

Anti-money-laundering practice in Crypto Valley

*Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland), Solicitor (Hong Kong),
Solicitor (England & Wales)*

Money laundering is the central risk that regulators associate with crypto-assets and Digital Assets. Transactions on public blockchains are pseudonymous, since the addresses are visible while the persons behind them remain hidden. Crypto-assets can move across borders within minutes without passing through a bank. Mixers and privacy-enhancing tokens make the tracing of flows more difficult. Criminals have used crypto-assets for ransom payments, for trading on darknet markets and for the laundering of the proceeds of fraud.

The Swiss answer has been to apply the ordinary anti-money-laundering rules to crypto service providers, with some specific additions. FINMA's guidance of 2019 required supervised institutions to apply the travel rule to transfers of crypto-assets. That rule obliges them to transmit information on the originator and the beneficiary with each transfer. Where a transfer came from or went to a wallet held by the client himself, institutions had to establish that the client controlled it.¹ This approach was stricter than that of the Financial Action Task Force, which adopted its own standard for virtual assets in June 2019.²

A practical industry developed around these rules. Analytics firms trace flows on the blockchain and assign risk scores to addresses. Compliance providers offer identification services adapted to online onboarding. Several of these firms settled in Zug, where they form one of the fastest-growing segments of the ecosystem. The CV VC report places security, auditing and compliance at 8 per cent of the Swiss and Liechtenstein blockchain companies.³

1 Notes

1. FINMA Guidance 02/2019 "Payments on the blockchain", 26 August 2019, finma.ch: Art. 10 AMLO-FINMA requires information on the

Anti-money-laundering practice in Crypto Valley

client and the beneficiary to be transmitted with payment orders, applied technology-neutrally to token transfers; as long as a supervised institution cannot send and receive this information, transfers are permitted only from and to external wallets belonging to its own customers, whose ownership must be proven by suitable technical means. ↩

2. FATF, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", 21 June 2019, [fatf-gafi.org](https://www.fatf-gafi.org). FINMA, press release of 26 August 2019, [finma.ch](https://www.finma.ch): unlike the FATF standard, the Swiss practice applies without the exception for unregulated wallets and is therefore one of the most stringent in the world. ↩
3. Netzwoche, 19 May 2025 (CV VC Top 50 Report): security, auditing and compliance 8 per cent of companies. ↩

For general information only. This article does not constitute legal or tax advice, does not replace advice on an individual case and creates no lawyer-client relationship. It reflects the legal position as of September 2026.

Online version: helveticaregister.com/zug-anti-money-laundering-practice-in-crypto-valley