

Quantum Threat: The Race Is Already Underway

Digital assets are secure today. But the threat must still be taken seriously.

By Thomas Brunner, Head of Custody and Staking, Sygnum

The codes that protect our payments, banking transactions and digital assets could one day be broken by a quantum computer. No one knows when, yet banks need to be prepared for that possibility.

Specialists have a name for that moment: “Q-day”, the day when a quantum computer will be able to break the codes that secure the financial system. No machine can do this today, and predictions about when it might happen remain wide-ranging.

The threat, however, is credible. These protective codes serve two purposes: making data unreadable and signing transactions to prove who authorised them. In digital assets, they form the keys that provide access to the assets themselves. Algorithms capable of withstanding quantum attacks already exist, and several governments are calling for their adoption now. The right approach is to stay calm about the timing and get to work.

A Present-Day Risk

Migrating a large institution takes time, and data stolen today could be read tomorrow. This is the logic behind “harvest now, decrypt later”: an attacker captures encrypted data and bets on future machines being able to decrypt it. For any information with a long lifespan, that threat already exists.

The risk that concerns me most is forgery. Forging signatures could make it possible to move digital assets that were thought to be protected.

Two Workstreams to Tackle in Parallel

A bank has to migrate two layers at the same time: the cryptography protecting clients’ assets and communications, and the core banking systems that support it, are often old and interconnected. Progress will be dictated by whichever of the two moves more slowly.

The heart of the problem is called cryptographic agility: being able to replace a signature or encryption scheme without breaking everything that depends on it, while keeping systems operational. That requires knowing where the keys are stored, often in unexpected places such as backups.

Digital assets add another layer of complexity. A custodian cannot simply change the keys of a client’s on-chain assets at will. Migration is as much about operations and consent as it is about cryptography.

That is why we believe banks’ programmes should be well progressed by 2027, ahead of the timelines set by the major networks. Most of the cost comes from untangling and testing everything that relies on cryptography.

A Board-Level Issue

For a board, three questions matter. Do we know where our cryptographic exposures lie? Do we have a migration plan? Do we have the agility to execute it? As soon as supervisors include this risk in their reporting requirements, it will move from the innovation roadmap to the audit agenda.

When communicating with clients, the honest message is also a reassuring one. No computer can break this cryptography today, assets are secure, and work is already underway to keep them that way. Clients want to know that their provider has a plan and is executing it to mitigate the risk ahead of time.

By 2030 or 2035, quantum-resistant cryptography will be standard across payments, custody and communications. Networks and custodians will be able to move clients' assets to new signatures cleanly and with their consent. The goal comes down to one capability: being able to change cryptography on demand. Institutions that build that capability now will be ready in time.