Krypto-Compliance in der Praxis


Prof. Dr. iur. Cornelia Stengel, Rechtsanwältin und Partnerin, Zürich*


Magdalena Boškić, MLaw, Crypto Compliance Expert, Zürich**

Die rasante Entwicklung von Kryptowerten wie Bitcoin, Ether und anderen digitalen Vermögenswerten stellt Compliance-Verantwortliche vor neue Herausforderungen. Gleichzeitig bieten die Technologien, auf welchen diese Vermögenswerte basieren, einzigartige Chancen.

Die Schweiz hat früh Rahmenbedingungen für die Blockchain-Technologie geschaffen – etwa mit dem DLT-Rahmengesetz von 2021, das einen flexiblen zivilrechtlichen Rahmen für digitale Geschäftsmodelle einführte. Gleichzeitig misst die Schweiz der Integrität und Transparenz des Kryptosektors eine hohe Bedeutung bei. Strikte Geldwäschereivorschriften und innovative technische Lösungen stellen sicher, dass Kryptogeschäfte genauso regelkonform und sicher ablaufen wie traditionelle Finanzgeschäfte. Zentrale Elemente sind das richtige Verständnis der Blockchain-Funktionalität und die Fähigkeit, durch gezielte Analysen illegale Aktivitäten früh zu erkennen. Die Transparenz vieler Blockchains bietet neue Möglichkeiten der Analyse: so etwa eine lückenlose Transaktionshistorie, welche die Aufdeckung von verdächtigen Geldflüssen – mit den richtigen Tools und genügend Erfahrung – oft sogar leichter macht als bei Fiat-Transaktionen, d.h. Geldflüssen in traditioneller Währung. Ein Bericht des Blockchain-Analyseunternehmens TRM Labs zeigt denn auch, dass nur ein sehr kleiner Teil der Kryptotransaktionen mit Kriminalität in Verbindung steht. Im Jahr 2024 stieg das Transaktionsvolumen im Kryptomarkt auf über 10,6 Billionen USD, wobei der Gesamtwert illegal empfangener Krypto-Assets mit rund 44,7 Mia. USD lediglich 0,42% des gesamten On-Chain-Transaktionsvolumens ausmachte.

Im Folgenden werden die wesentlichen rechtlichen Grundlagen, aufsichtsrechtlichen Vorgaben und praktischen Methoden der Krypto-Compliance in der Schweiz im Sinne eines kurzen Überblicks erläutert.

Grundlage: Schweizer Geldwäschereivorschriften

In der Schweiz fallen Aktivitäten im Zusammenhang mit Kryptowährungen unter die bestehenden Geldwäschereivorschriften. Der schweizerische Gesetzgeber verfolgt einen technologieneutralen Ansatz: Massnahmen zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung gelten unabhängig von der verwendeten Technologie uneingeschränkt, also auch für virtuelle Währungen und Kryptowährungen bzw. entsprechende Transaktionen auf einer Blockchain. Ein Kryptodienstleister (häufig als «VASP», d.h. Virtual Asset Service Provider, bezeichnet) unterliegt in der Schweiz als Finanzintermediär den (Sorgfalts-)Pflichten der Geldwäschereigesetzgebung. Diese umfassen insbesondere:

- Identifizierung der Vertragspartei («Know Your Customer» [KYC]) und Feststellung der wirtschaftlich an den Vermögenswerten berechtigten Person
- Dokumentation und Aufbewahrung der Unterlagen
- Überwachung von Transaktionen unter Einhaltung eines risikobasierten Ansatzes (z.B. Analyse von ungewöhnlichen Transaktionen)
- Meldepflicht bei Verdacht auf Geldwäscherei (Meldung an die Meldestelle für Geldwäscherei, MROS)

FINMA-Rundschreiben und Aufsichtspraxis

Die praktische Umsetzung der Krypto-Compliance wird in der Schweiz stark von der FINMA geprägt. Als Finanzmarktaufsicht konkretisiert sie die gesetzlichen Vorgaben durch Rundschreiben und Auf-

sichtsmitteilungen sowie teilweise in ihren Jahresberichten. Für den Kryptobereich hat die FINMA in den letzten Jahren mehrere wichtige Vorgaben im Kontext des Geldwäschereigesetzes (GwG) erlassen:

- *Absenkung der Schwellenwerte:* Seit 1. Januar 2021 müssen Kunden bereits ab CHF 1000 (statt zuvor CHF 5000) identifiziert werden, wenn sie Kryptowährungen gegen Bargeld oder andere Werte tauschen. Diese Verschärfung – eine Reaktion auf Empfehlungen der Financial Action Task Force – betrifft insbesondere Kryptoautomaten («Bitcoin-ATMs») und Schaltergeschäfte. So soll verhindert werden, dass die Identifikationspflicht durch Smurfing (Aufteilung grosser Transaktionsbeträge in viele Kleintransaktionen) umgangen wird. Die FINMA schreibt den Betreibern von Krypto-ATMs vor, technische Vorkehrungen zu treffen, damit ihre Automaten keine anonymen Überweisungen an Wallets (digitale Geldbörsen für Kryptowerte) von Drittparteien ermöglichen.

- *Travel Rule:* Die FINMA stellte bereits im August 2019 klar, dass die bestehenden Schweizer Vorschriften zum Informationsaustausch im Zahlungsverkehr – international als «Travel Rule» bekannt – auch im Blockchain-Bereich gelten. Dies bedeutet insbesondere, dass auch bei Überweisungen von Kryptowerten Absender- und Empfängerdaten mitgesendet werden müssen.

- *Wallet-Überprüfungen:* Darüber hinaus fordert die FINMA, dass Finanzintermediäre prüfen, ob ihre Kunden bzw. die involvierte Drittpartei tatsächlich die *Verfügungsmacht* über eine deklarierte Wallet haben – unabhängig davon, ob Kryptowerte auf diese Wallet transferiert werden oder von ihr stammen. Dazu stehen verschiedene technische Methoden zur Verfügung: Weit verbreitet sind etwa die Testtransaktion eines Mikrobetrags an die Wallet («Satoshi-Test»), die Signierung einer Nachricht mit dem privaten Schlüssel der betreffenden Wallet («Message Signing»), ein «Live-Wallet-Login» unter Aufsicht von Mitarbeitenden des Finanzintermediärs oder Identitäts-NFT-basierte Verfahren. Nach erfolgreicher Verfügungsmachtüberprüfung ist es zulässig, die entsprechende Wallet-Adresse (die eindeutige, alphanumerische Zeichenfolge, die mit der Wallet verknüpft ist, vergleichbar mit einer IBAN im traditionellen Bankensystem) für eine definierte Dauer auf eine «Whitelist» zu setzen, womit die Verfügungsmacht nicht bei jeder Transaktion, sondern nach einem risikobasierten Ansatz in angemessenen Abständen erneut zu verifizieren ist. Diese Verfahren zeigen, wie vielseitig die Umsetzung der Travel Rule gestaltet werden kann.

- *Spezifische Prüfmodule und Audits:* Die FINMA passte früh auch ihre Prüfprozesse an die neuen Gegebenheiten an. So wurde 2021 das bestehende geldwäschereirechtliche Audit-Raster um ein zusätzliches Modul für «virtuelle Vermögenswerte (VAs) und VASP» ergänzt. Revisionsstellen überprüfen im Auftrag der FINMA gezielt, wie Banken ihre Kryptogeschäfte überwachen. Zudem arbeitet die FINMA eng mit den Selbstregulierungsorganisationen (SRO) zusammen, da viele Kryptofinanzintermediäre ausschliesslich im GwG-Bereich durch eine SRO beaufsichtigt werden.

- *Kontrolle auch des Sekundärmarktes:* In ihrer Aufsichtsmitteilung 06/2024 geht die FINMA noch einen Schritt weiter und verlangt, dass sämtliche Personen, die über ausgegebene Stablecoins verfügen können – einschliesslich Erwerbern im Sekundärmarkt – vom Herausgeber oder von einem angemessen beaufsichtigten Finanzintermediär hinreichend identifiziert werden. Um diese Anforderung technisch und operativ sicherzustellen, müssen Stablecoins mit vertraglichen und technologischen Übertragungsbeschränkungen strukturiert werden. In der Praxis bedeutet dies, dass Transfers nur zwischen Wallet-Adressen zulässig sind, die einem identifizierten Kunden zugeordnet, vorgängig geprüft und einer «Whitelist» zugefügt wurden; Übertragungen an andere Adressen sind zu unterbinden. Damit sind P2P-Transaktionen, d.h. Transaktionen zwischen Haltern von Stablecoins ohne Zwischenschaltung von Finanzintermediären, unmöglich. Mit dieser Praxis geht die FINMA deutlich weiter als die meisten internationalen Aufsichtsbehörden, da sie den Identifikations- und Kontrollmechanismus nicht nur auf die Emission, sondern systematisch auch auf sekundärmarktbezogene Transfers ausdehnt. Der *Vorschlag des Bundesrats zu Art. 8a VE-GwG* ergänzt die Massnahmen zur Adressierung des geldwäschereirechtlichen Risikos in Zusammenhang mit Stablecoins um

die Möglichkeit von «Blacklisting»: Dabei handelt es sich um eine Liste von Wallet-Adressen, von und zu denen Transaktionen mit Stablecoins ausgeschlossen sind, beispielsweise weil sie auf einer Sanktionsliste stehen.

Zusammengefasst unterliegen Kryptotransaktionen in der Regel denselben strengen Kontrollen wie klassische Banktransaktionen – in einzelnen Bereichen, etwa bei der Verfügungsmachtprüfung oder im Bereich von Stablecoins, gehen die Vorgaben sogar über die traditionellen Bankenstandards hinaus. Dies unterstreicht theoretisch und praktisch: Krypto-Compliance wird in der Schweiz stringent durchgesetzt, was die Integrität des Finanzplatzes wahrt.

Praktische Umsetzung: Tools und Best Practices

Wie sieht nun Krypto-Compliance im Alltag eines Finanzinstituts aus? Entscheidend ist, dass Theorie und Praxis verzahnt werden – sprich, dass den genannten Regeln konkrete Prozesse und Werkzeuge gegenüberstehen. In der Schweizer Finanzbranche haben sich mittlerweile diverse Best Practices etabliert, um Kryptogeschäfte effektiv zu überwachen und zu kontrollieren:

- *Blockchain Analytics:* Diese spielen eine zentrale Rolle in der Überwachung von Kryptotransaktionen. Entgegen der weitverbreiteten Annahme ist die Blockchain nicht anonym, sondern bloss pseudonym. Zwar ist die Identität der hinter einer Transaktion oder Wallet-Adresse stehenden Person nicht unmittelbar ersichtlich, doch sind sämtliche Transaktionen auf einer öffentlichen Blockchain dauerhaft einsehbar. Dadurch lassen sich sowohl die Flüsse von Kryptovermögenswerten als auch transaktionsbezogene Daten (z.B. Betrag, Zeitpunkt, Asset-Typ) und Wallet-bezogene Informationen (z.B. aktueller Saldo, Zuflüsse, Abflüsse) nachvollziehen. Banken nutzen für diese Analysen spezialisierte Blockchain-Analysetools wie TRM Labs, Elliptic, oder CipherOwl. Diese Tools werten die grossen Datenmengen der Blockchains aus, verfolgen Transaktionsketten, visualisieren komplexe Wertflüsse und führen risikobasierte Analysen durch. Sie scannen ein- und ausgehende Transaktionen in Echtzeit und vergleichen Wallet-Adressen beispielsweise mit sanktionierten Adressen, Darknet-Marktplätzen oder bekannten Betrugsadressen. Dank solcher Blockchain Analytics lässt sich die Herkunft von kryptobasierten Vermögenswerten sehr gut nachvollziehen. Die Transparenz der Blockchain schreckt Kriminelle ab – Kryptovermögen sind damit weit weniger attraktiv für illegale Geschäfte als allgemein angenommen.

- *Aus- und Weiterbildungen:* In der Praxis hat es sich als sinnvoll erwiesen, intern Spezialisten für Kryptothemen aufzubauen oder externe Spezialisten beizuziehen, da Krypto-Compliance spezielles Know-how, solide Fachkenntnisse, Erfahrung und ein Verständnis für die geldwäschereirelevanten Risiken im Kryptobereich erfordert. Ausserdem entwickeln sich die Technologien, Transaktionsmuster und regulatorischen Anforderungen im Kryptobereich äusserst dynamisch. Deswegen sind regelmässige Weiterbildungen und praxisnahe Schulungen unerlässlich. Nur wenn Mitarbeitende in der Lage sind, neue Funktionen, Risiken und Markttrends zeitnah zu verstehen und einzuordnen, können Compliance-Anforderungen nachhaltig und wirkungsvoll erfüllt werden.

- *Customer Due Diligence bei Krypto:* KYC endet bekanntlich nicht bei der Identitätsprüfung – gerade im Kryptogeschäft ist es wichtig, auch die Krypto-Wallets der Kundschaft sorgfältig in die Compliance-Prozesse zu integrieren. Schweizer Institute handhaben dies meist so, dass Kunden bei Ein- und Auszahlungen von Kryptowerten ihre Wallet-Adressen angeben müssen, welche dann überprüft werden (siehe oben: Überprüfung der Verfügungsmacht). Zusätzlich fordern viele Banken einen Nachweis der Herkunft der Kryptowerte, insbesondere bei grösseren Beträgen oder wenn ein Kunde seine extern gehaltenen Kryptos auf eine Wallet bei einer Bank verschieben will. Hier kommen z.B. Transaktionsauszüge von Kryptobörsen oder Wallet-Screenshots zum Einsatz, um sicherzustellen, dass der Kunde die Kryptowerte rechtmässig erworben hat und diese nicht aus dubiosen Quellen stammen.

- *Transparente Kundenkommunikation spielt ebenfalls eine Rolle:* Compliance kann nur wirksam sein, wenn Kunden nachvollziehen können, weshalb

bestimmte Assets – etwa «Privacy Coins» wie Monero – aus regulatorischen Gesichtspunkten kritisch beurteilt werden oder weshalb einzelne Transaktionen nicht ausgeführt werden können. In der Praxis hat sich gezeigt, dass eine transparente und sachliche Kommunikation entscheidend ist. Werden die Gründe offen erläutert und der Zusammenhang zwischen regulatorischen Vorgaben, Sicherheit der Kunden und Reputation des Finanzplatzes verständlich erklärt, steigt die Akzeptanz merklich.

Fazit

Krypto-Compliance ist keine Utopie, sondern gelebte Praxis in der Schweiz. Der Schweizer Regulierungsrahmen zeigt, dass Kryptogeschäfte hierzulande auf solide Regeln gestellt wurden. Wer diese Regeln in der Praxis umsetzt, kann ein «sauberes» Kryptogeschäft betreiben, das den Vergleich mit dem klassischen Finanzsektor nicht scheuen muss. Im Gegenteil: Die Transparenz der Blockchain und moderne Analysetechniken erlauben es heute, die Herkunft von Vermögenswerten teilweise besser zu prüfen als bei Fiat-Vermögen. Vorausgesetzt sind eine richtige Compliance-Kultur, Schulung und der Einsatz der richtigen Tools.

Die Botschaft an Compliance Officers lautet daher: Krypto-Compliance ist machbar und lohnt sich. Wer die theoretischen Grundlagen kennt und die praktische Umsetzung beherrscht, kann den Kryptobereich erfolgreich und regelkonform erschliessen – und damit sogar einen Sicherheitsmehrwert gegenüber manch undurchsichtiger Fiat-Transaktion erzielen.

* **Prof. Dr. Cornelia Stengel** ist Partnerin bei Kellerhals Carrard und eine profilierte Expertin für Finanzmarktrecht, digitale Innovationen und regulatorische Transformation in der Schweiz.

** **Magdalena Boškić** verstärkt seit Oktober 2025 das Team von Prof. Dr. Cornelia Stengel. Sie ist eine ausgewiesene Spezialistin für Krypto-Compliance, die von zahlreichen Banken und Finanzintermediären als Trusted Advisor im Umgang mit Token-basierten Vermögenswerten geschätzt wird. Gemeinsam bieten sie ein neues, praxisnahes Beratungsangebot für Compliance Officers an, das regulatorische Exzellenz mit technischem Verständnis verbindet – insbesondere in Bereichen, in denen klassische Prozesse an ihre Grenzen stossen.