GLOBAL LEDGER

Vienna
October 28–29, 2025

Global Conference on Criminal Finances and Cryptoassets

Key Insights

Yulia Murat

Head of Regulatory Affairs
at Global Ledger

Executive Summary

On October 28–29, Yulia Murat, together with Lex Fisun, CEO and Co-Founder of Global Ledger, joined the 9th Global Conference on Criminal Finances and Cryptoassets in Vienna, hosted by UNODC and organised by Europol and the Basel Institute on Governance.

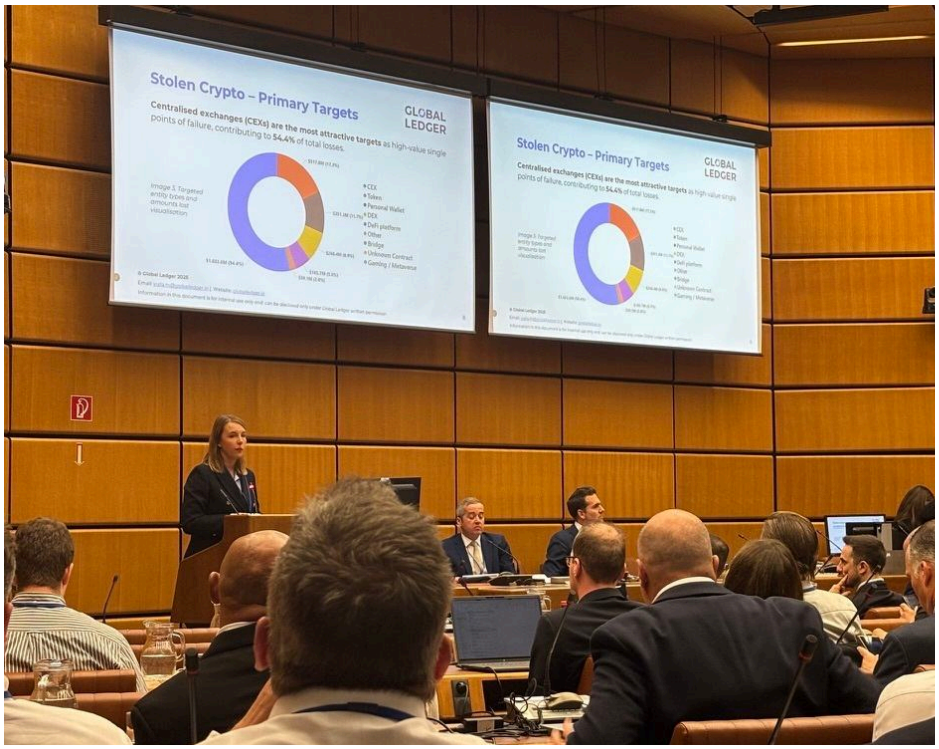
The conference brought together regulators, law enforcement agencies, and industry experts to explore how real-time data, intelligence sharing, and risk-based supervision can strengthen global resilience against crypto-enabled crime.

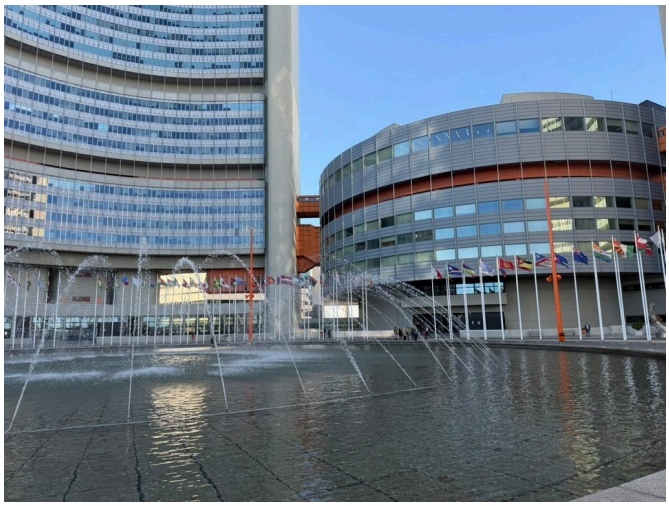
This PDF summarises the insights Yulia Murat shared during her session "How Crypto Supercharges Money Laundering and Strategies to Keep Up." Yulia spoke about how speed has become a defining threat in the digital era, supported by findings from Global Ledger's 2025 report on how fast crypto is laundered.

Email: yulia.m@globalledger.io | Website: globalledger.io

Event Context

- Hosted by UNODC, organised by Europol and the Basel Institute on Governance
- Brings together supervisory authorities, FIUs, investigators, and financial-crime experts
- Focus: strengthening global resilience against crypto-enabled crime
- Expert-level discussion setting





Email: yulia.m@globalledger.io | Website: globalledger.io

Insights Shared by Yulia Murat

Based on the findings, Yulia Murat highlighted the core challenges crypto businesses, CEXs, and regulators face today.

1 Speed is the new primary threat

Stolen assets often reach exchanges within minutes, far faster than alerting mechanisms. There is a critical time gap between an incident and industry-wide awareness.

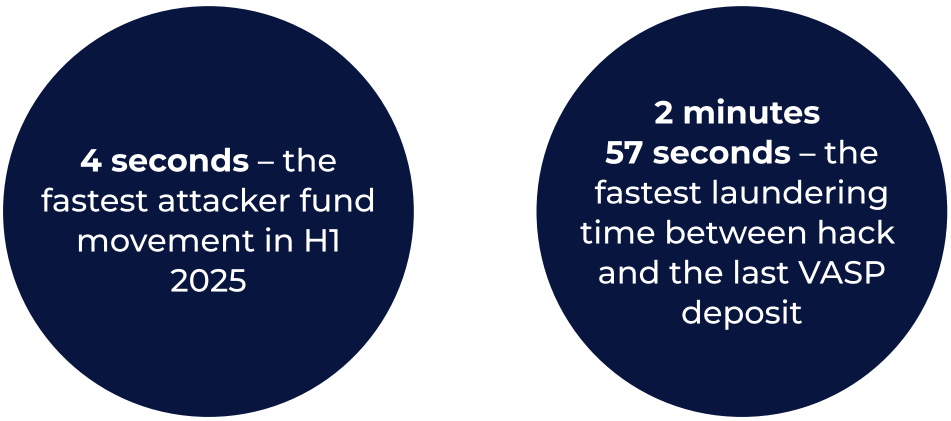


Image 1. The speed of crypto laundering

If funds are already in flow before the hack is publicly reported, then investigators and compliance teams have a significant time-related disadvantage.

2 CEXs are the most attractive targets

Centralised exchanges (CEXs) are the most attractive targets as high-value single points of failure, accounting for about **54%** of total losses.

Hackers continue to use a broad mix of techniques. That is, incident types are diverse, but the numbers are heavily skewed by the Bybit hack, which inflated malicious approval cases. Other leading categories include key compromises and rug pulls.

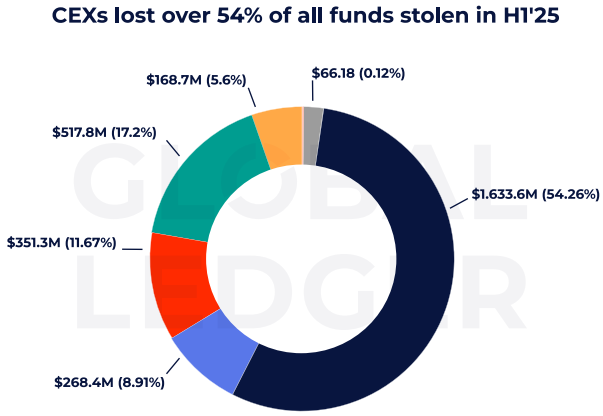


Image 2. Targeted entity types and amounts lost visualisation

3 Main crypto laundering techniques

Chain-hopping, cash-outs via limited KYC CEXs, DeFi use, and mixer services are the most common laundering methods in 2025. But surprisingly, hackers laundered **4.4x more via bridges than mixers** in H1'25, according to the same report.

Email: yulia.m@globalledger.io | Website: globalledger.io

Key Takeaways

1 Speed as a weapon

Speed has become the defining threat, with **stolen assets often reaching exchanges within minutes.**

2 CEXs remain the prime attack targets

Centralised exchanges remain the primary targets, representing more than half of all recorded losses.

3 Cross-chain movement is the new blind spot

Cross-chain movements are the new blind spot, making it harder to distinguish legitimate from illicit flows.

You can watch the full session with Yulia Murat here.

Recommended Solutions

1 Real-time tech-driven intelligence sharing

Tech-enabled collaboration between VASPs, FIUs, and regulators.

2 Automated real-time alerts

Notifications in seconds, not hours or days.

3 Risk-based tech-enabled controls and supervision

Dynamic scoring, proactive escalation flows, and continuous monitoring.

Global Ledger provides blockchain analytics, attribution-verified data, and investigation tools that help financial institutions, crypto exchanges, regulators, and law enforcement detect risks early, act with confidence, and strengthen international AML/CFT efforts.

Schedule a Demo

Email: yulia.m@globalledger.io | Website: globalledger.io