht darin, das Nettorisiko auf ein akzeptables Niveau zu reduzieren. Sofern das verbleibende Risiko als inakzeptabel eingeschätzt wird, sollen im Rahmen einer Risikoanalyse Empfehlungen abgegeben werden, wie weitere risikomindernde Faktoren gestaltet und umgesetzt werden könnten, um das Nettorisiko zu minimieren.

Gefährdungen und Verwundbarkeiten in Verbindung mit VAs wurden in der sektoriellen Risikoanalyse von 2018 sowie im Rahmen der nationalen Risikoanalyse von 2021 bereits weitgehend identifiziert.[108] Unter Rücksichtnahme der massgeblichen Veränderungen im VA-Sektor seit 2018 wird im vorliegenden Bericht geprüft, ob die damalige Beurteilung noch Gültigkeit hat und ob neue Gefährdungen und Verwundbarkeiten identifiziert werden können. Analog zur Vorgehensweise im sektoriellen Bericht von 2018 werden die Veränderungen in den Gefährdungen und Verwundbarkeiten sowie die identifizierten risikomindernden Faktoren am Ende des Berichts bilanziert (vgl. Kapitel 8).

[108] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018. KGGT, *Zweiter nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung*, Oktober 2021, S. 51 – 53.

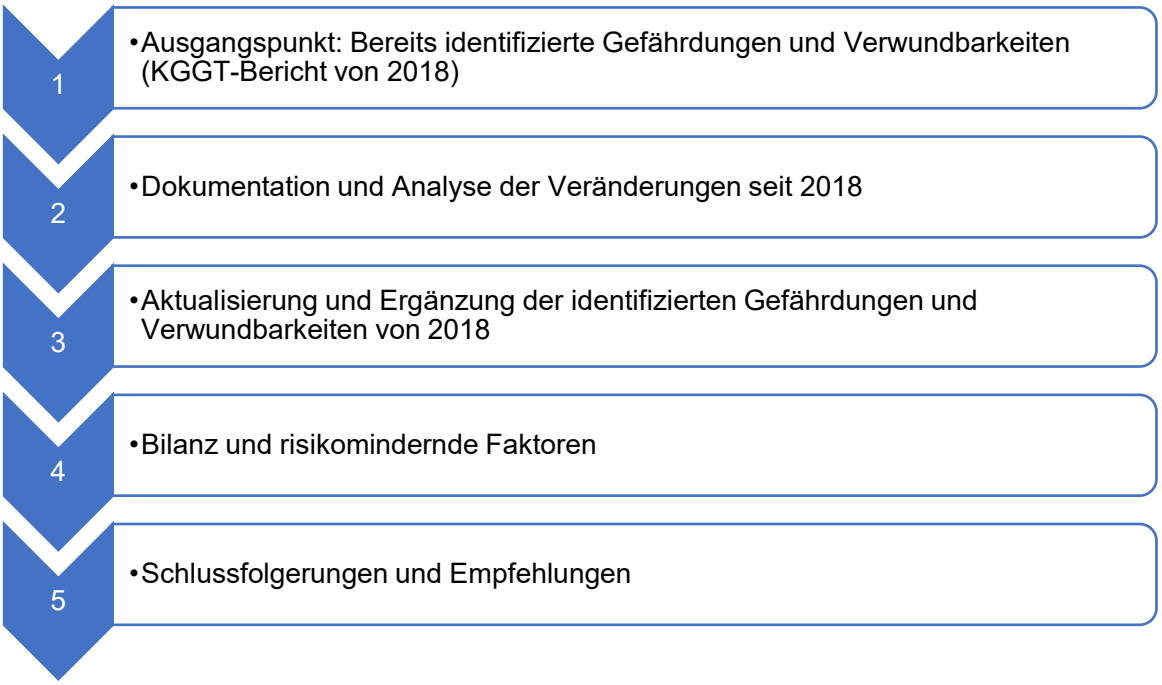


Abbildung 14: Vereinfachte Darstellung der Arbeitsschritte zur Erstellung vorliegenden GW/TF-Risikoanalyse

5.2 Akteure und verwendete Daten

Die Meldestelle für Geldwäscherei (MROS) war bei der Erstellung dieser Risikoanalyse federführend. Die MROS ist die schweizerische Financial Intelligence Unit (FIU). Sie nimmt Verdachtsmeldungen von Finanzintermediären in Bezug auf Geldwäscherei und Terrorismusfinanzierung entgegen und analysiert diese. Sie entscheidet, ob die daraus gewonnenen Informationen an eine schweizerische Strafverfolgungsbehörde übermittelt werden müssen. Dadurch nimmt die MROS eine zentrale Position im schweizerischen GW/TF-Abwehrdispositiv ein. Unterschiedliche Ämter und Behörden mit potentiellen Berührungspunkten zur vorliegenden Thematik haben an der Durchführung der Risikoanalyse teilgenommen und dabei Auskünfte, Angaben und Expertisen abgegeben:

- Ausgewählte kantonale Grundbuchämter, Amtsnotariate und Notariatsinspektorate
- Ausgewählte kantonale Steuerbehörden
- Bundesamt für Justiz (BJ)
- Bundesamt für Polizei (fedpol)
- Bundesanwaltschaft BA
- Bundeskriminalpolizei BKP
- Eidgenössische Finanzmarktaufsicht FINMA
- Eidgenössische Spielbankenkommission (ESBK)
- Eidgenössische Steuerverwaltung (ESTV)
- Eidgenössische Stiftungsaufsicht (ESA)
- Eidgenössisches Amt für Grundbuch- und Bodenrecht (EGBA)
- Eidgenössisches Zentralamt für Edelmetallkontrolle (ZEMK)
- Kantonale Staatsanwaltschaften
- Kantonale und städtische Polizeien
- Nachrichtendienst des Bundes (NDB)
- Nationales Zentrum für Cybersicherheit (NCSC)
- Staatssekretariat für Internationale Finanzfragen (SIF)

Bei der Durchführung von Risikoanalysen im GW/TF-Bereich sind methodologische Ansätze und bewährte Verfahren von internationalen Organisationen wie der FATF oder der Weltbank von massgeblicher Bedeutung. Gemäss den Methodologien der Weltbank und der FATF ist eine genaue Datenerhebung und -analyse wesentliche Voraussetzung für eine effektive und abgestufte Risikobewertung.[109] Verschiedene Finanzintermediäre mit VASP-Tätigkeit können namentlich ein höheres oder niedrigeres Risiko darstellen, abhängig von einer Vielzahl von Faktoren, einschliesslich Produkten, Dienstleistungen, Kunden, Geografie, Geschäftsmodellen und der Stärke des Compliance-Programms dieser Finanzintermediäre. Folglich sollten Länder Informationen über die Anzahl und Art von Finanzintermediären mit VASP-Tätigkeit, deren angebotene Dienstleistungen sowie deren Geschäftstätigkeiten sammeln und analysieren. Die Verfügbarkeit genauer und umfassender Daten ermöglicht es, im Rahmen der Analyse Risiken präzise zu identifizieren, zu bewerten und geeignete Massnahmen zur Risikominderung zu entwickeln.

Im Falle der vorliegenden Risikoanalyse stellen jedoch der weitgehende Mangel an und Informationen zu den spezifischen Dienstleistungen und Aktivitäten insbesondere im schweizerischen VA-Sektor eine methodologische Herausforderung dar. Die fehlenden Angaben zu den angebotenen Dienstleistungen sowie zur Intensität dieser Geschäftstätigkeiten erschweren die detaillierte Risikobewertung für einzelne Geschäftsmodelle (z.B. Verwahrung von VAs für Kunden, Umtausch von Fiatwährung in VAs, usw.).

Um die Herausforderung des Datenmangels zu bewältigen und trotzdem eine fundierte Risikoeinschätzung abzugeben, wurde bei der Durchführung dieser Risikoanalyse eine Kombination von verfügbaren Datenquellen, kooperativen Ansätzen mit relevanten inländischen und ausländischen Behörden sowie Schätzungen angewendet. Durch die Anwendung bewährter Methodologien der Weltbank und der FATF, angepasst an die spezifischen Gegebenheiten des schweizerischen VA-Sektors, konnten die GW/TF-Risiken trotz der vorhandenen Datenbeschränkungen in angemessener Weise beurteilt werden.

Hinweise zur allgemeinen Intensität der Verwendung von VAs und den angebotenen VA-(Finanz-) Dienstleistungen in der Schweiz konnten anhand verschiedener Umfragen, Presseberichte, Fachstudien zum schweizerischen VA-Sektor und weiteren verfügbaren Quellen (darunter auch Berichte aus dem internationalen Kontext, die Informationen zur Schweiz enthielten) gesammelt werden. Hinweise zur Verwendung von VAs für kriminelle Zwecke in der Schweiz im Allgemeinen sowie für GW/TF-Zwecke im Spezifischen wurden beispielsweise aus den Jahresberichten des Bundesamts für Polizei (fedpol), den Berichten des Nationalen Zentrums für Cybersicherheit (NCSC) sowie aus weiteren öffentlich verfügbaren Quellen wie der Polizeilichen Kriminalstatistik oder Presseberichten entnommen.

Zudem wurden nicht öffentliche Quellen und Datenbanken ausgewertet, um Aussagen über die kriminelle Verwendung von VAs in der Schweiz im Allgemeinen, sowie ihrer Verwendung für GW/TF-Zwecke im Spezifischen zu ermöglichen. Auf Bundesebene wurde hierfür eine Bestandesaufnahme der bisherigen Verfahren der Bundesanwaltschaft und den diesbezüglichen Vorermittlungen der Bundeskriminalpolizei vorgenommen, deren Sachverhalte auf die Verwendung von VAs für kriminelle Zwecke im Allgemeinen sowie für GW/TF-Zwecke im Speziellen schliessen liess. Diese Verfahren beinhalten Straftaten im Bereich der Schwerstkriminalität und fallen deshalb in die Kompetenz des Bundes. Auf Ebene der Kantone wurde die interkantonale Datenbank PICSEL (Plateforme d'Information de la Criminalité Sérielle En Ligne) ausgewertet, welche die digitale Sammlung von Strafanzeigen im Bereich Internetkriminalität zum Ziel hat, um die Priorisierung und Koordination der

[109] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Oktober 2021, S. 11. World Bank, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, Juni 2022, S. 14f.

Strafverfolgungsbehörden im Kampf gegen Cyberkriminalität zu fördern.[110] Dabei werden unter anderem die Anzahl der Vorfälle sowie die damit verbundenen Schadenssummen erfasst. Diese Daten ergeben nur einen partiellen Überblick, da weniger als die Hälfte der Kantone die Datenbank aktiv bewirtschaftet. Anhand einer Auswertung der darin gespeicherten Anzeigen, die einen Zusammenhang mit VAs aufweisen, lassen sich jedoch gewisse Tendenzen bei der Ver- bzw. Entwendung von VAs im Bereich der digitalen Kriminalität in der Schweiz erkennen.

Der wichtigste, nicht-öffentliche Datenbestand, der für diese Risikoanalyse ausgewertet wurde, waren die bei der Meldestelle für Geldwäscherei (MROS) eingereichten Verdachtsmeldungen sowie weitere ihr zur Verfügung stehende Daten. Informationen aus Verdachtsmeldungen, aus dem internationalen Informationsaustausch sowie aus weiteren der MROS zur Verfügung stehenden Datenbanken können konkrete Hinweise über die mutmassliche Verwendung von VAs für GW/TF-Zwecke in der Schweiz enthalten. In ihrer Gesamtheit ermöglicht eine Auswertung der Informationen, die der MROS zur Verfügung stehen, die Identifizierung von diesbezüglichen Merkmalen und Typologien diesbezüglich typische Muster und Vorgehensweisen zu identifizieren. Auf einer übergeordneten Stufe helfen diese Informationen auch bei der Beantwortung der Frage, inwiefern die der MROS bekannten Sachverhalte repräsentativ für Vorgänge im schweizerischen VA-Sektor stehen. Eine solche Abschätzung des Hellfelds und der Dunkelziffer von GW/TF-Handlungen im VA-Bereich in der Schweiz dient letztendlich der Identifizierung spezifischer Verwundbarkeiten, die dafür verantwortlich sein könnten, dass in Bezug auf bestimmte GW/TF-Phänomene im VA-Bereich blinde Flecken bestehen. [111] Zudem erfolgte im Rahmen der vorliegenden Analyse ein Informationsaustausch mit Fachpersonen im Bereich der Strafverfolgung[112] und mit verschiedenen Aufsichtsbehörden.[113] Mithilfe dieser auf qualitativen und teilweise quantitativen Angaben beruhenden Rückmeldungen lassen sich gewisse Trends bei der Verwendung von VAs für kriminelle Zwecke im Allgemeinen sowie für GW/TF-Zwecke im Speziellen feststellen. Sie ermöglichen allgemeine Schlüsse über gegenwärtige Chancen und Herausforderungen für schweizerische Strafverfolgungsbehörden bei der Aufklärung von Straftaten im Zusammenhang mit der Verwendung von VAs. Diese Gespräche dienten nebst der Gewinnung weiterer Erkenntnisse auch einer Auslegeordnung der Chancen und Herausforderungen im VA-Bereich, die derzeit für die die verschiedenen mit der Bekämpfung von GW/TF befassten Ämter und Behörden bestehen. Die Anfragen wurden dabei insbesondere an jene Behörden gestellt, die gemäss den zur Verfügung gestandenen Informationen bereits vertiefte Erfahrungen in diesem Bereich gemacht haben.

Um ein Bild der globalen VA-Risikolandschaft zu erhalten, wurde auf die Risikoanalysen anderer Länder sowie auf Jahresberichte ausländischer Meldestellen und Aufsichtsbehörden zurückgegriffen. Letztere enthalten auch Hinweise auf Tendenzen und Entwicklungen, die die Risiken im schweizerischen VA-Sektor beeinflussen können. Hierfür eignen sich ebenfalls die Berichte internationaler Organisationen und Körperschaften wie zum Beispiel der FATF, aber auch von privaten Unternehmen, zum Beispiel aus dem Bereich Blockchainanalyse. Sie enthalten ebenfalls wichtige Informationen und Zahlen zu entdeckten Fällen und Mustern sowie bereits identifizierte Risikofelder im Zusammenhang mit Geldwäscherei und Terrorismusfinanzierung im VA-Bereich. Aus den genannten Quellen lassen sich nebst einem

[110] Die Datenbank ist seit April 2021 operativ und wird bisher von den neun Kantonen Aargau, Fribourg, Genf, Graubünden, Jura, Neuenburg, Tessin, Waadt, Wallis genutzt. Mindestens ein weiterer Kanton wird demnächst hinzustossen (Stand Mai 2023).

[111] Als Dunkelziffer wird das Verhältnis zwischen den tatsächlich begangenen Straftaten und den in einer amtlichen Kriminalstatistik registrierten Fällen (Hellfeld) bezeichnet.

[112] Austausche wurden unter anderem mit Mitarbeitenden des Netzwerks digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) sowie mit weiteren kantonalen Staatsanwaltschaften und Polizeibehörden geführt.

[113] Zum Beispiel mit der Eidgenössischen Finanzmarktaufsicht (FINMA), der Eidgenössischen Stiftungsaufsicht (ESA), der Eidgenössischen Spielbankenkommission (ESBK) sowie dem Zentralamt für Edelmetallkontrolle (ZEMK).

möglichst kompletten Bild der globalen Risikolandschaft auch Gefährdungen und Verwundbarkeiten ableiten, die mit hoher Wahrscheinlichkeit für die Schweiz bestehen.

Abschliessend muss betont werden, dass letztendlich zu wenig Daten vorliegen, um die identifizierten Gefährdungen und Verwundbarkeiten sowie die Nettorisiken spezifischer finanzintermediären Tätigkeiten im VA-Bereich exakt zu quantifizieren (z.B. der Wechsel von Fiat/VA, die Verwahrung von VAs für Kunden, usw.). Ohne zuverlässige Zahlen (z.B. Transaktionsvolumen, Gesamtwert der verwahrten VAs, Anzahl und Herkunft der Kunden, usw.) kann nicht überprüft werden, ob und in welchem Mass die identifizierten Gefährdungen, Verwundbarkeiten und risikomindernden Faktoren die mit diesen Geschäftstätigkeiten verbundenen GW/TF-Risiken beeinflussen. Ebenfalls kann nicht beurteilt werden, inwiefern die bereits entdeckten (Verdachts-)Fälle bei spezifischen Geschäftstätigkeiten repräsentativ für Vorgänge in diesen Geschäftssparten stehen.

6. Globale Risikolandschaft

Viele der von VAs ausgehenden Gefährdungen und Verwundbarkeiten, für GW/TF-Zwecke missbraucht zu werden, sind entweder auf die technologische Beschaffenheit von VAs oder auf die Ausprägung des globalen VA-Sektors zurückzuführen. Sie betreffen deshalb alle Länder – und nicht nur die Schweiz – gleichsam.[114] Aus diesem Grund behandelt das vorliegende Kapitel den globalen Kontext, in welchem die Verwendung von VAs eingebettet ist. Im Vordergrund steht die globale Landschaft im VA-Sektor sowie die wichtigsten Veränderungen in diesem Bereich seit der letzten sektoriellen Risikoanalyse von 2018.

6.1 Globale Ausgangslage

Seit 2018 hat die Verwendung von VAs weltweit deutlich zugenommen, was auch zu einer wachsenden Bedeutung des VA-Sektors führte. Zwischen Frühjahr 2020 und Ende 2021 befand sich der VA-Sektor zuletzt in einer Aufschwungsphase. Die Marktkapitalisierung sämtlicher VAs stieg von rund 830 Milliarden US-Dollar im Jahr 2018 auf etwa 2.4 Billionen US-Dollar im Mai 2021.[115] Gemäss Schätzungen hat sich die Anzahl einzelner Nutzer von VAs zwischen 2018 und 2020 von 35 Millionen auf über 100 Millionen knapp verdreifacht.[116]
Der VA-Sektor erlebte eine starke mediale und politische Aufmerksamkeit und zog viele neue Akteure an. Grosse Beachtung fanden in dieser Zeit beispielsweise die Ankündigungen einzelner Länder, Bitcoin als gesetzliches Zahlungsmittel zu akzeptieren oder gar als Reserve zu halten.[117] Ebenfalls verkündeten bekannte Unternehmen ihre Cash-Reserven teilweise in Bitcoin umzuwandeln.[118] Mehrere weltweit operierende Grossbanken, Vermögensverwalter und Zahlungsdienstleister liessen zudem verlauten, die Verwahrung von VAs, aber auch VA-Investmentprodukte in ihr Dienstleistungsangebot aufzunehmen.[119]

Trotz des Preissturzes von VAs im Laufe des Jahres 2021 nahm ihre Verwendung nicht ab. Ende 2022, und damit zu einem Zeitpunkt als sich der VA-Sektor bereits wieder in einer Phase des Abschwungs befand, verzeichnete die Kryptobörse Coinbase alleine über 103 Millionen verifizierte Kunden, nachdem es im April 2021 noch 56 Millionen waren.[120] Studien prognostizieren, dass im Jahr 2030 über 10% der Weltbevölkerung, respektive bis zu einer Milliarde Menschen, VAs verwenden werden.[121]

Parallel zum Wachstum der Nutzer scheint eine Konsolidierung auf der Angebotsseite zentralisierter VA-Dienstleistungen stattgefunden zu haben, indem einzelne grosse VA-Börsen ihre Marktanteile ausbauen konnten.[122] Angesichts dieser Entwicklungen prognostizierte das Blockchainanalyse-Unternehmen Chainalysis im Februar 2021, dass diese Unternehmen künftig ihre Finanzflüsse, Kunden und Partner sorgfältiger prüfen müssen, um ihre Stellung im

---

[114] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 36.
[115] CoinMarketCap, *Global Cryptocurrency Market Charts*, zuletzt abgerufen im Mai 2023.
[116] Cambridge Centre For Alternative Finance (CCAF), *3rd Global Cryptoasset Benchmark Study*, September 2020, S. 12.
[117] BBC News, *Why the Central African Republic adopted Bitcoin*, 6. Juni 2022. New York Times, *In Global First, El Salvador Adopts Bitcoin as Currency*, 7. September 2021.
[118] Bloomberg, *Tesla Trails Only MicroStrategy in Treasury Bitcoin Allocation*, 8. Februar 2021.
[119] New York Times, *Banks Tried to Kill Crypto and Failed. Now They're Embracing It (Slowly)*, 1. November 2021.
[120] Vgl. Curry David, *Coinbase Revenue and Usage Statistics (2023)*, 28. März 2023.
[121] Finews, *1 Milliarde Krypto-Nutzer bis ins Jahr 2030*, 25. Juli 2022. Nasdaq, *Blockware Estimates 10% Global Bitcoin Adoption By 2030: Report*, 9. Juni 2022.
[122] Chainalysis, *Cryptocurrency Exchanges in 2021*, November 2021, S. 3 – 10. Barron's, *The Cryptocurrency Crash Could Lead to a Wave of M&A*, 23. Juni 2022.

Markt nicht zu gefährden und die entsprechenden GW/TF-Risiken zu minimieren.[123] Tatsächlich erhielten seither mehrere grosse Finanzintermediäre mit VASP-Tätigkeit in den Vereinigten Staaten sowie in Europa Bussen in zwei- bis dreifacher Millionenhöhe, unter anderem, weil sie zu wenig Vorkehrungen gegen Geldwäscherei getroffen sowie die Einreichung von Verdachtsmeldungen vernachlässigt hatten.[124] Untersuchungen förderten beispielsweise zutage, dass diese Finanzintermediäre unter anderem Transaktionen mit Ransomware-Banden, Darknetmärkten und sanktionierten Personen, Entitäten oder Adressen ermöglichten.[125] Zu erwähnen ist in diesem Zusammenhang auch die MiCa-Verordnung der Europäischen Union (*Markets in Cryptro Assets Regulation*), welche die VA-Regulierung innerhalb der EU harmonisiert und voraussichtlich ab 2024 in Kraft tritt.[126] Ungefähr seit Beginn des Jahres 2022 ist zu beobachten, dass Finanzintermediäre mit VASP-Tätigkeit auf internationaler Ebene stärker mit durchgreifenden Massnahmen seitens Regulierungs- und Strafverfolgungsbehörden konfrontiert sind als noch vor wenigen Jahren.[127]

6.2 Globale sektorielle Veränderungen 2018 – 2023

Gegenüber 2018 hat sich der VA-Sektor global sowohl in seiner Grösse als auch seiner Ausgestaltung grundlegend geändert. Gemäss Berichten internationaler Organisationen und Firmen im Bereich Blockchainanalyse haben in den letzten fünf Jahren die drei folgenden sektoriellen Veränderungen stattgefunden: Erstens entstand mit *Decentralized Finance* (DeFi) und der damit verbundenen Popularität von Non-Fungible Tokens (NFTs) ein neuer Geschäftsbereich im VA-Sektor, zweitens nahm durch die Entstehung dieses Bereichs die Verwendung von Stablecoins stark zu, und drittens hat sich die geografische Nutzung von VAs weltweit diversifiziert. Diese Entwicklungen brachten neue GW/TF-Risiken mit sich und werden im folgenden Abschnitt summarisch dargestellt.

6.2.1 Erhöhte Reichweite und erhöhte Risiken

Mit dem DeFi-Sektor (*Decentralized Finance*) entstand ein komplett neuer Bereich von VA-Finanzdienstleistungen. DeFi stützt sich für die Geschäftsabwicklung prinzipiell auf *Smart Contracts* statt auf die traditionelle Finanzintermediation (TradFi bzw. *Traditional Finance*, oder CeFi bzw. *Centralized Finance*). *Decentralized Finance* bezieht sich auf eine Gruppe von Finanzanwendungen und -dienstleistungen, die auf einer dezentralisierten Blockchain-Plattform aufbauen. Nutzer können die Dienstleistungen (z.B. Kredite, Anlageprodukte oder Zahlungsabwicklungen) dieser Plattformen in Anspruch nehmen, ohne sich dabei registrieren und identifizieren zu müssen, wie es in der Finanzintermediation sonst der Fall ist. Dies ist darauf zurückzuführen, dass die Abwicklung der über diese Plattformen getätigten

[123] Chainalysis, *The 2021 Crypto Crime Report*, Februar 2021, S. 111.
[124] Financial Crimes Enforcement Network (FinCEN), *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, 10. August 2021. Monroe Brian, *FinCEN, OFAC fine crypto exchange Bittrex nearly $30 million on AML, sanctions failings, missed SARs, links to darknet markets, mixers, ransomware gangs*, 11. Oktober 2022. New York Times, *Coinbase Reaches $100 Million Settlement With New York Regulators*, 4. Januar 2023. Reuters, *Dutch central bank fines cryptocurrency exchange Coinbase 3.3 mln euros*, 26. Januar 2023. Reuters, *Dutch central bank fines Binance 3.3 million euros*, 18. Juli 2022
[125] Ibid.
[126] European Parliament, *Crypto-assets: green light to new rules for tracing transfers in the EU*, April 2023.
[127] Vgl. z.B.: New York Times, *Government Cracks Down on Crypto Industry With Flurry of Actions*, 18. Februar 2023. Europol, *Bitzlato: senior management arrested*, 23. Januar 2023. Chainalysis, *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, 5. April 2022s, Chainalysis, *The 2023 Crypto Crime Report*, Februar 2023, S. 12.

Transaktionen nicht durch einen Finanzintermediär, sondern durch den zugrundeliegenden Code – dem *Smart Contract* – ausgeführt wird.

Im Jahr 2021 war das *on-chain*-Transaktionsvolumen sämtlicher dezentralisierter VA-Börsen (DEX, bzw. *Decentralized Exchange*) durchwegs grösser als jenes sämtlicher zentralisierter VA-Börsen (CEX, bzw. *Centralized Exchange*).[128] Ein Grund für die steigende Beliebtheit von DeFi liegt im vereinfachten und preisgünstigeren Zugang zu diesen Finanzdienstleistungen. Für die Nutzung von DeFi-Plattformen benötigt es lediglich Internetzugang und eine VA-Wallet. Im Unterschied zu CeFi-Plattformen müssen sich die Nutzer weder registrieren noch einen KYC-Prozess durchlaufen, bleiben also unidentifiziert.[129] Da diese Plattformen von *Smart Contracts*, bzw. Software betrieben werden, gibt es auch keine zentrale Entität, die Transaktionen stoppt, Konten einfriert oder Meldungen bei Geldwäschereiverdacht einreichen könnte. Dadurch gibt es bei solchen Plattformen de facto auch keine Ansprechpartner für Regulatoren oder Strafverfolgungsbehörden. Ebenfalls bleiben durch die Abwesenheit eines Finanzintermediärs (bzw. VASP) die auf DeFi-Plattformen deponierten VAs der Nutzer grundsätzlich unter ihrer Kontrolle. Diese Kontrolle ist allerdings nur insofern «garantiert», wie es im zugrundeliegende *Smart Contract* vorgesehen ist, bzw. programmiert wurde.

In der Realität führten – teilweise sogar bewusst eingebaute – Schwachstellen in diesen *Smart Contracts* zu zahlreichen spektakulären Hacks oder sogenannten *Rugpulls* mit anschliessendem Diebstahl sämtlicher auf den gehackten Plattformen deponierten VAs. Berichte aus dem Bereich der Blockchainanalyse beziffern die im Jahr 2020 durch Hacks von DeFi-Plattformen gestohlenen VAs auf rund 162 Millionen US-Dollar. Für das Jahr 2022 stieg diese Summe auf insgesamt 3.1 Milliarden US-Dollar an.[130] Mit dem Wachstum des DeFi-Sektors entstanden für Kriminelle somit profitable neue Möglichkeiten für grossangelegte Diebstähle von VAs. Die gestohlenen VAs müssen im Anschluss allerdings auch gewaschen werden. Dadurch hat sich wiederum die Nachfrage nach Techniken zum Waschen von gestohlenen VAs entsprechend erhöht – ebenso wie die potentiellen Gewinne für jene, die solche Techniken verkaufen oder anbieten. Die allermeisten DeFi-Plattformen emittieren eigene Token, die deren Besitzer beispielsweise dazu berechtigen, an den auf der Plattform entstehenden Transaktionsgebühren mitzuverdienen. Bezeichnenderweise wurden so die aus DeFi-Hacks gestohlenen VAs primär über andere DeFi-Plattformen gewaschen, also in andere VAs umgetauscht. Schätzungsweise floss in den Jahren 2021 und 2022 ungefähr die Hälfte der jeweils in diesen Jahren gestohlenen Kryptowährungen zu DeFi-Plattformen, was deren Gefährdung, für Geldwäschereizwecke missbraucht zu werden, klar aufzeigt.[131]

Gefährdung 1

Sicherheitslücken bei den zugrundeliegenden VA-Technologien (2018 identifiziert, 2023 erhöht)[132]

Bereits in der sektoriellen Risikoanalyse von 2018 wurden Sicherheitslücken in den VA-Technologien sowie die Geldwäscherei von illegal erworbenen VAs als Gefährdungen identifiziert. Beide Gefährdungen scheinen sich erstens angesichts des deutlichen Wachstums von DeFi und zweitens aufgrund der in diesem Bereich zahlreichen *Hacks, Scams* und *Rugpulls* erhöht zu haben. Zwar sind die Sicherheitslücken von VAs gegenüber 2018 nicht

[128] Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6. Juni 2022.
[129] KYC steht für "Know Your Customer" (Kenne deinen Kunden) und bezeichnet das Verfahren, das von Finanzintermediären eingesetzt wird, um die Identität von Kunden zu überprüfen, das Kundenrisiko zu bewerten und zu überwachen sowie illegale Aktivitäten wie Geldwäscherei zu verhindern, vgl. Glossar.
[130] Chainalysis, *The 2023 Crypto Crime Report*, Februar 2023, S. 58.
[131] Ibid., S. 61. Chainalysis, *The Crypto Crime Report 2022*, Februar 2022, S. 74.
[132] Vgl. KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 22 – 24.

gravierender geworden. Da die Anzahl VAs mittlerweile um ein Vielfaches höher liegt als noch 2018 sind die Sicherheitslücken jedoch zahlreicher geworden.

Die Verfügbarkeit von Stablecoins ist für die Funktionalität der meisten DeFi-Dienstleistungen eine wichtige Voraussetzung. Entsprechend nahm ihre Verwendung in den letzten Jahren deutlich zu. Zwischen 2018 und 2022 stieg der Anteil von Stablecoins am weltweiten VA-Transaktionsvolumen von knapp 10% auf rund 45% an.[133] Nebst der Nachfrage nach Stablecoins seitens DeFi-Anwendungen ist dieser Anstieg gemäss Untersuchungen des Blockchainanalyse-Unternehmens Chainalysis insbesondere auf die wachsende Verwendung in Schwellenländern zurückzuführen, wo Stablecoins vermehrt für internationale Überweisungen sowie für persönliche Ersparnisse benutzt werden.[134] Insofern ermöglichten Stablecoins weltweit den indirekten Zugang zu Devisen wie dem US-Dollar oder dem Euro, was die Reichweite von VAs wie auch deren Anzahl Nutzer stark erhöhte. Stablecoins und VAs mit Smart-Contract-Funktionalität (insb. Ethereum) – die zwei entscheidenden Treiber hinter DeFi – machten sodann zusammen im Jahr 2022 knapp 90% des gesamten VA-Transaktionsvolumens aus. [135]

Mit dem medialen Wirbel um die Schlagwörter «Metaverse» und «Web3» (grundsätzlich ein Blockchain-basiertes World Wide Web) entstand auch ein grosser Hype um NFTs. NFT steht für "Non-Fungible Token" («nicht-austauschbare Token») und bezieht sich auf eindeutig identifizierbare VAs, die über Alleinstellungsmerkmale verfügen und auf einer Blockchain gespeichert werden.[136] NFTs können verschiedene digitale Medien wie Kunstwerke, Musik, Videos und Spiele darstellen und werden oft als Sammlerstücke betrachtet. Die Verfügungsrechte über ein NFT – also, welche VA-Adresse in der Lage ist, ein bestimmtes NFT zu versenden bzw. zu verkaufen – sind auf der entsprechenden Blockchain kryptografisch festgeschrieben. Im Gegensatz zum traditionellen Kunsthandel können NFT-Kunstwerke direkt zwischen Sender und Empfänger gehandelt werden, ohne dass für die Überprüfung der Echtheit oder das Festhalten des Besitzerwechsels ein Finanzintermediär oder eine sonstige zentrale Entität benötigt wird (z.B. eine Fachpersonen, welche die Echtheit eines Picasso-Gemäldes zertifiziert).

Die drei Begriffe «Metaverse», «Web3» und «NFTs» sind letztendlich Elemente, die dem wachsenden DeFi-Sektor zuzurechnen sind. Hinter diesen Schlagwörtern liegt die Vision (bzw. teilweise bereits die Realität), dass im VA-Sektor neue Geschäftsfelder entstehen, die neue Nutzer anziehen und ebenso bisher externe Geschäftsfelder wie Kunst, Musik, Gaming oder Sport, in den Einflussbereich des VA-Sektors rücken. Im Jahr 2021 wurden Milliardenbeträge für NFTs ausgegeben, was unter anderem auf die Popularität diverser Metaverse-Projekte sowie die Bewerbung von NFTs durch berühmte Persönlichkeiten und Unternehmen zurückzuführen ist.[137] Gemäss dem Blockchainanalyse-Unternehmen Elliptic sind identifizierte Geldwäschereifälle mit NFTs bisher selten.[138] Seit 2017 seien insgesamt 8 Millionen US-Dollar in VAs über NFT-basierte Plattformen gewaschen worden, was nur einem Bruchteil der gesamten NFT-bezogenen Handelsaktivität entspricht. Allerdings bezieht sich diese Summe lediglich auf bereits identifizierte Geldwäschereihandlungen und ist deshalb Minimalsumme zu verstehen.[139] Wie sonstige DeFi-Projekte sind auch NFT-Plattformen anfällig für Hacks, Scams und *Rugpulls*. Gemäss Elliptic wurden zwischen Juli 2021 und Juli 2022 NFTs im Wert

[133] Chainalysis, *The Crypto Crime Report 2022*, Februar 2022, S.9.
[134] Vgl. Chainalysis, *The State of Web3*, Juni 2022, S. 3.
[135] Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6. Juni 2022.
[136] Ein spezifisches NFT entspricht *nie* einem anderen NFT, da es eindeutig identifizierbar ist.
[137] Elliptic, *NFTs and Financial Crime*, August 2022, S. 5.
[138] Ibid., S. 4.
[139] Laut Elliptic stammten beispielsweise weitere 328.6 Millionen US-Dollar an NFT-Plattformen überwiesene VAs aus Verschleierungsdiensten wie z.B. Mixing Services, was auf Erlöse aus kriminellen Aktivitäten hindeuten könnte, vgl. Ibid., S. 4.

von über 100 Millionen Dollar durch verschiedene Betrugsschemas gestohlen.[140] NFTs könnten zudem für GW/TF-Zwecke missbraucht werden, insbesondere für handelsbasierte Geldwäscherei oder zur Plausibilisierung der Herkunft von Vermögenswerten, da die Einschätzung des Wertes eines NFT subjektiv ist und auch keine Standards für die Preisfindung existieren.[141] Die Attraktivität von NFTs für GW/TF-Zwecke sei derzeit allgemein allerdings relativ niedrig, da sie zu den transparentesten VAs gehören: Für fast jedes NFT kann dessen vollständige Historie seines Preises und den Adressen der vormaligen Besitzer eingesehen werden. Demgegenüber existieren etabliertere und anonymere Techniken zum Waschen von VAs (bspw. Privacy Coins oder Mixer, vgl. Infobox 4 in Kapitel 7.4.1), sodass der derzeitige Anreiz für Geldwäscher wohl eher gering sei, auf NFTs umzusteigen.[142] Falls die Popularität von NFTs und damit der Zuwachs der zuvor genannten neuen VA-Geschäftsfelder weiter zunimmt, vergrössert sich entsprechend auch die Reichweite des VA-Sektors. Ebenso vervielfältigen sich damit die potentiellen Möglichkeiten für Kriminelle, NFTs für GW/TF-Zwecke zu missbrauchen.

6.2.2 Geographische Diversifizierung in der Nutzung von VAs

Mittlerweile scheinen VAs von den unterschiedlichsten Menschen für die unterschiedlichsten Zwecke eingesetzt zu werden. Obschon hierfür zuverlässige Zahlen fehlen, existieren für einzelne Weltregionen Schätzungen, wie stark die allgemeine Verwendung von VAs in den letzten Jahren gewachsen ist: Von den 20 höchstplatzierten Ländern auf dem «Global Crypto Adoption Index» des Blockchainanalyse-Unternehmens Chainalysis waren lediglich zwei Volkswirtschaften mit hohen Einkommen vertreten, namentlich die Vereinigten Staaten sowie Grossbritannien.[143] Demgegenüber gehörten die Hälfte der Top-20-Länder zum unteren mittleren Einkommensbereich (Vietnam, Philippinen, Ukraine, Indien, Pakistan, Nigeria, Marokko, Nepal, Kenia und Indonesien) sowie acht zum oberen mittleren Einkommensbereich (Brasilien, Thailand, Russland, China, Türkei, Argentinien, Kolumbien und Ecuador).

Die Tatsache, dass VAs inzwischen weltweit von einer breiten Palette von Menschen für verschiedene legitime Zwecke eingesetzt werden, macht es im Allgemeinen schwieriger, GW/TF-Risiken zu identifizieren und zu bekämpfen. Der Missbrauch von VAs kann fortan in den unterschiedlichsten Sektoren und über diverse Kanäle erfolgen, was die Entdeckung spezifischer Risiken erschwert.

Verwundbarkeit 3

Defizit an Ressourcen und Kapazitäten seitens der mit der GW/TF-Bekämpfung betrauten Institutionen angesichts der rasanten Entwicklungen im VA-Bereich (2023 identifiziert)

Die rasche Entwicklung des globalen VA-Sektors erfordert, dass diese Veränderungen weltweit durch die mit der GW/TF-Bekämpfung befassten Stakeholder im In- und Ausland sowie internationalen Organisationen aufmerksam beobachtet werden. Nur auf diese Weise kann im Hinblick auf eine Minimierung der GW/TF-Risiken eine sachkundige Überwachung und Regulierung des Sektors sichergestellt werden, die den steten Veränderungen und Neuerungen Rechnung tragen. Um dies zu erreichen, ist es von entscheidender Bedeutung, dass in- und ausländische Stakeholder sowie internationale Organisationen die notwendigen

[140] Ibid., S. 4 und S. 12 – 35.
[141] Elliptic, *NFTs and Financial Crime*, August 2022, S. 77 – 79.
[142] Ibid., S. 79.

[143] Chainalysis, *The 2022 Geography of Cryptocurrency Report*, September 2022, S. 7.

Ressourcen und Kapazitäten dafür besitzen. Dies umfasst beispielsweise die Einigung über die Sammlung, Auswertung und Bereitstellung von Daten zur wirtschaftlichen und technologischen Entwicklung des Sektors, die Schulung von Personal für (Straf-)Ermittlungen im VA-Bereich sowie eine enge Zusammenarbeit zwischen den involvierten Stakeholder auf nationaler und internationaler Ebene. Weltweit scheint eine entsprechende Zuteilung von Ressourcen und Kapazitäten nicht gegeben. Sowohl zwischen als auch innerhalb der einzelnen Länder scheinen starke Unterschiede zu bestehen, einerseits im Hinblick auf die Verfügbarkeit von Ressourcen und Kapazitäten, andererseits zum allgemeinen Wissensstand und der politischen Aufmerksamkeit, die den GW/TF-Risiken gewidmet wird. Obwohl die politische Aufmerksamkeit für die Veränderungen im VA-Bereich gestiegen ist (vgl. Kapitel 6.3), bleibt die Reaktionszeit der mit der GW/TF-Bekämpfung befassten Stakeholder und Organisationen im Vergleich zu den dynamischen Entwicklungen im Sektor weiterhin zu langsam. Solange nicht mit den Entwicklungen des Sektors Schritt gehalten werden kann, wird es auch nicht möglich sein, die Entwicklung der GW/TF-Risiken angemessen einzuschätzen und letztere zu minimieren.

6.3 Kriminelle Verwendung von VAs sorgt für politische Aufmerksamkeit

Hinweise für die Zunahme in der kriminellen Verwendung von VAs finden sich in diversen Berichten internationaler Organisationen und nationaler Behörden. Auf einer übergeordneten Ebene lässt sich daran auch erkennen, dass die allgemeine Aufmerksamkeit seitens Aufsichts- und Strafverfolgungsbehörden gegenüber den GW/TF-Risiken im VA-Sektor zugenommen hat. Mehrere FIU-Jahresberichte und Risikoanalysen verschiedener Länder warnen vor der Gefahr, dass VAs vermehrt für Geldwäscherei- und Terrorismusfinanzierungszwecke missbraucht werden. Meist wird die Attraktivität von VAs für solche Handlungen hervorgehoben, indem auf die Geschwindigkeit von VA-Transaktionen, die dabei eingesetzten Verschlüsselungstechniken und die grenzüberschreitenden, internetbasierten Übertragungswege verwiesen wird, was eine Überwachung und Rückverfolgung erschwere bis verunmögliche.[144] Diverse FIUs konstatierten für die vergangenen Jahre einen steigenden Trend in der Anzahl Verdachtsmeldungen mit Bezügen zu VAs.[145] Mehrere erschienene nationale Risikoanalysen (NRA) warnen vor erhöhten GW/TF-Risiken und einem hohen Missbrauchspotenzial.[146] Die nationale Risikoanalyse Estlands – weltweit ein bedeutender Standort für VASPs – hat zum Beispiel gezeigt, dass die Mehrheit der dort angesiedelten VASPs ihre Geldwäscherei- und Terrorismusfinanzierungsrisiken unzureichend kontrollieren. Beinahe 75% der über 250 estnischen VASPs erstatteten im Jahr 2021 keine einzige Verdachtsmeldung, während Untersuchungen zeigten, dass sie in dieser Zeit ihre Sorgfaltspflichten erheblich vernachlässigten.[147]

---

[144] Financial Intelligence Unit (Deutschland), *Jahresbericht 2019*, Juni 2020 S. 33. Financial Crimes Enforcement Network (FinCEN), *Advisory on Illicit Activity Involving Convertible Virtual Currency*, Mai 2019, S. 1 – 2.

[145] Financial Intelligence Unit (Deutschland), *Jahresbericht 2019*, Juni 2020 S. 46. Financial Intelligence Unit (Deutschland), *Jahresbericht 2021*, August 2022, S. 48. Financial Intelligence Unit (Niederlande), *Annual Review 2019*, Juni 2020, S. 13. Financial Intelligence Unit (Niederlande), *Annual Review 2021*, Juni 2022, S. 7 und S. 27. Financial Intelligence Unit (Estland), *Yearbook 2019*, 2020, S. 29. Financial Intelligence Unit (Liechtenstein), *Jahresbericht 2020*, März 2021, S. 5. Financial Intelligence Unit (Liechtenstein), *Jahresbericht 2021*, April 2022, S. 6. Vgl. auch Vedrenne Gabriel, *In Europe, Suspicious Payments Triple Thanks to VASPs, Cryptocurrency*, 25. Oktober 2022.

[146] HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, Dezember 2020, S. 70. Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France*, September 2019, S. 65. State Financial Service of Ukraine, *Report on the National Risk Assessment*, 2019, S. 78 – 80. Government Of The Grand Duchy Of Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers*, Dezember 2020, S. 3 – 4.

[147] Financial Intelligence Unit (Estland), *The Risks related to Virtual Asset Service Providers in Estonia*, Januar 2022, S. 5.

Laut der FATF konzentrieren sich VA-bezogene Straftaten primär auf Geldwäschereidelikte oder deren Vortaten, allerdings nutzten Kriminelle VAs auch, um Finanzsanktionen zu umgehen oder Gelder zur Unterstützung des Terrorismus zu beschaffen. Die von den verschiedenen FATF-Ländern gemeldeten Arten von Straftaten umfassten insbesondere den illegalen Handel mit Betäubungsmitteln und anderen Waren (bspw. Schusswaffen), Betrug, Steuerhinterziehung, Cyberkriminalität, Vertrieb von Kindsmissbrauchsmaterial, Menschenhandel, die Umgehung von Wirtschaftssanktionen sowie Terrorismusfinanzierung. Die häufigsten beobachteten Straftaten seien im Bereich des Betäubungsmittelhandels zu verorten; entweder durch Verkäufe, die direkt in VAs abgewickelt werden, oder durch die Verwendung von VAs für Geldwäschereizwecke. Die zweithäufigste Art des Missbrauchs stehe im Zusammenhang mit Betrug, Ransomware und Erpressung. Zudem würden professionelle Geldwäschereinetzwerke VAs vermehrt als Instrument zum Waschen von Vermögenswerten benutzen.[148]

Infobox 3

Ransomware: Gestiegene politische Aufmerksamkeit gegenüber VAs

Ransomware ist eine Art von Schadsoftware (Malware), die dazu verwendet wird, den Zugriff auf Daten oder Systeme zu sperren, indem sie verschlüsselt werden. Die Angreifer fordern dann ein Lösegeld von den Opfern, um die Daten oder den Zugang wiederherzustellen. Ransomware-Attacken haben in den letzten Jahren global deutlich zugenommen. Die Angreifer verlangen von ihren Opfern beinahe ausschliesslich, dass das Lösegeld in VAs gezahlt wird.[149] Die Nutzung von VAs bei Ransomware-Angriffen als Lösegeld erleichtert es den technisch versierten Angreifern, ihre Identität wie auch den Geldfluss zu verschleiern. Gegenüber dem traditionellen Zahlungsverkehr haben VAs den Vorteil, dass sie – solange sie sich in einer *non-custodial* Wallet befinden – nicht durch Dritte gesperrt oder eingezogen werden können.

Die politische Aufmerksamkeit gegenüber VAs ist in den letzten Jahren unter anderem deshalb gestiegen, da sich Ransomware-Attacken inzwischen weltweit auch auf volkswirtschaftlich oder infrastrukturell systemrelevante Institutionen sowie grosse Finanzinstitutionen ausgeweitet haben. [150] Ransomware wird deshalb inzwischen von vielen Ländern nicht nur als bedeutende Cyber-Bedrohung, sondern auch als Bedrohung der nationalen Sicherheit betrachtet.[151]

Gemäss das Blockchain-Analyseunternehmen Chainalysis hat sich die Gesamtsumme der an bekannte Ransomware-Adressen versendeten VAs zwischen 2019 und 2020 mehr als vervierfacht.[152] Interessanterweise landete die Hälfte aller VAs, die von bekannten Ransomware-Adressen an Finanzintermediäre mit VASP-Tätigkeit, die den Umtausch VA-Fiat anbieten (sog. Fiat Off-Ramps), auf lediglich 21 Adressen, was eine starke Konzentration und Organisation in der Geldwäscherei von Erlösen aus Ransomware-Attacken suggeriert.[153]
In der Schweiz nimmt das Nationale Zentrum für Cybersicherheit (NCSC) Meldungen zu Cybervorfällen aus der Bevölkerung und der Wirtschaft entgegen, analysiert diese und gibt den Meldenden eine Einschätzung zum Vorfall mit Empfehlungen für das weitere Vorgehen. Gemäss dem NCSC sei es sehr schwierig festzustellen sei, wohin gegebenenfalls erpresste VAs aus Ransomware-Attacken fliessen und wer die tatsächlichen Empfänger dieser Zahlungen seien. Dies hat unter anderem damit zu tun, dass die Zurverfügungstellung von

[148] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, September 2020, S. 4.
[149] FATF, *Countering Ransomware Financing*, März 2023, S. 6.
[150] Prestige Business, *Cyber-Attacken in der Schweiz nehmen auch 2023 zu*, 3. Mai 2023.
[151] CNET, *Ransomware rises as a national security threat as bigger targets fall*, 18. Oktober 2021.
[152] Chainalysis, *The 2023 Crypto Crime Report*, Februar 2023, S. 27.
[153] Ibid., S. 50.

Ransomware sich mittlerweile zu einer eigentlichen Dienstleistung entwickelt hat (*Ransomware as a Service*) und primär im Darknet an «Kunden» vermietet oder verkauft wird, die selbst wiederum keine IT-Kenntnisse besitzen müssen. Die Verteilung der damit erzielten Einnahmen und die Nachverfolgung dieser Zahlungsströme wird durch diese Entwicklung weiter erschwert. Bisher hat das NCSC keine Daten über Anzahl und Höhe von allfälligen Lösegeldzahlungen erfasst. Es geht jedoch davon aus, dass viele Fälle, in welchen Lösegeld gezahlt wurde, gar nicht erst dem NCSC gemeldet werden.

Im Dezember 2022 hat der Bundesrat angekündigt, eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen einführen zu wollen.[154] Die Vorlage schafft die gesetzlichen Grundlagen zur Meldepflicht für Betreiberinnen und Betreiber kritischer Infrastrukturen und definiert die Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC), welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist.

Gefährdung 2

Ransomware und Malware (2018 identifiziert, 2023 erhöht)[155]
Bereits im sektoriellen Bericht von 2018 wurde festgestellt, dass VAs ein beliebtes Instrument für Hacker im Zusammenhang mit Ransomware sind. Gegenüber 2018 haben Ransomware-Fälle in ihrer Anzahl, der Höhe der dabei erbeuteten VAs sowie die von ihnen ausgehenden Risiken für private und staatliche Infrastrukturen eine neue Dimension erreicht, wodurch sich die Gefährdungslage folglich erhöht hat.

Gefährdung 3

VAs als Zahlungsmittel für illegale Güter und Dienstleistungen (2018 identifiziert, 2023 erhöht)[156]

Auch im Jahr 2023 sind VAs ein bevorzugtes Zahlungsmittel für illegale Güter und Dienstleistungen im Internet, beispielsweise für den Kauf und Verkauf von Betäubungsmitteln oder gestohlenen Kreditkarteninformationen im Darknet, oder eben auch für Ransomware- oder andere Malware-Software.[157] Die Umsätze auf Darknetmärkten sind seit 2018 von rund 750 Millionen auf 1.5 Milliarden US-Dollar angestiegen.[158]

Auch in der Schweiz sind Fälle bekannt, in denen VAs auch als Zahlungsmittel für den organisierten Verkauf von Betäubungsmittel eingesetzt wurden.[159] Die Anerkennung der Risiken in diesem Bereich führte zu einer Anpassung des Schwellenwerts von CHF 5 000 auf CHF 1 000 bei Geschäften mit virtuellen Währungen (Art. 51*a* GwV-FINMA).

Zwar bleibt unklar, in welchem Verhältnis die Verwendung von VAs als Zahlungsmittel für illegale Güter und Dienstleistungen gegenüber dem allgemeinen Wachstum des VA-Sektors angestiegen ist. *Dass* VAs jedoch häufiger und diverser als solches Zahlungsmittel eingesetzt werden, ist jedoch belegt und zeigt, dass sich diese Gefährdungslage erhöht hat.

[154] BBl 2023 84 – *Botschaft zur Änderung des Informationssicherheitsgesetzes* (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen) vom 2. Dezember 2022, 18. Januar 2023.
[155] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 26.
[156] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 28 – 30.
[157] Chainalysis, *The 2023 Crypto Crime Report*, Februar 2023, S. 71 – 84.
[158] Ibid., S. 71. Chainalysis, *The Crypto Crime Report 2022*, Februar 2022, S. 100.
[159] Vgl. z.B. Tages Anzeiger, *Schweizer Online-Drogenversand – «Hippe Kleider, Typ Studentin, und das Täschli voller Drogen»*, 18. März 2021.

6.4 Schätzungen zu weltweiten VA-Finanzflüssen mit GW/TF-Relevanz

Grundsätzlich existieren keine zuverlässigen Zahlen zu GW/TF-relevanten Finanzflüssen im VA-Bereich. Schätzungen von Blockchainanalyse-Unternehmen sind oft die einzige Grundlage, aus denen sich quantitative Erkenntnisse über die Verwendung von VAs für GW/TF-Zwecke ziehen lassen – dies ist auch ein Grund, weshalb sie in den meisten FIU-Jahresberichten und National Risk Assessments zitiert werden. Die Zahlen dieser Unternehmen geben lediglich eine Vorstellung der Grössenordnung, sind aber aus mehreren Gründen mit Vorsicht zu geniessen.

Erstens ist unklar, was unter dem von unterschiedlichen Blockchainanalyse-Unternehmen verwendeten allgemeinen Begriff «Crypto Crime» fällt. Eine genaue Definition, welche Straftaten und Zahlungen darunter zusammengefasst werden, existiert nicht. Damit bleibt auch unklar, welche der unter «Crypto Crime» subsumierten Handlungen gemäss schweizerischer Gesetzgebung als Vortaten zur Geldwäscherei infrage kommen würden. Chainalysis lieferte in ihrem im Februar 2022 erschienen «Crypto Crime Report» zumindest die Eingrenzung, dass die darin publizierten Zahlen sich nur auf «cryptocurrency-native crime» beziehen würden, wie z.B. Verkäufe auf Darknet-Märkten oder Ransomwareattacken. Es sei schwieriger zu messen, wie viel Bargeld aus der «Offline-Kriminalität» wie zum Beispiel aus dem traditionellen Drogenhandel, für Geldwäschereizwecke in Kryptowährung umgewandelt werde.

Zweitens ist unklar, inwiefern sich der Anteil an «Crypto Crime» am jährlichen VA-Transaktionsvolumen mit illegalen Finanzflüssen in anderen Sektoren vergleichen lässt.
Drittens wurden solche Zahlen im Nachhinein teilweise signifikant nach oben korrigiert.[160]
Viertens müssen die kriminellen Aktivitäten, ebenso wie die damit assoziierten VA-Adressen, bereits erkannt worden sein: Erfahrungsgemäss finden sich in den Berichten primär Analysen zu Straftaten im Bereich Cyberkriminalität (Ransomware, Hacks, Phishing, Anlagebetrug, etc.) sowie zum illegalen Handel mit Waren und Dienstleistungen in Darknetmärkten. Es scheint klar, dass Zahlungen, beispielsweise im Bereich der handelsbasierten Geldwäscherei, der Korruption, des Menschenhandels oder der Terrorismusfinanzierung von den Analysetools dieser Unternehmen schwieriger zu entdecken sind, sofern nicht bereits externe Anhaltspunkte für ihre strafrechtlicher Relevanz vorliegen (Medienberichte oder bekannte VA-Adressen).

Fünftens sind in diesen Analysen sämtliche Off-Chain-Transaktionen nicht berücksichtigt, deren Volumen gemäss Schätzungen mindestens zehnmal grösser ist als das *on-chain*-Volumen.[161] Insofern spiegeln ihre Analysen und Zahlen nur einen Bruchteil der tatsächlich stattfindenden VA-Transaktionen wider. Letztendlich ist auch unklar, ob ein Rückgang des Anteils der entdeckten Transaktionen mit kriminellem Hintergrund damit zusammenhängt, dass die Kriminalitätsrisiken im VA-Sektor allgemein gesunken sind, oder ob umgekehrt mit dem zunehmenden Reifegrad des VA-Sektors Kriminelle vermehrt dazu übergegangen sind, ausgeklügelte Verschleierungstechniken zu verwenden – beispielsweise anhand nicht überwachbarer Privacy Coins oder durch die Verwendung von Mixern und dezentralisierten Handelsbörsen.

Trotz dieser Unklarheiten ist der Anstieg von VA-Finanzflüssen mit einem kriminellen Hintergrund allgemein unbestritten. Chainalysis schätzte die weltweite Gesamtsumme aller von bekannten Adressen mit kriminellem Hintergrund erhaltenen VAs für das Jahr 2022 auf über 20 Milliarden US-Dollar gegenüber 8 Milliarden im Jahr 2020.[162] Umgekehrt versendeten

[160] McGuire Michael, *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy*, April 2018, S. 4. Chainalysis, *The 2020 Crypto Crime Report*, Februar 2022, S.4.
[161] Vgl. Jimenez Alison, *3 Misconceptions about Cryptocurrency Crime Estimates*, 11. Januar 2022.
[162] Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12. Januar 2023.

diese Adressen im Jahr 2022 VAs im Wert von rund 23.8 Milliarden US-Dollar.[163] Dies entspricht einem Anstieg von 68% gegenüber 2021 mit rund 14.2 Milliarden US-Dollar.[164] Mehr als die Hälfte des Werts dieser VAs floss hierbei zu den grossen VA-Handelsbörsen. Die entsprechenden Kontoinhaber bei diesen Handelsbörsen waren jedoch sogenannte Over-The-Counter (OTC) Broker. Das sind Finanzintermediäre mit VASP-Tätigkeit, die für ihre Dienstleistungen die Plattformen der grossen Handelsbörsen nutzen («nested services», vgl. Infobox 4 in Kapitel 7.4.1). Trotzdem sollte diese Zahl aufhorchen lassen, da die grossen Handelsbörsen jene Orte sind, an denen VAs in Fiatwährung umgewandelt werden können und dadurch in den traditionellen Finanzkreislauf Eingang finden. Grosse Handelsbörsen verfügen auch am ehesten über grosse Compliance-Abteilungen, die diese Transaktionen melden und Massnahmen gegen die betreffenden Nutzer ergreifen.

Relativiert werden diese Summen allerdings dadurch, dass der Anteil von VA-Transaktionen mit bekanntem kriminellem Hintergrund, darunter Geldwäscherei und Terrorismusfinanzierung, gemessen an der Gesamtheit sämtlicher VA-Transaktionen zurückgeht. Dieser Anteil liegts – je nach Quelle – zwischen 0.24% (2022) und 3.3% (2019).[165] Zum Vergleich: Die UNO schätzt die Menge an Geld, die weltweit in einem Jahr gewaschen wird, auf 2-5% des globalen Bruttoinlandprodukt.[166] Auch in nationalen Risikoanalysen und ähnlich gelagerten Berichten wurde indes betont, dass die Verwendung von VAs für Geldwäschereizwecke trotz steigender Risiken noch weit unter derjenigen von Fiat-Währung und traditionelleren Methoden liege.[167]

Für den nominellen Anstieg der Gesamtsumme von VA-Transaktionen mit möglichem kriminellem Hintergrund bei gleichzeitiger prozentualer Abnahme dieses Anteils am gesamten VA-Transaktionsvolumen gibt es mehrere Erklärungen. Viele VA-Diebstähle geschahen während des Aufschwungs der VA-Preise, sodass auch der Wert der gestohlenen VAs sozusagen von alleine anstieg. Umgekehrt könnte die relative Abnahme mit der zunehmenden Regulierung der grossen «Player» erklärt werden, die dazu übergegangen sind, ihre Kunden genauer zu prüfen und Blockchainanalyse-Tools für ihr Transaktionsmonitoring zu verwenden. Letztlich wäre es sowieso überraschend und alarmierend, wenn mit dem spektakulären Wachstum des VA-Sektors die kriminelle Verwendung proportional zugenommen hätte.

Im Bereich von «Crypto Crime» scheint Geldwäscherei als Straftat *die* zentrale Rolle zu spielen: Aus Hacks, Ransomware-Attacken, Scams, Verkäufen von Kindsmissbrauchs-material oder Betäubungsmittel über das Darknet unrechtmässig erlangte VAs müssen zu irgendeinem Zeitpunkt gewaschen werden, sofern sie in den legalen Kreislauf zurückkehren. Allein im Oktober 2022, also bereits nach dem erheblichen Rückgang von VA-Preisen, wurden im Zuge von 11 Hacks bei DeFi-Plattformen VAs im Wert von 718 Millionen US-Dollar entwendet.[168] Im Jahr 2022 wurde die Gesamtsumme der mittels Hacks erbeuteten VAs auf 3.8 Milliarden US-Dollar geschätzt.[169]

---

[163] Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26. Januar 2023.
[164] Ibid.
[165] Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12. Januar 2023. Ciphertrace, *Cryptocurrency crime and anti-money laundering*, Juni 2022, S. 5. TRM Labs, *Ensuring Responsible Development of Digital Assets; Request for Comment*, November 2022.
[166] United Nations Office on Drugs and Crime (UNODC), *Money Laundering*, zuletzt abgerufen im Mai 2023.
[167] Exemplarisch: Department of the Treasury (USA), *National Money Laundering Risk Assessment*, Februar 2022, S. 41. Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, Dezember 2021, S. 2.
[168] Finews, *Chainalysis: Crypto Hacks Reach Record $3 Billion*, 13. Oktober 2022.
[169] Chainalysis, *The 2023 Crypto Crime Report*, Februar 2023, S. 56.

Gefährdung 4

Geldwäscherei von VAs krimineller Herkunft (in Fiatgeld) (2018 identifiziert, 2023 erhöht)[170]

Kriminelle machten sich seit 2018 diverse Sicherheitslücken in VA-Protokollen und -Plattformen zunutze und erbeuteten Milliardenbeträge in VAs auf illegale Weise. Zur Einspeisung dieser inkriminierten Vermögenswerte in den legalen Finanzkreislauf müssen diese Milliardenbeträge gewaschen werden. Folglich hat sich gegenüber 2018 auch die Nachfrage nach Möglichkeiten zum Waschen von illegal erworbenen VAs deutlich erhöht. Einzelne Finanzintermediäre mit VASP-Tätigkeit sind im Vergleich zu 2018 stärker gefährdet, für das Waschen dieser VAs missbraucht zu werden.

Hacks von CeFi- und DeFi-Plattformen scheinen überdies nicht nur von «gewöhnlichen» Hackern, sondern auch von staatlichen Akteuren für Proliferationsfinanzierungszwecke durchgeführt zu werden. Laut mehreren Berichten des Expertengremiums für Nordkorea-Sanktionen, die vom Sicherheitsrat der Vereinten Nationen veröffentlicht wurden, würden Einnahmen aus solchen Hacks zur Unterstützung der nordkoreanischen Programme für Massenvernichtungswaffen und ballistische Raketen verwendet.[171] Laut anderen Berichten bilde der Diebstahl von VAs inzwischen eine der Haupteinnahmequellen für Nordkorea, wobei bis zu einem Drittel der finanziellen Mittel für sein Raketenprogramm über diese Wege beschafft würde.[172] Für das Jahr 2022 ordnete Chainalysis VAs in der Höhe von 1.7 Milliarden US-Dollar Hackergruppen zu, die mit dem nordkoreanischen Staat in Verbindung stehen.[173] Diese Summe entspricht mehr als 10% des nordkoreanischen Bruttoinlandprodukts.[174] Im April 2023 betonte die Kontaktgruppe für VAs und VASPs der Financial Action Task Force (FATF) mit direktem Verweis auf Nordkorea, dass die Länder weltweit dringend die FATF-Standards umsetzen müssen, da das Risiko zunehme, dass VAs für Geldwäscherei, Terrorismusfinanzierung und Proliferationsfinanzierung missbraucht werden. [175]

Eine wichtige Änderung in der kriminellen Verwendung von VAs beobachtete Europol darin, dass der Einsatz von VAs nicht mehr auf Aktivitäten der Cyberkriminalität beschränkt sei, sondern sich mittlerweile auf alle Arten von Verbrechen ausgeweitet habe, die die Übertragung von Geldwerten erfordern.[176] Die von den verschiedenen FATF-Ländern gemeldeten Arten von Straftaten veranschaulichen die Diversität in der Verwendung von VAs durch verschiedenste Akteure und für verschiedenste kriminelle Zwecke.

Ebenso scheinen VAs für das Waschen von Erträgen krimineller Organisationen aus ihren «Offline-Aktivitäten» missbraucht zu werden. Im Jahr 2021 beschlagnahmten italienische Behörden über 80 Millionen Euro, bei denen davon ausgegangen wird, dass eine Fraktion der sizilianischen Cosa Nostra diese Summe über eine von ihr selbst kontrollierte und in Malta

[170] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 26f. Die Gefährdung wurde im KGGT-Bericht von 2018 zu Kryptowährungen mit «Waschen von illegal erworbenen Krypto-Assets» betitelt und wurde zur Verdeutlichung «Geldwäscherei von VAs krimineller Herkunft (in Fiatgeld)» umbenannt, um sie der Gefährdung «Geldwäscherei von Fiatgeld krimineller Herkunft (in VAs)» klarer gegenüberzustellen.
[171] United Nations Security Council, *S/2022/668 Midterm report of the 1718 Panel of Experts*, September 2022, S. 75 – 78. United Nations Security Council, *S/2022/132 Report of the 1718 Panel of Experts*, März 2022, S. 80. United Nations Security Council, *S/2021/211 final report of the Panel of Experts*, März 2021, S. 56f.
[172] Financial Times, *How North Korea became a crypto crime hub*, 14. November 2022. Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, 13. Januar 2022. Coindesk, *'Ship-to-Ship' Trade and Other Secrets of North Korea's Illicit $1.5B Crypto Stash*, 7. April 2020.
[173] Chainalysis, *The 2023 Crypto Crime Report*, Februar 2023, S. 60.
[174] Für das Jahr 2021 lag das BIP der Demokratischen Volksrepublik Korea bei rund 16.4 Milliarden US-Dollar. Vgl. United Nations Data Retrieval System, *Democratic People's Republic of Korea*, zuletzt abgerufen im Mai 2023.
[175] FATF, *Press Release - Virtual Assets Contact Group (VACG)*, 14. April 2023.
[176] Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, Dezember 2021, S. 2.

lizenzierte Sportwetten-Website gewaschen hat.[177] Dasselbe Geldwäschereischema soll auch von weiteren kriminellen Organisationen wie z.B. der kalabrischen 'Ndrangheta, der neapolitanischen Camorra, aber auch von rumänischen und chinesischen OK-Gruppen angewendet worden sein.[178] Online-Casinos in Malta würden hohe GW/TF-Risiken bergen, wurde in Maltas eigener Nationalen Risikoanalyse zu VAs festgehalten.[179] In Malta sind rund 10% der weltweit existierenden Glücksspielunternehmen domiziliert.[180] Die daraus generierten Steuereinnahmen machten im Jahr 2019 rund 12% des maltesischen Bruttoinlandsprodukts aus.[181] Ein- und Auszahlungen über sogenannte E-Wallets, die typischerweise auch Transaktionen mit VAs ermöglichen, machten in den Jahren 2019 bis 2021 volumenmässig rund 10-15% der Umsätze aus.[182] Öffentlich bekannt sind auch Fälle, in denen VAs für Bestechungszahlungen, zur Finanzierung von Terrorismus durch Al-Qaïda und ISIS, aber auch beispielsweise von südamerikanischen Drogenkartellen für Geldwäschereizwecke missbraucht wurden.[183]

Der VA-Sektor hat global seit 2018 stark an Grösse und Reichweite gewonnen. Weltweit scheinen deutlich mehr Menschen VAs zu verwenden. Unklar bleibt, wie stark die kriminelle Verwendung von VAs mitgewachsen ist. Die oben ausgeführten Schätzungen sind deshalb wohl als Mindestangaben zu verstehen. Der Anstieg von Geldwäscherei-Verdachtsmeldungen in verschiedenen Ländern deutet jedoch daraufhin, dass insbesondere die Verwendung von VAs für GW/TF-Zwecke häufiger vermutet wird als noch vor einigen Jahren – wobei dieses Wachstum auch mit einer zunehmenden Regulierung und Sensibilisierung von VASPs erklärt werden kann. *Dass* es jedoch ein allgemeines Wachstum in der kriminellen Verwendung von VAs gab, wird aus den diesbezüglichen Berichten verschiedener Länder, supranationaler Organisationen und Blockchainanalyse-Unternehmen klar ersichtlich.

Zudem scheint die kriminelle Nutzung von VAs diverser geworden zu sein. VAs sind längst nicht mehr nur im Bereich Cyberkriminalität anzutreffen, sondern treten mittlerweile auch im Zusammenhang mit den verschiedensten Straftaten im «Offline»-Bereich auf. Konsolidierte Zahlen hierzu fehlen allerdings. Dadurch ist es schwierig abzuschätzen, wie häufig illegal erworbene Vermögenswerte aus diesen «traditionellen» Kriminalitätsfeldern mittels VAs gewaschen werden und wie hoch die entsprechenden Beträge sind. Diese Vorgänge zu entdecken scheint für Blockchainanalyse-Unternehmen und VASPs eine grosse Herausforderung zu sein, sodass in diesem Bereich von einer erheblichen Dunkelziffer auszugehen ist.

[177] Organized Crime & Corruption Reporting Project (OCCRP), *Italian Mafia Bets on Illegal Online Gambling*, 4. März 2021. Süddeutsche Zeitung, *Wieso die Mafia Fan von Maltas Online-Casinos ist*, 18. Dezember 2022.
[178] L'avvenire di Calabria, *Boom delle scommesse online, ma per la Dia c'è l'ombra dei clan*, 23. Januar 2020.
[179] National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (Malta), *Key Results of the Sectoral Risk Assessment on Virtual Financial Assets*, Februar 2020, S. 12.
[180] Forbes, *Scandals And Mafia Allegations May Force Malta To Reconsider Its Reliance On Online Betting*, 13. März 2021.
[181] Ibid.
[182] Malta Gaming Authority, *Annual Report 2021*, September 2022, S. 79. Forbes, *Scandals And Mafia Allegations May Force Malta To Reconsider Its Reliance On Online Betting*, 13. März 2021.
[183] Vgl. Stalinsky Steven, *The Coming Storm – Terrorists Using Cryptocurrency*, 21. August 2019. Department of Justice (USA), *Two Chinese Intelligence Officers Charged with Obstruction of Justice in Scheme to Bribe U.S. Government Employee and Steal Documents Related to the Federal Prosecution of a PRC-Based Company*, 24. Oktober 2022. Chainalysis, *The Crypto Crime Report 2022*, Februar 2022, S. 93 – 98. AP News, *Mexican cartels turn to bitcoin, internet, e-commerce*, 10. März 2022. Europol, *Underground drug-money bank laundering EUR 180 million liquidated by law enforcement*, 13. April 2023.

Gefährdung 5

Geldwäscherei von Fiatgeld krimineller Herkunft (in VAs) (2018 identifiziert, 2023 unverändert)[184]

Im sektoriellen Bericht von 2018 wurden zwei Gefährdungen im Zusammenhang mit der Verwendung von VAs für Geldwäschereizwecke identifiziert: Einerseits das Waschen von VAs krimineller Herkunft (zum Beispiel aus einem Hack einer VA-Börse) und andererseits das Waschen von Fiatgeld krimineller Herkunft. Für die erste Gefährdung liegen konkrete Zahlen von Blockchainanalyse-Unternehmen vor, die zeigen, dass sich diese Gefährdung seit 2018 erhöht hat (vgl. Gefährdung 4 in Kapitel 6.4). Für die zweite Gefährdung fehlen konsolidierte Zahlen, die auf ihre Ver- oder Entschärfung schliessen lassen. Vereinzelte Erkenntnisse zur Verwendung von VAs für Geldwäschereizwecke durch kriminelle Organisationen zeigen jedoch, dass sich diese Gefährdung zumindest nicht entschärft hat. Die Gefährdung besteht unverändert.

[184] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 30f. Hinweis: Die im Jahr 2018 betitelte Gefährdung «Investition von Geldern krimineller Herkunft in Krypto-Assets» wurde zur Verdeutlichung «Geldwäscherei von Fiatgeld krimineller Herkunft (in VAs)» umbenannt.

7. Risikoentwicklung Schweiz

Gefährdungen in Verbindung mit VAs und diesbezügliche Verwundbarkeiten der Schweiz wurden bereits im sektoriellen Bericht zu den GW/TF-Risiken im VA-Bereich von 2018 identifiziert, wobei die Gefährdungen in zwei grundlegende Kategorien eingeteilt wurden: Untrennbar mit der VA-Technologie verbundene Gefährdungen einerseits sowie Gefährdungen durch die betrügerische Verwendung von VAs für andererseits.[185]

Untrennbar mit VA-Technologien verbundene **Gefährdungen**	**Gefährdungen** durch die betrügerische Nutzung von VAs	**Verwundbarkeiten** der Schweiz angesichts der Gefahr der Geldwäscherei und Terrorismusfinanzierung durch VAs
1. Anonymität der Transaktionen und schwierige Identifikation der wirtschaftlich Berechtigten 2. Sicherheitslücken in den zugrundeliegenden VA-Technologien 3. Gefährdungen in Verbindung mit dem Neuigkeitseffekt und der Unerfahrenheit der Nutzer 4. Malware und Ransomware 5. Geldwäscherei von VAs krimineller Herkunft (in Fiatgeld)	1. Terrorismusfinanzierung mittels VAs 2. VAs als Zahlungsmittel für illegale Güter und Dienstleistungen 3. Rückgriff auf VAs bei Phishing-Attacken 4. Geldwäscherei von Fiatgeld krimineller Herkunft (in VAs)	1. Verwundbarkeiten von Finanzinter-mediären, die VA-Transaktionen durchführen 2. Schwierige Repression von GW/TF im VA-Bereich

Abbildung 15: KGGT-Bericht 2018: Identifizierte Gefährdungen und Verwundbarkeiten im Zusammenhang mit VAs[186]

Um einen Vergleich mit den Ergebnissen von 2018 zu ziehen, werden im vorliegenden Kapitel die für die GW/TF-Bekämpfung im VA-Bereich massgeblichen Veränderungen für die Schweiz herausgearbeitet. Dadurch kann geprüft werden, inwiefern sich die 2018 identifizierten Gefährdungen und Verwundbarkeiten geändert haben oder neue hinzugekommen sind. Für den exakten Nachweis solcher Veränderungen braucht es idealerweise statistische Angaben

[185] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 20 – 36.

[186] Ibid. Hinweis: Die im Jahr 2018 betitelte Gefährdung «Waschen von illegal erworbenen Krypto-Assets» wurde zur Verdeutlichung «Geldwäscherei von VAs krimineller Herkunft (in Fiatgeld)» umbenannt. Die Gefährdung «Investition von Geldern krimineller Herkunft in Krypto-Assets» wurde zur Verdeutlichung «Geldwäscherei von Fiatgeld krimineller Herkunft (in VAs)» umbenannt. Zudem wurde die im Jahr 2018 betitelte Verwundbarkeit «Finanzintermediäre, die Kryptotransaktionen durchführen» umbenannt zu «Finanzintermediäre, die VA-relevante Transaktionen durchführen (in VAs oder Fiat)», um die Erweiterung dieser Verwundbarkeit erkenntlich zu machen (vgl. Verwundbarkeit 6).

zu den spezifischen Phänomenen. Dies gestaltet sich aufgrund des erheblichen Datenmangels in diesem Bereich als sehr schwierig, was bereits ein Risiko an sich darstellt (vgl. Kapitel 7.1).

Der wichtigste Datenbestand, der im Rahmen der vorliegenden Risikoanalyse für den Nachweis solcher Veränderungen ausgewertet wurde, waren die bei der Meldestelle für Geldwäscherei (MROS) eingereichten Verdachtsmeldungen sowie weitere ihr zur Verfügung stehende Daten. Zu den letzteren gehören insbesondere auch die Erkenntnisse aus dem Informationsaustausch mit ausländischen Meldestellen. Ausgewertet wurden hierfür Informationsanfragen und Spontaninformationen von ausländischen Meldestellen, die an die Schweiz gerichtet wurden und einen Zusammenhang mit VAs oder VASPs aufwiesen. Um sämtliche ihr zur Verfügung stehenden Daten vertieft zu analysieren, konnte die MROS im Rahmen dieser Risikoanalyse erfolgreich neue Auswertungsmethoden verwenden, die seit der Einführung des Datenverarbeitungssystems goAML nun möglich sind (vgl. Kapitel 11.1). Die Auswertungen zeigen unter anderem deutlich auf, dass VAs seit 2020 immer häufiger Bestandteil von Verdachtsmeldungen sind.

Zudem wurde im Rahmen der Durchführung der vorliegenden Risikoanalyse sowie der Beantwortung der Postulate 22.3017 (*Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen*) und 22.3145 (*Wie fit sind die Kantone in der Cyber-Strafverfolgung?*) eine Umfrage bei den verschiedenen kantonalen (und städtischen) Polizeien und Staatsanwaltschaften durchgeführt.[187] Verlangt wurden dabei einerseits quantitative Angaben zu bereits geführten Strafverfahren mit VA-Bezügen (beispielsweise die Anzahl Verfahren, die involvierten Straftaten und Summen, usw.). Andererseits wurden die Adressaten gebeten, qualitative Einschätzungen zu den Herausforderungen und Chancen im VA-Bereich für die Arbeit der Strafverfolgungsbehörden zu liefern. Mangels eines Monitorings von VA-relevanten Strafverfahren war nur eine kleine Minderheit der angefragten Strafverfolgungsbehörden in der Lage, konsolidierte Angaben zu liefern. Die quantitativen Ergebnisse aus der Umfrage sind entsprechend fragmentiert und nur begrenzt aussagekräftig. Sie ersetzen nicht den Bedarf an einer schweizweiten Übersicht. In ihrer Gesamtheit scheinen die erhaltenen Angaben jedoch bestimmte Annahmen und Trends zu bestätigen, was die kriminelle Verwendung von VAs sowie die damit verbundene Arbeit der Strafverfolgungsbehörden betrifft (vgl. Kapitel 7.2 bis 7.4). Ergänzend zu den erhaltenen Antworten der Strafverfolgungsbehörden im Rahmen der genannten Umfrage wurden mit verschiedenen Schweizer Strafverfolgungs- und Aufsichtsbehörden vertiefte Gespräche geführt.

Weitere quantitative Erkenntnisse konnten durch die Auswertung weiterer einzelner Datenbestände schweizerischer Strafverfolgungsbehörden gewonnen werden. Zu den letzteren gehören insbesondere die Datenbank PICSEL (interkantonale Datenbank für Strafanzeigen im Bereich Cyberkriminalität) sowie die bisherig von der Bundeskriminalpolizei geführten (Vor-)Ermittlungen, bei denen die Verwendung von VAs ein zentrales Element des Sachverhalts darstellte und letztendlich in Verfahrenseröffnungen mündeten. Nebst der durchgeführten Umfrage bei kantonalen Strafverfolgungsbehörden waren die Erkenntnisse der Bundeskriminalpolizei am Ergiebigsten, weshalb in diesem Kapitel häufig auf sie verwiesen wird. Basierend auf den Informationen, die der Meldestelle für Geldwäscherei vorliegen, war es zudem möglich, qualitativ begründete Typologien zu erstellen, die verschiedene mögliche Ausprägungen und Merkmale von GW/TF-Handlungen mittels VAs beispielhaft aufzeigen. Diese basieren hauptsächlich auf Verdachtsmeldungen, welche bei der Meldestelle für Geldwäscherei in den Jahren 2020 bis 2022 eingereicht wurden. Sie veranschaulichen unterschiedliche Techniken, die zur Geldwäscherei oder Terrorismusfinanzierung eingesetzt werden.

[187] Vgl. 22.3145 (Postulat), *Wie fit sind die Kantone in der Cyber-Strafverfolgung?*, eingereicht von der Sicherheitspolitischen Kommission des Nationarats am 15. Februar 2022. 22.3017 (Postulat), *Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen*, einigereicht von Nationalrat Andri Silberschmidt am 16. März 2022. Beide Postulate wurden im Juni 2022 vom Nationalrat angenommen. Zuständig für die Beantwortung der zwei Postulate ist das Eidgenössische Justiz- und Polizeidepartement (EJPD).

7.1 Datenmangel als inhärentes Risiko

Während bereits nur sehr wenige Angaben zur allgemeinen Verwendung von VAs in der Schweiz existieren, spitzt sich diese Problematik bei Angaben zur kriminellen Verwendung von VAs in der Schweiz nochmals zu: Für die Schweiz existieren nur vereinzelt aggregierte statistische Daten zur Verwendung von VAs bei Straftaten im Allgemeinen. Umso weniger liegen quantitative Angaben zur spezifischen Verwendung von VAs für Geldwäscherei oder Terrorismusfinanzierung vor. Auch zu Rechtshilfegesuchen aus dem Ausland, deren Sachverhalt Bezüge zu VAs aufweisen, existiert keine schweizweite Übersicht. Die Frequenz solcher Gesuche sowie die damit verbundenen Herausforderungen für Strafverfolgungsbehörden bleibt damit unklar.

Die mangelnden Zahlen zu VA-relevanten Finanzflüssen – wozu auch Fiat-Finanzflüsse gehören können – sind keine nationale Besonderheit. Da VA-Zahlungen im Unterschied zum traditionellen Zahlungsverkehr grundsätzlich anonym (bzw. pseudonym) abgewickelt werden, ist es schwierig, die Standorte der beteiligten Parteien zu bestimmen. Daher ist es kompliziert, präzise Aussagen über die Nutzung von VAs in einem spezifischen geographischen Bereich wie der Schweiz zu machen. Die Behauptung, dass Blockchains "transparent" sind, ist folglich nur teilweise wahr. Auch Aussagen zum tatsächlichen Volumen von VAs sind nur begrenzt möglich, da die meisten VA-Transaktionen *off-chain* stattfinden und nicht auf der Blockchain (*on-chain*) registriert werden.[188] So sind beispielsweise sämtliche interne Transaktionen von VASPs häufig *off-chain*. Zusätzlich zur Haupt- oder «Basis»-Ebene von Blockchains, die öffentlich einsehbar ist, existieren überdies sogenannte *Second-Layer*-Protokolle. Diese sind zusätzliche Ebenen, die auf der ursprünglichen Blockchain aufbauen und dazu dienen, die Skalierbarkeit zu verbessern und Transaktionskosten zu senken. Ein gängiges Beispiel für ein solches Protokoll ist das Lightning Network im Bitcoin-Ökosystem. Transaktionen, die auf diesen Second-Layer-Protokollen durchgeführt werden, erscheinen nicht unmittelbar oder in voller Detailtiefe auf der Blockchain. Deshalb tragen sie zur Komplexität und Intransparenz des gesamten Systems bei und erschweren die Nachverfolgung von VA-Finanzflüssen. Einige Schätzungen gehen davon aus, dass letztlich nur rund ein Zehntel aller tatsächlich abgewickelten VA-Transaktionen *on-chain* registriert werden.[189] Der Grossteil der Informationen über VA-Transaktionen ist folglich auf verschiedenen privaten Datenbanken diverser Unternehmen gespeichert. Demzufolge haben grosse zentralisierte VA-Börsen wahrscheinlich am ehesten einen Überblick über weltweite Finanzflüsse im Zusammenhang mit VAs. Diese Daten werden aber nicht veröffentlicht.

Trotz dieser Herausforderungen bedeutet die Existenz von *off-chain*-Transaktionen und *Second-Layer*-Protokollen nicht, dass Strafverfolgungsbehörden im Dunkeln tappen. Es erfordert zwar zusätzlichen Aufwand und Ressourcen, die verschlungenen Pfade von Transaktionen zu verfolgen, aber es ist nicht unbedingt unmöglich. Die grundlegende Transparenz des Systems bleibt erhalten, auch wenn sie durch zusätzliche Schichten komplizierter wird. Daher ist es für Strafverfolgungsbehörden noch immer machbar, kriminelle Aktivitäten aufzudecken, allerdings sind hierfür entsprechende Kapazitäten und Ressourcen notwendig, da die Arbeit geeignetes Fachwissen und Ermittlungsinstrumente erfordert und zeitintensiv sein kann. Die Transparenz von Blockchains ist also nicht verloren, sie ist aber schwieriger zu durchdringen und erfordert entsprechend angepasste Untersuchungsmethoden.

Das genaue Ausmass der Verwendung von VAs für einzelne Weltregionen und Länder lässt sich folglich nur schwer messen. Auf diese Problematik haben auch bereits der Internationale Währungsfonds (IWF) sowie die Europäische Zentralbank (EZB) hingewiesen. Bereits 2019 schlug der IWF in diesem Zusammenhang einen internationalen Austausch statistischer Daten

[188] Jimenez Alison, *3 Misconceptions about Cryptocurrency Crime Estimates*, 11. Januar 2022.
[189] Von Luckner, Reinhart & Rogoff, *Decrypting New Age International Capital Flows, NBER Working Paper No. 29337*, Oktober 2021, S. 1, Fussnote Nr. 2.

bezüglich VA-Transaktionen und -Kapitalisierung vor, um die mangelhafte Verfügbarkeit dieser Daten zu beheben und aussagekräftige makroökonomische Einschätzungen zu ermöglichen.[190] Auch die EZB empfahl ein intensives Monitoring der Entwicklungen und wies auf die mangelnde Verfügbarkeit zuverlässiger statistischer Daten zur tatsächlichen Grösse des VA-Sektors sowie den mit VAs verbundenen Finanzflüssen.[191] Diese Empfehlungen wurden bisher jedoch nicht umgesetzt. Stand 2022 hielt der IWF fest, dass es aufgrund erheblicher Datenlücken – welche überdies auch die Risikoanalysen von Behörden erschweren würden – immer noch schwierig sei, den vollen Umfang der Nutzung von VAs im Finanzsystem zu beurteilen.[192] Derzeit scheint es noch keinen Konsens zu geben, wie unterschiedliche Arten von VAs kategorisiert werden sollen und welche Messtechniken verwendet werden können, um die wirtschaftlichen Aktivitäten sowie die Finanzflüsse des im Kern globalen VA-Sektors unter dem Blickwinkel einzelner Länder zu untersuchen. Zudem bestehe laut dem IWF laufend die Möglichkeit, dass sektorspezifische Empfehlungen aufgrund der raschen Entwicklungen im VA-Bereich schnell veraltet sein könnten.

Auf den Mangel an verlässlichen Daten zum VA-Sektor wiesen bereits der 2018 erschienene KGGT-Bericht über das «Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding» sowie[193] der Ende 2021 erschienene zweite nationale Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung.[194] Auch der vorliegende Bericht hält fest, dass insbesondere für die Schweiz keine zuverlässigen Zahlen existieren.

Abklärungen bei verschiedenen schweizerischen Behörden und Organisationen zeigen auf, dass derzeit kein Monitoring existiert, welches Aufschluss über das Wachstum des Sektors, über die in der Schweiz versteuerten Einkommen und Vermögen in Kryptowährungen, oder über die Frequenz und Grösse der Finanzflüsse gibt, die auf den Finanzplatz Schweiz gelangen oder diesen verlassen, und in Verbindung mit dem Kauf, Verkauf, oder der Verwahrung von VAs stehen. Ebenso ist auf nationaler Ebene derzeit kein derartiges Monitoring in Planung.[195] Dieser Informationsmangel hat sich angesichts der rasanten Entwicklungen im VA-Bereich während der letzten Jahre zu einer erheblichen Verwundbarkeit entwickelt, da unerwartete Entwicklungen im GW/TF-Bereich für längere Zeit unentdeckt bleiben könnten.

Verwundbarkeit 4

Unzureichende Zahlen und Statistiken auf nationaler und internationaler Ebene (2023 identifiziert)

Angesichts der rasanten Entwicklungen in den vergangenen fünf Jahren kann sich der Mangel an flächendeckenden Daten auf nationaler und internationaler Ebene als problematisch erweisen der Seit der Entstehung von Bitcoin, der ältesten Kryptowährung, sind bereits rund 15 Jahre vergangen. Die Schweiz und das Crypto Valley haben international einen Ruf als regulatorisch «sicherer Hafen», nicht zuletzt aufgrund der im internationalen Vergleich relativ zügig voranschreitenden Anstrengungen, Rechtssicherheit bezüglich des Umgangs mit der

[190] International Monetary Fund (IMF), *Treatment of Crypto Assets in Macroeconomic Statistics*, 2019, S. 3.
[191] European Central Bank (ECB), *Understanding the crypto-asset phenomenon, its risks and measurement issues*, Mai 2019.
[192] International Monetary Fund (IMF), *F.18 Recording of Crypto Assets in Macroeconomic Statistics*, März 2022, S. 40.
[193] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 35f.
[194] KGGT, *Zweiter nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung*, Oktober 2021, S. 52.
[195] Die Meldestelle für Geldwäscherei befragte dafür die Eidgenössische Finanzmarktaufsicht FINMA, das Bundesamt für Statistik BFS, die Schweizerische Nationalbank SNB, das Staatssekretariat für internationale Finanzfragen SIF, die Eidgenössische Steuerverwaltung ESTV sowie neun kantonale Steuerbehörden.

Kryptobranche zu schaffen. Gleichzeitig fehlen flächendeckende Zahlen, wie beispielsweise die VA-relevanten Finanzflüssen, die auf den Finanzplatz Schweiz gelangen oder diesen verlassen. Daten aus dem Bereich der Blockchainanalyse bilden nicht die einzigen Quellen, auf deren Basis Informationen über die Verwendung von VAs für GW/TF-Zwecke erlangt werden können. So können beispielsweise auch Informationen aus dem traditionellen Zahlungsverkehr, aus Handelsregistern, Steuerunterlagen, von verschiedenen Aufsichtsorganen und öffentlichen Quellen dabei helfen, das GW/TF-Abwehrdispositiv in Bezug auf VAs zu beurteilen und zu stärken. Sämtliche Behörden, Stakeholder sowie weitere involvierte Akteure benötigen diese Informationen, um bei ihrer Arbeit sachkundige Entscheidungen koordiniert zu fällen und entsprechende Schwerpunkte setzen zu können. Dieser allgemeine Informationsmangel erhöht das Risiko, dass unerwartete Entwicklungen für längere Zeit unentdeckt bleiben und den Finanzplatz Schweiz sowie weitere internationale Finanzzentren abrupt wirtschaftlich und politisch exponieren.

7.2 Steigende Risiken bei steigender Verwendung

Mit der deutlichen Zunahme in der Verwendung von VAs sind auch die GW/TF-Risiken gestiegen, wie ein Einblick in die Daten der MROS sowie schweizerischer Strafverfolgungsbehörden zeigt.

Schweizerische Strafverfolgungsbehörden und die MROS sind bei ihrer Arbeit immer häufiger mit Fällen konfrontiert, die in Verbindung mit der Verwendung von VAs stehen. So sind Informationen, die die MROS von schweizerischen Finanzintermediären oder ausländischen *Financial Intelligence Units* (FIUs) erhält, seit Beginn des Jahres 2020 immer öfter «VA-relevant»[196], beziehen sich folglich zunehmend auf Sachverhalte oder verdächtige Transaktionen, die in Verbindung mit der Verwendung von VAs stehen.

Eine VA-Relevanz kann sowohl bei Verdachtsmeldungen von Finanzintermediären mit als auch ohne VASP-Tätigkeit vorliegen. Eine Verdachtsmeldung wurde als VA-relevant eingestuft, wenn mindestens eines von zwei Szenarien auf die Meldung zutraf:

- Einerseits, wenn die Verdachtsmeldung VA-relevante Transaktionen enthielt; das heisst, wenn Verdachtsmeldungen Transaktionen zwischen den dabei gemeldeten Konten und Konten von Finanzintermediären mit VASP-Tätigkeit beinhalteten (Meldungen von FIs ohne VASP-Tätigkeit) *oder* die gemeldeten Transaktionen in VAs denominiert waren (Meldungen von FIs mit VASP-Tätigkeit).
- Andererseits, wenn aufgrund des vom meldenden Finanzintermediär schriftlich geschilderten Sachverhalts ein klarer Zusammenhang mit VAs bestand, selbst wenn auf den gemeldeten Konten keine relevanten Transaktionen im obigen Sinne festgestellt werden konnten.

VA-relevante Verdachtsmeldungen haben einerseits in Bezug auf ihre Anzahl deutlich zugenommen, andererseits ist ihr Anteil an sämtlichen in diesem Zeitraum erhaltenen Verdachtsmeldungen deutlich gestiegen.

Ebenfalls intensiviert hat sich der Austausch von VA-relevanten Informationen mit ausländischen Meldestellen sowie die Übermittlung von VA-relevanten MROS-Informationen an schweizerische Strafverfolgungsbehörden. Letztere verzeichneten seit 2020 ebenfalls eine deutliche Zunahme an Strafanzeigen und -Verfahren, deren Sachverhalt Bezüge zu VAs aufwiesen.

[196] Für eine detaillierte Beschreibung der Auswertungsmethode, vgl. Kapitel 11.1.

7.2.1 Zunahme von VA-relevanten Verdachtsmeldungen

Für das Jahr 2020 konnten 5.8% aller erhaltenen Verdachtsmeldungen als VA-relevant eingestuft werden. Bis im Jahr 2022 hat sich ihr Anteil mehr als verdoppelt (13.8%). Für den Zeitraum 2020 bis 2022 waren 10% aller Meldungen VA-relevant.

	2020	**2021**	**2022**	**2020-2022** (Summe)
Verdachtsmeldungen (Jahresbestand)	5'334	5'964	7'639	18'937
VA-relevante Verdachtsmeldungen (in % des Jahresbestands)	312 (5.8%)	499 (8.4%)	1056 (13.8%)	1867 (9.9%)

Abbildung 16: VA-relevante Verdachtsmeldungen im Verhältnis zum Jahresbestand sämtlicher Verdachtsmeldungen

Die Aussagekraft dieser Informationen muss allerdings relativiert werden. Beispielsweise beziehen sich Erkenntnisse über erhaltene Verdachtsmeldungen zur Verwendung von VAs für GW/TF-Zwecke eben nur auf die *erhaltenen* Verdachtsmeldungen von Finanzintermediären. Dabei bleibt offen, inwiefern die daraus gewonnenen Erkenntnisse repräsentativ für die tatsächliche Verwendung von VAs für GW/TF-Zwecke in der Schweiz sind. Insbesondere aufgrund der Tatsache, dass VA-Transaktionen grundsätzlich direkt zwischen Nutzern abgewickelt werden können und somit nur teilweise in den Bereich der Finanzintermediation – und erst dadurch in den Anwendungsbereich des GwG – fallen, muss davon ausgegangen werden, dass die diesbezügliche Dunkelziffer erheblich ist.

7.2.2 Intensivierung des FIU-Informationsaustauschs

Ein weiterer Zweig der Tätigkeit de MROS ist der Informationsaustauch mit ausländischen Financial Intelligence Units (FIUs). Dabei sind zwei unterschiedliche Kontaktaufnahmen aus dem Ausland mit der MROS möglich. Einerseits sind dies Anfragen, welche aus dem Ausland an die MROS gerichtet werden oder sogenannte Spontaninformationen, welche ohne Aufforderung an die MROS gesendet werden und für die Schweiz von Relevanz sein könnten. Bei diesem Informationsverkehr ist es ebenfalls möglich, die Informationen auf ihre VA-Relevanz auszuwerten. Dabei wird dieselbe Methode wie bei den Verdachtsmeldungen verwendet.

	2020	**2021**	**2022**
FIU Informationen (Anfragen oder Spontaninformationen)	1397	1312	1557
Davon mit VA-Bezug	18	42	132
Prozentualer Anteil mit VA-Bezug	1.3%	3.2%	8.5%

Abbildung 17: FIU-Informationen mit einem VA-Bezug in den Jahren 2020 bis 2022

Seit 2020 haben VA-Bezüge im Informationsaustausch mit ausländischen FIUs an Bedeutung gewonnen, wenn auch weniger stark als beiden in diesem Zeitraum erhaltenen Verdachtsmeldungen. Mindestens jede zwölfte Auslandinformation die bei der MROS im Jahr 2022 eingegangen ist, wies einen VA-Bezug auf.

7.2.3 Übermittlungen von VA-relevanten Informationen an Strafverfolgungsbehörden haben zugenommen

Die MROS analysiert die Informationen aus sämtlichen erhaltenen Verdachtsmeldungen. Sie entscheidet, ob Informationen aus diesen Meldungen an eine Schweizer Strafverfolgungsbehörde übermittelt werden. Letztere sind mit dem Anstieg VA-relevanter Verdachtsmeldungen immer häufiger mit Übermittlungen VA-relevanter Informationen konfrontiert, insbesondere die kantonalen Staatsanwaltschaften Aargau, Bern, Genf, Waadt und Zürich sowie die Bundesanwaltschaft. Allerdings zeigt sich, dass seit 2020 bereits beinahe alle kantonalen Staatsanwaltschaften Empfänger von VA-relevanten Informationen waren und auch hier diese Übermittlungen in der Tendenz zugenommen haben.

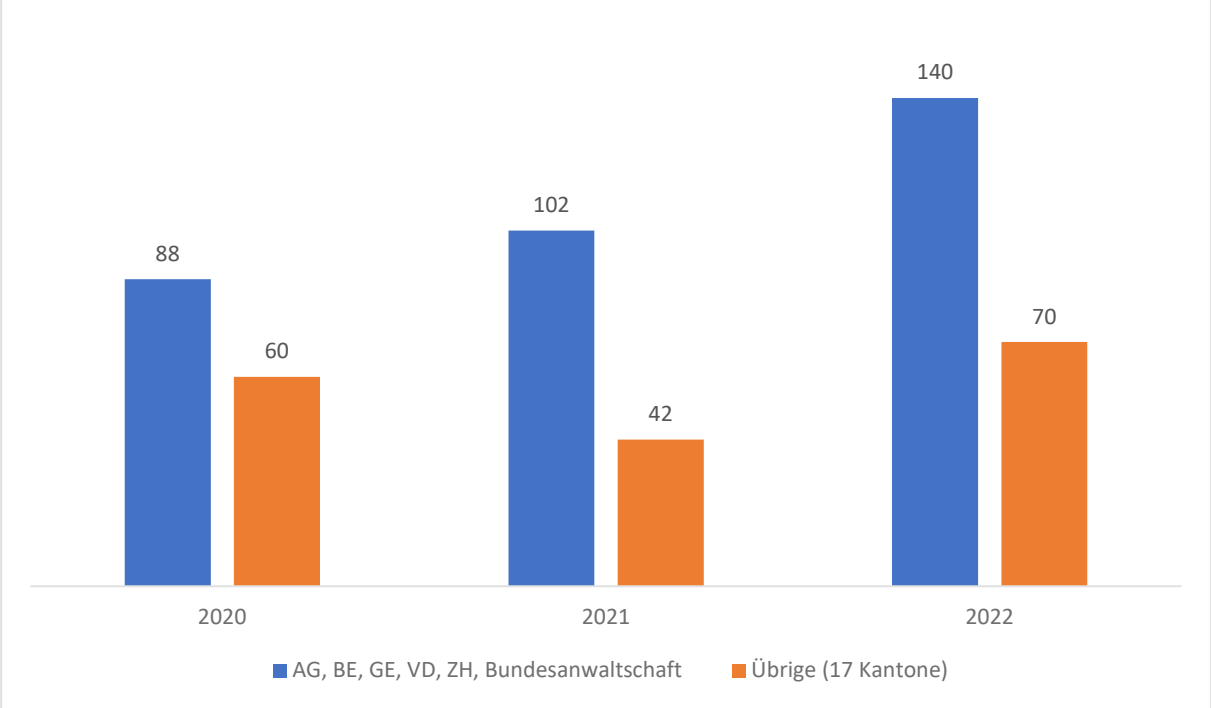


Abbildung 18: Anzahl Übermittlungen VA-relevanter Informationen an die verschiedenen kantonalen Staatsanwaltschaften sowie an die Bundesanwaltschaft (CH), 2020 – 2022

7.2.4 Zunahme von VA-relevanten Strafverfahren

Gemäss den eingeholten Informationen erfasst die Mehrheit der Schweizer Polizeien und Staatsanwaltschaften in ihren Strafverfahren die Verwendung von Kryptowährungen nicht systematisch, so dass hierzu keine nationale Übersicht existiert. Zwischen 2020 und 2022 sind jedoch die schweizweit polizeilich registrierten Straftaten im Bereich der digitalen Kriminalität

um 37% auf 33 345 Straftaten angestiegen (91 pro Tag).[197] 89% (29 677) dieser Straftaten wurden dem Bereich «Cyber-Wirtschaftskriminalität» zugeordnet sowie 67% (22 207) der entsprechenden Unterkategorie «Cyberbetrug».[198] Hierbei kann gemäss den geführten Gesprächen mit verschiedenen Strafverfolgungsexperten davon ausgegangen werden, dass die Involvierung von VAs in irgendeiner Form bei diesen Straftaten sehr häufig festzustellen sei.[199] Bei bestimmten Straftaten im Bereich Cyber-Wirtschaftskriminalität – etwa bei Ransomware- bzw. Erpressungsfällen sowie im Bereich des Online Anlagebetrugs – seien VAs in der Regel in irgendeiner Phase fast immer involviert.[200]

Verschiedene Erhebungen und Auswertungen von Daten schweizerischer Strafverfolgungsbehörden scheinen ebenfalls zu bestätigen, dass die Anzahl Strafverfahren in der Schweiz, die mit VAs in einem Zusammenhang stehen, seit 2018 deutlich zugenommen hat. Überdies enthalten die Erhebungen auch Hinweise, dass die dabei involvierten Summen bedeutend sind und seit 2018 einen Aufwärtstrend aufweisen. Zuletzt sind die dabei im Vordergrund stehenden Straftaten mehrheitlich dem Bereich der Cyber-Wirtschaftskriminalität zuzuordnen. Dies deutet darauf hin, dass von diesen Straftaten die grösste Gefährdung für nachgelagerte Geldwäschereidelikte im Zusammenhang mit der kriminellen Verwendung von VAs ausgeht.

Die erhaltenen Antworten aus der Umfrage bei Schweizer Strafverfolgungsbehörden scheinen diesen Trend zu bestätigen.[201] So wurden beispielsweise allein von sieben kantonalen Staatsanwaltschaften seit 2018 insgesamt 119 Strafverfahren geführt, bei denen VAs eine wichtige Rolle spielten. In mehr als einem Drittel (45) dieser Strafverfahren ging es um Straftatbestände im Bereich der Geldwäscherei, deren Vortaten, der organisierten Kriminalität oder der Terrorismusfinanzierung. Aufgrund der lediglich vereinzelten Rückmeldungen muss davon ausgegangen werden, dass die tatsächliche Anzahl VA-relevanter Strafverfahren seit 2018 deutlich höher liegt. Bei den sieben antwortenden kantonalen Staatsanwaltschaften handelt es sich namentlich lediglich um jene, die überhaupt über konsolidierte Zahlen verfügten. Insbesondere die Angaben von Staatsanwaltschaften mehrerer bevölkerungsreicher Kantone waren dabei nicht enthalten.

Lediglich sechs kantonale Staatsanwaltschaften konnten Angaben zu den bei diesen Verfahren gegenständlichen Straftaten liefern. Nebst Verstössen gegen das Betäubungsmittelgesetz sind diese Straftaten beinahe ausschliesslich im Bereich der Cyber-Wirtschaftskriminalität zu verorten, wobei Betrug (Art. 146 StGB) und betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB) am häufigsten genannt wurden. Zu den bei VA-relevanten Strafverfahren involvierten Beträgen konnten lediglich drei kantonale Staatsanwaltschaften konkrete Angaben liefern. Demzufolge war bei den in diesen drei Kantonen geführten VA-relevanten Strafverfahren seit 2018 eine Gesamtsumme von über 130 Millionen Schweizerfranken involviert, wobei davon allerdings über 100 Millionen einem einzigen Verfahren zuzuordnen sind. Die jährlichen Gesamtsummen sind dabei seit 2018 im Aufwärtstrend. Zwar konnten lediglich drei kantonale Staatsanwaltschaften konkrete Angaben zu den involvierten Beträgen liefern, aber weitere Auswertungen aus Datenbeständen anderer Kantone zeichnen dasselbe Bild.

---

[197] Frühere Zahlen zum Bereich «digitale Kriminalität» existieren nicht, da diese erstmals in der PKS des Geschäftsjahres 2020 veröffentlicht wurden. Vgl. Bundesamt für Statistik (BFS), *Polizeiliche Kriminalstatistik (PKS) – Jahresbericht 2021*, März 2022, S. 58. Ebenso: Bundesamt für Statistik (BFS), *Polizeiliche Kriminalstatistik (PKS) – Jahresbericht 2022*, März 2023, S. 60.

[198] Ibid. (Jahresbericht 2022), S. 58 – 60.

[199] Zusammengefasst werden unter dieser Kategorie insgesamt 12 unterschiedliche Tatvorgehen, z.B. CEO-Betrug, Betrügerische Internetshops, Online Anlagebetrug, Romance Scam, etc., ibid., S. 60.

[200] Vgl. z.B. auch Nationales Zentrum für Cybersicherheit (NCSC), *Halbjahresbericht 2022/II (Juli – Dezember)*, Mai 2023, S. 9.

[201] Die Umfrage wurde federführend von der Bundeskriminalpolizei zwischen Februar und April 2023 durchgeführt. Angefragt wurden unter anderem sämtliche kantonalen Polizeien und Staatsanwaltschaften.

Namentlich geht dies auch aus einer Auswertung der Datenbank PICSEL hervor. PICSEL (Plateforme d'Information de la Criminalité Sérielle En Ligne) ist eine interkantonale Datenbank zur Erfassung von Anzeigen im Bereich digitalen Kriminalität mit dem Ziel, Vorfälle und Schadenssummen zentral zu erfassen, und die Priorisierung und Koordination der Strafverfolgungsbehörden im Kampf gegen Cyberkriminalität zu fördern. Hierbei werden die bei den teilnehmenden kantonalen Strafverfolgungsbehördenerstatteten Anzeigen im Bereich der Cyberkriminalität in PICSEL erfasst.[202] Im Zuge dessen werden die Anzeigen unter anderem nach Phänomenen (bspw. Ransomware, Online-Anlagebetrug, Romance Scam, usw.) und Schadenssummen (bspw. aus einer Wallet gestohlene Kryptowährungen, entwendete Fiatwährungen aus einem E-Banking-Zugang via Phishing oder Hacking, Bezahlung mittels Prepaidkarten bei Ransomware Attacken, usw.) kategorisiert. Zudem existiert ein Pilotprojekt, das auf der Funktionsweise von PICSEL basiert, sich aber ausschliesslich dem Thema Online-Anlagebetrug widmet und sämtliche Kantone der Schweiz einbezieht.

Die teilnehmenden Kantone nutzen die Datenbank PICSEL unterschiedlich. Gewisse kantonale Strafverfolgungsbehörden erfassen beispielsweise keine Daten zu den bei ihnen eingegangenen Anzeigen, sondern nutzen die Plattform lediglich zur Recherche und Kooperation mit anderen kantonalen Strafverfolgungsbehörden. Obwohl diese Daten folglich nur einen partiellen Überblick erlauben, zeigt eine Auswertung repräsentativ das Wachstum der Ver- wie auch der Entwendung von VAs im Bereich der digitalen Kriminalität in der Schweiz auf. Verglichen mit anderen Zahlungsformen hat die Ver- und Entwendung von VAs seit 2020 nicht nur in absoluten Zahlen, sondern auch anteilsmässig an der Gesamtschadenssumme stark zugenommen. Zwischen 2020 und 2021 hat sich die durch Entwendung von VAs entstandene finanzielle Schadenssumme seitens der Anzeigeerstatter verdreifacht. Verglichen mit dem Jahr 2020 hat sich sowohl für 2021 als auch für 2022 der prozentuale Anteil von entwendeten VAs an der Gesamtschadenssumme sämtlicher in PICSEL registrierter Anzeigen deutlich erhöht.

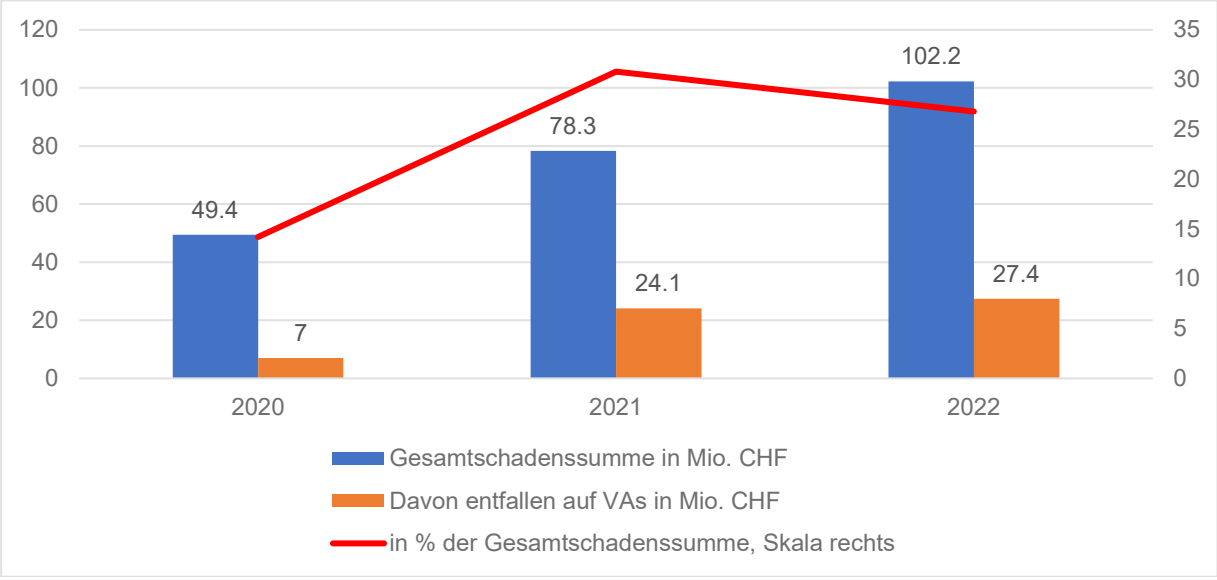


Abbildung 19: Nominale und prozentuale Zunahme der VA-Schadenssumme der in PICSEL registrierten Anzeigen gegenüber 2020

Während der letzten Jahre scheint unter den registrierten Phänomenen die Ver- bzw. Entwendung von VAs am stärksten im Zusammenhang mit Online-Anlagebetrug angestiegen

[202] Die Datenbank ist seit April 2021 operativ und wird bisher von den neun Kantonen Aargau, Fribourg, Genf, Graubünden, Jura, Neuenburg, Tessin, Waadt, Wallis genutzt. Mindestens ein weiterer Kanton wird demnächst hinzustossen (Stand Mai 2023).

zu sein. Zwar machte ihr Anteil im Jahr 2020 bereits rund ein Viertel der Gesamtschadenssumme aus, stieg bis Ende 2022 jedoch sogar auf über die Hälfte der Gesamtschadenssumme an.

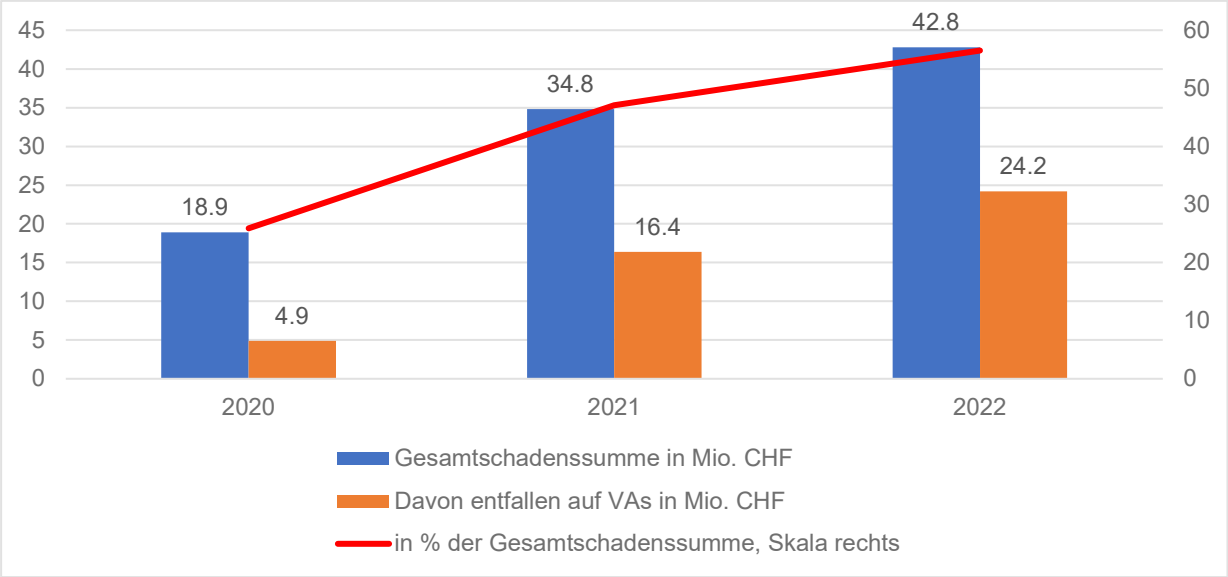


Abbildung 20: Nominale und prozentuale Zunahme der VA-Schadenssumme im Zusammenhang mit Online-Anlagebetrug gegenüber 2020

Obwohl anhand der hier präsentierten Zahlen keine abschliessende Bewertung möglich ist, scheinen diese klar aufzuzeigen, dass die kriminelle Verwendung von VAs in der Schweiz seit 2018 zugenommen hat.

Gemäss Informationen der verschiedenen angefragten Strafverfolgungsbehörden sei Geldwäscherei als nachgelagerte Straftat zwar eine logische Folge der meisten von ihnen untersuchten Fälle, da die durch Straftaten erlangten VAs gewaschen werden müssen. Konsolidierte Erkenntnisse zu nachgelagerten Geldwäschereihandlungen in Zusammenhang mit den von ihnen untersuchten Straftaten – egal, ob dabei der Erlös in Fiatwährung oder VAs denominiert war – scheinen bei den Strafverfolgungsbehörden nicht vorzuliegen. Fundierte Informationen zu diesen Geldwäschereihandlungen fehlen jedoch insbesondere, da der Ermittlungsfokus der Strafverfolgungsbehörden meist auf die Aufklärung der angezeigten Straftaten sowie auf eine mögliche Restituierung der gestohlenen Gelder der Opfer gerichtet ist, während die mutmasslichen Täter in der Regel im Ausland zu verorten sind und ihre Identität in den meisten Fällen nicht ermittelt werden kann. Mittels Blockchainanalyse und Kontaktaufnahmen mit ausländischen Finanzintermediären mit VASP-Tätigkeit konnten allerdings einzelne Hinweise auf VA-Geldwäschereinetzwerke in osteuropäischen Ländern sowie im nah- und fernöstlichen Raum gesammelt werden, was sich mit Erkenntnissen aus weiteren Recherchen deckt.[203]

[203] «Die LockBit-Führung behauptet, dass sie in erster Linie Bitcoin-Börsen in Hongkong und China nutze, um das erbeutete Geld zu waschen. Man vertritt die Ansicht, dass Chinas feindschaftliches Verhältnis zu den USA die Durchführung von Geldwäscheoperationen sicherer mache.» Vgl. Schurter Daniel, *Das ist die gefährlichste Hackerbande, die auch in der Schweiz wütet*, 23. Januar 2023.

7.3 Grösste Gefährdungen

Die meldenden Finanzintermediäre teilen der MROS bei der Erstattung einer Verdachtsmeldung mit, welche Vortaten sie im Zusammenhang mit den gemeldeten Personen oder Konten vermuten.[204] Auch wenn diese vermuteten Vortaten nicht immer mit den Analyseergebnissen der MROS übereinstimmen, kann eine quantitative Auswertung der vermuteten Vortaten bei VA-relevanten Verdachtsmeldungen helfen, die Gefährdungen genauer zu identifizieren, die von der Verwendung von VAs für kriminelle Zwecke im Allgemeinen sowie für GW/TF-Zwecke im Spezifischen ausgehen.

7.3.1 Betrügerische Nutzung von VAs als bedeutendste Gefährdung

Im Rahmen der Risikoanalyse von 2018 war der Bestand der VA-relevanten Verdachtsmeldungen nicht gross. Die grösste Gefährdung, die sich anhand der Verdachtsmeldungen erkennen liess, konnte im Bereich der Emission von VAs verortet werden: Die von den meldenden Finanzintermediären gemeldeten Sachverhalte und die dabei vermuteten Vortaten standen mehrheitlich in Zusammenhang betrügerischen ICOs. ICOs standen in den Jahren 2018/19 sodann auch im Fokus der Aufsichtsbehörden, wie entsprechende Wegleitungen der FINMA aufzeigen.[205] Verdachtsmeldungen, die seit 2020 bei der MROS eingereicht wurden, sind einerseits in Bezug auf die vermuteten Vortaten deutlich diverser, andererseits lassen die gemeldeten Sachverhalte inzwischen keine besondere Gefährdung im Bereich der Emission mehr erkennen. Viel häufiger bilden Dienstleistungen in Zusammenhang mit der Verwahrung oder dem Wechsel von VAs eine zentrale Rolle beim gemeldeten Sachverhalt, der den Finanzintermediären verdächtig erscheint und deshalb der MROS im Rahmen einer Verdachtsmeldung zur Kenntnis bringen.

Die wenigen zwischen 2015 und 2019 bei der MROS eingegangenen Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit, beschränkten sich auf einige wenige vermutete Vortaten, insbesondere Betrug, Urkundenfälschung sowie Betrügerischer Missbrauch einer Datenverarbeitungsanlage.[206] Auch für die Jahre 2020 bis 2022 wurden diese Vortaten häufig vermutet – gegenüber dem Gesamtbestand sogar überdurchschnittlich oft (vgl. Abbildung 21).

[204] Hinweis: Pro Verdachtsmeldung können von den meldenden Finanzintermediären mehrere vermutete Vortaten angegeben werden.
[205] Vgl. Eidgenössische Finanzmarktaufsicht (FINMA), *Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs)*, Februar 2018. Eidgenössische Finanzmarktaufsicht (FINMA), *Ergänzung der Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs)*, September 2019.
[206] Dies deckt sich auch mit den Schlussfolgerungen des ersten KGGT-Berichts zu VAs von 2018. Vgl. KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 24 – 27.

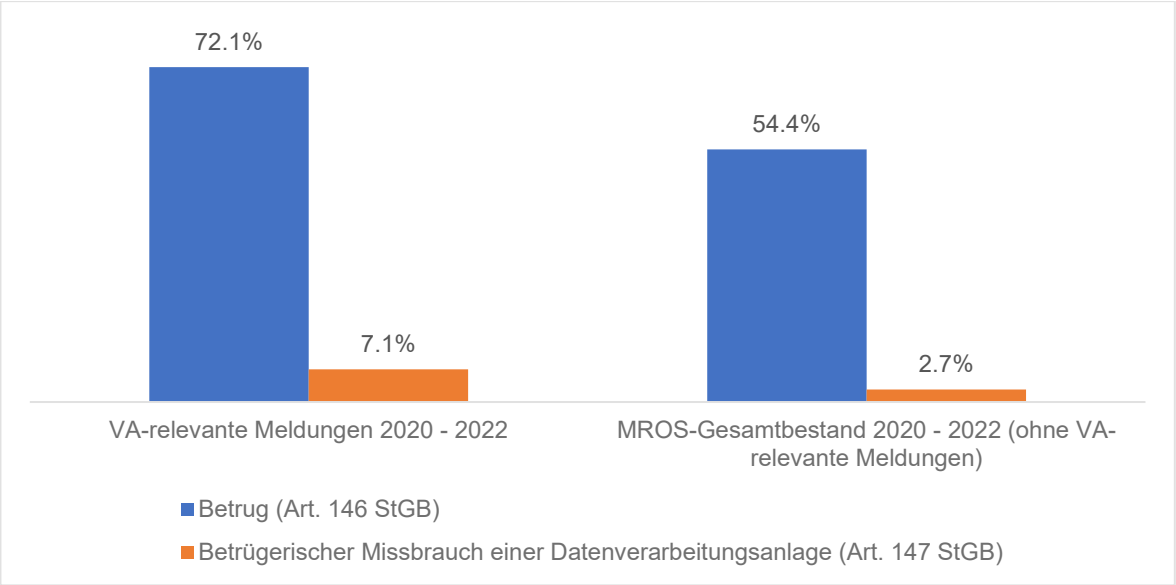


Abbildung 21: Die Vortaten Betrug sowie Betrügerischer Missbrauch einer Datenverarbeitungsanlage werden in VA-relevanten Verdachtsmeldungen überdurchschnittlich häufig vermutet (2020 – 2022)

Unklar bleibt, ob die Übervertretung dieser beiden Vortaten darauf zurückzuführen ist, dass sie in der Realität tatsächlich am häufigsten begangen wurden, oder ob sie von den meldenden Finanzintermediären im Vergleich zu anderen Vortaten einfacher entdeckt und gemeldet werden konnten. *Dass* diese beiden Vortaten in VA-relevanten Verdachtsmeldungen häufiger vermutet werden als in solchen ohne VA-Relevanz, deckt sich allerdings mit den Beobachtungen von FIUs anderer Länder.[207] Einerseits scheinen die mutmasslichen Täter die Einfachheit und Geschwindigkeit des Umsattelns von VA- auf Fiat-Zahlungsströme (und umgekehrt) auszunutzen, um die Nachverfolgung der ihnen zugutekommenden Finanzflüsse zu erschweren oder zumindest zu verzögern. Andererseits versuchen sie auch die Verwundbarkeit von VAs auszunutzen, den Strafverfolgungsbehörden die Sperrung oder Einziehung von VAs zu erschweren, indem sie VAs in der Regel auf *non-custodial* Wallets transferieren. Zahlreiche Netzwerke von Betrügern scheinen diese Verwundbarkeit erkannt und für verschiedene Tatvorgehen instrumentalisiert zu haben. VA-relevante Meldungen mit vermuteten Vortaten in diesem Bereich standen in der Regel im Zusammenhang mit Online-Anlagebetrug, Schneeballsystemen und *Money Mule*-Fällen - oder einer Kombination dieser Phänomene. Bei den dabei gemeldeten Konten handelte es sich in der Regel um Durchlaufkonten, die die Kontoinhaber wissentlich oder unwissentlich mutmasslichen Betrügern zur Verfügung stellten.[208] Sofern auch Betrügerischer Missbrauch einer Datenverarbeitungsanlage als Vortat vermutet wurde, handelte es sich in der Regel um (durch Hacking, Social Engineering und Phishing) betrügerisch ausgelöste Zahlungen, die von Konten bei (in- oder ausländischen) traditionellen Finanzintermediären ohne VASP-Tätigkeit auf Konten bei (in- oder ausländischen) Finanzintermediären mit VASP-Tätigkeit überwiesen wurden. Das Ziel der mutmasslichen Täter war offenkundig, die betrügerisch erlangten Fiat-Vermögenswerte des Opfers auf einer VASP-Plattform schnellstmöglich in VAs umzutauschen und auf eine *non-custodial* Wallet zu transferieren.

Sofern schweizerische Finanzintermediäre mit VASP-Tätigkeit Meldungen dieser Art einreichten, wurde Betrug oder Betrügerischer Missbrauch einer Datenverarbeitungsanlage

[207] Vgl. z.B: Swedish Police Authority, *The Financial Intelligence Unit Annual Report 2021*, Mai 2022, S. 15f. Financial Intelligence Unit (Liechtenstein), *Jahresbericht 2021*, April 2022, S. 11.

[208] Kriminelle rekrutieren im Internet hauptsächlich mittels attraktiven Stellenangeboten Personen als Finanzagent*innen, auch *Money Mules* genannt. Letztere sollen deliktisch erwirtschaftete Gelder an die Täter (die sich in der Regel im Ausland befinden) transferieren und dafür ihre persönlichen Konten zur Verfügung stellen. Wer an solchen «Geschäften» mitwirkt, kann sich der Geldwäscherei strafbar machen. Vgl. Schweizerische Kriminalprävention, *Money Mules*, zuletzt abgerufen im Mai 2023.

mehrheitlich auch im Verbund mit Urkundenfälschung als Vortat vermutet, da die mutmasslichen Täter oft mit gestohlenen oder gefälschten Identitätsdokumenten ein VASP-Konto eröffneten, um ihre eigene Identität zu verschleiern. Hierbei konnte die MROS in zahlreichen Fällen feststellen, dass die für die Eröffnung einer Geschäftsbeziehung erforderlichen Identifikationsdokumente bei den Finanzintermediären mit VASP-Tätigkeit zwar vorhanden waren, die tatsächlichen Personen allerdings aufgrund unterschiedlicher Betrugsmaschen selbst gar keinen Zugriff auf diese Konten hatten. Mit einigen Ausnahmen handelte es sich bei solchen Meldungen allerdings jeweils um relativ geringe Beträge im drei- bis vierstelligen Bereich.

Gefährdung 6

Gefährdungen in Verbindung mit dem Neuigkeitseffekt und der Unerfahrenheit der Nutzer (2018 identifiziert, 2023 erhöht)[209]

Seit 2018 hat sich die Anzahl Benutzer von VAs vervielfacht. VAs sind in der medialen Öffentlichkeit beinahe etwas Alltägliches geworden. Die damit verbundenen Risiken sind den Anlegern bekannt respektive sollten bekannt sein. Trotzdem lässt die Aussicht auf hohe Gewinne noch immer viele Menschen unvorsichtig werden, zum Beispiel bei der Auswahl eines Dienstleisters für ihre geplanten Investitionen oder auch bei der Eingabe ihrer persönlichen Daten im Internet. Sowohl MROS-Informationen als auch die verfügbaren Angaben der Strafverfolgungsbehörden lassen darauf schliessen, dass im Vergleich zu 2018 zahlenmässig viel mehr Menschen Betrugsschemas mit VA Bezug zum Opfer fallen, welche die Unerfahrenheit neuer Nutzer ausnutzen. Die Gefährdungslage hat sich folglich erhöht.

Gefährdung 7

Rückgriff auf VAs bei Phishing-Attacken (2018 identifiziert, 2023 erhöht)[210]

Teilweise werden Betrugsopfer durch reine Überredungskunst am Telefon oder über Messaging-Dienste durch die Täterschaft zu einer Überweisung an letztere verleitet. Häufig kommen aber auch Phishing-Methoden zum Einsatz. Solche Fälle kommen im Vergleich zu 2018 – allein aufgrund der Zunahme in der Verwendung von VAs – zahlenmässig deutlich häufiger vor. Die Gefährdungslage hat sich folglich erhöht.

7.3.2 Neue Gefährdungen erweitern das Risikospektrum

Allerdings hat sich mit dem Fortlauf der Zeit und dem allgemeinen Wachstum von VA-relevanten Verdachtsmeldungen auch das Spektrum der von den meldenden Finanzintermediären vermuteten Vortaten erweitert.

[209] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 24 – 26.
[210] Ibid., S. 30.

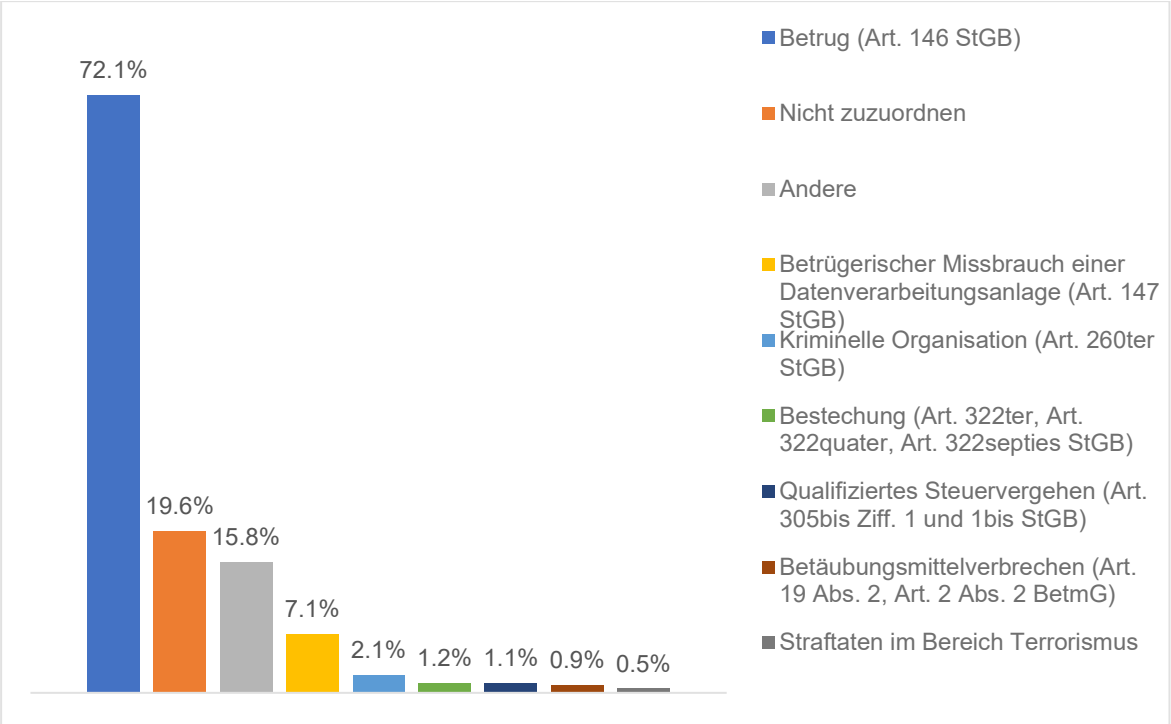


Abbildung 22: Veranschaulichung der Diversität vermuteter Vortaten in 1 867 VA-relevanten Verdachtsmeldungen (2020 – 2022). Zahlreiche weitere und unter «Andere» zusammengefasste Vortaten sind in Kapitel 11.2 im Anhang aufgelistet.[211]

Wie in Abbildung 22 ersichtlich, werden die einzelnen Vortaten zwar verhältnismässig selten vermutet, nichtsdestotrotz decken sie in ihrer Gesamtheit ein breites Spektrum an Straftaten ab, was auf eine breitere kriminelle Verwendung von VAs im Zahlungsverkehr schliessen lässt. So sind in der Kategorie «Andere» eine mittlere zweistellige Zahl weiterer Vortaten zusammengefasst, was darauf hindeutet, dass VAs inzwischen in unterschiedlichsten Formen und Schemas für GW/TF-Zwecke missbraucht werden.[212] Dementsprechend befanden sich unter den VA-relevanten Meldungen auch gemeldete Sachverhalte, die Risikoindikatoren enthielten, welche üblicherweise bei der GW/TF-Bekämpfung im traditionellen Zahlungsverkehr vorzufinden wären und auf «herkömmliche» GW/TF-Schemas hinweisen. Dazu zählen beispielsweise die aus wirtschaftlicher Sicht unnötige Involvierung von Offshore-Gesellschaften bei relativ einfachen Handelsgeschäften (z.B. Import von Lebensmitteln) oder die Einbindung des Vertragspartners in ein verzweigtes Geflecht von Firmen, deren hohe Transaktionsvolumen untereinander mit gegenseitigen (teilweise mit in VAs denominierten) Darlehensverträgen gerechtfertigt wurden (vgl. Typologie 1). Die Analysen der MROS verstärken diesen Eindruck: Oft identifiziert die MROS bei ihren Analysearbeiten weitere Straftaten als jene, die von den meldenden Finanzintermediären überwiegend angegeben werden (z.B. Betrug). Nicht selten fallen diese sodann in den Bereich schwerwiegender Formen der Kriminalität.

[211] Hinweis: Meldende Finanzintermediäre können verschiedene Straftaten vermuten und deshalb pro erstattete Verdachtsmeldung mehrere davon als Vortaten vermuten. Der prozentuale Anteil der vermuteten Vortaten kann folglich berechnet werden und die Summe sämtlicher Anteile übersteigt deshalb auch 100 Prozent. Ebenso: Unter «Straftaten im Bereich Terrorismus» sind die Straftaten 1.) Finanzierung des Terrorismus (Art. 260^{quinquies} StGB) sowie 2.) Art. 2 des Bundesgesetzes über das Verbot der Gruppierungen Al-Qaïda und Islamischer Staat sowie verwandter Organisationen zusammengefasst.

[212] Die vollständige Liste der in VA-relevanten Verdachtsmeldungen vermuteten Vortaten findet sich in Kapitel 11.2 im Anhang.

Typologie 1

Netzwerk ausländischer Scheinfirmen kauft VAs zum mutmasslichen Waschen von Fiatwährung

Beim Eröffnungsprozess einer Geschäftsbeziehung mit einer ausländischen Gesellschaft fiel dem meldenden Finanzintermediär auf, dass sich das Geschäftsmodell der Firma sowie die von ihr benutzten Formulierungen denjenigen eines bereits registrierten Geschäftskunden sehr ähnelten. Daraufhin verlangte der Finanzintermediär vom potentiellen Neukunden zusätzliche Unterlagen zur Mittelherkunft. Dieser reichte Bankauszüge und Rechnungen für scheinbar getätigte Dienstleistungen ein. Dies erschien dem Finanzintermediär plausibel, woraufhin die Geschäftsbeziehung eröffnet wurde. In den darauffolgenden Tagen überwies der neue Firmenkunde von einem ausländischen Konto in mehreren Transaktionen Fiatwährung auf die Geschäftsbeziehung, kaufte damit VAs und transferierte diese umgehend auf eine *non-custodial* Wallet. Im gleichen Monat kam es beim meldenden Finanzintermediär zu einer weiteren ähnlich gestalteten Anfrage zur Eröffnung einer Geschäftsbeziehung durch eine dritte, im selben Land wie die anderen beiden angesiedelten Firmen. Wieder wurden weitere Dokumente zur Mittelherkunft verlangt, wobei die daraufhin eingereichten Dokumente mangelhaft schienen. Auf eine erneute Nachfrage reagierte der potentielle Neukunde nicht mehr. Bei einer näheren Überprüfung konnte der Finanzintermediär feststellen, dass zwei dieser Firmen dieselbe Adresse benutzten. Sodann wurden zusätzliche Auffälligkeiten bei allen drei besagten Firmen festgestellt: Identifizierungsdokumente wurden teilweise nicht korrekt ausgefüllt und die Websites schienen unseriös und ad-hoc aufgesetzt worden zu sein. Weitere Kontaktaufnahmen blieben bei allen drei Firmen erfolglos. Die dadurch entstandenen Zweifel an der Herkunft der eingebrachten Vermögenswerte veranlassten den Finanzintermediär zu einer Meldung bei der MROS.

Ebenfalls fanden sich in VA-relevanten Meldungen vereinzelt Hinweise auf Betäubungsmittelhandel im grossen Stil sowie Terrorismusfinanzierung (vgl. Typologie 2).

Typologie 2

Mutmassliche Terrorismusfinanzierung mit VAs

Ein Finanzintermediär stellte seinen Kunden die Dienstleistung Krypto ATM zur Verfügung. Dieser Service macht es möglich, dass Schweizer Franken an einem Bankomaten einbezahlt und anschliessend vom anbietenden Finanzintermediär in Bitcoin umgetauscht werden. Für den Umtausch der CHF in Bitcoin arbeitete dieser Finanzintermediär mit einer VA-Handelsbörse in einem Nachbarland zusammen, welche die von den Kunden gekauften Bitcoins jeweils an die von ihnen angegebene Bitcoin-Adresse versendete. Diese Börse machte den Finanzintermediär darauf aufmerksam, dass von einer solchen Adresse eine Bitcoin-Transaktion zum damaligen Wert von etwa hundert Franken an eine Bitcoinadresse versendet wurde, die der Gruppierung Al-Qaïda zuzuordnen sei. Diese Bitcoinadresse sei Gegenstand von Untersuchungen einer Staatsanwaltschaft in einem Drittland gewesen. Die Möglichkeit von Finanzintermediären im VASP-Bereich, übertragene VAs auch nachzuverfolgen, nachdem diese dem Kunden bereits ausgehändigt wurden, führte in diesem Fall zur Entdeckung der verdächtigen Zahlung. Gegenüber dem traditionellen Zahlungsverkehr eröffnen sich dadurch neue Möglichkeiten im Bereich des VA-Transaktionsmonitorings.

Der an die MROS gemeldete Überweiser konnte durch die Einzahlung am Krypto ATM weitgehend anonym bleiben und musste nur eine Kontaktinformation angeben. Die MROS konnte den Überweiser aufgrund dieser Angabe jedoch identifizieren. Abklärungen zur Person

zeigten, dass diese vor vier Jahren in sozialen Medien durch das Teilen von gewalttätiger jihadistischer Propaganda aufgefallen war. Neben der bereits erwähnten Transaktion wurden im Rahmen der Transaktionsanalyse weitere 17 Transaktionen – im Gesamtwert von etwa CHF 3 000 – an dieselbe Bitcoin Adresse identifiziert. Die Adresse soll gemäss einem Blockchain-Analysetool zum Al-Qaïda Bitcoin Transfer Office gehören.

Gefährdung 8

Terrorismusfinanzierung mittels VAs (2018 identifiziert, 2023 unverändert)[213]

Seit 2018 wurden bei der MROS mehrere VA-relevante Verdachtsmeldungen eingereicht, bei denen die meldenden Finanzintermediäre Straftaten im Bereich Terrorismus vermuteten.[214] Daten des Blockchainanalyse-Unternehmens Chainalysis lassen zwar darauf schliessen, dass die Beträge, die an bekannte Adressen terroristischer Organisationen versendet werden, seit 2020 zurückgehen.[215] Allerdings ist hinlänglich bekannt, dass bei der Terrorismusfinanzierung bereits kleine Beträge ausreichen, um grossen Schaden anzurichten. Gesamthaft betrachtet liegen keine Informationen vor die gegenüber 2018 auf eine wesentliche Veränderung der Gefährdungslage hindeuten.

Eine Verdachtsmeldung lieferte auch Hinweise auf die Involvierung von Akteuren bei mutmasslichen Geldwäschereihandlungen mit VAs, wobei davon auszugehen ist, dass diese Handlungen die Finanzierung des Rüstungsprogramms eines durch UN-Sanktionen betroffenen ausländischen Staates bezweckten (vgl. Typologie 3).

Typologie 3

Mutmassliche Proliferationsfinanzierung mit VAs

Ein schweizerischer Finanzintermediär mit VASP-Tätigkeit wurde dahingehend missbraucht, dass aus einer Cyberattacke auf eine ausländische Kryptobörse gestohlene Kryptowährungen über diesen Finanzintermediär gewaschen wurden. Die Plattform des meldenden Finanzintermediärs wurde von der Täterschaft verwendet, um die gestohlenen Kryptowährungen in eine andere Kryptowährung umzutauschen und folglich ihre Spuren zu verwischen. Gemäss den Einschätzungen verschiedener Experten im Bereich Blockchainanalyse konnte dieser Angriff einer dem nordkoreanischen Regime nahestehenden Hackergruppe zugeordnet werden.

[213] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 27 – 28.
[214] Unter «Straftaten im Bereich Terrorismus» sind die Straftaten 1.) Finanzierung des Terrorismus (Art. 260^{quinquies} StGB) sowie 2.) Art. 2 des Bundesgesetzes über das Verbot der Gruppierungen Al-Qaïda und Islamischer Staat sowie verwandter Organisationen zusammengefasst.
[215] Chainalysis, *The 2023 Crypto Crime Report*, Februar 2023, S. 6.

Gefährdung 9

Proliferationsfinanzierung mittels VAs (2023 identifiziert)

Gemäss Informationen, die der MROS vorliegen, sind auch schweizerische Finanzintermediäre mit VASP-Tätigkeit gefährdet, als Knotenpunkt für Finanzflüsse missbraucht zu werden, die der Proliferationsfinanzierung dienen.

Ebenfalls konnten in einigen Meldungen Bezüge zu verschiedenen internationalen Korruptionsskandalen festgestellt werden. Unter den Vertragsparteien, wirtschaftlich Berechtigten oder Gegenparteien von Geschäftsbeziehungen, die ebenfalls Gegenstand von VA-relevanten Meldungen waren, konnten zudem politisch exponierte Personen (PEP) identifiziert werden. In weiteren Meldungen konnte die MROS natürliche oder juristische Personen identifizieren, die gemäss Presseberichten oder Angaben aus bestimmten Strafverfahren in Verbindung mit kriminellen Organisationen standen.

Dass VAs in der Schweiz nicht nur bei Delikten im Bereich der Cyberkriminalität zur Anwendung kommen, zeigt überdies eine Auswertung von zwölf Fällen mit VA-Bezügen, die während der letzten zehn Jahre zu Ermittlungen seitens der Bundeskriminalpolizei (BKP) führten und schliesslich in Verfahrenseröffnungen mündeten. Die BKP nimmt die Ermittlungskompetenz des Bundes wahr und führt damit sämtliche Ermittlungen bezüglich jener Delikte, die in die Bundeszuständigkeit fallen. Obwohl die Rolle von VAs bei den untersuchten Fällen unterschiedlich ist und ihre Anzahl relativ bescheiden ist, haben die Fälle gemeinsam, dass sie alle zeitlich nicht weit zurückliegen: Die älteste der dieser zwölf Ermittlungen geht auf das Jahr 2018 zurück.

Sämtliche Ermittlungsabteilungen der Bundeskriminalpolizei waren bereits mit Fällen konfrontiert, in denen Kryptowährungen verwendet wurden. Das Spektrum der dabei untersuchten, bzw. mutmasslich begangenen Straftaten, zeigt einmal mehr die vielfältigen Einsatzmöglichkeiten von VAs wie auch die wachsende Diversität der damit möglicherweise verbundenen kriminellen Handlungen auf:

Befasste Ermittlungsabteilung der Bundes-kriminalpolizei	**Rechtshilfe, Terrorismus, Völkerstrafrecht**	**Staatsschutz, Kriminelle Organisationen**	**Wirtschafts-kriminalität**
Untersuchte Straftaten	• Kriminelle und terroristische Organisationen (Art. 260ter StGB) • Bundesgesetz über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen (Art. 2) • Raub (Art. 140 StGB) • Erpressung (Art. 156 StGB) • Gefährdung durch Spreng-stoffe und giftige Gase in verbrecherischer Absicht (Art. 224 StGB)	• Geldfälschung (Art. 240 StGB) • Einführen, Erwerben, Lagern falschen Geldes (Art. 244 StGB)	• Geldwäscherei (Art. 305bis StGB) • Unbefugte Datenbeschaffung (Art. 143 StGB) • Datenbeschädigung (Art. 144bis StGB) • Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB)
Beobachtete GW-Methoden	• Mixing-Dienste und Privacy Wallets • Peel Chains • Privacy Coins • Chain Hopping • Bewusste Nutzung von VASPs mit schwachen oder inexistenten KYC-Anforderungen / Nutzung von OTC-Brokerdienstleistungen («nested services»)		

Abbildung 23: Übersicht über die von der Bundeskriminalpolizei durchgeführten Ermittlungen im VA-Bereich zwischen 2018 und 2022

Bei den Ermittlungen im Bereich der Cyberkriminalität beobachtete die BKP jeweils eine ähnliche Vorgehensweise seitens der Täter: Nachdem sich diese durch verschiedene Phishing-Techniken oder Trojaner-Arten Zugang zum E-Banking der Geschädigten verschafft haben, führen sie Überweisungen zu Konten bei ausländischen VASPs durch, die im Vornherein unter dem Namen der Geschädigten (Identitätsdiebstahl) oder weiteren zuvor angeworbenen *Money Mules* eröffnet wurden. Die eingetroffenen Gelder werden sodann auf der VASP-Plattform in Kryptowährungen umgetauscht und meistens umgehend auf eine externe Wallet transferiert. Der Einsatz von Kryptowährungen scheint also als Mittel zu dienen, die ursprünglich von Bankkonten in der Schweiz gestohlenen Vermögenswerte im Ausland zu waschen sowie deren Auffindung zu erschweren. Umgekehrt war die BKP auch bereits mit einem Fall konfrontiert, in dem die von einem ausländischen VASP durch Hacking gestohlenen Kryptowährungen auf eine VASP-Plattform in der Schweiz überwiesen wurden, um diese in eine andere Kryptowährung umzutauschen und umgehend wieder von der Plattform weg zu

transferieren. Der Umtausch von einer Kryptowährung scheint dabei die Verschleierung als Ziel zu haben, da für die Nachverfolgung sodann mehrere unterschiedliche Blockchains analysiert werden müssen. Diese Technik des sogenannten *Chain Hopping* wird oft wiederholt und teilweise mit weiteren Verschleierungstechniken wie *Mixing* kombiniert (vgl. Infobox 4 in Kapitel 7.4.1).

Bei Fällen im Zusammenhang mit Terrorismus und dessen Finanzierung scheinen Kryptowährungen für Sender und Empfänger aus mehreren Gründen attraktiv zu sein: Personen, die mittels Kryptowährungen zur Finanzierung von Terrororganisationen beitragen, scheinen vermeintlich davon auszugehen, dass sich die von ihnen durchgeführten VA-Transaktionen nicht nachverfolgen lassen. Umgekehrt erweitern Terrororganisationen durch die Publikation ihrer VA-Adressen im Internet ihre Reichweite und erhalten Zugang zu einem viel breiteren potentiellen Finanzierungsnetzwerk, als wenn sie für ihre Finanzierung lediglich auf persönliche Kontakte angewiesen wären. Durch den Einsatz von *non-custodial* Wallets können diese Organisationen zudem die erhaltenen Kryptowährungen vor Sperrung und Einziehung schützen. Die BKP konnte diese Vorgehensweise auch bei Fällen von Ransomware sowie bei weiteren Erpressungsfällen beobachten.

Letztlich führte die BKP auch zwei Ermittlungen im Bereich Falschgeld durch, wobei sie feststellte, dass im Darknet Falschgeld mit Kryptowährungen gekauft wird. Nebst dem «einfachen» Motiv des Erwerbs von Falschgeld im Sinne einer vermeintlichen Geldvermehrung (Erwerb eines gefälschten 50-Euro-Scheins für einen Bruchteil dieses «Geldwertes») kann sich dahinter auch eine Technik verbergen, die es ermöglicht, Kryptowährungen aus kriminellen Aktivitäten auszugeben, ohne diese über einen VASP-Anbieter in Fiat-Geld umtauschen zu müssen.

7.3.3 Vertragspartner und involvierte Beträge

Ein Abgleich der vermuteten Vortaten mit den dabei involvierten Summen zeigt auf, dass bei Meldungen mit Transaktionen von einem hohen Gesamtwert (ab CHF 250'000.-) das Spektrum der vermuteten Vortaten diverser war (bspw. qualifiziertes Steuervergehen, Betäubungsmitteldelikte, Beteiligung oder Unterstützung einer kriminellen Organisation, etc.) als bei Meldungen mit geringen involvierten Beträgen, bei welchen von den meldenden Finanzintermediären überwiegend Betrug vermutet wurde.

	2020	2021	2022
VA-relevante Meldungen von Finanzintermediären mit VASP-Tätigkeit	104	178	143
Davon Meldungen ohne VA-relevante Transaktionen	50	88	75
Davon Meldungen mit VA-relevanten Transaktionen	54	90	68
Gesamtwert der VA-relevanten Transaktionen (CHF)	1.8 Mio.	28.5 Mio.	50.5 Mio.
Durchschnittswert aller VA-relevanten Transaktionen pro Meldung (CHF)	4 976	32 477	53 618
Medianwert aller VA-relevanten Transaktionen (CHF)	1 385	3 000	3 500

Abbildung 24: Involvierte Beträge bei Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit, in denen verdächtige Transaktionen gemeldet wurden, haben seit 2020 deutlich zugenommen.

Im Jahr 2020 erhielt die MROS von Finanzintermediären mit VASP-Tätigkeit insgesamt 104 Verdachtsmeldungen mit einem VA-Bezug. In den Meldungen mit VA-bezogenen, verdächtigen Transaktionen wurde ein Gesamtwert von über 1.8 Millionen Schweizerfranken gemeldet. Im Durchschnitt wurden in jeder dieser Meldungen Transaktionen mit einem Gesamtwert von knapp CHF 5000.- gemeldet, während der entsprechende Median bei rund CHF 1’385 pro Meldung lag. Demgegenüber meldeten Finanzintermediäre mit VASP-Tätigkeit im Jahr 2021 in 178 Meldungen einen VA-Bezug. 68 Meldungen enthielten verdächtige Transaktionen mit einem Gesamtwert von 28.5 Millionen Schweizerfranken, wobei der durchschnittliche Gesamtwert pro Meldung bei rund CHF 32’477.- sowie der entsprechende Median bei CHF 3’000.- lag. Im Jahr 2022 wurden 143 Meldungen von Finanzintermediären mit VASP-Tätigkeit bei der MROS abgesetzt. Bei 68 Meldungen wurde ein direkter VA-Bezug in den Transaktionen festgestellt, welche einem Gesamtwert von 50.5 Millionen Schweizerfranken, mit einer durchschnittlichen Transaktionshöhe von CHF 53'618.- und einem Median von CHF 3’500.- entsprechen. Der jeweils relativ tiefe Medianwert veranschaulicht, dass die MROS in den betrachteten Jahren zahlreiche Meldungen mit gemeldeten Transaktionen von relativ geringem Gesamtwert erhielt. Hierbei handelte es sich mit überwiegender Mehrheit um mutmasslich betrügerisch ausgelöste Überweisungen von Konten bei traditionellen Finanzintermediären ohne VASP-Tätigkeit zu Konten bei Finanzintermediären mit VASP-Tätigkeit. Oft sind solche Fälle mit einem Verdacht auf Hacking/Phishing (Betrügerischer Missbrauch einer Datenverarbeitungsanlage) verbunden, wobei die mutmasslichen Betrüger über die E-Banking-Login-Daten der Opfer verfügen und auch die Überweisung vom Konto des Opfers selbstständig tätigen. Sie wurden von den schweizerischen Finanzintermediären mit VASP-Tätigkeit vereinzelt bemerkt, da sich die Betrüger beispielsweise über dieselbe IP-Adresse in verschiedene Benutzerkonten auf der VASP-Plattform einloggten, oder weil bei mehreren Benutzerkonten dieselbe Mobiltelefonnummer hinterlegt war, welche nicht im Herkunftsland des Kunden registriert war. Als wiederkehrendes Muster liess sich feststellen, dass mutmassliche Betrüger scheinbar gezielt grenzüberschreitende Zahlungsströme anstreben, um die Nachverfolgung der Transaktionen oder die Sperrung und Einziehung von Vermögenswerten zu erschweren oder zu verzögern: So waren das Fiat-Konto, von welchem Geld überwiesen wurde, sowie das Konto des VASPs, auf das die Überweisung für den Kauf von VAs stattfand, üblicherweise in unterschiedlichen Ländern zu verorten. Sofern das Konto, von dem die Überweisung getätigt wurde, bei einem schweizerischen Finanzintermediär ohne VASP-Tätigkeit geführt wurde, war der entsprechende VASP, zu dem die Gelder transferiert wurden, in der Regel im Ausland, und umgekehrt: Sofern ein schweizerischer Finanzintermediär mit VASP-Tätigkeit involviert war, wurden die Gelder in der Regel von ausländischen Konten überwiesen.

Die involvierten Beträge in VA-relevanten Meldungen von Finanzintermediären ohne VASP-Tätigkeit sind deutlich weniger aussagekräftig, da der Anteil der von diesen Finanzintermediären stammenden VA-relevanten Meldungen *mit* VA-relevanten Transaktionen relativ klein war. Eine VA-Relevanz liess sich mehrheitlich mittels bestimmter Schlagwörter feststellen, die der meldende Finanzintermediär bei der Schilderung des Sachverhalts verwendete (z.B. «Bitcoin» oder «Krypto»). Hierbei verwiesen die meldenden Finanzintermediäre häufig summarisch auf eine Reihe von Überweisungen zwischen den gemeldeten Konten und jenen eines VASPs, ohne dass diese Transaktionen im dafür vorgesehenen digitalen Formular erfasst wurden und dadurch auch nicht quantitativ ausgewertet werden konnten. Ebenfalls konnten zahlreiche Fälle beobachtet werden, in denen die meldenden Finanzintermediäre zwar eine VA-Relevanz schriftlich erwähnten (bspw. die Geschäftstätigkeit ihres Kunden im VA-Bereich), jedoch selbst die transaktionellen Verbindungen zwischen dem von ihnen gemeldeten Konto und jenem eines VASP nicht erkannten und deshalb die entsprechenden Transaktionen auch nicht im dafür vorgesehenen digitalen Formular übermittelten.

Bei den untenstehenden Angaben handelt es sich folglich um absolute Mindestangaben, wobei die tatsächlichen Beträge mit grosser Wahrscheinlichkeit deutlich höher liegen.

	2020	2021	2022
VA-relevante Meldungen von Finanzintermediären ohne VASP-Tätigkeit	208	321	913
Davon Meldungen ohne VA-relevante Transaktionen	166	258	835
Davon Meldungen mit VA-relevanten Transaktionen	42	63	78
Gesamtwert der VA-relevanten Transaktionen (CHF)	1.6 Mio.	15 Mio.	7.4 Mio.

Abbildung 25: Involvierte Beträge bei VA-relevanten Verdachtsmeldungen von Finanzintermediären ohne VASP-Tätigkeit, 2020 – 2022

Der Schweizer Finanzplatz ist weltweit führend in der grenzüberschreitenden Vermögensverwaltung für Privatpersonen. Dementsprechend sind die Vertragspartner von Geschäftsbeziehungen, die der MROS gemeldet werden, häufig im Ausland domiziliert. Mindestens 46% der zwischen 2020 und 2022 gemeldeten Vertragspartner waren entweder juristische Personen mit Domizil im Ausland oder natürliche Personen mit ausländischer Nationalität (vgl. Balken links in Abbildung 26).

Eine sogar noch stärkere internationale Kundenausrichtung lässt sich in den Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit erkennen: In mindestens 69% der Fälle handelte es sich bei den gemeldeten Vertragspartnern um natürliche Personen mit ausländischer Nationalität oder juristische Personen mit ausländischem Domizil. Zudem waren natürliche Personen in 72% der Fälle als Vertragspartner gemeldet, was als Hinweis gewertet werden kann, dass die meldenden Finanzintermediäre mit VASP-Tätigkeit vor allem im Privatkundengeschäft aktiv sind.

Gemeldete Vertragspartner in Meldungen von Finanzintermediären ohne VASP-Tätigkeit sind mehr oder weniger repräsentativ für den MROS-Gesamtbestand der letzten drei Jahre, was den Status der gemeldeten Rechtssubjekte (natürliche oder juristische Person) sowie deren Herkunft betrifft (Nationalität bei natürlichen Personen, Domizil bei juristischen Personen, vgl. linker sowie mittlerer Balken in Abbildung 26). Die einzig deutliche Abweichung in der Verteilung stellt hierbei die verhältnismässig häufige Meldung von natürlichen Personen mit schweizerischer Staatsangehörigkeit als Vertragspartner dar (33%). Hierfür scheinen mehrere Gründe plausibel. Zum Beispiel die nebst der internationalen Vermögensverwaltung starke Ausrichtung dieser Finanzintermediäre auf Privatkunden in der Schweiz. Letztere haben gemäss diversen Umfragen und Studien in den letzten Jahren begonnen, VAs vermehrt zu verwenden, während diese Entwicklung im grenzüberschreitenden Vermögensverwaltungsgeschäft dieser Finanzintermediäre vermutlich weniger stark ausgeprägt war. Eine weitere Erklärung könnte die Tatsache liefern, dass es sich bei den hierbei gemeldeten Vertragspartnern häufig um mutmassliche *Money Mules* oder Betrugsopfer handelte – beide Muster finden sich eher im Privatkundengeschäft als in der internationalen Vermögensverwaltung.

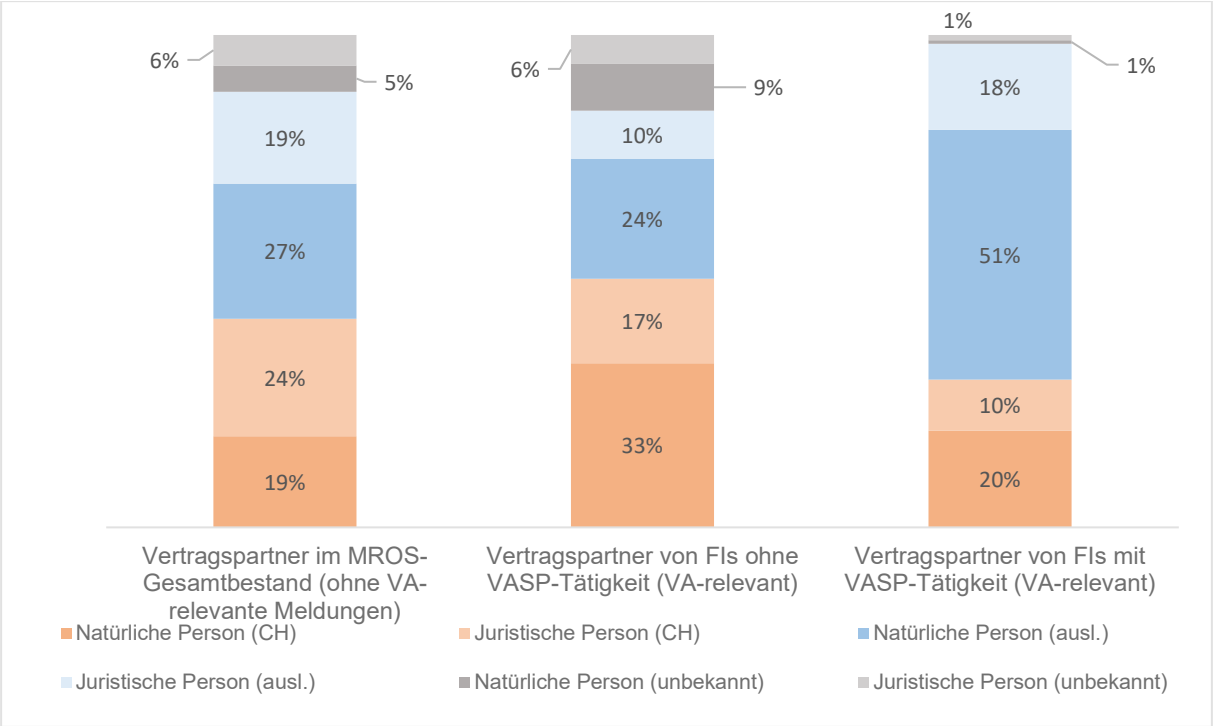


Abbildung 26: Gemeldete Vertragspartner bei den 1867 VA-relevanten Verdachtsmeldungen (2020 – 2022) im Vergleich mit den gemeldeten Vertragspartnern in sämtlichen Meldungen desselben Zeitraums (abzüglich die 1867 VA-relevanten Meldungen). Über die Hälfte aller gemeldeten Vertragspartner von Geschäftsbeziehungen bei Finanzintermediären mit VASP-Tätigkeit sind natürliche Personen mit ausländischer Nationalität.[216]

7.4 Verwundbarkeiten bei der Strafverfolgung im VA-Bereich

Im VA-Bereich sehen sich Strafverfolgungsbehörden mit zusätzlichen Chancen und Herausforderungen konfrontiert. Zusammengefasst sind diese Herausforderungen ressourcen- und ausbildungstechnischer, technologischer sowie rechtlicher Natur. Konkrete Herausforderungen bestehen insbesondere in der Nachverfolgung von VA-Transaktionen, der Identifizierung des Besitzers einer Wallet, der Sicherstellung einer Wallet und der Einziehung der darin gespeicherten VAs, sowie letztlich in der grenzüberschreitenden Informations- und Beweisbeschaffung. Chancen bestehen insbesondere im Bereich der Blockchainanalyse sowie der engeren und vereinfachten nationalen und internationalen Zusammenarbeit.

[216] Hinweis: Bei natürlichen Personen mit doppelter Staatsbürgerschaft wurde jeweils nur die erste bzw. älteste Angabe berücksichtigt, die in der MROS-Datenbank zu diesen Personen hinterlegt ist. Die Aussagekraft der Grafik in Bezug auf die Nationalitätsangaben der natürlichen Personen sinkt insofern, je grösser die Anzahl natürlicher Personen mit doppelter Staatsbürgerschaft unter den gemeldeten Vertragspartnern ist.

7.4.1 Aufklärung von Straftaten im VA-Bereich

VAs bieten den Strafverfolgungsbehörden grundsätzlich den Vorteil, die finanziellen Aktivitäten einer Person auf der Blockchain in Echtzeit zu verfolgen. Die Blockchain-Technologie ermöglicht es theoretisch, die Herkunft sowie die Destination von VAs nachzuvollziehen. Insbesondere für die Beweisführung ist dies sehr wichtig: Wenn beispielsweise eine Straftat im Ausland begangen wird und die Gelder in der Schweiz gewaschen werden, ist es von entscheidender Bedeutung, die Geldwäschereihandlung mit der vorangehenden Straftat (Vortat) in Verbindung bringen zu können. Dies kann bei transparenten Blockchain-Zahlungen erleichtert werden, da in diesem Falle die Transaktionen öffentlich einsehbar sind.

Um Blockchainanalyse selbstständig effektiv durchführen zu können, müssen spezielle Tools und Kenntnisse in diesem Bereich erworben werden. Dass sich die Aufwendungen in die Weiterentwicklung solcher Fähigkeiten lohnen, zeigen mehrere ausländische jüngst bekannt gewordene Fälle, in deren Rahmen VA-Vermögenswerte in mehrfacher Milliardenhöhe durch Strafverfolgungsbehörden beschlagnahmt werden konnten – selbst wenn die damit zusammenhängenden Straftaten bereits vor vielen Jahren begangen wurden.[217]

Aus der Umfrage bei 27 Schweizer Polizeibehörden geht hervor, dass sich mehr als die Hälfte der Befragten mit mindestens einem Tool zur Blockchainanalyse ausgerüstet hat (Stand Ende April 2023).[218] Die überwiegende Mehrheit der anderen Hälfte gab jedoch an, über einen indirekten Zugriff auf solche Tools zu verfügen (vgl. NEDIK in Kapitel 7.4.2). Lediglich zwei Behörden gaben an, weder über einen (indirekten) Zugang zu Tracingtools zu verfügen, noch eine Beschaffung eines solchen Tools zu beabsichtigen. Dies zeigt, dass die schweizerischen Strafverfolgungsbehörden den Handlungsbedarf in diesem Bereich erkannt haben und daran sind, sich die erforderlichen Instrumente zu beschaffen.

Allerdings gab auch die Mehrheit der 27 angefragten Behörden an, dass erhebliche Herausforderungen bei der Verwendung von Blockchainanalyse-Tools bestehen, namentlich in Zusammenhang mit *off-chain*- und *Second-Layer*-Transaktionen. Parallel zu den Fortschritten bei der Nachverfolgung von VA-Transaktionen mittels Blockchainanalyse-Tools sind nämlich auf der anderen Seite auch die Verschleierungstechniken ausgeklügelter geworden (vgl. Gefährdung 10). So sind auch Fälle bekannt, bei denen Blockchainanalysen wenig bis keine auswertbaren Möglichkeiten mit sich brachten. Mit der alleinigen Beschaffung solcher Tools sind die Herausforderungen in diesem Bereich folglich noch nicht gemeistert. Ein hohes Mass an Fachwissen, kontinuierliche Weiterbildungen und Weiterentwicklungen von Analysetools sind notwendig, damit Strafverfolgungsbehörden in diesem Rüstungswettlauf zwischen Ver- und Entschleierungstechniken auf dem neuesten Stand bleiben.

Mangels konsolidierter Daten bei kantonalen und städtischen Polizeibehörden wurde im Rahmen des vorliegenden Berichts die Bundeskriminalpolizei (BKP) und die MROS angefragt, welchen Techniken sie bei ihrer Arbeit bereits begegnet sind. Hierzu gehörten der Einsatz von *Peel Chains*, *Mixer*, *Chain Hopping*, *Privacy Coins*, *Wash Trading* sowie die Nutzung von VASPs mit schwachen oder inexistenten KYC-Anforderungen (vgl. Infobox 4).

[217] Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26. Januar 2023.
[218] Hinweis: Angefragt wurden nebst städtischen und kantonalen Polizeien auch das Schweizerische Polizei-Institut sowie die Schweizerische Kriminalprävention SKP.

Infobox 4

Verschleierungstechniken

Mixing-Dienste und Privacy Wallets: Ein Mixing-Dienst kann mit kriminellen Aktivitäten "behaftete" VAs mit anderen, «sauberen» VAs vermischen. Dies geschieht in der Regel durch das Zusammenführen von VAs aus diversen Quellen für einen langen Zeitraum mit dem Ziel, diese ununterscheidbar zu machen. Sogenannte Privacy Wallets (bspw. Wasabi Wallet) verwenden integrierte Anonymisierungstechniken wie CoinJoin, um für sämtliche auf solchen Wallets deponierte VAs diesen Mischeffekt zu erzielen.

Peel Chain: Eine lange Reihe von Transaktionen durch die Aufteilung grosser Beträge in kleine Beträge an Adressen, die zur Verschleierung des Ursprungs oder des Ziels eines Transaktionsstroms verwendet wird. Aufgrund der geringen Beträge bei den einzelnen Überweisungen ist es weniger wahrscheinlich, dass die Eingänge von Geldern auf Tauschbörsen Alarmsignale auslösen.

Privacy Coins: Einige Kryptowährungen (bspw. Monero) wurden mit dem Ziel gestaltet, dass die mit ihnen durchgeführten Transaktionen nicht auf der jeweiligen Blockchain transparent einsehbar sind – damit Transaktionen nicht nachverfolgt werden können.

Chain Hopping ist das Verschieben von VAs von einer Blockchain auf eine andere – häufig in rascher Abfolge und mehrfacher Wiederholung mittels diverser unterschiedlicher Blockchains – um eine Nachverfolgung zu erschweren.

Wash Trading: Diese Technik besteht darin, VAs an sich selbst oder an Komplizen weiter zu «verkaufen», indem VAs zwischen Wallets hin- und her gesendet werden. Dabei wird künstlich eine Transaktionshistorie erstellt und der Eindruck geweckt, dass das entsprechende VA (bspw. ein spezifisches NFT oder eine Kryptowährung mit geringem Handelsvolumen und geringer Marktkapitalisierung) begehrter ist, als es tatsächlich der Fall ist und wodurch auch der Wert des betreffenden VA künstlich aufgebläht werden kann. Wash Trading von VAs eignen sich für Geldwäschereizwecke, da damit einerseits die Herkunft von Vermögenswerten anhand einer langen Transaktionshistorie verschleiert werden kann. Andererseits kann mit dieser Technik auch das Zustandekommen eines Vermögens plausibilisiert werden oder auch der ursprüngliche, inkriminierte Betrag durch Wash Trading gesteigert werden.[219]

Nutzung von VASPs mit schwachen oder inexistenten KYC-Anforderungen (zumeist sog. «nested services»): Gewisse Plattformen können sich in Jurisdiktionen befinden, die internationale Standards zur GW/TF-Bekämpfung nicht genügend umsetzen. Viele von Kriminellen genutzten Dienste, um VAs in Fiatwährung umzuwandeln (Fiat Off-Ramps), sind sogenannte Over-The-Counter Broker. Diese nutzen die grossen VA-Handelsbörsen, um die Liquidität und die Handelspaare dieser grösseren Dienstleister anzuzapfen. Sie werden deshalb auch «nested services» (verschachtelte Dienste) genannt, da sich die von ihnen benutzten Adressen in einem ersten Ermittlungsschritt lediglich den grossen Handelsbörsen zuordnen lassen. Bei den meisten OTC-Broker handelt es sich um bekannte und seriöse Unternehmen. Ausgewertete *on-chain*-Daten von Unternehmen im Bereich Blockchainanalyse deuten jedoch darauf hin, dass eine kleine Gruppe von ihnen den Grossteils der Geldwäscherei in Zusammenhang mit der Umwandlung von VAs in Fiatwährung ermöglicht.[220]

[219] Chainalysis, *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class*, 2. Februar 2022.
[220] Wired Magazine, *Most Criminal Cryptocurrency Funnels Through Just 5 Exchanges*, 26. Januar 2023. Europol, *Bitzlato: senior management arrested*, 23. Januar 2023.

Sofern ein mit einer kriminellen Aktivität verbundenes Wallet identifiziert wurde und sich die inkriminierten VAs noch auf der Wallet befinden, stellt die Sicherstellung der sich darauf befindenden VAs ebenfalls eine grosses Herausforderung dar. Wenn sich die mit der kriminellen Aktivität verbundenen VAs auf einer *custodial* Wallet befinden, ist es möglich, über den Finanzintermediär bzw. VASP, der das Wallet verwaltet und folglich den privaten Schlüssel dazu besitzt, auf das Wallet zuzugreifen. Voraussetzung hierfür ist erstens die Möglichkeit zur Kontaktaufnahme seitens Strafverfolgungsbehörden, und zweitens die Bereitschaft zur Zusammenarbeit seitens des VASP. Bei verschiedenen von der BKP bearbeiteten Fällen konnten sich auf einer *custodial* Wallet befindende VAs sichergestellt werden.

Wenn sich die inkriminierten VAs jedoch auf einer *non-custodial* Wallet befinden, hat nur der tatsächliche Besitzer des Wallets den privaten Schlüssel (oder mehrere Personen im Falle einer *Multisig Wallet*). In diesem Fall ist es für die Strafverfolgungsbehörden deutlich schwieriger, auf das Wallet zugreifen zu können, die VAs zu beschlagnahmen und damit mögliche zukünftige Transaktionen zu blockieren. Ein von der BKP bearbeiteter Fall hat allerdings gezeigt, dass es unter günstigen Umständen durchaus möglich ist, VAs auch auf einem *non-custodial* Wallet sicherzustellen.

Gefährdung 10

Anonymität der Transaktionen und schwierige Identifikation der wirtschaftlich Berechtigten (2018 identifiziert, unverändert) [221]

Im sektoriellen Bericht von 2018 wurde festgehalten, dass VAs bezüglich Anonymität (bzw. Pseudonymität) mit einem ähnlichen Risiko wie Bargeld verbunden sei. Die Gefährdung, die von VAs ausgehe, sei aber durch die technologiebedingte Schnelligkeit und Mobilität der Transaktionen erhöht.

Seit 2018 sind die Tools von Blockchainanalyse-Unternehmen deutlich effizienter geworden und verfügen zum Beispiel über Features zur automatischen Erkennung von spezifischen Verschleierungstechniken und Transaktionsmustern. Verschiedene Fälle zeigen, dass der Einsatz dieser Tools und die Zusammenarbeit mit Blockchainanalyse-Unternehmen erfolgreich sein kann (vgl. Kapitel 8.2.2 und 8.2.4). Gleichzeitig bestehen jedoch nicht zu unterschätzende Bestrebungen innerhalb der «Crypto Community», die Möglichkeiten zur Verschleierung und Wahrung der Anonymität sicherzustellen und auszubauen. Die Bemühungen dieser beiden antagonistischen Interessengruppen können als Wettrüsten angesehen werden, dessen Ende oder Gewinner noch nicht absehbar ist. Gegenüber 2018 hat sich diese Gefährdung folglich nicht signifikant verändert.

7.4.2 Nationale und internationale Kooperation

Eine weitere Herausforderung technologischer Natur – und einer der Hauptgründe für die Entwicklung der Datenbank PICSEL – stellt die Erkennung von zusammenhängenden Fällen (Straftatenserien) dar. Im Rahmen der Umfrage bei Schweizer Polizeibehörden sprachen sich einige Behörden für einen verstärkten Austausch von Daten und Informationen untereinander aus, um die Erkennung von Serien zu erleichtern.

[221] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 21 – 22.

Typologie 4

Erkennung eines organisierten Betrugsschemas

Ein schweizerischer Finanzintermediär mit VASP-Tätigkeit bietet seinen Kunden den Kauf von VAs via seine App an. Dort können VAs mit Kreditkarten und weiteren elektronischen Zahlungsmitteln wie Apple Pay oder Google Pay erworben werden. Der Finanzintermediär wurde von einer ausländischen Strafverfolgungsbehörde kontaktiert und informiert, dass ein mutmassliches Betrugsopfer eine Anzeige erstattet hätte, da dessen Kreditkarteninformationen ohne sein Wissen benutzt wurden, um VA-Käufe auf der Plattform des Finanzintermediärs zu erwerben. Daraufhin erstattete der Finanzintermediär eine Verdachtsmeldung bei der MROS. Die Verdachtsmeldung enthielt jedoch nur sehr wenige Informationen, die der MROS dienlich waren, um die gemeldeten Zahlungsflüsse zurück- und nachzuverfolgen sowie mit bereits vorhandenen Angaben in der Datenbank der MROS in Verbindung zu setzen. Aus dem beigelegten Schreiben der ausländischen Strafverfolgungsbehörde war der Name des mutmasslichen Betrugsopfers ersichtlich, wobei jedoch beim Finanzintermediär keine Geschäftsbeziehung auf diesen Namen eröffnet wurde. Der Finanzintermediär besass auch nicht die vollständigen Kreditkartenangaben des Betrugsopfers, da die Bezahlung für die vom Finanzintermediär ausgehändigten VAs indirekt über einen Zahlungsabwickler erfolgte. Er konnte der MROS lediglich die sechs ersten sowie die vier letzten Ziffern der benutzten Kreditkarte mitteilen. Auch zu ihrem «Kunden» – bei dem es sich offensichtlich nicht um dieselbe Person wie das ausländische Betrugsopfer handelte – besass der meldende Finanzintermediär nur wenige Angaben. Der Finanzintermediär hatte keine Angaben zu diesem Kunden (Name, Adresse, Geburtsdatum, usw.) und konnte der MROS lediglich mitteilen, von welcher IP-Adresse und mit welchem Mobiltelefon-Modell sich der mutmassliche Betrüger in die App des Finanzintermediärs eingeloggt hatte. Die erworbenen VAs wurden direkt nach Eingang des von der Kreditkarte des Opfers abgebuchten Betrags auf eine VA-Adresse versendet, über die der Finanzintermediär selbst keine Verfügungsmacht hatte und folglich nicht sperren konnte (*non-custodial* Wallet). Die Analyse durch die MROS anhand von Informationen aus weiteren Verdachtsmeldungen desselben Finanzintermediärs zeigte, dass verschiedene mutmasslich betrügerisch ausgelöste Transaktionen, die der MROS in unterschiedlichen Verdachtsmeldungen zur Kenntnis gebracht wurden, nach mehreren Zwischenstationen auf ein- und derselben Zieladresse landeten, was ein starker Hinweis für ein organisiertes Betrugsschema darstellt.

Tatsächlich erhielt die MROS im untersuchten Zeitraum zahlreiche Verdachtsmeldungen mit ähnlichem Sachverhalt, wie sie in der obigen Typologie beschrieben werden. Die mutmasslichen Betrugsopfer waren dabei fast ausschliesslich im Ausland domiziliert. Gemeinsamer Nenner dieser Meldungen war jeweils einerseits, dass die Finanzintermediäre fast keine Informationen zu den mitgeteilten Geschäftsbeziehungen besassen.[222] Andererseits handelte es sich bei den einzelnen Meldungen jeweils um gemeldete Transaktionen von geringem Gegenwert. Es ist naheliegend, dass Verdachtsmeldungen mit solch ähnlich gelagerten Sachverhalten auf grössere, organisierte Betrugsschemas hindeuten, umso mehr, wenn bei der Nachverfolgung der mutmasslich gestohlenen VAs durch die MROS Verschleierungstechniken identifiziert werden. Im Rahmen der Analysetätigkeit der MROS sowie bei der Behandlung solcher Fälle durch Strafverfolgungsbehörden ist die Herstellung von inhaltlichen Zusammenhängen dieser «Einzelfälle», beispielsweisse mittels Tracingtools oder durch den Informationsaustausch mit ausländischen Behörden, mit grossen Herausforderungen und Ressourcenaufwand verbunden. Die einzelnen Verdachtsmeldungen oder Strafanzeigen enthalten häufig wenig bis keine relevanten Informationen, die bei der Ermittlung der mutmasslichen Täterschaft helfen könnten. Die gemeldeten Transaktionen sind

[222] Zum Beispiel persönliche Angaben zu den konkreten Benutzern der App sowie zu den Konten, woher eingezahlten Gelder stammten, mit denen VAs erworben wurden.

zudem meistens von geringem Gegenwert, was zur Folge haben kann, dass die Beantwortung von Informationsanfragen durch ausländische Meldestellen viel Zeit in Anspruch nimmt, da diese Anfragen nicht prioritär behandelt werden. Hier besteht auf Seiten der Strafverfolgungsbehörden eine hohe Verwundbarkeit, dass solche organisierte Betrugssysteme zur Entwendung und zum Waschen von VAs nicht entdeckt werden.

Nebst der interkantonalen Datenbank PICSEL, die als Instrument zur analytischen Verknüpfung solcher Einzelfälle zu einem Gesamtbild dienen kann, existiert in der Schweiz mit NEDIK (Netzwerk digitale Ermittlungsunterstützung Internetkriminalität) ein Gefäss, in dem Spezialistenressourcen gebündelt sind und in dessen Rahmen einzelne kantonale Polizeikorps Leistungen zugunsten aller Polizeikorps in der Schweiz erbringen. Von NEDIK werden regelmässige Treffen zur VA-Thematik durchgeführt, die den Informationsaustausch sicherstellen und diesbezügliche Standards festlegen. Kleinere Kantone mit wenig Ressourcen können analog zu anderen Spezial-Werkzeugen via Amtshilfe beim Bund oder bei kompetenten Kantonen um Hilfe ersuchen. Gemäss den eingeholten Informationen investierten hierbei einzelne grosse Kantone wie Zürich Ressourcen in den Aufbau ihres Know-Hows und ihrer Tools, um in Eigenregie oder für anfragende Behörden Analysen im Bereich der Cyberkriminalität durchzuführen. Ebenfalls haben sich die spezialisierten Ermittler weltweit mit weiteren polizeilichen VA-Spezialisten vernetzt. So stehen Strafverfolgungsbehörden international über verschiedene Netzwerke in Kontakt zueinander und können beispielsweise via Interpol oder Europol Informationen austauschen und Ermittlungen koordinieren.

Eine weitere Möglichkeit bildet der Austausch zwischen den nationalen Geldwäschereimeldestellen, zum Beispiel im Rahmen der Egmont Group of Financial Intelligence Units. Die MROS als schweizerische Financial Intelligence Unit (FIU) erhält von ihren Partnerbehörden im Ausland wertvolle Informationen und Anfragen in Zusammenhang mit der Verwendung von VAs für GW/TF-Zwecke mit Bezug zur Schweiz. Diese Informationen kann sie zu Intelligence-Zwecken gegebenenfalls an andere mit der GW/TF-Bekämpfung befassten Behörden und Ämtern in der Schweiz weiterleiten. Umgekehrt versendet die MROS den ausländischen FIUs Spontaninformationen und Informationsanfragen, teilweise für eigene Analysezwecke, teilweise aber auch amtshilfeweise für andere schweizerische Behörden. Aus den hier genannten Austauschplattformen sind mehrere Projekte und Produkte entstanden, wie beispielsweise Kataloge mit Informationen über die in unterschiedlichen Ländern angesiedelten Finanzintermediäre mit VASP-Tätigkeit oder «Best Practices»-Anleitungen für Strafverfolgungsbehörden bei Ermittlungen im Zusammenhang mit VAs sowie Kontaktaufnahmen mit Finanzintermediären mit VASP-Tätigkeit im Ausland.

Hierbei zeigten Gespräche mit Strafverfolgungsbehörden auf Kantons- und Bundesebene, dass in mehreren Fällen VAs auf Plattformen ausländischer Finanzintermediäre mit VASP-Tätigkeit gesperrt und den Opfern zurückerstattet werden konnten. Dies erfolgte teilweise mittels internationaler Rechtshilfe, teilweise mithilfe der Budapester Konvention (Vgl. Infobox 5).

Infobox 5

Die Budapester Konvention

Das Übereinkommen vom 23. November 2001 über die Cyberkriminalität («Budapester Konvention») ist ein internationales Übereinkommen zur Bekämpfung von Cyberkriminalität. Diese Konvention wurde im Jahr 2001 vom Europarat verabschiedet und hat mittlerweile 65 Unterzeichnerstaaten, einschliesslich der meisten europäischen Länder, der USA und Japan.

In der Schweiz trat die Budapester Konvention im Jahr 2012 in Kraft.[223] Strafverfolgungsbehörden können von der Budapester Konvention profitieren, um auf elektronische Beweismittel, die sich im Ausland befinden, zuzugreifen, einschliesslich der Daten, die von privaten Unternehmen gespeichert werden, ohne über die Wege der Rechtshilfe zu gehen.

So sieht Artikel 32 der Konvention vor, dass unter bestimmten Bedingungen ein grenzüberschreitender Zugriff auf elektronische Beweismittel möglich ist. Dies beinhaltet auch Daten zu Geschäftsbeziehungen bei Finanzintermediären mit VASP-Tätigkeit, die in den Unterzeichnerstaaten domiziliert sind. Auf diese Weise kann beispielsweise zeitnah ermittelt werden, auf welchen Namen ein Konto bei einem ausländischen Finanzintermediär mit VASP-Tätigkeit lautet, wer daran wirtschaftlich berechtigt ist, oder welche Transaktionen zu welchem Zeitpunkt über dieses Konto abgewickelt wurden. Da Geldwäscherei und Terrorismusfinanzierung mittels VAs oft transnational und mit sekundenschnellen Transaktionen stattfinden, kann die Konvention die Arbeit der Strafverfolgungsbehörden beschleunigen, zu höheren Aufklärungsraten sowie zu mehr Sperrungen und Einziehungen von VA-Vermögenswerten führen. Dies ist eine Chance gegenüber herkömmlichen Ermittlungen, deren Erfolg von der Reaktionszeit ausländischer Behörden bei der Ausführung internationaler Rechtshilfeersuchen und von den Fristen für die Zurückhaltung von Finanzdokumenten durch die Banken abhängt, die je nach Gerichtsbarkeit sehr unterschiedlich sind.

Auf die Budapester Konvention wurde bereits im sektoriellen KGGT-Bericht von 2018 verwiesen, wobei damals erst wenige Erkenntnisse zu dieser Möglichkeit des grenzüberschreitenden Zugriffs auf elektronische Beweismittel vorlagen.[224] Gemäss den im Rahmen der vorliegenden Risikoanalyse eingeholten Informationen sind Erfahrungen der Schweizerischen Strafverfolgungsbehörden im Zusammenhang mit der Anwendung der Budapester Konvention durchzogen. Einige Strafverfolgungsbehörden scheinen tendenziell gute Erfahrungen gemacht zu haben. Andere betonen, dass sich die Zusammenarbeit mit privaten Unternehmen im Ausland schwierig gestalte und von Fall zu Fall unvorhersehbar sei, ob diese die Herausgabe von Daten genehmigen oder verweigern und sodann auf den Rechtshilfeweg verweisen würden, wodurch wertvolle Ermittlungszeit verloren gehe. Manche Unternehmen würden einen Mittelweg gehen, indem sie zwar die Daten herausgeben, jedoch nicht für Beweis- sondern lediglich für «Intelligence»-Zwecke. Dadurch liesse sich anhand der Daten zwar weiterermitteln, diese seien jedoch erst als Beweismaterial verwendbar, wenn sie in einem zweiten Schritt über die internationale Rechtshilfe eingeholt werden.

Verwundbarkeit 5

Schwierige Repression von GW/TF im VA-Bereich (2018 identifiziert, 2023 unverändert)[225]

Die prinzipielle Anonymität oder Pseudonymität in Bezug auf die Funktionsweise von VAs, die Dezentralität in ihrer Architektur insbesondere im Bereich von DeFi und DAOs, sowie die ausgeprägten internationalen Verflechtungen von Geschäftsbeziehungen im VA-Bereich führt dazu, dass die Strafverfolgungsbehörden Schwierigkeiten haben, entsprechende Ansprechpartner zu identifizieren und zu kontaktieren, wenn es darum geht, die für ihre Ermittlungen oder Verfahren relevanten Informationen einzuholen. Falls Ansprechpartner identifiziert werden, sind diese in der Regel nicht im selben Land angesiedelt wie die

[223] SR 0.311.43 – *Übereinkommen vom 23. November 2001 über die Cyberkriminalität*, Fassung vom 14.09.2020.
[224] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 40 – 41.
[225] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 34 – 35.

entsprechende Strafverfolgungsbehörde. Sofern nicht auf Basis der Budapester Konvention die entsprechenden Informationen eingeholt werden können, müssen die Strafverfolgungsbehörden über die internationale Rechtshilfe diese Informationen beantragen. Dies ist in der Regel zeitintensiv, was bereits bei nicht VA-relevanten Ermittlungen und Verfahren in Zusammenhang mit der Nachverfolgung von Finanzflüssen eine Herausforderung für Strafverfolgungsbehörden darstellt. Diese Herausforderung wird umso grösser im VA-Bereich, der im Vergleich zum traditionellen Zahlungsverkehr von sekundenschnellen Transaktionen über mehrere Blockchains, Finanzintermediäre, dezentralisierte Plattformen und nationale Grenzen hinweg geprägt ist. Dies erschwert die Aufklärung von Straftaten in diesem Bereich im Allgemeinen sowie die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung im Spezifischen.

Untereinander verglichen – sowohl international als auch innerhalb der einzelnen Länder – scheint es zudem starke Unterschiede in Bezug auf die Expertise von Strafverfolgungsbehörden im VA-Bereich zu geben. Während einzelne Behörden frühzeitig in den Wissens- und Kapazitätsaufbau investierten und über die notwendigen Tools zur Aufklärung von Straftaten verfügen, fehlt diese Entwicklung bei anderen Behörden gänzlich. Dadurch wird die nationale und internationale Zusammenarbeit sowohl auf kommunikativer als auch auf ermittlungs- und verfahrenstechnischer Ebene erschwert. Die weltweit ungleichen oder auch vollständig abwesenden Regulierungsansätze, gepaart mit einer unterschiedlichen Gewichtung und Priorisierung von Fällen im VA-Bereich, erhöhen dabei die Risiken einer regulatorischen Arbitrage durch Kriminelle, die gezielt regulatorische Schlupflöcher ausnützen, um die Entdeckung oder strafrechtliche Verfolgung ihrer Aktivitäten zu erschweren.

7.4.3 Rechtsprechung

Gemäss den im Rahmen der vorliegenden Risikoanalyse getätigten Nachforschungen scheinen in der Schweiz bisher weder auf Bundes- noch auf Kantonsebene rechtsgültige Gerichtsurteile in Zusammenhang mit Geldwäscherei und der Verwendung von VAs vorzuliegen. Solche Urteile könnten detailliert aufzeigen, unter welchen Bedingung der Straftatbestand der Geldwäscherei in Zusammenhang mit der Verwendung erfüllt ist. Lediglich ein Urteil des Bundesstrafgerichtes vom Dezember 2022 enthält hierzu mehr Informationen. Dabei ging es um eine durch das Bundesstrafgericht abgewiesene Beschwerde einer Person, die sich dagegen wehren wollte, dass die Genfer Staatsanwaltschaft im Rahmen der internationalen Rechtshilfe gegenüber einem anderen europäischen Staat dessen Bankunterlagen übermittelte. Eine Strafverfolgungsbehörde im betreffenden Land wirft dieser Person (sowie weiteren Personen) unter anderem Steuerhinterziehung und bandenmässige Geldwäscherei vor. Im Urteil heisst es wörtlich (aus dem Französischen übersetzt): «Der Umtausch von Geld in Kryptowährungen oder [Anm.: weitere Handlungen] sind Verhaltensweisen, die die Identifizierung der Herkunft, die Entdeckung oder die Einziehung von Vermögenswerten im Sinne von Art. 305bis StGB erschweren können.»[226]. Der «einfache» Umtausch von Fiatgeld in VAs genügt aus Sicht des Bundesstrafgerichts folglich bereits, um den Straftatbestand der Geldwäscherei zu erfüllen.

7.5 Verwundbarkeiten bei der Finanzintermediation im VA-Bereich

Die Verwundbarkeit bei Finanzintermediären, für Geldwäscherei- oder Terrorismus-finanzierungszwecke missbraucht zu werden, kann unter anderem, allerdings nicht

[226] RR.2022.45, *Arrêt du 20 décembre 2022*, Urteil des Bundesstrafgerichts, Bellinzona, 21. Dezember 2022.

vollumfänglich, durch eine angemessene Aufsicht mitigiert werden. Die überwiegende Mehrheit der schweizerischen Finanzintermediäre mit VASP-Tätigkeit ist einer Selbstregulierungsorganisation (SRO) angeschlossen (174) und wird folglich von diesen beaufsichtigt, während Banken und Wertpapierhäuser mit VASP-Tätigkeit direkt der FINMA unterstellt sind (ca. 30).[227]

Konsolidierte Informationen zur konkreten Aufsicht über die Finanzintermediäre mit VASP-Tätigkeit durch die verschiedenen SROs konnten nicht erhältlich gemacht werden. Ein Informationsaustausch, den die MROS bereits im Jahr 2021 mit einer Selbstregulierungsorganisation geführt hatte, zeigte allerdings, dass die ihr angeschlossenen Mitglieder mit VASP-Tätigkeit strengeren Aufsichtsregeln unterstehen als die übrigen Mitglieder. So werden Mitglieder mit VASP-Tätigkeit beispielsweise innerhalb von maximal sechs (anstelle von den sonst in der Regel üblichen maximal 12) Monaten nach Aufnahme in die Selbstregulierungsorganisation einer Prüfung unterzogen. Die Prüfung der Einhaltung von GwG-Vorschriften wird entweder von den SROs selber oder von durch die jeweiligen SROs akkreditierten Prüfgesellschaften durchgeführt.

Typologie 5

Schweizer Aktiengesellschaft mit SRO-Lizenz durch anonyme Käufer mit VAs erworben

Ein schweizerischer Finanzintermediär mit VASP-Tätigkeit meldete die Geschäftsbeziehung mit einem schweizerischen Firmenkunden, der sich offenbar auf die Errichtung von schweizerischen Gesellschaften und Treuhanddienstleistungen spezialisierte. Letzterer bewarb auf seiner Website die Errichtung von Gesellschaften in der Schweiz für ausländische Personen sowie die Übernahme sämtlicher «bürokratischer» Arbeiten wie die Errichtung einer Firmenwebsite, eines Firmenlogos, einer Firmenbroschüre, die Erstellung von Visitenkarten, bis zur Zurverfügungstellung von c/o-Briefkasten sowie einer «kurzfristigen» Zurverfügungstellung eines voll ausgestatteten Büroplatzes. Für einen Aufpreis «verkaufte» er zudem Postadressen ohne «c/o» – allem Anschein nach, um den Eindruck zu vermeiden, dass es sich bei den gegründeten Gesellschaften um Briefkastenfirmen handeln könnte. Letztlich wurde auch die Unterstützung bei der Erlangung einer SRO-Lizenz von Mitarbeitern der Firmenkunden in sozialen Netzwerken im Internet beworben.

Der besagte Firmenkunde eröffnete beim meldenden Finanzintermediär eine Geschäftsbeziehung mit der Begründung, seiner Kundschaft die Möglichkeit zur Zahlung in Kryptowährungen anbieten zu können. Einige Zeit nach Eröffnung der Geschäftsbeziehung wurde der meldende Finanzintermediär auf drei Zahlungseingänge von einer unbekannten Kryptoadresse aufmerksam, die im Abstand weniger Minuten eintrafen und sich zu einem mittleren sechsstelligen Betrag (in Schweizer Franken) addierten. Jede der drei Zahlungen blieb allerdings leicht unter der Betragsschwelle, bis zu welcher der meldende Finanzintermediär solche Zahlungen überhaupt erlaubte. Dies erschien dem meldenden Finanzintermediär verdächtig (*Smurfing*), weshalb er den Firmenkunden kontaktierte und den wirtschaftlichen Hintergrund der eingehenden Transaktionen klären wollte. Der Firmenkunde antwortete, dass diese Zahlungen mit dem Verkauf einer seiner Firmen im Zusammenhang stehen würden. Hierfür reichte er dem Finanzintermediär einen Verkaufsvertrag zur Plausibilisierung ein, aus welchem ersichtlich wurde, dass der Firmenkunde 100% der Aktien einer schweizerischen Gesellschaft an zwei Käufer veräusserte – wobei allerdings die Namen der Käufer durch den Firmenkunden selbst geschwärzt wurden. Auf die Frage nach dem Grund für die Aufteilung der Zahlung in drei Teile erklärte der Firmenkunde, dass dies dem Wunsch der Käufer entspreche, um die Rechnung bei Bedarf zu unterschiedlichen Zeitpunkten bezahlen zu können und dabei günstige Wechselkurse zu wählen. Dies erschien dem meldenden Finanzintermediär hinsichtlich der in Minutenabständen eingetroffenen Zahlungen

[227] Stand Ende 2022.

nicht plausibel, weshalb er der MROS eine Verdachtsmeldung erstattete. Die verkaufte Aktiengesellschaft selbst war Mitglied einer Selbstregulierungsorganisation (SRO) und damit ein in der Schweiz regulierter Finanzintermediär.

Folglich wurde im vorliegenden Fall ein Verkauf eines schweizerischen Finanzintermediärs an anonyme Käufer mittels VAs abgewickelt.

Gefährdung 11

***Travel Rule* wird bei Händlerkonten schweizerischer Finanzintermediäre mit VASP-Tätigkeit nicht angewendet** (2023 identifiziert)

In der Schweiz können natürliche und juristische Personen für die von ihnen erbrachten Dienstleistungen VAs als Zahlungsmittel akzeptieren. Schweizerische Finanzintermediäre mit VASP-Tätigkeit bieten juristischen Personen mit Sitz in der Schweiz sogenannte Händlerkonten an. Laut der Website eines schweizerischen Finanzintermediärs mit VASP-Tätigkeit können die besagten juristischen Personen mit diesen Konten VA-Zahlungen empfangen. Die Einhaltung der Sorgfalts- und Meldepflichten obliegt dabei dem schweizerischen Finanzintermediär, der diese Händlerkonten anbietet. Im Unterschied zu den Bestimmungen der *Travel Rule* scheinen hierbei im Vornherein keine Angaben zum Absender der VAs durch den schweizerischen Finanzintermediär mit VASP-Tätigkeit eingeholt zu werden (vgl. Abbildung 9 in Kapitel 4.6.4). Dadurch erhöht sich das Risiko, dass solche Angebote durch schweizerische juristische Personen für das Waschen von VAs, insbesondere in Zusammenhang mit handelsbasierter Geldwäscherei, missbraucht werden können. Der MROS sind zudem Fälle bekannt, bei denen der Grenzwert von VA-Zahlungen mittels *Smurfing* überschritten wurde.

Wie die SROs setzt auch die FINMA Prüfgesellschaften ein, um die ihr unterstellten Institute risikoorientiert nach Geldwäschereigesetz zu prüfen. Im Sommer 2021 hat die FINMA ihre Erwartungen an die Prüfgesellschaften für die Prüfung von Instituten, die im VA-Bereich tätig sind, präzisiert. Die Prüfgesellschaften examinieren anhand eines spezifischen VA-/VASP-Prüfmoduls die FINMA-unterstellten Institute mit VASP-Tätigkeit.

Die FINMA prüfte zudem bei mehreren ihr unterstellten Finanzdienstleistern, wie sie die Prüfung der wirtschaftlichen Berechtigung ihrer Kunden an einer *non-custodial* Wallet umsetzen. Eine oft angetroffene Lösung besteht darin, dass der Finanzintermediär im Voraus mit seinem Kunden den Betrag (etwa eine Mikrozahlung) und den Zeitpunkt, zu dem eine Überweisung getätigt wird, vereinbart. Eine zweite Lösung fordert den Kunden auf, innerhalb einer bestimmten Frist eine eindeutige Nachricht auf der Blockchain zu verschicken. Dieses Verfahren ist bei der ersten Überweisung durchzuführen. Danach kann die Adresse auf eine «White List» gesetzt werden, womit sich bei späteren Überweisungen mit derselben Adresse eine entsprechende Überprüfung erübrigt. Dieses Verfahren wird anschliessend in regelmässigen, vom Institut festgelegten Abständen und zum Beispiel nach Transaktionen mit erhöhten Risiken wiederholt sowie wenn an der Verfügungsmacht über die externe Wallet ein Zweifel aufkommen. Bei Transaktionen, bei denen auf der Gegenseite ein Dienstleister mit Sammel-Wallets steht, sind diese Verfahren technisch nicht umsetzbar. Für solche Fälle akzeptiert die FINMA eine Verifizierung der Verfügungsmacht via Screenshot: Der empfangende Finanzintermediär verlangt einen Screenshot der vom Kunden angekündigten Transaktion. Das gelieferte Dokument dient als Nachweis, dass der Kunde Verfügungsmacht

über das beim VASP belastete Konto hat.[228] Neu zu den angemessenen Prüfmethoden hinzugekommen ist das Time-Boxing-Verfahren. Dabei wird einer vorangehenden Mikrotransaktion ein Betrag von den Kundinnen und Kunden direkt überwiesen. Letztere müssen die Transaktion und den gewünschten Betrag voranmelden, woraufhin der Finanzintermediär ihnen die Adresse sowie ein kurzes Zeitfenster (Time Box) zur Verfügung stellt. Innerhalb dieser Angaben lässt sich die vereinbarte Transaktion vornehmen. Der Nachweis der Verfügungsmacht erfolgt über die Überprüfung, ob diese Vorgaben eingehalten werden. Ebenfalls neu hinzugekommen ist das Wallet-Log-in der Kundinnen und Kunden in Anwesenheit von Mitarbeitenden des Finanzintermediärs. Sofern der Vorgang hinreichend dokumentiert wird, ist auch diese Massnahme im Sinne der FINMA- Aufsichtsmitteilung 02/2019 «Zahlungsverkehr auf der Blockchain» geeignet.

Geschäftsmodelle mit Bezug zur Blockchain-Technologie stossen bei Anlegerinnen und Anlegern nach wie vor auf grosses Interesse. Dies machen sich auch unseriös agierende Marktteilnehmer weiterhin zunutze, indem sie entsprechende Angebote lancieren und oftmals über einen Internetauftritt Kunden anwerben. Typischerweise wird dabei versucht, Anleger unter Vorspiegelung nicht existenter Unternehmen und Produkte zur Investition in Kryptowährungen zu verleiten. Sofern sie ihr bekannt sind, nimmt die FINMA solche Marktteilnehmer in ihre Warnliste auf und warnt so Anleger. Zudem stimmt sie sich diesbezüglich mit inländischen Strafbehörden sowie mit ausländischen Aufsichtsbehörden ab. Im Bereich Fintech hat sich die FINMA intensiv mit ICOs in der Schweiz befasst. Aufgrund des frühen Stadiums vieler ICO können dabei zahlreiche Unsicherheiten in Bezug auf die zu finanzierenden und durchzuführenden Projekte bestehen. Die FINMA kann nicht ausschliessen, dass ICO-Aktivitäten in betrügerischer Absicht erfolgen. Betrügerisches oder missbräuchliches Verhalten oder die Umgehung des regulatorischen Rahmens werden von der FINMA nicht toleriert, und bei Bedarf ergreift sie erforderliche Enforcementmassnahmen.

Insgesamt klärte sie rund 60 ICOs ab, wobei mehr als die Hälfte der Abklärungen abgeschlossen werden konnten. Bei mehr als zehn ICOs hat die FINMA eine Verletzung des Geldwäschereigesetzes festgestellt und Strafanzeige gegen die verantwortlichen Personen erstattet. In acht weiteren Fällen kam es zu einem Eintrag auf der Warnliste der FINMA. Gegen drei Gesellschaften führte die FINMA schliesslich ein Enforcementverfahren, wovon eines bereits abgeschlossen ist. Bei einem dieser Verfahren ignorierte die Gesellschaft die vorgängige Einschätzung der FINMA im Rahmen der Beantwortung der Unterstellungsanfrage. Darüber hinaus hat die FINMA bei mehreren Unternehmen Massnahmen zur Wiederherstellung des ordnungsgemässen Zustands angeordnet. Diese Massnahmen umfassten unter anderem die Rückzahlung unerlaubt entgegengenommener Publikumseinlagen nach Bankengesetz und die Entfernung des Begriffs Bank oder von Werbung mit nicht vorhandenen FINMA-Bewilligungen. Als neuere Entwicklung ist ein Trend hin zum Angebot von Stablecoins feststellbar, die insbesondere Fragen zur Anwendbarkeit des Geldwäscherei-, des Banken- und des Kollektivanlagengesetzes aufwerfen.

Neben Marktaktivitäten im Bereich ICO stellte die FINMA auch ein zunehmendes Engagement von Schweizer Anbietern in sekundärmarktbezogenen Finanzdienstleistungen im Kryptobereich fest. Diese umfassten beispielsweise den Handel und die Aufbewahrung von Token sowie den Betrieb von Handelsplätzen und diese unterstützenden Tätigkeiten. Der Geschäftsbereich Enforcement führte in den letzten Jahren Abklärungen gegen mehrere solcher Anbieter. Bei einem Handels- und Aufbewahrungsdienstleister für Token stellte die FINMA Verstösse gegen das Banken- und das Börsengesetz fest, ordnete umfangreiche Massnahmen zur Wiederherstellung des ordnungsgemässen Zustands an und erstattete Strafanzeige. Die FINMA führt zudem ein Enforcementverfahren gegen einen Anbieter von Money Transmitting zwischen Kryptohandelsplätzen und deren Kunden wegen unerlaubter Entgegennahme von Publikumseinlagen. In einem weiteren Fall eröffnete die FINMA ein Enforcementverfahren wegen unerlaubten Effektenhandels mit Token. Ebenso hat die FINMA

[228] Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2020*, März 2021, S. 43 – 44.

unterschiedliche Coin-Anbieter verboten und im Mai 2023 ein Verfahren gegen eine im Kryptobereich tätige Stiftung sowie deren Stiftungsgründer abgeschlossen. Dabei kam sie zum Schluss, dass die aufsichtsrechtlichen Bestimmungen in verschiedener Hinsicht schwer verletzt wurden. Gegen die Stiftung wurde bereits im März 2023 ein Konkursverfahren eingeleitet. Gegenüber dem Stiftungsgründer hat die FINMA eine Unterlassungsanweisung ausgesprochen. Diese bleibt für die Dauer von fünf Jahren auf ihrer Webseite veröffentlicht.[229] Insgesamt beobachtet die FINMA im Zusammenhang mit VA-Dienstleistungen eine zunehmende Anzahl betrügerischer Internetseiten, die ihren Kunden vermeintliche Investitionen in Kryptowährungen anbieten, ohne die einbezahlten Mittel zweckgemäss zu verwenden. Nach Möglichkeit warnt die FINMA vor solchen Angeboten mittels ihrer Warnliste. Im Bereich des illegalen Glücksspiels behandelte die Eidgenössische Spielbankenkommission (ESBK) als Aufsichtsbehörde über die Spielbanken im Jahr 2019 zwei Fälle, bei denen in einem Spieletablissement ein VA-Automat für die Gewinnauszahlung an die Spieler stationiert war. Hierbei kam es in einem Fall zu einer Anklage, wobei das Verfahren noch hängig ist. Im anderen Fall konnte nicht rechtsgenügend nachgewiesen werden, dass der vorgefundene VA-Automat tatsächlich für die Auszahlung von Spielgewinnen verwendet wurde, bzw. wer der eigentliche Betreiber der illegalen Plattform ist. Die ESBK geht davon aus, dass sich VAs in Zusammenhang mit illegalen Glückspielangeboten in der Schweiz zu einem beliebten Zahlungsmittel entwickeln könnten.

7.5.1 Meldende Finanzintermediäre

Die Auswertung der VA-relevanten Verdachtsmeldungen der Jahre 2020 bis 2022 zeigt auf, dass die Finanzintermediäre ein sehr unterschiedliches Meldeverhalten aufweisen, je nachdem, ob sie selbst eine VASP-Tätigkeit ausüben oder nicht.

	2020		**2021**		**2022**		**2020-2022** (Summe)	
VA-relevante Verdachts-meldungen	312		499		1056		1867	
	Mit VASP	**Ohne VASP**	**Mit VASP**	**Ohne VASP**	**Mit VASP**	**Ohne VASP**	**Mit VASP**	**Ohne VASP**
Anzahl meldende Finanz-intermediäre	12	40	19	57	12	93	24	118
Anzahl Meldungen mit VA-Bezug	104	208	178	321	143	913	425	1442

Abbildung 27: VA-relevante Verdachtsmeldungen und ihr Anteil am gesamten Meldeaufkommen (2020 – 2022), eingeteilt nach Tätigkeit des Finanzintermediärs (VASP oder nicht).

Bemerkenswerterweise stammen 1442 der 1867 (77%) der in der ausgewerteten Zeitperiode erhaltenen Meldungen von insgesamt 118 unterschiedlichen Finanzintermediären *ohne* VASP-Tätigkeit.

[229] Eidgenössische Finanzmarktaufsicht (FINMA), *FINMA schliesst Verfahren gegen Krypto-Plattform und deren Gründer ab*, Mai 2023.

Dabei handelte es sich in der Regel um Meldungen, in denen der Finanzintermediär die MROS auf verdächtige Transaktionen zwischen den gemeldeten Konten und den Konten von Finanzintermediären mit VASP-Tätigkeit im In- oder Ausland aufmerksam machte. Die Anzahl der von diesen Finanzintermediären erhaltenen VA-relevanten Verdachtsmeldungen hat sich seit 2020 kontinuierlich gesteigert.

Typologie 6

VA-relevante Verdachtsmeldung eines Finanzintermediärs ohne VASP-Tätigkeit

Eine Bank erstattete eine Verdachtsmeldung zu einer Geschäftsbeziehung mit einer natürlichen Person. Diese erhielt über mehrere Monate diverse Gutschriften von verschiedenen Bankkonten, die alle auf die Namen von unterschiedlichen natürlichen Personen lauteten. Die eingegangenen Überweisungen dieser Drittpersonen wurden jeweils umgehend vom gemeldeten Konto auf das Konto einer ausländischen VA-Börse überwiesen. Der meldende Finanzintermediär äusserte den Verdacht, dass die Drittpersonen, welche Geld auf das gemeldete Konto überwiesen hatten, wohl Opfer eines Betrugs seien. Der gemeldete Vertragspartner habe vermutlich als *Money Mule* gehandelt, indem er sein Konto gegen Entgelt unbekannten Auftraggebern zur Verfügung gestellt hätte, die am Betrug beteiligt seien. Der gemeldete Vertragspartner leitete diese Fiat-Beträge sodann an die VA-Börse weiter, wo sie in VAs umgetauscht und auf *non-custodial* Wallets transferiert wurden, die vermutlich von den unbekannten Auftraggebern kontrolliert wurden.

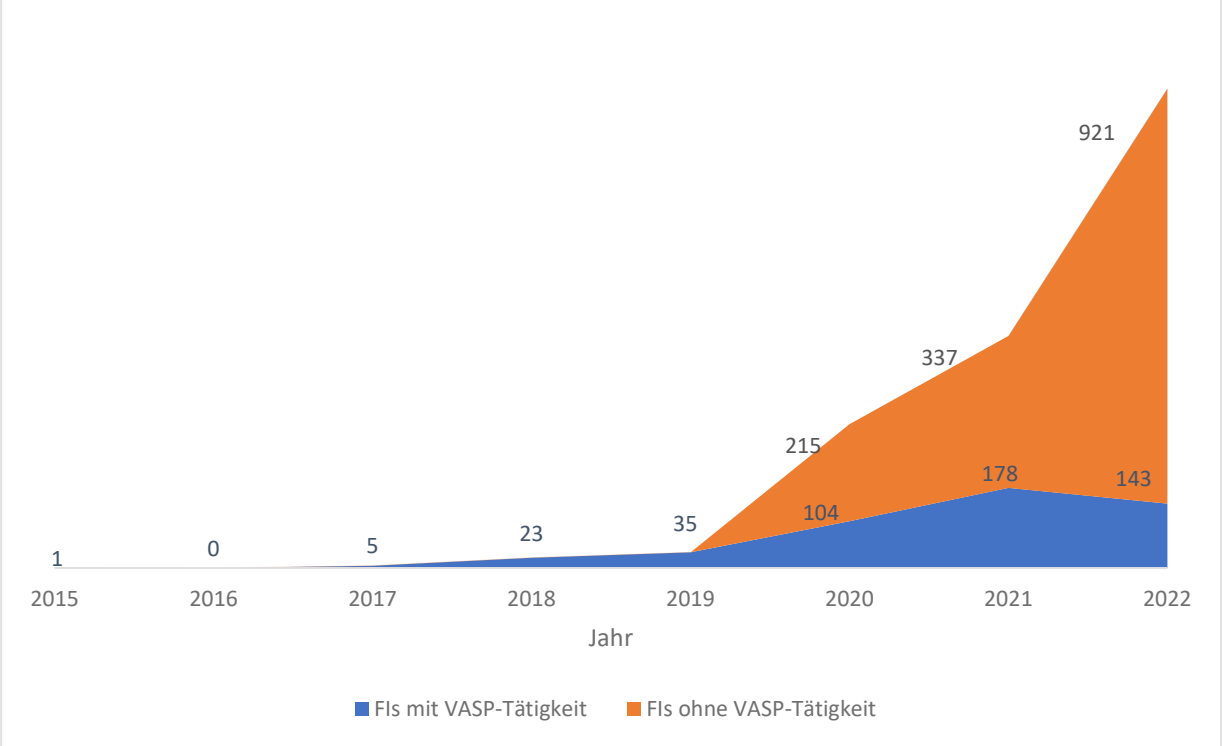


Abbildung 28: VA-relevante Verdachtsmeldungen von Finanzintermediären ohne VASP-Tätigkeit haben seit 2020 deutlich zugenommen als jene von Finanzintermediären mit VASP-Tätigkeit.[230]

[230] Hinweis: Für den Zeitraum vor 2020 wurden nur Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit gezählt, vgl. Kapitel 11.1.1 im Anhang.

Das Wachstum des VA-Bereichs, die zunehmende allgemeine Verwendung von VAs sowie die gesteigerte Verflechtung von Finanzintermediären mit und ohne VASP-Tätigkeit scheint dazu geführt zu haben, dass die Verwundbarkeit von Finanzintermediären, für GW/TF-Zwecke im Zusammenhang mit der Verwendung von VAs missbraucht zu werden, nicht mehr primär auf Finanzintermediäre mit VASP-Tätigkeit beschränkt ist. Die hohe Anzahl VA-relevanter Verdachtsmeldungen von Finanzintermediären ohne VASP-Tätigkeit ist ein starkes Indiz hierfür. Eine Auswertung dieser Meldungen zeigt, dass die bei diesen Finanzintermediären geführten Konten zum Beispiel für Durchlauftransaktionen, an deren Anfangs- oder Endpunkt eine Überweisung von oder zu einem Fiat-Konto einer VA-Börse steht, oder zum Parkieren von mutmasslich inkriminierten Vermögenswerten missbraucht werden, die zuvor bei einem Finanzintermediär mit VASP-Tätigkeit von VAs in Fiatwährung umgetauscht wurden. Aufgrund der verbreiteten Verwendung und der allgemeinen Etablierung des VA-Sektors sind Finanzintermediäre ohne VASP-Tätigkeit im Vergleich zu 2018 deutlich verwundbarer, für GW/TF-Zwecke unter Verwendung von VAs missbraucht zu werden, auch wenn sie keine eigenständige VASP-Tätigkeit ausüben. Diesbezügliche Fälle wurden häufiger und die damit verbundenen Beträge deutlich höher. Zudem sind diese Finanzintermediäre häufig auf externe Expertisen angewiesen, um mittels Blockchainanalysen zu plausibilisieren, welchen wirtschaftlichen Hintergrund die auf ihren Konten deponierte Fiatwährung hat, die zuvor über andere Anbieter von VAs in Fiat gewechselt wurde.[231] Hierbei sind der MROS Fälle bekannt, die klar aufzeigen, dass diese Expertisen nur bis zu einem gewissen Grad «Sicherheit» in Bezug auf die Plausibilisierung der Vermögensherkunft liefern können. Sofern Finanzintermediäre ohne VASP-Tätigkeit den Grad der Plausibilisierung nicht in eigenständiger Weise verstehen und einschätzen können, laufen sie Gefahr, dass sich Geldwäschereirisiken auf sie übertragen. Nicht nur, aber insbesondere in Fällen, bei denen Unternehmen[232] solche Expertisen ausstellen und an der Vermittlung von Kunden an Finanzintermediäre ohne VASP-Tätigkeit in irgendeiner Form mitverdienen, müssen sich letztere der Übertragung von Geldwäschereirisiken auf sie selbst bewusst sein.

Verwundbarkeit 6

Finanzintermediäre, die VA-relevante Transaktionen durchführen (in VAs oder Fiat) (2018 identifiziert, 2023 erhöht)[233]

Im sektoriellen Bericht von 2018 wurde die Verwundbarkeit von «Finanzintermediären, die Kryptotransaktionen durchfühen», festgestellt, für GW/TF-Zwecke missbraucht zu werden.[234] Denn selbst bei strenger Einhaltung ihrer Sorgfaltspflichten bleibe die Wirksamkeit dieser Massnahmen zwangsläufig beschränkt, da Kryptotransaktionen transnational seien und über Dienstleistungsgesellschaften laufen, die in sehr vielen Ländern registriert sind. Beispielsweise werden in der Schweiz registrierte Online-Wechselstuben oft von ausländischen *custodial* Wallet-Anbietern, die im Auftrag ihrer Kunden handeln, mit dem Umtausch von Kryptowährungen beauftragt. In solchen Fällen hat die Schweizer Plattform keinen Zugang zu den KYC-Daten des Kunden der ausländischen Plattform, für die sie diesen Umtausch vornimmt, und kennt somit die Identität des Kunden nicht.

Die MROS hat seit 2018 zahlreiche Verdachtsmeldungen von Finanzintermediären ohne VASP-Tätigkeit erhalten, die verdächtige Transaktionen von oder zu in- oder ausländischen

[231] Vgl. z.B. Gotham City, *L'enquête sur les pirates allemands de Movie2k passe par Genève*, Nr. 278, 26. Januar 2023.
[232] Dabei kann es sich um Finanzintermediäre mit VASP-Tätigkeit handeln, die beim Wechsel der VAs in Fiatwährung Gebühren einnehmen, oder auch um Unternehmen ohne finanzintermediäre Tätigkeit, die mit der Erstellung von Expertisen und/oder für die Vermittlung von Kunden an Finanzintermediäre ohne VASP-Tätigkeit von letzteren bezahlt werden.
[233] KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 34 – 35.
[234] Ibid., S. 34.

VASP-Plattformen auf den von ihnen geführten Konten festgestellt haben. Zudem wurden der MROS mehrere Fälle bekannt, in denen schweizerische Finanzintermediäre ohne VASP-Tätigkeit ausländischen Finanzintermediären mit VASP-Tätigkeit Geschäftskonten zur Verfügung stellten, über welche Fiat-Transaktionen abgewickelt wurden, die im Zusammenhang mit dem Kauf oder Verkauf von VAs auf ausländischen VASP-Plattformen standen. Dabei scheinen die schweizerischen Finanzintermediäre oft nicht in der Lage, den wirtschaftlichen Hintergrund der über ihre Konten transferierten Vermögenswerte abzuklären oder die daran wirtschaftlich berechtigte Person festzustellen. Dies, weil grundsätzlich nur der ausländische Finanzintermediär Informationen zu den über dieses Konto abgewickelten Transaktionen und den daran beteiligten Personen besitzt, nicht aber der schweizerische Finanzintermediär. Letzterer ist dadurch von der Einhaltung der Sorgfalts- und Meldepflichten des ausländischen Finanzintermediärs abhängig und kann selbst nicht sicherstellen, dass keine Kunden mit erhöhten Risiken oder Transaktionen mit unklarem wirtschaftlichem Hintergrund über seine Konten abgewickelt werden.

Der MROS sind mehrere Fälle bekannt, in denen die Zurverfügungstellung solcher Geschäftskonten durch die kontoführende Bank in der Schweiz für die Abwicklung von Zahlungen missbraucht wurden, die in Zusammenhang mit mutmasslich im Ausland begangenen Straftaten standen. In einzelnen Fällen waren es sogar die Geschäftskunden eines schweizerischen Finanzintermediärs, bzw. die ausländischen Finanzintermediäre mit VASP-Tätigkeit selbst, denen im Rahmen von Strafverfahren im Ausland Straftaten vorgeworfen wurden. Die Tatsache, dass der kontoführende Finanzintermediär in der Schweiz nur mangelhaft über die von ihr abgewickelten Transaktionen informiert ist, erhöht aus Sicht der GW/TF-Bekämpfung die Risiken in Zusammenhang mit solchen Geschäftskonstellationen. Diese Entwicklungen sind ein weiterer Hinweis für die Aufweichung der Grenzen zwischen den Geschäftstätigkeiten von Finanzintermediären mit und ohne VASP-Tätigkeit (vgl. Infobox 1 in Kapitel 4.2). Sie haben dazu geführt, dass letztendlich *sämtliche* Finanzintermediäre – sowohl mit als auch ohne VASP-Tätigkeit – verwundbar sind, als Durchgangs- oder Endpunkt für illegale Finanzflüsse – in VAs oder Fiat – mit Bezügen zu VAs aufweisen, missbraucht zu werden.

Zwischen Januar 2020 und Ende 2022 erhielt die MROS mehr als dreimal so viele VA-relevante Verdachtsmeldungen von Finanzintermediären ohne VASP-Tätigkeit (1442) als von jenen mit VASP-Tätigkeit (425). Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit nahmen ebenfalls zu, allerdings weniger konstant und weniger deutlich wie jene von Finanzintermediären ohne VASP-Tätigkeit – und dies trotz der steigenden Anzahl Finanzintermediäre mit VASP-Tätigkeit sowie mutmasslich steigenden Volumen ihrer Geschäftstätigkeiten.

Auffällig ist die Tatsache, dass zahlenmässig mehr verschiedene Finanzintermediäre ohne VASP-Tätigkeit VA-relevante Verdachtsmeldungen einreichten als Finanzintermediäre mit VASP-Tätigkeit: Während zwischen Januar 2020 bis Dezember 2022 118 verschiedene Finanzintermediäre ohne VASP-Tätigkeit mindestens eine VA-relevante Verdachtsmeldung einreichten, taten dies in derselben Periode lediglich 24 verschiedene Finanzintermediäre mit VASP-Tätigkeit.[235] Überdies stammen über drei Viertel dieser Meldungen (329 von 425 Meldungen von Finanzintermediären mit VASP-Tätigkeit) von denselben vier Finanzintermediären mit VASP-Tätigkeit. Diese vier Finanzintermediäre mit VASP-Tätigkeit haben regelmässig eine Verdachtsmeldung eingereicht, während 20 Finanzintermediäre mit VASP-Tätigkeit sporadisch eine Meldung einreichten.

[235] Zu beachten ist, dass es sich bei den VA-relevanten Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit nicht um *sämtliche* von diesen Finanzintermediären in dieser Zeitperiode eingereichten Meldungen handeln muss, da von gewissen Finanzintermediäre mit VASP-Tätigkeit auch Verdachtsmeldungen eingereicht wurden, die im Zusammenhang mit weiteren Geschäftsaktivitäten dieser Finanzintermediäre eingereicht und keinen Bezug zu VAs oder VASPs aufwiesen (vgl. Kapitel 4.2).

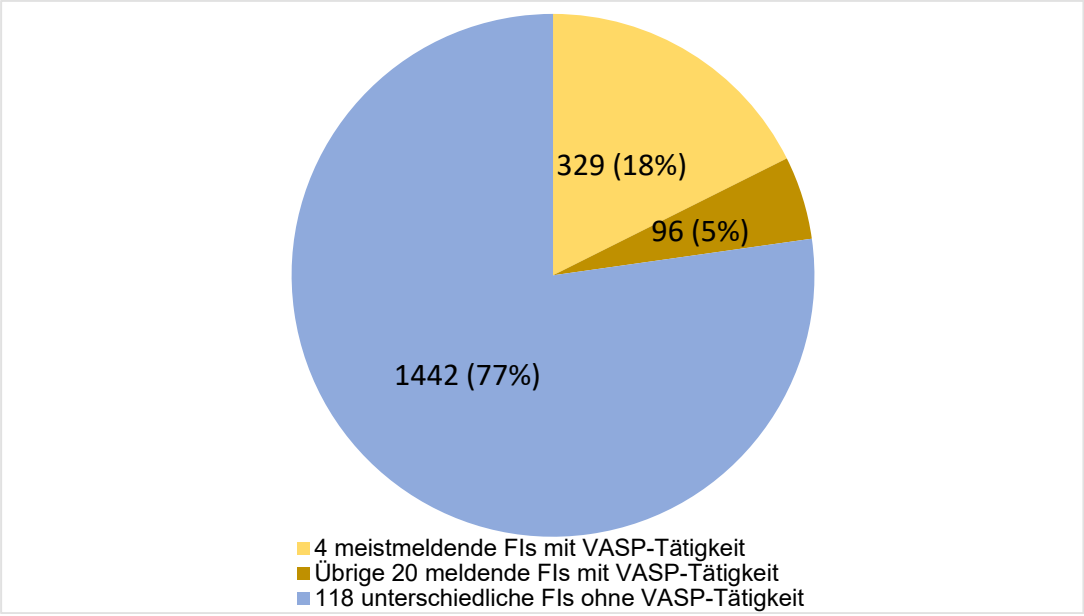


Abbildung 29: Meldende Finanzintermediäre hinter den 1'867 VA-relevanten Verdachtsmeldungen der Jahre 2020 – 2022. Erstaunlicherweise haben Finanzintermediäre mit VASP-Tätigkeit deutlich weniger zahlreich und deutlich weniger häufig VA-relevante Verdachtsmeldungen erstattet als Finanzintermediäre ohne VASP-Tätigkeit.

Verwundbarkeit 7

Ausbleibende Meldungen von Finanzintermediären mit VASP-Tätigkeit (2023 identifiziert)

Per Ende 2022 existierten in der Schweiz mindestens 204 Finanzintermediäre mit VASP-Tätigkeit, die entweder unter direkter Aufsicht der FINMA, oder aber unter jener der Selbstregulierungsorganisationen stehen. Mindestens 180 von ihnen haben zwischen Januar 2020 und Dezember 2022 keine einzige Verdachtsmeldung bei der MROS eingereicht. Die grosse Mehrheit dieser Finanzintermediäre ist einer Selbstregulierungsorganisation angeschlossen. Mangels quantitativer Angaben zu den von schweizerischen Finanzintermediären mit VASP-Tätigkeit angebotenen Dienstleistungen und verwalteten VA-Vermögen ist es nicht möglich, im Detail zu prüfen, ob ausbleibende Meldungen der überwältigenden Mehrheit dieser Finanzintermediäre mit einer mangelhaften Einhaltung ihrer Sorgfalts- und Meldepflichten oder mit einer ausbleibenden Geschäftstätigkeit zusammenhängt. Angesichts des Wachstums des schweizerischen VA-Sektors und einer offensichtlichen Intensivierung der diesbezüglichen Geschäftsaktivitäten von Finanzintermediären mit VASP-Tätigkeit scheint es jedoch, dass die MROS nicht alle Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit erhält, die sie erhalten sollte.

7.5.2 Verdachtsbegründende Elemente

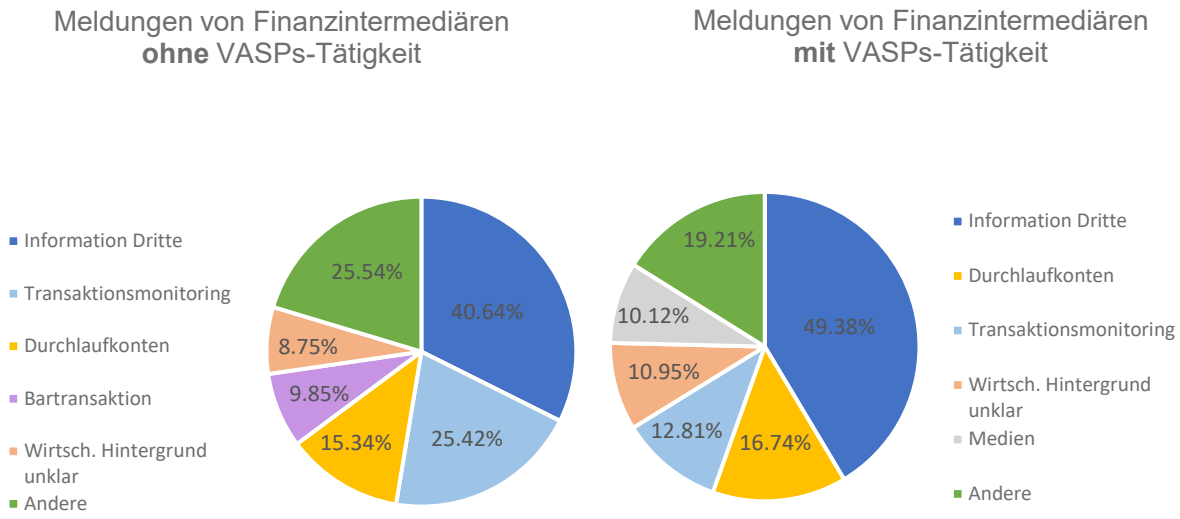


Abbildung 30: Verdachtsbegründende Elemente unterscheiden sich je nachdem, ob eine Meldung von einem Finanzintermediär mit oder ohne VASP-Tätigkeit eingereicht wurde. Finanzintermediäre ohne VASP-Tätigkeit erstatteten deutlich häufiger aufgrund ihres internen Transaktionsmonitorings eine Meldung, während Informationen Dritter deutlich häufiger zur Erstattung einer Meldung durch einen Finanzintermediär mit VASP-Tätigkeit führten.

Dass Finanzintermediäre mit VASP-Tätigkeit aufgrund ihres Transaktionsmonitorings eigenständige Feststellungen erarbeiteten und eine Meldung mit VA-Bezug erstatteten, war im Vergleich zu VA-relevanten Meldungen von Finanzintermediären ohne VASP-Tätigkeit eher selten (12.8% bei Finanzintermediären mit VASP-Tätigkeiten gegenüber 25.4% bei Finanzintermediären ohne VASP-Tätigkeit).

Bei jeder zweiten Meldung mit VA-Bezug (49.4%) von Finanzintermediären mit VASP-Tätigkeit wurde als Meldegrund ein Überweisungsrückruf von Drittbanken bezüglich betrügerisch ausgelöster Zahlungen, eine Kontaktaufnahme durch ausländische Strafverfolgungsbehörden oder eine Editionsverfügung von schweizerischen Strafverfolgungsbehörden (im Folgenden zusammengefasst unter dem Begriff «Informationen Dritter») angegeben. Bei VA-relevanten Meldungen von Finanzintermediären ohne VASP-Tätigkeit waren Informationen Dritter deutlich seltener (40.6% der Meldungen) ein Grund für die Erstattung einer Verdachtsmeldung. Bei beiden Arten von Finanzintermediären ist dies ein hoher Prozentsatz und scheint damit eine generelle Problematik im VA-Bereich zu widerspiegeln. Dabei scheinen Finanzintermediäre mit VASP-Tätigkeit allerdings signifikant häufiger auf diese Informationen Dritter angewiesen, um verdächtige Vorgänge zu erkennen.

Aus den Meldungen von Finanzintermediären mit VASP-Tätigkeit wird zudem ersichtlich, dass diese häufig direkt von ausländischen Strafverfolgungsbehörden (überwiegend von Staatsanwaltschaften in Deutschland) mit der Aufforderung kontaktiert wurden, bestimmte Angaben – beispielsweise den Namen des Kontoinhabers, welcher Empfänger einer betrügerisch ausgelösten Zahlung war – über eine bei ihnen geführte Geschäftsbeziehung zu liefern.

Verwundbarkeit 8

Das Meldeverhalten von Finanzintermediären mit VASP-Tätigkeit scheint oft reaktiv und nicht auf proaktiven Abklärungen zu beruhen (2023 identifiziert)

Bei der Verfassung von Verdachtsmeldungen schildern die meldenden Finanzintermediäre schriftlich den Sachverhalt der verdächtigen Vorgänge sowie die Gründe für die Einreichung einer Verdachtsmeldung. Hierbei beobachtete die MROS Unterschiede zwischen Finanzintermediären mit und ohne VASP-Tätigkeit in Bezug auf deren Erkennungssysteme, die verschiedenen Verdachtsquellen und -gründen Rechnung tragen sollten.

Meldende Finanzintermediäre mit VASP-Tätigkeit wurden häufiger als Finanzintermediäre ohne VASP-Tätigkeit erst durch externe Informationen auf verdächtige Vorgänge aufmerksam, die sie zur Einreichung einer Verdachtsmeldung bewegten. Gemäss eigenen Angaben der meldenden Finanzintermediäre mit VASP-Tätigkeit waren in den von ihnen erstatteten Meldungen der Jahre 2020 bis 2022 Informationen Dritter der häufigste Verdachtsauslöser (49.4% der Meldungen von Finanzintermediären mit VASP-Tätigkeit). Dabei gaben diese Finanzintermediäre an, durch Überweisungsrückrufe von Drittbanken bezüglich betrügerisch ausgelöster Zahlungen, Kontaktaufnahmen durch mutmassliche Betrugsopfer oder deren Rechtsvertreter, Anfragen ausländischer Strafverfolgungsbehörden oder Editionsverfügungen von schweizerischen Strafverfolgungsbehörden auf die gemeldete Geschäftsbeziehung aufmerksam geworden zu sein. Demgegenüber waren es bei den VA-relevanten Meldungen von Finanzintermediären ohne VASP-Tätigkeit nur in 40.7% der Meldungen Informationen Dritter, welche zur Erstattung einer Meldung führten.

Bei den VA-relevanten Meldungen von Finanzintermediären ohne VASP-Tätigkeit wurde doppelt so häufig (25.4%) das Transaktionsmonitoring als Verdachtsauslöser angegeben als bei den Meldungen von Finanzintermediären mit VASP-Tätigkeit (12.8%). Finanzintermediäre mit VASP-Tätigkeit scheinen folglich eher mit Schwierigkeiten konfrontiert, anhand ihres Monitorings verdächtige Transaktionen und Vorgänge zu erkennen und deren wirtschaftliche Hintergründe in Eigenregie abzuklären. Dies scheint keine nationale Besonderheit zu sein: Ein Informationsaustausch mit der FIU Liechtenstein zeigte, dass auch letztere ein tendenziell reaktives Meldeverhalten bei Finanzintermediären mit VASP-Tätigkeit beobachtet. Dadurch scheint auch die Vermutung naheliegend, dass bei einzelnen Finanzintermediären mit VASP-Tätigkeit ein signifikantes Dunkelfeld besteht in Bezug auf mutmasslich geldwäschereirelevante Zahlungen. Sofern diese Vorgänge weder anhand interner Abklärungen noch mittels externer Informationen als verdächtig erkannt werden und dadurch meldepflichtig wären, führen sie auch nicht zu einer Verdachtsmeldung an die Meldestelle.

8. Bilanz und risikomindernde Faktoren

In den bisherigen Kapiteln wurden die bereits 2018 identifizierten Gefährdungen und Verwundbarkeiten unter Rücksichtnahme der massgeblichen Veränderungen und Abweichungen seit 2018 im VA-Sektor erneut beurteilt und ergänzt. Diese Gefährdungen und Verwundbarkeit werden nachfolgend zusammengetragen und bilanziert.
Analog zum sektoriellen Bericht von 2018 umfasst die Bilanz der Risikoanalyse lediglich die Veränderungen in den Gefährdungen und Verwundbarkeiten im Sinne einer Übersicht über die Bruttorisiken. Eine Aufstellung der identifizierten risikomindernden Faktoren folgt nach der Bilanzierung. Die Prüfung und quantitative Bewertung der Nettorisiken, die mit den in der Schweiz ausgeübten Finanzintermediation im VA-Bereich verbunden sind, kann mangels verfügbarer Angaben zu diesen Tätigkeiten nicht durchgeführt werden (vgl. Kapitel 5.2). Diese Zahlen wären notwendig, um eine präzise Risikogewichtung der Geschäftstätigkeiten anhand ihrer Intensität und Reichweite vorzunehmen, um in einem zweiten Schritt zu prüfen, inwiefern die einzelnen Geschäftstätigkeiten von den identifizierten Gefährdungen und Verwundbarkeiten tangiert sind und wie stark dabei der Einfluss der risikomindernden Faktoren wirkt.

8.1 Bilanz der Risikoanalyse

Keine der bereits 2018 identifizierten neun Gefährdungen und zwei Verwundbarkeiten haben sich in den letzten fünf Jahren entschärft, beziehungsweise vermindert. Vielmehr haben sie sich mehrheitlich erhöht (7 von 11), während drei Gefährdungen und eine Verwundbarkeit unverändert weiter bestehen. Zudem wurden im Rahmen der vorliegenden Risikoanalyse zwei Gefährdungen sowie sechs Verwundbarkeiten neu identifiziert.

	Gefährdungen	**2018**	**2023**
1	Sicherheitslücken bei den zugrundeliegenden VA-Technologie	Identifiziert	Erhöht
2	Ransomware und Malware	Identifiziert	Erhöht
3	VAs als Zahlungsmittel für illegale Güter und Dienstleistungen	Identifiziert	Erhöht
4	Geldwäscherei von VAs krimineller Herkunft (in Fiatgeld)	Identifiziert	Erhöht
5	Geldwäscherei von Fiatgeld krimineller Herkunft (in VAs)	Identifiziert	Unverändert
6	Gefährdungen in Verbindung mit dem Neuigkeitseffekt und der Unerfahrenheit der Nutzer	Identifiziert	Erhöht
7	Rückgriff auf VAs bei Phishing-Attacken	Identifiziert	Erhöht
8	Terrorismusfinanzierung mittels VAs	Identifiziert	Unverändert

9	Proliferationsfinanzierung mittels VAs		Identifiziert
10	Anonymität der Transaktionen und schwierige Identifikation der wirtschaftlich Berechtigten	Identifiziert	Unverändert
11	*Travel Rule* wird bei Händlerkonten schweizerischer Finanzintermediäre mit VASP-Tätigkeit nicht angewendet		Identifiziert

Abbildung 31: Übersicht über die identifizierten Gefährdungen und deren Veränderungen seit 2018

	Verwundbarkeiten	**2018**	**2023**
1	Tendenziell abnehmende Bedeutung der Finanzintermediation im VA-Bereich stellt bestehende GW/TF-Regulierungsansätze vor Herausforderungen		Identifiziert
2	Ungenügende und ungleiche internationale Um- und Durchsetzung der *Travel Rule* im VA-Bereich		Identifiziert
3	Defizit an Ressourcen und Kapazitäten seitens der mit der GW/TF-Bekämpfung betrauten Institutionen angesichts der rasanten Entwicklungen im VA-Bereich		Identifiziert
4	Unzureichende Zahlen und Statistiken auf nationaler und internationaler Ebene		Identifiziert
5	Schwierige Repression von GW/TF im VA-Bereich	Identifiziert	Unverändert
6	Finanzintermediäre, die VA-relevante Transaktionen durchführen (in VAs oder Fiat)	Identifiziert	Erhöht
7	Ausbleibende Meldungen von Finanzintermediären mit VASP-Tätigkeit		Identifiziert
8	Das Meldeverhalten von Finanzintermediären mit VASP-Tätigkeit scheint oft reaktiv und nicht auf proaktiven Abklärungen zu beruhen		Identifiziert

Abbildung 32: Übersicht über die identifizierten Verwundbarkeiten und deren Veränderungen seit 2018

8.2 Risikomindernde Faktoren

Obwohl von VAs erhebliche Gefährdungen ausgehen und sie ebenso erhebliche Verwundbarkeiten aufweisen, gibt es mehrere risikomindernde Faktoren. Diese Faktoren können bestehende Gefährdungen und Verwundbarkeiten entschärfen. Die meisten von ihnen wurden in diesem Bericht bereits erwähnt und werden im Folgenden summarisch zusammengefasst. Einige davon wirken auf globaler Ebene, während sich andere auf den nationalen Kontext beschränken, wobei allfällige Unterschiede zwischen diesen beiden Ebenen hervorgehoben werden.

	Risikomindernde Faktoren
1	Verstärkter FATF-Fokus und gestiegene politische Aufmerksamkeit
2	Verstärkte internationale Zusammenarbeit verzeichnet bereits Erfolge
3	Konsolidierung und zunehmender Compliance-Reifegrad der «Big Players»
4	Grundsätzliche Transparenz der meisten Blockchains
5	Aufsichtstätigkeit und Implementierung der *Travel Rule* in der Schweiz
6	Weitreichende Definition von Finanzintermediation im DLT-Gesetz

Abbildung 33: Übersicht über die identifizierten risikomindernden Faktoren

8.2.1 Verstärkter FATF-Fokus und gestiegene politische Aufmerksamkeit

Auf internationaler Ebene kann die allmähliche Implementierung der VA-spezifischen Empfehlungen der FATF als risikovermindernder Faktor angesehen werden. Die FATF scheint die Umsetzung in den einzelnen Ländern intensiv zu beobachten und veröffentlicht in regelmässigen Zeitabständen Wegweisungen und Berichte zum Stand der Umsetzung der VA-spezifischen Empfehlungen.

Eine verstärkte Aufmerksamkeit der FATF und der internationalen politischen Gemeinschaft erhöht den Druck auf die Länder und Unternehmen im VA-Bereich, sich an die internationalen Standards zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung zu halten. Dies kann zu einer verstärkten Umsetzung von entsprechenden Massnahmen führen, die das Risiko der Verwendung von VAs für GW/TF-Zwecke verringern können. Diese verstärkte Aufmerksamkeit kann in einem zweiten Schritt auch zu einer besseren Identifizierung und Überwachung verdächtiger Aktivitäten und Transaktionen führen, was ebenfalls dazu beitragen kann, das Risiko von GW/TF im Zusammenhang mit VAs zu minimieren. Beispielsweise werden mit der Implementierung der *Travel Rule* Finanzflüsse zwischen Konten bei Finanzintermediären mit VASP-Tätigkeit transparenter und der Kontrollmassstab für die Einhaltung der Sorgfaltspflichten bei zentralisierten VA-Dienstleistungen dem SWIFT-Zahlungsverkehr angeglichen. Eine weitreichende Definition des Begriffs "VASP" gemäss der FATF-Empfehlung 15 stellt zudem sicher, dass die im Bereich der traditionellen Finanzintermediation bereits geltenden GW/TF-Bestimmungen auch im VA-Bereich Anwendung finden. Finanzintermediäre mit VASP-Tätigkeit müssen beispielsweise sicherstellen, dass sie die Identität ihrer Kunden kennen, verdächtige Transaktionen melden und ein effektives Risikomanagement implementieren. Eine weltweit umfassendere Regulierung und Überwachung von Finanzintermediären mit VASP-Tätigkeit kann sicherstellen, dass letztere die Verwendung von VAs für GW/TF-Zwecke besser erkennen und verhindern können, was die GW/TF-Risiken entsprechend vermindern würde.

8.2.2 Verstärkte internationale Zusammenarbeit verzeichnet bereits Erfolge

Eine verstärkte internationale Zusammenarbeit auf verschiedenen Ebenen im VA-Sektor, wie beispielsweise zwischen den nationalen Regulierungsbehörden, Strafverfolgungsbehörden, FIUs, sowie zwischen Strafverfolgungsbehörden und privaten Unternehmen kann zu einer Verminderung GW/TF-Risiken im VA-Sektor führen. Indem VA-Kenntnisse aufseiten der Behörden vertieft, Informationen über Verdachtsfälle schneller und effektiver geteilt, sowie die Zusammenarbeit mit Unternehmen im Bereich Blockchainanalyse intensiviert wurde, konnten

bereits mehrere Erfolge, beispielsweise in Zusammenhang mit der Nachverfolgung, Sperrung und Einziehung von VAs erzielt werden.[236] Durch den Austausch bewährter Praktiken und Erfahrungen können die verschiedenen Länder und Institutionen voneinander lernen und ihre Massnahmen verbessern, was ebenfalls zu einer Verringerung der Risiken beitragen kann, wenn dadurch GW/TF-Aktivitäten im Zusammenhang mit VAs schneller identifiziert und strafrechtlich verfolgt werden. Eine verstärkte Zusammenarbeit kann letztlich dazu beitragen, bestehende Lücken und Schwachstellen in der Regulierungsarchitektur aufzudecken und zu beheben und dadurch die Regulierung und Überwachung im Allgemeinen zu verbessern. Eine engere Zusammenarbeit fördert auch die Harmonisierung in der Umsetzung internationaler Standards und kann so die Wirksamkeit der GW/TF-Massnahmen im VA-Sektor erhöhen.[237]

8.2.3 Konsolidierung und zunehmender Compliance-Reifegrad der «Big Players»

Eine weltweite Konsolidierung auf der Angebotsseite des VA-Sektors, bei der es einige wenige grosse und zentralisierte VA-Handelsbörsen gibt, die über reifere Compliance-Abteilungen verfügen, kann dazu beitragen, GW/TF-Risiken im VA-Sektor zu reduzieren. Weniger VASPs, die jedoch grösser und besser reguliert sind, führen zu einer Verringerung in der Anzahl der Risiken und ermöglicht eine bessere Kontrolle und Überwachung der verbleibenden VASPs. Grössere VASPs sind zudem in der Regel besser in der Lage, in Compliance-Abteilungen und Technologien zur Überwachung von Transaktionen zu investieren, was wiederum bewirken kann, dass illegale Aktivitäten im Zusammenhang mit VAs eher verhindert werden können. Auch Regulierungsbehörden können effektiver mit einer kleineren Anzahl von grösseren VASPs interagieren, um Regulierungs- und Überwachungsstandards durchzusetzen. Dies erleichtert die Überwachung der Einhaltung von Anti-GW/TF-Standards und die Durchsetzung von Massnahmen im Falle von Nichteinhaltung. Eine Konsolidierung des VASP-Sektors kann letztlich auch helfen, die Verwendung von VAs für GW/TF-Zwecke schneller zu identifizieren und zu unterbinden, da es weniger Orte gibt, an denen diese Aktivitäten stattfinden können.

8.2.4 Grundsätzliche Transparenz der meisten Blockchains

Die grundsätzliche Transparenz von Blockchains bietet momentan Chancen, Finanzflüsse im VA-Bereich zu beobachten, wie es im traditionellen Zahlungsverkehr nicht möglich ist.[238] Gewisse Software-Lösungen zur Blockchainanalyse können digitale Informationen mit Personen und Ereignissen in der analogen Welt verknüpft werden, wodurch bisher ungekannte Möglichkeiten für vertiefte Analysen vorhanden sind, wobei die Qualität dieser Auswertungen immer abhängig ist von der Qualität der zugrundeliegenden Daten aus der analogen Welt. Diesbezüglich haben sich noch keine einheitlichen Standards durchgesetzt. Diese Lösungen bauen darauf, dass zum einen VA-Transaktionen in der Regel öffentlich einsehbar sind, was es einfacher macht, verdächtige Aktivitäten aufzudecken und zu verfolgen. Dies kann wiederum die Identifizierung und Verfolgung von Geldflüssen in Echtzeit erleichtern, was im traditionellen Zahlungsverkehr nicht möglich ist. Zum anderen kann die Blockchain durch ihre dauerhafte und unveränderliche Aufzeichnung von Transaktionen im Gegensatz zum traditionellen Zahlungsverkehr mittel- bis langfristig dazu beitragen, allgemeine Risiken in Zusammenhang mit Betrug und Fälschung zu reduzieren, indem einmal getätigte Transaktionen öffentlich verifiziert und nicht mehr manipuliert werden können. Da DeFi-Protokolle in der Regel auf öffentlichen Blockchains basieren, kann eine höhere Transparenz

[236] Für Angaben zu verschiedenen Einziehungen von VAs in mehrfacher Milliardenhöhe im Jahr 2022, vgl. Chainalysis, *The Crypto Crime Report 2022*, Februar 2022, S. 23.
[237] Basel Institute On Governance and Europol, *Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering*, 2022, S. 4 – 5.
[238] Ibid., S. 3.

vorhanden sein. Allerdings existieren auch DeFi-Anwendungen, die die Nachvollziehbarkeit der Transaktionen absichtlich (z.B. Mixer, Tumbler, Privacy Wallets) oder als Nebenfolge der Funktionalität (Cross Chain Bridges, Lending Pools, Automated Market Makers) erschweren oder verunmöglichen. Zwar wird jede Transaktion innerhalb eines DeFi-Protokolls in Echtzeit auf der Blockchain aufgezeichnet und ist öffentlich einsehbar, die Nachverfolgbarkeit und Zuordenbarkeit kann je nach Umständen aber verunmöglicht werden. Folglich bestehen auch im DeFi-Bereich aufgrund der mehrheitlich anonymen Nutzer erhebliche Geldwäscherei- und Terrorismusfinanzierungsrisiken Es gibt nach wie vor Herausforderungen bei der Identifizierung und Überwachung verdächtiger Transaktionen, insbesondere durch die Verwendung von Anonymisierungstechnologien. Allerdings existiert ein wachsendes Feld von Unternehmen und Forschungseinrichtungen, die sich auf die Analyse von Blockchain-Daten spezialisiert haben. Diese Branche entwickelt fortschrittliche Tools und Technologien, um VA-Transaktionen zu analysieren und verdächtige Aktivitäten zu identifizieren. Dies kann den Regulierungs- und Strafverfolgungsbehörden helfen, Fälle von Geldwäscherei oder Terrorismusfinanzierung aufzudecken und zu verfolgen. Es gab bereits mehrere Fälle, in denen Regulierungs- und Strafverfolgungsbehörden aufgrund von Blockchainanalysen in der Lage waren, GW/TF-Fälle aufzudecken, VAs zu sperren und einzuziehen, und insbesondere dank Blockchainanalysen die kriminellen Handlungen den Tätern nachzuweisen und sie strafrechtlich zu verfolgen. CeFi-Plattformen basieren hingegen auf zentralisierten Datenbanken und Systemen, die nicht transparent sind. Der Zugang zu den Daten hängt damit von der Kooperationsbereitschaft des Betreibers ab, was die Überwachung und Analyse von Transaktionen erschweren kann.

8.2.5 Aufsichtstätigkeit und Implementierung der *Travel Rule* in der Schweiz

Angesichts der erheblichen Gefährdung der Schweiz durch Geldwäscherei, misst die FINMA der Geldwäschereiproblematik im Generellen aber auch in Bezug auf die VASPs eine hohe Priorität bei. Entsprechend führte sie diverse Aufsichts- und Überwachungsmassnahmen in diesem Bereich ein und führt bei schwerwiegenden Verstössen Abklärungen und Enforcementverfahren durch.

Seit sich auf den Finanzmärkten Tätigkeiten mit Bezug zu Kryptowährungen zu entwickeln begannen, hat die Schweiz den bestehenden Rechtsrahmen zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung auf einige Kryptowährungen sowie auf Anbieter von Dienstleistungen im Zusammenhang mit virtuellen Vermögenswerten (Virtual Asset Service Providers, VASPs), die eindeutig mit herkömmlichen Finanzintermediären gemäss Definition der FINMA gleichgesetzt werden, angewendet. Nach diesem Rechtsrahmen fallen sämtliche Finanzintermediationstätigkeiten im Zusammenhang mit Kryptowährungen in den Geltungsbereich des Geldwäschereigesetzes (GwG). Dazu zählen insbesondere die Wechseldienstleistungen zwischen Anbietern von Kryptowährungen und Fiat-Währungen und/oder zwischen einer oder mehrerer Formen von Kryptowährungen, alle Tätigkeiten im Zusammenhang mit der Übertragung, der Verwahrung und/oder Verwaltung von Kryptowährungen oder Instrumenten zur Kontrolle der Kryptowährungen. Für weitergehende Informationen wird an dieser Stelle auf die bereits gemachten Aussagen im Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz von Oktober 2021 verwiesen.[239]

Zudem müssen mit der Änderung der GwV-FINMA seit dem 1. Januar 2021 alle schweizerischen Finanzintermediäre mit VASP-Tätigkeit bei Geschäften mit VAs die Vertragspartei identifizieren, wenn eine Transaktion oder mehrere solche Transaktionen, die miteinander verbunden erscheinen, den Betrag von 1000 Franken erreichen oder übersteigen,

[239] Vgl. Kapitel 3.8, S. 42, Neuerungen im Bereich der der Virtual Assets (VA) und Virtual Asset Service Providers (VASPs), KGGT, *Zweiter nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung*, Oktober 2021.

sofern diese Transaktionen keine Geld- und Wertübertragungen darstellen und mit diesen Geschäften keine dauernde Geschäftsbeziehung verbunden ist. Zusammen mit Erfordernissen, welche sich aus Art. 10 der GwV-FINMA (Angaben bei Zahlungsaufträgen) ergeben, nimmt die Schweiz ihre Finanzintermediäre mit VASP-Tätigkeit stärker in die Pflicht, als es die *Travel Rule* der FATF vorsieht, da diese Regelung in der Schweiz auch im Hinblick auf Zahlungen zwischen *custodial* Wallets und *non-custodial* Wallets angewendet wird. Bei korrekter Umsetzung dieser Erfordernisse sind derzeit VA-Ein- und Ausgänge von Kundenkonten bei schweizerischen Finanzintermediären mit VASP-Tätigkeit nur von/zu *non-custodial* Wallets möglich, an welchen die entsprechenden Kunden wirtschaftlich berechtigt sind. Das verstärkt das GW/TF-Abwehrdispositiv der Finanzintermediäre. Die Möglichkeiten, auf diese Weise die tatsächliche wirtschaftliche Berechtigung an Vermögenswerten in einer *non-custodial* Wallet sowie die Herkunft dieser Vermögenswerte zu ermitteln, bleiben allerdings durch die technologische Ausgestaltung von VAs beschränkt. Diese Möglichkeiten sind aber auch in Bezug auf Fiatwährung und sonstige Vermögenswerte im traditionellen Finanzbereich beschränkt. Die Anonymität bzw. Pseudonymität von Transaktionen wird zumindest bei jenen zwischen *custodial* Wallets – bei entsprechender globaler Umsetzung der FATF-Empfehlungen – künftig erheblich eingeschränkt, da hierbei jeweils die Angaben zu Sender und Empfänger der Zahlungen zwischen den Finanzintermediären mit VASP-Tätigkeit ausgetauscht werden.

8.2.6 Weitreichende Definition von Finanzintermediation im DLT-Gesetz

Mit dem Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register sowie der zugehörigen Mantelverordnung wird künftig der Begriff des Finanzintermediärs ausgeweitet, sodass die Verfügungsmacht über Vermögenswerte nicht mehr das alleinige Kriterium darstellt, um als Finanzintermediär in den Geltungsbereich des Geldwäschereigesetzes zu fallen. Die Ausweitung des Begriffs des Finanzintermediärs entspricht den neuesten Empfehlungen der FATF, den Begriff «VASP» so weit wie nötig zu interpretieren, damit keine Lücken im GW/TF-Abwehrdispositiv entstehen.[240] Im schweizerischen VA-Sektor gilt fortan als Finanzintermediär, wer «hilft, virtuelle Währungen an eine Drittperson zu übertragen, sofern er mit der Vertragspartei eine dauernde Geschäftsbeziehung unterhält oder sofern er für die Vertragspartei Verfügungsmacht über virtuelle Währungen ausübt, und er die Dienstleistung nicht ausschliesslich gegenüber angemessen beaufsichtigten Finanzintermediären erbringt».[241] Nicht dem GwG unterstellt werden weiterhin Anbieter von reinen *non-custodial* Wallets, welche «bloss einmalig eine Software zur Verfügung stellen».[242] Es wird sich allerdings zeigen müssen, inwiefern die Unterscheidung zwischen einer «dauernden Geschäftsbeziehung» und einer «einmaligen Zurverfügungstellung einer Software» tatsächlich praxisnah ist und als sinnvolles Differenzierungskriterium im VA-Bereich längerfristig taugt.

[240] Vgl. FATF, *Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers*, März 2021, S. 29-30.
[241] Vgl. Eidgenössisches Finanzdepartement (EFD): *Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens*, Oktober 2020.
[242] Ibid.

9. Schlussfolgerungen und Empfehlungen

Im Jahr 2018 veröffentlichte die KGGT ihre erste sektorielle Risikoanalyse zur vorliegenden Thematik, wobei die damit verbundenen Gefährdungen und Verwundbarkeiten der Schweiz gegenüber Geldwäscherei und Terrorismusfinanzierung als «erheblich» eingestuft wurden.[243] Gleichzeitig wurde festgehalten, dass die MROS erst wenige Verdachtsmeldungen in diesem Zusammenhang erhalten hatte und sich aus diesen noch keine zuverlässigen statistischen Daten ableiten liessen. Seit 2018 hat sich die Risikolandschaft deutlich verändert. Die MROS erhält inzwischen *täglich* Verdachtsmeldungen, die einen Zusammenhang mit VAs oder VASPs aufweisen. Der Einfluss und die Bedeutung von VAs hat sich gegenüber 2018 grundlegend geändert. Übergeordnet lassen sich dabei vier massgebliche Entwicklungen identifizieren.

Erstens kann festgestellt werden, dass die Anzahl Finanzintermediäre mit VASP-Tätigkeit in der Schweiz von unter 10 im Jahr 2018 auf mindestens 204 per Ende 2022 massiv angestiegen ist. Die wenigen Angaben, die zu diesen Finanzintermediären vorliegen, lassen eine Intensivierung der Geschäftstätigkeit während der letzten Jahre vermuten. Ende 2021 wurde von Finanzintermediären mit VASP-Tätigkeit in der Schweiz mindestens ein zweistelliger Milliardenbetrag verwaltet.

Zweitens kann festgestellt werden, dass die allgemeine Verwendung von VAs in der Schweiz in den letzten fünf Jahren deutlich zugenommen hat. Diverse Studien und Umfragen zeigen diese Entwicklung klar auf. Immer mehr Menschen sehen VAs als legitimes Zahlungsmittel an. Parallel dazu sind auch die Möglichkeiten, VAs als Zahlungsmittel zu verwenden, vielfältiger und prävalenter geworden. Die zunehmende Verschmelzung des VA-Bereichs mit dem traditionellen Finanzsektor, zum Beispiel durch die Integration von VAs in etablierte Zahlungsplattformen, hat dazu geführt, dass die Anzahl der Geschäfte und Dienstleister in der Schweiz, die VAs als Zahlungsmittel akzeptieren, vermutlich gestiegen ist.

Drittens haben sowohl die kriminelle Verwendung von VAs sowie die aufsichtsrechtlichen Verletzungen in der Schweiz zugenommen. Schweizer Strafverfolgungsbehörden sind immer häufiger mit Verfahren konfrontiert, die Bezüge zu VAs aufweisen. Obwohl die Angaben diesbezüglich nicht flächendeckend vorhanden sind, zeigen die verfügbaren Daten nominal und prozentual zunehmende Schadenssummen, die auf VAs entfallen und sich für die Schweiz im Jahr 2022 mindestens in zweistelliger Millionenhöhe bewegten. Die kriminelle Verwendung von VAs scheint jedoch nicht nur zugenommen, sondern sich auch erweitert und diversifiziert zu haben. Einerseits ist die Verwendung von VAs inzwischen bei gewissen Straftaten zumindest üblich, wenn nicht sogar eine zentrale Bedingung für einen aus Tätersicht erfolgreichen Ausgang der Straftat – beispielsweise um das erpresste Lösegeld bei Ransomware-Attacken zu empfangen. Während bis vor wenigen Jahren beinahe sämtliche VA-Finanzflüsse in Bitcoin denominiert waren, haben Kriminelle ihre Strategien angepasst und nutzen nun je nach Bedarf unterschiedliche VAs, darunter Stablecoins, NFTs und insbesondere Privacy Coins, die für Strafverfolgungswerkzeuge schwerer zu verfolgen sind. Dies stellt eine wachsende Herausforderung für die Strafverfolgungsbehörden dar. Gefährdungen gehen überdies längst nicht mehr nur von Vortaten im Bereich der Cyberkriminalität und der «kryptospezifischen» Delikte aus. Das Spektrum der Sachverhalte, die verschiedenen angefragten Strafverfolgungsbehörden sowie der MROS zur Kenntnis gebracht worden sind und in denen sich die Verwendung von VAs beobachten lässt, hat sich dadurch ebenfalls erweitert. Mittlerweile gehen Gefährdungen auch von den verschiedensten Straftaten im «Offline»-Bereich aus, darunter schwerste Formen der Wirtschaftskriminalität und letztlich auch die Verwendung von VAs durch professionelle Geldwäschereinetzwerke und staatliche Akteure. In unterschiedlichen VA-relevanten Verdachtsmeldungen, die bei der

[243] KGGT, *National Risk Assessment: Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018, S. 4.

MROS eintrafen, konnten Bezüge zu politisch exponierten Personen (PEP), internationalen Korruptionsaffären, transnationalen Gruppen im Bereich der organisierten Kriminalität oder staatlichen Akteuren festgestellt werden. Offenbar wurde das Potential von VAs für Geldwäscherei-, Terrorismusfinanzierungs- sowie Proliferationsfinanzierungszwecke erkannt, weshalb sie inzwischen zu den üblich verwendeten Werkzeugen der Finanzkriminalität gehören. Auch die FINMA stellt eine Zunahme der Fälle fest und hat in ihren zahlreichen Publikationen auf die Risiken mit VA/VASPs hingewiesen sowie ihre aufsichtsrechtlichen Erwartungen klargestellt. Zudem hat die FINMA diverse Abklärungen und Enforcementverfahren in diesem Zusammenhang durchgeführt.

Viertens zeigt letztlich auch der starke Anstieg VA-relevanter Verdachtsmeldungen, die bei der MROS seit 2020 eingereicht wurden, dass auch Finanzintermediäre in der Schweiz immer häufiger verdächtige, GW/TF-relevante Vorgänge auf den von ihnen geführten Konten feststellen, die im Zusammenhang mit der Verwendung von VAs stehen. Im Jahr 2022 waren bereits fast 14% der bei der MROS eingereichten Verdachtsmeldungen VA-relevant.

Die vier genannten Entwicklungen haben dazu geführt, dass sich die in der Risikoanalyse von 2018 identifizierten Gefährdungen und Verwundbarkeiten erhöht und darüber hinweg auch erweitert haben. Keine der damals identifizierten neun Gefährdungen und zwei Verwundbarkeiten haben sich in den letzten fünf Jahren reduziert. Vielmehr haben sie sich mehrheitlich erhöht (7 von 11), während drei Gefährdungen und eine Verwundbarkeit unverändert einzustufen sind. Zudem wurden im Rahmen der vorliegenden Risikoanalyse zwei Gefährdungen sowie sechs Verwundbarkeiten neu identifiziert. Die vorliegende Risikoanalyse macht deutlich, dass VAs aufgrund ihres gestiegenen Stellenwerts und den mit ihnen verbundenen GW/TF-Risiken eine erhöhte Aufmerksamkeit seitens der zuständigen Behörden im Bereich der GW/TF-Bekämpfung erfordern.

Der VA-Sektor ist von einer hohen Dynamik und rasanten Entwicklungen geprägt. Die neuen technologischen Möglichkeiten, die VAs bieten, sind in Bezug auf die GW/TF-Bekämpfung sowohl mit Chancen als auch mit Risiken verbunden. Diese hängen primär mit den Eigenschaften von VAs zusammen und können je nach Stossrichtung künftiger Entwicklungen die Risikolandschaft entscheidend verändern.

VAs existieren als parallele Zahlungssysteme neben dem traditionellen Zahlungsverkehr und ermöglichen schnelle internationale Überweisungen. Die zunehmende Verschmelzung von VAs und dem traditionellen Zahlungsverkehr führt zu einer wachsenden Anzahl von Berührungs- und Schnittpunkten zwischen den Zahlungssystemen. Diese Entwicklung bringt Risiken in Bezug auf Geldwäscherei und Terrorismusfinanzierung mit sich. Erstens erhöht sich für Strafverfolgungsbehörden und sämtliche mit der Aufsicht betrauten Behörden und Institutionen der Aufwand bei Ermittlungen und der Nachverfolgung von Transaktionen, da nun mehrere separate Zahlungssysteme untersucht werden müssen. Dies erfordert einerseits zusätzliches Fachwissen und kann andererseits bisherige Ermittlungsabläufe erschweren und damit verbundene Arbeitsschritte sowie den Ressourcenaufwand erhöhen. Zweitens erleichtert die zunehmende Integration von VAs in den traditionellen Zahlungsverkehr kriminellen Akteuren den Zugang und die Nutzung beider Zahlungssysteme. Dies birgt das Risiko, dass diese Akteure ihr Repertoire an Geldwäschereitechniken mit einem zusätzlichen Instrument erweitern. Zudem könnten sie den Einsatz von VAs mit herkömmlichen Verschleierungstechniken kombinieren oder VAs in bereits risikobehafteten Sektoren verstärkt einsetzen, um die Identifizierung verdächtiger Aktivitäten zusätzlich zu erschweren. Drittens erhöht sich durch die wachsende Anzahl der Berührungs- und Schnittpunkte zwischen beiden Zahlungssystemen die Verwundbarkeit sämtlicher Finanzintermediäre (mit oder ohne VASP-Tätigkeit), als Durchgangs- oder Endpunkt für illegale, VA-relevante Finanzflüsse (in VAs oder Fiat) missbraucht zu werden. Diese Verwundbarkeit erhöht sich zusätzlich, solange die Empfehlung 16 der FATF (*Travel Rule*) nicht in sämtlichen Ländern umgesetzt ist.

Das weltweite Volumen der VA-Finanzflüsse ist im Vergleich mit anderen Finanzflüssen jedoch noch relativ überschaubar. Verglichen mit anderen Sektoren scheinen die GW/TF-Risiken im VA-Sektor deshalb noch begrenzt. Die erfolgreiche Verschleierung von VA-Finanzflüssen erfordert zudem ein vertieftes Verständnis der Funktionsweise von VAs. Es ist davon auszugehen, dass die Anzahl Experten in diesem Bereich noch begrenzt ist und sich der Grossteil ihrer Aktivitäten auf den Bereich der Cyberkriminalität und «kryptospezifischer» Delikte wie zum Beispiel *Rugpulls*, Phishing von Wallet-Daten und Hacks von VASPs beschränkt. Dennoch ist das Potenzial von VAs deutlich erkennbar, einem «erweiterten Publikum» die Verschleierung von Geldflüssen zu ermöglichen – zum Beispiel professionellen Geldwäschern mit Verwurzelung im traditionellen Finanzsektor oder transnationalen OK-Gruppen mit Geldern inkriminierter Herkunft aus dem «Offline»-Bereich. Diese Entwicklung ist in Teilen bereits erkennbar und erfordert ein erhöhtes Bewusstsein für die damit im Zusammenhang stehenden Gefahren. Die steigende Akzeptanz von VAs für Zahlungen, einschliesslich hoher Beträge, verbunden mit der zunehmenden Verschmelzung des VA- und des traditionellen Finanzbereichs, könnte mittel- bis langfristig zu erhöhten Geldwäscherei- und Terrorismusfinanzierungsrisiken in beiden Bereichen führen.

Nichtsdestotrotz beeinflusst das Wachstum des VA-Sektor bereits jetzt einen signifikanten Teil des Wirtschafts- und Finanzbereichs und erfordert die Aufmerksamkeit von vielen Stakeholdern: Finanzintermediäre, Aufsichts- und Strafverfolgungsbehörden sowie weitere mit der GW/TF-Bekämpfung befassten Stellen und Akteuren. Der vorliegende Bericht zeigt auf, dass hierbei teilweise Defizite bestehen und betont die Wichtigkeit des Aufbaus von Wissen und Ressourcen.

Unzureichende Ressourcen und Kapazitäten können sowohl die nationale als auch die internationale Zusammenarbeit zwischen den an der GW/TF-Bekämpfung beteiligten Stakeholdern als herausfordernd gestalten, insbesondere dann, wenn letztere nicht über denselben Wissensstand und vergleichbare Fähigkeiten bei Ermittlungen und Analysen im VA-Bereich verfügen. Dadurch kann die Identifizierung und Verfolgung von GW/TF-Fällen mit VA-Relevanz empfindlich gehemmt und verzögert werden, obschon entsprechende Fälle vielleicht gar nicht schwer zu entdecken wären. Diese Problematik besteht bereits auf nationaler Ebene, verschärft sich aber auf internationaler Ebene, da die Aufklärung von GW/TF-Fällen im VA-Bereich fast immer von einer gut funktionierenden internationalen Zusammenarbeit zwischen FIUs, Strafverfolgungs- und weiteren Behörden abhängt. Ein schwaches Glied in dieser Kette kann bereits ausreichen, um die grenzüberschreitende Aufklärung von GW/TF-Fällen erheblich zu verzögern oder zu hemmen. Aktuell besteht für die Schweiz (genauso wie für andere Länder) folglich insbesondere das Risiko, dass die an der GW/TF-Bekämpfung beteiligten Stakeholder zum Teil nicht genügend in der Lage sind, GW/TF-Fälle mit Bezügen zu VAs zu entdecken und straf- oder aufsichtsrechtlich zu verfolgen, da sie nicht ausreichend für diese neuen Herausforderungen gewappnet sind und über ungenügende Ressourcen in diesem Bereich verfügen.

Die Regulierung des schweizerischen VA-Sektors ist jedoch im internationalen Vergleich robust und bisherige FATF-Empfehlungen für den VA-Sektor wurden jeweils zeitnah umgesetzt. Der vorliegende Bericht offenbarte aber auch nebst den zumeist global bestehenden Gefährdungen und Verwundbarkeiten nationalspezifische Problemfelder. Übergeordnet sind die meisten davon auf eine mangelnde Verfügbarkeit zuverlässiger Daten für den schweizerischen VA-Sektor zurückzuführen.

Verschiedene Faktoren tragen zur Minderung von Risiken im Zusammenhang mit VAs bei. Erstens konnte die internationale Zusammenarbeit bei VA-Ermittlungen durch die verstärkte Nachverfolgung, Sperrung und Einziehung von VAs bereits einzelne Erfolge verzeichnen, was zeigt, dass mit ausreichender Ausrüstung relevanter Behörden GW/TF im VA-Bereich effektiv bekämpft werden kann. Zweitens hat die Konsolidierung der Anbieter im VA-Sektor tendenziell zu einem erhöhten Compliance-Reifegrad der grossen Akteure beigetragen. Drittens bietet die

inhärente Transparenz der meisten Blockchains einzigartige Möglichkeiten zur Nachverfolgung von Finanzflüssen, wie es bei herkömmlichen Zahlungsverkehrssystemen nicht möglich ist. Durch den Einsatz von Blockchainanalyse-Tools können unter Umständen verdächtige Aktivitäten leichter identifiziert und verfolgt werden. Viertens hat die Schweiz einen geltenden Rechtsrahmen und die Aufsichtserwartungen im Zusammenhang mit VA/VASPs früh und transparent kommuniziert bzw. umgesetzt. Insbesondere die *Travel Rule* der FATF wird konsequent umgesetzt, indem sie auch Zahlungen von und zu *non-custodial* Wallets miteinbezogen hat, was die Kontrolle und Nachverfolgbarkeit von Transaktionen verbessert. Schliesslich hat die Erweiterung der Definition von Finanzintermediation dazu beigetragen, eine breitere Palette von Akteuren in den Anwendungsbereich des Geldwäschereigesetzes zu bringen, um so Lücken in den GW/TF-Abwehrmassnahmen zu schliessen.

Auf der Grundlage der in dieser Risikoanalyse identifizierten Gefährdungen und Verwundbarkeiten schlägt die KGGT die folgenden vier Massnahmen vor, um das aktuelle Dispositiv zu stärken:

1. **Verbesserung des Daten- und Kenntnisstands zum VA-Sektor in der Schweiz**
   Für die exakte Identifizierung, das Verständnis und die Bewertung von GW/TF-Risiken im Zusammenhang mit VAs sowie zur Entwicklung von geeigneten Massnahmen sind Daten zum VA-Sektor sowie zur kriminellen Verwendung von VAs in der Schweiz unerlässlich. Dazu gehören Informationen über die Grösse, Aktivitäten und Schwerpunkte des Sektors sowie Daten zur Anzahl Verfahren, den untersuchten Straftatbeständen und den involvierten Beträgen. Dies ist von entscheidender Bedeutung, um eine effektive Bekämpfung von Geldwäscherei und Terrorismusfinanzierung zu gewährleisten und die Integrität des Finanzplatzes zu schützen. Das Fehlen von flächendeckenden nationalen und internationalen Daten und Angaben erschwert nicht nur eine Gesamtbeurteilung der Risiken, sondern kann auch dazu führen, dass Entwicklungen unterschätzt werden und notwendige Massnahmen nicht oder erst zu spät getroffen werden. Vor diesem Hintergrund sollten die wichtigsten Kennzahlen zu diesem Sektor regelmässig und flächendeckend erhoben werden.

2. **Förderung eines proaktiven Meldeverhaltens von Finanzintermediären mit VASP-Tätigkeit**
   Die Zahlen zu den bei der MROS eingereichten VA-relevanten Verdachtsmeldungen zeigen, dass weniger als ein Viertel aller VA-relevanten Verdachtsmeldungen – in der Periode 2020 bis 2022 – von Finanzintermediären mit VASP-Tätigkeit stammen. Hierbei gilt es zu beachten, dass vier Finanzintermediäre mit VASP-Tätigkeit für einen Grossteil dieser Meldungen verantwortlich sind. Insgesamt haben in der erwähnten Periode lediglich 24 FIs mit VASP-Tätigkeit mindestens eine Verdachtsmeldung erstattet, obwohl in der Schweiz per Ende 2022 bereits über 204 Finanzintermediäre mit VASP-Tätigkeit existierten. Die Analyse der erhaltenen Meldungen von Finanzintermediären mit VASP-Tätigkeit zeigt somit ein eher reaktives Meldeverhalten des Sektors. Die mit der Aufsicht betrauten Behörden und Institutionen sollten deshalb die von ihnen beaufsichtigten Finanzintermediäre mit VASP-Tätigkeit auf die Erkenntnisse dieser Risikoanalyse aufmerksam machen und ein proaktiveres Meldeverhalten fordern, gegebenenfalls durch regelmässige Überprüfungen der Compliance- und Monitoring-Massnahmen dieser Finanzintermediäre.

3. **Bereitstellung von ausreichenden Kapazitäten und Ressourcen für die GW/TF-Bekämpfung im VA-Bereich**
   Eine verstärkte Zusammenarbeit zwischen den zuständigen Behörden ist erforderlich, um den Herausforderungen bei der GW/TF-Bekämpfung im VA-Bereich gerecht zu werden. Die verfügbaren Zahlen und Daten zeigen, dass VAs immer häufiger und diverser für kriminelle Zwecke verwendet werden. Zudem entwickeln sich die Techniken der Verwendung von VAs für kriminelle Zwecke stetig weiter. Die Weiterentwicklung von Wissen, Fähigkeiten und Ressourcen sind folglich zentrale

Aspekte im GW/TF-Abwehrdispositiv. Zu den wichtigsten Instrumenten der Strafverfolgungsbehörden gehören nebst den eigenen Ermittlungsinstrumenten (z.B. Blockchainanalyse-Tools) die nationale und internationale Zusammenarbeit, die justizielle und polizeiliche Rechtshilfe mit ihren ausländischen Partnerstellen sowie die Budapester Konvention. Die Effektivität dieser Instrumente ist jedoch abhängig vom Wissensstand, von den Ressourcen und den Fähigkeiten der jeweils betroffenen Akteure. Die einzelnen an der GW/TF-Bekämpfung beteiligten Behörden in der Schweiz müssen deshalb mit ausreichenden Ressourcen und Kapazitäten ausgestattet werden, um Geldwäscherei und Terrorismusfinanzierung im VA-Bereich effizient bekämpfen zu können.

4. Stärkung der internationalen Zusammenarbeit

Die Schweiz setzt sich auf internationaler Ebene weiterhin für eine wirksame Bekämpfung der Kriminalitätsrisiken im Finanzsektor ein. Dieses Engagement ist wichtig und kann zu einer Verminderung der GW/TF-Risiken im VA-Bereich beitragen. Die Schweiz wird sich weiterhin besonders einsetzen, damit die in diesem Bereich international entwickelten Standards rasch umgesetzt werden. Viele der von VAs ausgehenden Gefährdungen und Verwundbarkeiten betreffen alle Länder – auch die Schweiz – gleichsam. Durch den transnationalen Charakter der Risiken im VA-Bereich müssen die wichtigsten Massnahmen zu ihrer Verminderung deshalb auf internationaler Ebene koordiniert werden.

10. Bibliografie

22.3145 (Postulat), *Wie fit sind die Kantone in der Cyber-Strafverfolgung?*, eingereicht von der Sicherheitspolitischen Kommission des Nationarats am 15. Februar 2022.

22.3017 (Postulat), *Stärkung der Strafverfolgungsbehörden im Bereich der Kryptowährungen*, einigereicht von Nationalrat Andri Silberschmidt am 16. März 2022.

Aktionariat, *Create a market for your shares*, zuletzt abgerufen im Mai 2023.

Amtsblatt der Europäischen Union, *Verordnung (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849, ABl. L 150*, 9. Juni 2023.

AP News, *Mexican cartels turn to bitcoin, internet, e-commerce*, 10. März 2022

Bank for International Settlements (BIS), *OTC foreign exchange turnover in April 2022*, Oktober 2022.

Barron's, *The Cryptocurrency Crash Could Lead to a Wave of M&A*, 23. Juni 2022.

Basel Institute On Governance, Europol, *Seizing the Opportunity: 5 recommendations for crypto-assets-related crime and money laundering*, 2022.

BBC News, *Why the Central African Republic adopted Bitcoin*, 6. Juni 2022

BBl 2020 7801, *Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register*, Oktober 2020.

BBl 2023 84 – *Botschaft zur Änderung des Informationssicherheitsgesetzes* (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen) vom 2. Dezember 2022, Januar 2023.

Bithome, *Buy and Sell Real Estate with Bitcoin or Cryptos*, zuletzt abgerufen im Mai 2023.

Bloomberg, *Tesla Trails Only MicroStrategy in Treasury Bitcoin Allocation*, 8. Februar 2021.

Bundesamt für Statistik (BFS), *Polizeiliche Kriminalstatistik (PKS) – Jahresbericht 2021*, März 2022.

Bundesamt für Statistik (BFS), *Polizeiliche Kriminalstatistik (PKS) – Jahresbericht 2022*, März 2023.

Bundesrat, *Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwab (13.3687) und Weibel (13.4070) vom 25. Juni 2014*.

Bundesrat, *Weltweit führend, verankert in der Schweiz: Politik für einen zukunftsfähigen Finanzplatz Schweiz*, Dezember 2020.

Cambridge Centre For Alternative Finance (CCAF), *3rd Global Cryptoasset Benchmark Study*, September 2020.

Cash, *Handelsvolumen an der SIX 2022 rückläufig*, 3. Januar 2023.

Center for Philanthropy Studies (CEPS), Universität Basel SwissFoundations, Verband der Schweizer Förderstiftungen Zentrum für Stiftungsrecht, Universität Zürich, *Der Schweizer Stiftungsreport 2022*, Mai 2022.

Center for Philanthropy Studies (CEPS), Universität Basel SwissFoundations, Verband der Schweizer Förderstiftungen Zentrum für Stiftungsrecht, Universität Zürich, *Der Schweizer Stiftungsreport 2023*, Juni 2023.

Chainalysis, *The 2020 Crypto Crime Report*, Januar 2020.

Chainalysis, *The 2021 Crypto Crime Report*, Februar 2021.

Chainalysis, *The 2021 Geography of Cryptocurrency Report*, Oktober 2021.

Chainalysis, *Cryptocurrency Exchanges in 2021*, November 2021.

Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, 13. Januar 2022.

Chainalysis, *The Crypto Crime Report 2022*, Februar 2022.

Chainalysis, *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class*, 2. Februar 2022.

Chainalysis, *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, 5. April 2022.

Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6. Juni 2022.

Chainalysis, *The State of Web3*, Juni 2022.

Chainalysis, *The 2022 Geography of Cryptocurrency Report*, September 2022.

Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12. Januar 2023.

Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26. Januar 2023.

Chainalysis, *The 2023 Crypto Crime Report*, Februar 2023.

Ciphertrace, *Cryptocurrency crime and anti-money laundering*, Juni 2022.

City of Lugano, Tether, *Lugano's Plan B*, zuletzt abgerufen im Mai 2023.

CNET, *Ransomware rises as a national security threat as bigger targets fall*, 18. Oktober 2021.

Coin ATM Radar, *Bitcoin ATM Map*, zuletzt abgerufen im Mai 2023.

Coindesk, *'Ship-to-Ship' Trade and Other Secrets of North Korea's Illicit $1.5B Crypto Stash*, 7. April 2020.

Coinmap, *Crypto ATMs & merchants of the world*, zuletzt abgerufen im Mai 2023.

CoinMarketCap, *Global Cryptocurrency Market Charts*, zuletzt abgerufen im Mai 2023.

Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France*, September 2019.

Curry David, *Coinbase Revenue and Usage Statistics (2023)*, 28. März 2023.

Department of Justice (USA), *Two Chinese Intelligence Officers Charged with Obstruction of Justice in Scheme to Bribe U.S. Government Employee and Steal Documents Related to the Federal Prosecution of a PRC-Based Company*, 24. Oktober 2022.

Department of the Treasury (USA), *National Money Laundering Risk Assessment*, Februar 2022.

Eidgenössisches Finanzdepartement (EFD), *Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens*, Oktober 2020.

Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2016*, März 2017.

Eidgenössische Finanzmarktaufsicht (FINMA), *Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs)*, Februar 2018.

Eidgenössische Finanzmarktaufsicht (FINMA), *Aufsichtsmitteilung 02/2019 - Zahlungsverkehr auf der Blockchain*, August 2019.

Eidgenössische Finanzmarktaufsicht (FINMA), *Ergänzung der Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs)*, September 2019.

Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2020*, März 2021.

Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2021*, März 2022.

Eidgenössische Finanzmarktaufsicht (FINMA), *Risikomonitor 2022*, November 2022.

Eidgenössische Finanzmarktaufsicht (FINMA), *Jahresbericht 2022*, März 2023.

Eidgenössische Finanzmarktaufsicht (FINMA), *FINMA schliesst Verfahren gegen Krypto-Plattform und deren Gründer ab*, Mai 2023.

Elliptic, *NFTs and Financial Crime*, August 2022.

European Central Bank (ECB), *Understanding the crypto-asset phenomenon, its risks and measurement issues*, Mai 2019.

European Parliament, *Crypto-assets: green light to new rules for tracing transfers in the EU*, April 2023.

Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, Dezember 2021.

Europol, *Bitzlato: senior management arrested*, 23. Januar 2023.

Europol, *Underground drug-money bank laundering EUR 180 million liquidated by law enforcement*, 13. April 2023.

FATF, *Virtual Currencies. Key Definitions and Potential AML/CFT Risks*, Juni 2014,

FATF, *Guidance for a Risk-Based Approach to Virtual Currencies*, Juni 2015.

FATF, *Outcomes FATF Plenary, 17-19 October 2018*, Oktober 2018.

FATF, *Guidance to a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Juni 2019.

FATF, *Anti-money laundering and counter-terrorist financing measures - Switzerland, Enhanced Follow-up Report & 2nd Technical Compliance Re-Rating*, Januar 2020.

FATF, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, Juni 2020.

FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, September 2020.

FATF, *Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers*, März 2021.

FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Oktober 2021.

FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, Juni 2022.

FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, Juni 2023.

FATF, *The FATF Recommendations*, Februar 2023.

FATF, *Countering Ransomware Financing*, März 2023.

FATF, *Press Release - Virtual Assets Contact Group (VACG)*, 14. April 2023.

Financial Crimes Enforcement Network (FinCEN), *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, 10. August 2021.

Financial Crimes Enforcement Network (FinCEN), *Advisory on Illicit Activity Involving Convertible Virtual Currency*, Mai 2019, S. 1 – 2.

Financial Intelligence Unit (Deutschland), *Jahresbericht 2019*, Juni 2020.

Financial Intelligence Unit (Deutschland), *Jahresbericht 2021*, August 2022.

Financial Intelligence Unit (Estland), *Yearbook 2019*, 2020.

Financial Intelligence Unit (Estland), *The Risks related to Virtual Asset Service Providers in Estonia*, Januar 2022.

Financial Intelligence Unit (Liechtenstein), *Jahresbericht 2020*, März 2021.

Financial Intelligence Unit (Liechtenstein), *Jahresbericht 2021*, April 2022.

Financial Intelligence Unit (Niederlande), *Annual Review 2019*, Juni 2020.

Financial Intelligence Unit (Niederlande), *Annual Review 2021*, Juni 2022.

Financial Stability Board (FSB), *FSB Chair's letter to G20 Finance Ministers and Central Bank Governors*, März 2018.

Financial Stability Board (FSB), *Assessment of Risks to Financial Stability from Crypto-assets*, Februar 2022.

Financial Stability Institute, *Supervising cryptoassets for anti-money laundering*, April 2021.

Financial Times, *How North Korea became a crypto crime hub*, 14. November 2022.

Finews, *Tessiner dürfen ihre Steuern jetzt in Bitcoin zahlen*, 7. Juli 2022.

Finews, *1 Milliarde Krypto-Nutzer bis ins Jahr 2030*, 25. Juli 2022.

Finews, *Chainalysis: Crypto Hacks Reach Record $3 Billion*, 13. Oktober 2022.

Finews, *EU erhält europaweite Krypto-Regulierung*, 21. April 2023.

Forbes, *Scandals And Mafia Allegations May Force Malta To Reconsider Its Reliance On Online Betting*, 13. März 2021.

Gotham City, *L'enquête sur les pirates allemands de Movie2k passe par Genève*, Nr. 278, 26. Januar 2023.

Government Of The Grand Duchy Of Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers*, Dezember 2020.

Handelszeitung, *6000 Kunden kaufen bei der SBB Bitcoins | Handelszeitung*, 1. November 2017.

Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, 22. Juni 2021.

Handelszeitung, *85'000 Händler in der Schweiz können nun Zahlungen mit Bitcoin und Ether annehmen*, 19. August 2021.

HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, Dezember 2020.

Home of Blockchain, *Swiss Digital Asset Market Report 2022*, Mai 2022

Institute of Financial Services Zug IFZ (Hochschule Luzern), *Crypto Assets Study 2021*.

Institute of Financial Services Zug IFZ (Hochschule Luzern), *Crypto Assets Study 2022*.

Institute of Financial Services Zug IFZ (Hochschule Luzern), *Fintech Study 2023*.

International Monetary Fund (IMF), *Treatment of Crypto Assets in Macroeconomic Statistics*, 2019.

International Monetary Fund (IMF), *F.18 Recording of Crypto Assets in Macroeconomic Statistics*, März 2022

Jimenez Alison, *3 Misconceptions about Cryptocurrency Crime Estimates*, 11. Januar 2022.

Kanton Zug, *Kanton Zug akzeptiert ab 2021 Kryptowährungen für Steuerzahlungen* (Medienmitteilung), 3. September 2020.

KGGT, *Erster nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung*, Juni 2015.

KGGT, *Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding*, Oktober 2018.

KGGT, *Zweiter nationaler Bericht über die Risiken der Geldwäscherei und der Terrorismusfinanzierung*, Oktober 2021.

L'avvenire di Calabria, *Boom delle scommesse online, ma per la Dia c'è l'ombra dei clan*, 23. Januar 2020.

Malta Gaming Authority, *Annual Report 2021*, September 2022.

McGuire Michael, *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy*, April 2018.

Meldestelle für Geldwäscherei (MROS), *Jahresbericht 2020*, Mai 2021.

Migros Bank, *Kryptowährungen bei jüngeren Generationen beliebter als Gold*, 27. Februar 2020.

Monetary Authority of Singapore, *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, März 2020.

Moneyland, *Wie legen Schweizer ihr Geld an?*, 22. April 2020.

Moneyland, *So investieren Schweizerinnen und Schweizer ihr Geld*, 19. Juli 2022.

Monroe Brian, *FinCEN, OFAC fine crypto exchange Bittrex nearly $30 million on AML, sanctions failings, missed SARs, links to darknet markets, mixers, ransomware gangs*, 11. Oktober 2022.

National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (Malta), *Key Results of the Sectoral Risk Assessment on Virtual Financial Assets*, Februar 2020.

Nationales Zentrum für Cybersicherheit (NCSC), *Halbjahresbericht 2022/II (Juli – Dezember)*, Mai 2023.

Nasdaq, *Blockware Estimates 10% Global Bitcoin Adoption By 2030: Report*, 9. Juni 2022.

New York Times, *In Global First, El Salvador Adopts Bitcoin as Currency*, 7. September 2021.

New York Times, *Banks Tried to Kill Crypto and Failed. Now They're Embracing It (Slowly)*, 1. November 2021.

New York Times, *Coinbase Reaches $100 Million Settlement With New York Regulators*, 4. Januar 2023.

New York Times, *Government Cracks Down on Crypto Industry With Flurry of Actions*, 18. Februar 2023.

Organized Crime & Corruption Reporting Project (OCCRP), *Italian Mafia Bets on Illegal Online Gambling*, 4. März 2021.

Prestige Business, *Cyber-Attacken in der Schweiz nehmen auch 2023 zu*, 3. Mai 2023.

Reuters, *Crypto exchange Bittrex to pay $29-mln penalty to U.S. Treasury Department*, 11. Oktober 2022.

Reuters, *Dutch central bank fines cryptocurrency exchange Coinbase 3.3 mln euros*, 26. Januar 2023.

Reuters, *Dutch central bank fines Binance 3.3 million euros*, 18. Juli 2022.

RR.2022.45, *Arrêt du 20 décembre 2022 – Cour des plaintes*, Urteil des Bundesstrafgerichts, Bellinzona, 21. Dezember 2022.

Schurter Daniel, *Das ist die gefährlichste Hackerbande, die auch in der Schweiz wütet*, 23. Januar 2023.

Schweizerische Bankiervereinigung (SBVg), *Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken*, 2020.

Schweizerische Bundesbahnen (SBB), *Mit Bitcoin bequem und einfach einkaufen | SBB*, zuletzt abgerufen im Mai 2023.

Schweizerische Kriminalprävention, *Money Mules*, zuletzt abgerufen im Mai 2023.

Schweizer Radio und Fernsehen (SRF), *Die Schweiz tut sich schwer mit Gesetzesverschärfungen zum Gold*, 10. Mai 2022.

SR 0.311.43 – *Übereinkommen vom 23. November 2001 über die Cyberkriminalität*, Fassung vom 14.09.2020.

SR 935.51 – *Bundesgesetz über Geldspiele* (Geldspielgesetz, BGS), Fassung vom 01.01.2021.

SR 935.511 – *Verordnung über Geldspiele* (Geldspielverordnung, VGS), Fassung vom 01.01.2021.

SR 941.31 – *Bundesgesetz über die Kontrolle des Verkehrs mit Edelmetallen und Edelmetallwaren* (Edelmetallkontrollgesetz, EMKG), Fassung vom 1. Januar 2023.

SR 955.0 – *Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung*, (Geldwäschereigesetz, GwG), Fassung vom 23. Januar 2023.

SR 955.01 – *Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung* (Geldwäschereiverordnung, GwV), Fassung vom 01.01.2016.

SR 955.01 – *Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung* (Geldwäschereiverordnung, GwV), Fassung vom 01.08.2021.

SR 955.033.0 – *Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor* (Geldwäschereiverordnung-FINMA, GwV-FINMA), Fassung vom 01.01.2021.

SR 958.1 – *Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel* (Finanzmarktinfrastrukturgesetz, FinfraG).

SR 958.11 – *Verordnung über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel* (Finanzmarktinfrastrukturverordnung, FinfraV).

Staatssekretariat für internationale Finanzfragen (SIF), *Auftrag der Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung*, bewilligt durch den Bundesratsbeschluss vom 17. November 2021.

Staatssekretariat für internationale Finanzfragen (SIF), *Faktenblatt Krypto*, Januar 2022.

Staatssekretariat für internationale Finanzfragen (SIF), *Finanzstandort Schweiz, Kennzahlen 2023,* April 2023.

Staatssekretariat für internationale Finanzfragen (SIF), *Blockchain/DLT*, zuletzt abgerufen im Mai 2023.

Stalinsky Steven, *The Coming Storm – Terrorists Using Cryptocurrency*, 21. August 2019.

State Financial Service of Ukraine, *Report on the National Risk Assessment*, 2019.

Süddeutsche Zeitung, *Wieso die Mafia Fan von Maltas Online-Casinos ist*, 18. Dezember 2022.

Swedish Police Authority, *The Financial Intelligence Unit Annual Report 2021*, Mai 2022

Swiss Foundations, *Der Schweizer Stiftungsreport*, CEPS Forschung und Praxis. Band 30, Juni 2023.

Swissinfo, *Die Gold-Schweiz im Fokus vom Menschenrechtsrat*, 3. Oktober 2022,

Tages Anzeiger, *Schweizer Online-Drogenversand – «Hippe Kleider, Typ Studentin, und das Täschli voller Drogen»*, 18. März 2021.

Triple-A, *Global Cryptocurrency Ownership Data*, zuletzt abgerufen im Mai 2023.

TRM Labs, *Ensuring Responsible Development of Digital Assets; Request for Comment*, November 2022.

United Nations Data Retrieval System, *Democratic People's Republic of Korea*, zuletzt abgerufen im Mai 2023.

United Nations Office on Drugs and Crime (UNODC), *Money Laundering*, zuletzt abgerufen im Mai 2023.

United Nations Security Council, *S/2021/211 final report of the Panel of Experts*, März 2021.

United Nations Security Council, *S/2022/132 Report of the 1718 Panel of Experts*, März 2022.

United Nations Security Council, *S/2022/668 Midterm report of the 1718 Panel of Experts*, September 2022.

Vedrenne Gabriel, *In Europe, Suspicious Payments Triple Thanks to VASPs, Cryptocurrency*, 25. Oktober 2022.

Von Luckner, Reinhart & Rogoff, *Decrypting New Age International Capital Flows, NBER Working Paper No. 29337*, Oktober 2021, S. 1, Fussnote Nr. 2.

Wired Magazine, *Most Criminal Cryptocurrency Funnels Through Just 5 Exchanges*, 26. Januar 2023.

World Bank, *GDP (current US$) – World*, zuletzt abgerufen im Mai 2023.

World Bank, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, Juni 2022.

11. Anhang

11.1 Methodologie zur Auswertung von Verdachtsmeldungen der MROS

Mit der Einführung des Systems goAML eröffneten sich für die MROS neue Möglichkeiten zur Auswertung der ihr zur Verfügung stehenden Daten, die sie von Finanzintermediären, inländischen Behörden und ausländischen Financial Intelligence Units erhält. Sämtliche Daten werden seither in einem relationalen Datenverarbeitungssystem abgespeichert und können durch verschiedene Abrufverfahren vertiefter analysiert werden. Im Rahmen des vorliegenden Berichts konnte die MROS diese neuen Auswertungsmethoden erfolgreich verwenden. Sie werden nachfolgend vereinfacht erläutert.

Für die in Kapitel 7 präsentierten Ergebnisse aus der Auswertung von Verdachtsmeldungen wurde untersucht, welche der in den Jahren 2020 bis 2022 eingereichten Verdachtsmeldungen eine VA-Relevanz aufwiesen. Um als «VA-relevante» Meldung kategorisiert zu werden, musste eine Verdachtsmeldung mindestens eines der folgenden Kriterien erfüllen musste:

1. Identifizierung relevanter Meldungen mittels Transaktions-, Konto- und Kontoinhaberinformationen: Eine Verdachtsmeldung musste Transaktionen zwischen den in der Meldung angezeigten Konten und (von der MROS eindeutig identifizierte) Konten von schweizerischen oder ausländischen Finanzintermediären mit VASP-Tätigkeit aufweisen. Dies beinhaltet per Definition einerseits Meldungen, die von Schweizerischen Finanzintermediären mit VASP-Tätigkeit eingereicht wurden, sofern diese Meldungen verdächtige Transaktionen oder Sachverhalte in Zusammenhang mit VAs enthielten.[244] Andererseits sind auch Meldungen von Finanzintermediären *ohne* VASP-Tätigkeit beinhaltet, deren gemeldete Transaktionen einen (durch die MROS eindeutig identifizierten) Finanzintermediär mit VASP-Tätigkeit im In- oder Ausland als Gegenpartei der Transaktion (Empfänger oder Sender) enthielt.
2. Identifizierung relevanter Meldungen anhand einer Liste von VA-relevanten Schlagworten[245]: Jede bei der MROS eingereichte Verdachtsmeldung enthält einen vom meldenden Finanzintermediär schriftlich geschilderten Sachverhalt. Dieser musste mindestens eines von mindestens 50 Schlagwörtern enthalten, um in den vertieft zu analysierenden Bestand aufgenommen zu werden (z.B. «Bitcoin», «Krypto», etc.). Dabei wurde darauf geachtet, dass diese mit Schlagwörtern identifizierten Meldungen nur dann als VA-relevant eingestuft wurden, wenn sie keine falschen positiven Ergebnisse aufwiesen (z.B. FIAT als Automarke oder «Mining» im Sinne des Bergbaus, etc.).

Für die Jahre 2020 bis und mit 2022 erfüllten insgesamt 1867 Meldungen mindestens eines dieser Kriterien. Dies ist eine konservative Schätzung. Es kann nämlich nicht ausgeschlossen werden, dass sich unter den in den in diesem Zeitraum empfangenen 18’937 Verdachtsmeldungen noch mehr Meldungen befanden, welche Bezüge zu VAs aufweisen. Erstens besteht die Möglichkeit, dass weitere Meldungen Transaktionen zwischen den in der Meldung angezeigten Konten sowie Konten von schweizerischen oder ausländischen Finanzintermediären mit VASP-Tätigkeit aufwiesen, diese Transaktionen von den

[244] Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit müssen nicht zwingend VA-relevant sein, da solche Finanzintermediäre teilweise auch herkömmliche Finanzdienstleistungen anbieten, die keinen Zusammenhang mit VAs aufweisen. Vgl. Abbildung 4 in Kapitel 4.2.

[245] Die Schlagworte wurden von der MROS im Zuge der Erstellung dieser Analyse gesucht und gesammelt. Sämtliche Schlagworte wurden jeweils in unterschiedlichen Sprachen (Deutsch, Italienisch, Französisch, Englisch) und möglichen Schreibweisen für die Textsuche verwendet.

Finanzintermediären jedoch nicht angezeigt wurden,[246] oder aber, dass diese Konten der MROS nicht bekannt waren und die entsprechenden Meldungen deshalb nicht identifiziert werden konnten. Zweitens ist es möglich, dass eine Verdachtsmeldung tatsächlich einen relevanten Zusammenhang mit VAs oder VASPs aufwies, dieser aber auch anhand der Stichwortsuche nicht identifiziert werden konnte. Die angewandte Methode der Stichwortsuche impliziert folglich, dass damit nur jene Meldungen identifiziert werden konnten, bei welchen der meldende Finanzintermediär bereits einen Zusammenhang mit VAs feststellte und diesen im schriftlich geschilderten Sachverhalt explizit erwähnte, und diese explizite Erwähnung mittels der Liste der Stichwörter auch tatsächlich identifiziert werden konnte. Zudem wurden zusätzlich von der MROS verlangte Informationen zur Analyse einer Meldung (Anfragen gemäss Art. 11a GwG) nicht bei der Analyse berücksichtigt. Folglich handelt es sich bei den Angaben zur Anzahl VA-relevanter Verdachtsmeldungen um Mindestangaben.

Die durch diese Methode erlangte Auswahl wurde sodann danach kategorisiert, ob eine Meldung von einem Finanzintermediär mit oder ohne VASP-Tätigkeit eingereicht wurde, da sich je nach Zugehörigkeit zur einen oder anderen Kategorie verschiedene Formen von Finanzflüssen und folglich auch unterschiedliche Typologien feststellen liessen. Bei Meldungen von Finanzintermediären ohne VASP-Tätigkeit waren die Finanzflüsse lediglich in Form von Fiatwährung, während die Meldungen von Finanzintermediären mit VASP-Tätigkeit sowohl Fiattransaktionen als auch VA-Transaktionen beinhalten konnten. Zu beachten ist zudem, dass es sich bei den Verdachtsmeldungen von Finanzintermediären mit VASP-Tätigkeit nicht um *sämtliche* von diesen Finanzintermediären eingereichten Meldungen handelt, da von ihnen auch Verdachtsmeldungen eingereicht wurden, die keinen Zusammenhang mit VAs oder VASPs aufwiesen, namentlich dann, wenn diese Finanzintermediäre (z.B. Banken) ihren Kunden traditionelle Finanzdienstleistungen anbieten, die keinen Zusammenhang mit VAs aufweisen (vgl. Abbildung 4 in Kapitel 4.2). Die 1867 Meldungen wurden quantitativ und qualitativ anhand einer Liste von auszuwertenden Indikatoren analysiert. Im Vordergrund standen dabei vor allem Angaben zu den meldenden Finanzintermediären, den vom meldenden Finanzintermediär vermuteten Vortaten, den verdachtsbegründenden Elementen, den gemeldeten Vertragspartnern, den festgestellten Finanzflüssen und die dabei involvierten Summen.

11.1.1 Meldungen von Finanzintermediären mit VASP-Tätigkeit vor 2020

Obschon sich die vorliegende Risikoanalyse primär auf die Zeitperiode nach 2020 konzentriert, wurde für die Jahre 2015 bis und mit 2019 zusätzlich ausgewertet, wie viele Verdachtsmeldungen die MROS in diesem Zeitraum von Finanzintermediären mit VASP-Tätigkeit erhielt. Damit wurde das Wachstum der Meldungen sowie das Meldeverhalten dieser Finanzintermediäre über einen längeren Zeitrahmen beleuchtet.

Für das Verständnis des Vergleichs der Zahlen für die Zeitperiode ab 2020 mit denen der Vorjahre bedarf es jedoch einiger Erläuterungen: Vor 2020 wurde von der MROS eine einzelne gemeldete Geschäftsbeziehung als einzelne Verdachtsmeldung gezählt. Durch die Einführung des Systems goAML per Ende 2019 hat sich die Zählweise der von der MROS erhaltenen Verdachtsmeldungen geändert.[247] Ab diesem Zeitpunkt konnten in einer einzelnen Verdachtsmeldung mehrere Geschäftsbeziehungen gleichzeitig gemeldet werden, namentlich wenn diese vom meldenden Finanzintermediär im selben Zusammenhang, beziehungsweise aufgrund ein- und desselben verdächtigen Sachverhalts, gemeldet wurden. Seit dem 1. Januar 2020 zählt die Meldestelle deshalb die Anzahl Meldungen und nicht wie bis anhin die Anzahl

[246] Bei der MROS eingereichte Meldungen beinhalten gemäss Vorgaben der MROS grundsätzlich Transaktionsangaben in strukturierter Form zu den vom Finanzintermediär als verdächtig eingestuften Transaktionen.
[247] Meldestelle für Geldwäscherei (MROS), *Jahresbericht 2020*, Mai 2021, S. 16.

gemeldeter Geschäftsbeziehungen. Es ist deshalb grundsätzlich schwierig, die Zahlen bis und mit 2019 mit denjenigen ab 2020 präzise zu vergleichen. Um diesen Vergleich im vorliegenden Fall zu bewerkstelligen, wurden die zwischen 2015 und 2019 gemeldeten 185 Geschäftsbeziehungen analysiert und mehrere davon jeweils als eine Verdachtsmeldung gezählt, sofern sie vom selben Finanzintermediär, zum selben Zeitpunkt sowie im selben zugrundeliegenden Sachverhalt gemeldet wurden.[248] Anhand dieser Methode konnten die 185 Geschäftsbeziehungen in 53 Verdachtsmeldungen zusammengelegt werden.

11.2 Erläuterungen zu spezifischen Abbildungen

Abbildung 22, Kapitel 7.3.2
Folgende weitere Vortaten wurden von den meldenden Finanzintermediären vermutet und unter der Kategorie «Andere» zusammengefasst:

- Ausländer- und Integrationsgesetz (Art. 116 Abs. 3, Art. 118 Abs. 3 AIG)
- Bankengesetz (Art. 47 Abs. 1bis BankG)
- Bundesgesetz über Geldspiele (Art. 130 Abs. 2 BGS)
- Diebstahl (Art. 139 StGB)
- Einführen, Erwerben, Lagern falschen Geldes (Art. 244 Abs. 2 StGB)
- Erpressung (Art. 156 StGB)
- Geldfälschung (Art. 240 Abs. 1 StGB)
- Güterkontrollgesetz (Art. 14 Abs. 2 GKG)
- Heilmittelgesetz (Art. 86 Abs. 2 HMG)
- Insiderhandel oder Marktmanipulation (Art. 154 Abs. 2, Art. 155 Abs. 2 FinfraG)
- Konkurs- und Betreibungsverbrechen (Art. 163 Ziff. 1, Art. 164 Ziff. 1, Art. 165, Art. 171 Abs. 1 StGB)
- Leistungs- und Abgabebetrug (Art. 14 Abs. 4 VStrR, Art. 51 LVG)
- Mord (Art. 112 StGB)
- Sexualdelikte (Art. 187 Ziff. 1, Art. 189, Art. 190, Art. 191, Art. 195, Art. 197 Abs. 4 StGB)
- Sonstige Delikte
- Sportförderungsgesetz (Art. 22 Abs. 2 und 3 SpoFög)
- Unbefugte Datenbeschaffung (Art. 143 StGB)
- Ungetreue Amtsführung (Art. 314 StGB)
- Ungetreue Geschäftsbesorgung (Art. 158 Ziff. 1 und 2 StGB)
- Urheberrechtsgesetz (Art. 67 Abs. 2, Art. 69 Abs. 2 URG)
- Urkundenfälschung (Art. 251 Ziff.1, Art. 253, Art. 254, Art. 317 Ziff. 1 StGB)
- Verbrechen oder Vergehen gegen den Staat (Art. 265, Art. 266bis, Art. 266b, Art. 267 Ziff. 1 und 2, Art. 271 Ziff. 1 Abs. 4, Ziff. 2 und Ziff. 3 StGB)
- Verstoss gegen das Embargogesetz (Art. 9 Abs. 2 EmbG)
- Veruntreuung (Art. 138 StGB)
- Vorsätzliche Tötung (Art. 111 StGB)
- Warenfälschung (Art. 155 Abs. 2 StGB)
- Weitere strafbare Handlungen gegen das Vermögen (Art. 140, Art. 144bis Ziff. 2, Art. 148, Art. 157, Art. 160 StGB

[248] Beispielsweise wurden der MROS über 100 dieser 185 Geschäftsbeziehungen vom selben Finanzintermediär aufgrund ein- und derselben verdächtigen Vorgänge gemeldet.