

The losses are not a technology problem

What three years of industry losses say about how digital assets are actually run.

FIGURE 1 · THE EXPOSURE, AND WHAT THE ASSESSMENT DOES ABOUT IT

THE RECORD

Stolen in digital assets: about \$1.8 billion in 2023, \$2.2 billion in 2024, more than \$3.4 billion in 2025. In 2024, private key compromise alone accounted for 43.8% of everything stolen — the largest single category.

THE MECHANISM

February 2025: \$1.5 billion left Bybit in one transaction, the largest digital theft on record. The cryptography was never broken. The screen showed a routine transfer; the signers authorised something else. Every signature was valid.

NOT ONLY EXCHANGES

In 2025, compromises of personal wallets took \$713 million across roughly 158,000 incidents and at least 80,000 identified victims. Those are the losses visible on a public chain. A family office that loses assets does not publish.

WHAT WE EXAMINE THAT AN AUDIT DOES NOT

- Who can move assets, and what stops one person acting alone.
- What an approver can actually verify on the device in front of them.
- Whether the record of holdings reconciles to the chain, and how often.
- How much sits with one counterparty, custodian or venue.
- What happens on death, incapacity, departure or a dispute.
- What the staking, lending and collateral agreements actually say.

WHAT YOU GET

- A risk register, rated, with the reasoning visible.
- Recommendations ordered by priority, effort and urgency, as a 30, 60 and 90-day roadmap.
- An immediate attention notice if something should not wait for the report.
- A reassessment later that shows what moved and what did not.

Source: Chainalysis, 2025 and 2026 Crypto Crime Reports; NCC Group technical analysis of the Bybit incident, March 2025. Addresses at the foot of this page.

Where to start

A scoping conversation, of about an hour. We go through what you hold, how it is held today and who is involved, and you get a straight answer on whether an assessment is worth your time. If it is not, we will say so. Nothing is recorded, and no keys, recovery phrases, passwords or balances are ever discussed.

Olivier Busolini

Who we are

Chief Information Security Officer and Managing Director of Sygnum Bank, Zurich, from August 2021 to April 2023 — a FINMA-regulated, crypto-native digital asset bank and one of the first institutionally licensed. The group information security function was built there from inception, and security crisis response and FINMA engagement were run through the 2022 market downturn with clean supervisory standing. Twenty-five years in cybersecurity leadership in regulated institutions behind it. Delivered from Dubai, across Switzerland, Europe and the GCC.

The framework is maintained rather than published once: every regulatory citation is verified against the primary text, dated, and re-checked twice a year.

<https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/> · <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/> · <https://www.nccgroup.com/research/in-depth-technical-analysis-of-the-bybit-hack/>