SWISS BLOCKCHAIN FEDERATION

QuantumBasel
Center of Competence
for Quantum Computing and AI

Position Paper

Quantum Security in Blockchains

An initiative of the Digital Assets Working Group of the Swiss Blockchain Federation in Collaboration with QuantumBasel.

Purpose: This position paper aims to provide a structured overview of what quantum computing means for blockchain applications, the associated risks, and how the Swiss blockchain community should prepare for them.

Distributed ledger technologies, stablecoins, and crypto assets are here to stay. We therefore need to start preparing now to ensure that quantum computing does not compromise the cryptographic foundations at the very core of these technologies and undermine the benefits they provide.

Date of publication: 26 October 2026

SBF Authors: Mauro Cappiello (Blockchain Innovation Group, BIG), Daniel Diemers (SNGLR Group), Daniel Rutishauser (Accelarium), Vasily Suvorov (accelerate).

QuantumBasel Authors: Damir Bogdan, Frederik Flöther.

Acknowledgements

The Swiss Blockchain Federation would like to thank all experts and contributors who provided their knowledge, perspectives, and valuable input to this position paper.

Our particular thanks go to **QuantumBasel**, and especially to **Damir Bogdan and Frederik Flöther**, for their expertise, valuable contributions, and critical review. Their insights into quantum computing and its implications for cryptography and digital assets have significantly contributed to the quality and relevance of this paper.

We greatly appreciate their commitment to strengthening Switzerland's quantum readiness and helping prepare the Swiss blockchain ecosystem for the challenges and opportunities of the quantum era.

Disclaimer

This Paper reflects the state of knowledge as of mid-October 2026. Quantum computing is maturing quickly, and neither the arrival of a cryptographically relevant quantum computer nor the path to it can be predicted with certainty. Published estimates for "Q-Day", the point at which such a machine becomes available, differ by several years and have been revised repeatedly, in both directions. The timelines and figures in this Paper are therefore informed assumptions, not forecasts.

This uncertainty does not reduce the need to act. Migrating decentralized networks to quantum-safe cryptography takes years, so preparation has to begin before the date is known. The assumptions will be reviewed as part of the proposed semi-annual SBF Quantum Readiness Report.

This Paper does not constitute legal or investment advice. The views expressed are those of the authors and do not necessarily reflect the position of every SBF member.

Table of Contents

Acknowledgements **2**

Disclaimer **2**

1 Executive Summary **4**

2 Current Situation **6**

2.1 Overview of Swiss Quantum Initiatives 6

2.2 Blockchain and Quantum Computing: The Connection 8

3 Purpose and Objectives **11**

3.1 Purpose 11

3.2 Objectives 12

3.3 Scope and Limitations 13

4 Risk Landscape **14**

5 Excursus: Mosca's Theorem or Why the Clock Is Already Ticking **18**

6 Regulatory Environment of Quantum Technology **20**

7 Key Areas for Action **22**

8 Recommendations **30**

8.1 For the Swiss Blockchain Federation (SBF) and its members 30

8.2 For Financial Infrastructure Providers, Regulators, and Research Institutions 31

9 Sources **32**

1 Executive Summary

The rapid advancement of quantum computing (QC) marks a turning point for global cybersecurity. A **cryptographically relevant quantum computer (CRQC)** will be capable of breaking the fundamental asymmetric cryptographic schemes underpinning today's blockchain technologies. Recent resource estimates[1] have lowered the hardware threshold for such a machine considerably, and Google, Microsoft and Cloudflare have set 2029 as the target for completing their own post-quantum cryptography (PQC) migrations [Q3]. Neither is a forecast of **Q-Day**, and expert surveys show a wide spread of expectations [Q4]. This Paper therefore uses 2029–2033 as its planning horizon throughout, i.e. the period from which a CRQC can no longer be ruled out.

Quantum computing is also a major economic opportunity. According to McKinsey estimates[2], quantum computing could create **USD 1.3 to 2.7 trillion in economic value for companies worldwide by 2035**, with financial services among the sectors where it is gaining traction. For the financial and crypto sectors, protecting the cryptographic foundations of digital assets is a precondition for sharing in that value. Parts of the threat already exist today: public keys exposed on-chain can be attacked as soon as a CRQC exists, without any prior harvesting, and encrypted off-chain data such as API traffic, backups and client data can be intercepted now and decrypted later (**"harvest now, decrypt later"**).

As decentralized networks may require years to implement fundamental architectural upgrades, the Swiss blockchain community must prepare now. To this end, this Position Paper (hereinafter the "Paper") analyses vulnerabilities across all layers of the technology stack and presents a strategic roadmap for addressing them. At the heart of its recommendations is the establishment of a **semi-annual SBF "Quantum Readiness" Report**, enabling Switzerland to take a leading international role and position itself as a pioneer in **quantum-secure digital assets**.

[1] Resource estimates: see [Q1] and [Q2]. PQC migration targets (not Q-Day forecasts): see [Q3].

[2] McKinsey (2026). *McKinsey Quantum Technology Monitor 2026: A commercial tipping point*. Report, 28 April 2026. https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/mckinsey-quantum-technology-monitor-2026-a-commercial-tipping-point

This Paper of the Swiss Blockchain Federation first outlines the current situation, including the opportunities of quantum technology, and then examines the risks in detail (chapter Risk Landscape). Furthermore, the regulatory environment is outlined. The following chapter (Key Areas for Action) outlines a possible path forward. In the last chapter (Recommendations), this Paper concludes with a final set of recommendations. Central among them is the SBF Quantum Readiness Report, an industry-wide monitor where blockchain organizations can indicate the current status of their projects and the challenges they need to address, as well as the projected timeline for the remaining changes.

This Paper is intended to help decision makers in assessing the risks associated with DLT-based solutions and in choosing which technology stack to build on and operate, and where to deploy their envisioned solutions.

It is recommended that Switzerland should take a coordinated and proactive approach to quantum security for use cases based on DLT, such as digital assets and stablecoins. The Swiss Blockchain Federation should lead this effort through a **Quantum Readiness Report**, providing transparent, industry-wide monitoring of blockchain protocols and their progress towards post-quantum security, complemented by practical standards for cryptographic agility and asset recovery. Banks and crypto custodians should systematically assess and upgrade their HSM and MPC-based infrastructures, while regulators should incorporate quantum readiness into their ongoing supervisory dialogue. At the same time, Swiss research institutions should advance efficient post-quantum cryptography to ensure that quantum-safe blockchain infrastructure remains both secure and economically viable.

2 Current Situation

2.1 Overview of Swiss Quantum Initiatives

Relative to its size, Switzerland ranks among the world's leading quantum technology hubs. More than 200 research groups across the country are working on quantum-related topics, and 88% of Swiss quantum publications are produced through international collaboration, a level surpassed by only one other country [Q5]. This strength in numbers has been built over decades. For the blockchain community, it represents a strategic locational advantage that should be leveraged for the upcoming migration of the industry to post-quantum cryptography (PQC).

Federal Government and Funding

The Federal Council launched the Swiss Quantum Initiative (SQI) in 2022. The initiative is supported by the State Secretariat for Education, Research and Innovation (SERI) and coordinated by the Swiss Academy of Sciences (SCNAT). Following initial funding of CHF 10 million for 2023–2024, up to CHF 82.1 million in Federal funding has been allocated for the 2025–2028 period, distributed among SCNAT (CHF 22.9 million), the Swiss National Science Foundation (SNSF; CHF 29.6 million), and Innosuisse (CHF 29.6 million) [Q6]. In 2026, the Swiss Quantum Commission, established under the auspices of SQI, also presented Switzerland's first Quantum Strategy. The ambition is to position Switzerland as an international hub for quantum science, education, and innovation, built on four pillars: interdisciplinary research, translational infrastructure, scaling and commercialization, and education [Q5].

Research

Switzerland has a broad academic foundation in quantum science and technology. It includes, among others, the Quantum Center at ETH Zurich and the joint ETH Zurich–PSI Quantum Computing Hub, EPFL's Center for Quantum Science and Engineering, the National Centres of Competence in Research NCCR SPIN (spin qubits) and NCCR SwissMAP, as well as the Universities of Geneva and Basel. The University of Basel and QuantumBasel have entered into a partnership to scale the Center for Quantum Computing and Quantum Coherence (QC2), with the aim of accelerating the transition from academic research to industrial

applications through closer integration of quantum hardware and algorithms. At CERN, the Open Quantum Institute, launched by GESDA, promotes broad and equitable access to quantum technologies [Q5], [Q7].

Industry and Startups

IBM Research Zurich has been conducting quantum technology research at its Rüschlikon site for decades. ID Quantique, founded in Geneva in 2001 and acquired by US-based IonQ in 2025, is a pioneer in quantum cryptography; its QKD system became the world's first to be deployed commercially in 2007 [Q8]. Other notable players include Terra Quantum, Zurich Instruments, and ETH spin-off ZuriQ, which is developing scalable two-dimensional ion-trap processors and raised USD 25.5 million in seed funding in 2026 [Q9]. Basel-based quantum sensing company Qnami was acquired by US instrumentation manufacturer Quantum Design in 2026 [Q10].

QuantumBasel operates Switzerland's first commercial quantum hub at the uptownBasel campus and is a partner of IonQ. It operates its own IonQ quantum computer with 36 algorithmic qubits (AQ), with a next-generation system scheduled to succeed it in 2027. QAI Ventures complements the ecosystem as an accelerator and early-stage investor [Q7]. At the industry-association level, the Swiss Quantum Industry Network (SQIN), established in 2024, together with Swissphotonics, SATW, Swissnex, Swissmem and the Swiss Quantum Initiative, connects industry, research, and policymakers [Q7], [Q11].

Financial Centre and Quantum-Safe Readiness

The Swiss Bankers Association recommended in its November 2024 expert report that financial institutions assess their IT architectures for vulnerabilities arising from quantum computing [Q12]. FINMA has gone one step further by establishing quantum risk management as a supervisory expectation through Guidance 05/2026 [Q13]. FINMA notes that its existing principle-based requirements already cover quantum risk and that no immediate full migration is required. It recommends a PQC roadmap by mid-2027 and a board-approved PQC strategy.

From the SBF Working Group's perspective, this combination is internationally unique: nowhere else does such a dense quantum ecosystem intersect with a blockchain industry as

concentrated as Switzerland's Crypto Valley. This convergence underpins the ambition of this paper to position Switzerland as a **"Quantum-Safe Jurisdiction for Digital Assets"**.

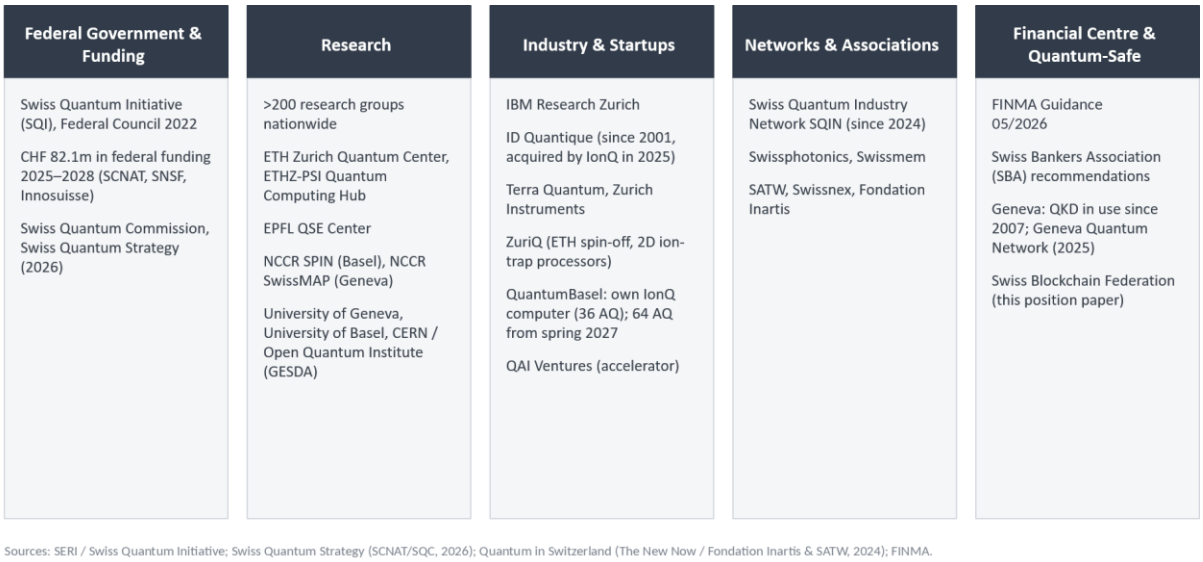


Figure 1: Overview on the Swiss Quantum Ecosystem

2.2 Blockchain and Quantum Computing: The Connection

First, an important distinction. Blockchain as a concept, meaning a decentralized, immutable ledger, is not inherently vulnerable to quantum computing. What is vulnerable are the cryptographic mechanisms that today's blockchains use to safeguard ownership and authorization. Shor's algorithm can break the elliptic-curve signature schemes, such as ECDSA, Schnorr and EdDSA (e.g. Ed25519), on which virtually all major networks rely. Once a public key is exposed, a sufficiently capable quantum computer could derive the corresponding private key. Whoever controls the private key can forge valid signatures [Q14]. The situation is more favorable for hash functions. Grover's algorithm provides only a quadratic speed-up for attacks against them, meaning that SHA-256-based structures are generally considered manageable. For Proof-of-Work mining, Grover's algorithm is not expected to give quantum computers a practical advantage over specialized classical hardware. The quantum threat therefore concentrates primarily on the **signature layer**, precisely where ownership and authorization are determined.

Three characteristics make blockchains particularly vulnerable compared with conventional IT systems:

1. **Public-key exposure is permanent.** Depending on the protocol used, every address that ever sent a transaction has permanently exposed its public key on-chain.
2. **There is no rollback.** A forged signature allows transactions to be initiated against the will of the address holder and can therefore result in an irreversible loss of assets, with no central issuer or authority able to cancel or reverse the transaction.
3. **Both pending and long-exposed keys can be attacked.** A sufficiently fast quantum computer could perform an **"on-spend" attack**, intercepting a pending transaction, deriving its private key, and injecting a forged transaction within the block confirmation window. A slower quantum computer would be limited to **"at-rest" attacks** against public keys that have already been exposed for extended periods [Q1].

What does this mean in practice? In the short term, three measures are particularly important: avoid address reuse (where possible), minimize public-key exposure, and prepare for migration to post-quantum signature schemes [Q1].

The greatest challenge lies in the migration. The NIST standards were not optimized for blockchain environments. The conservative hash-based SLH-DSA scheme produces signatures of around 8 kilobytes [Q15], two orders of magnitude larger than today's 64-byte ECC signatures, which would sharply reduce Bitcoin's transaction throughput. Optimized proposals such as Blockstream's SHRINCS, at around 550 bytes or more in its August 2026 draft BIP [Q16], significantly reduce the overhead but still require roughly nine times the signature size of the status quo [Q17].

Moreover, migration does not happen automatically. Every holder would need to actively transfer all holdings to quantum-safe addresses. This includes the roughly one million BTC attributed to Satoshi Nakamoto [Q18], held largely in early pay-to-public-key outputs whose public keys are directly visible on-chain. Coins for which the private keys have been lost cannot be migrated. The community therefore faces an uncomfortable choice: leave such holdings permanently vulnerable to quantum attacks, or restrict them after a defined migration deadline, ideally combined with a recovery path for legitimate owners, as BIP-361 proposes [Q17], [Q19].

Encouragingly, the migration path for the Bitcoin ecosystem, as well as Ethereum and the broader blockchain landscape, is beginning to take concrete shape. BIP-360 introduces Pay-to-Merkle-Root, an output type designed to eliminate the quantum-vulnerable spending path that exposes public keys, thereby establishing a structural foundation for post-quantum signatures. BIP-361 complements this approach by outlining a phased sequence of soft forks, ultimately leading to a migration deadline combined with a recovery path [Q17], [Q19]. Emerging industry consensus suggests that high-value assets and critical systems should achieve quantum-safe readiness by around 2029 or shortly thereafter. Given that consensus-driven upgrades in decentralized networks may take several years, this timeline leaves little room for delay [Q17].

The relationship between blockchain and quantum technology is not purely defensive. Quantum technologies can also contribute building blocks for next-generation security architectures, including certifiable quantum random number generation (QRNG) and Quantum Key Distribution (QKD). Beyond security, the convergence of quantum computing and artificial intelligence may enable entirely new classes of applications.

The specific technical vulnerabilities across the full blockchain stack – including consensus mechanisms, ZK-Proofs, and HSM infrastructure – are detailed in the Risk Landscape section below.

For the Swiss blockchain community, the conclusion is clear: **crypto-agility and migration readiness are not peripheral technical concerns. They will determine whether the manifold benefits as well as public trust in blockchain technology can be preserved beyond Q-Day.**

3 Purpose and Objectives

3.1 Purpose

Quantum computing is no longer a distant theoretical concern – it is an immediate strategic priority for the blockchain and digital asset industry.

FINMA Guidance 05/2026, based on a survey of 60 institutions, reports that about two thirds of Swiss financial institutions expect quantum computing to become relevant within seven years, while only 8% have a concrete migration roadmap, which means that more than 90% do not [Q13]. Google Quantum AI's paper published in March 2026 further estimated that the physical-qubit count needed to break the cryptography securing Bitcoin and Ethereum is roughly 20 times smaller than a previous estimate [Q1].

As outlined in the Executive Summary, recent resource estimates and the 2029 migration targets of Google, Microsoft and Cloudflare do not forecast Q-Day, but they make it prudent to plan for a CRQC within the 2029–2033 window.

Migrating cryptographic algorithms and protocols to newer, more robust standards has always been a complex, multi-year undertaking. Given the specific challenges facing the digital asset and blockchain industry, e.g. decentralized decision making and asset transfers to new addresses, the **PQC** migration process is very likely going to be more complex and will require more effort and coordination compared to the other types of IT systems or even the Internet as a whole.

It is therefore crucial to swiftly establish a consensus around best practices and critical milestones leading to acceleration of the PQC migration involving key actors in our industry.

The SBF publishes this Paper to bridge the gap between regulatory expectation, looming cryptographical risks and operational reality — providing decision-makers across the Swiss and international blockchain ecosystem with strategic orientation, a structured risk landscape, and role-specific starting points, without requiring technical expertise in quantum computing or cryptography.

This paper focuses on four actor layers — Protocol Teams, Key Management providers, Digital Asset Custodians, and Traditional Financial Institutions — each with distinct risk exposures and migration imperatives. The actors listed are illustrative, not exhaustive.

Regulators, research institutions, and industry associations play an enabling role addressed in the Recommendations section.

3.2 Objectives

1. Establish a shared risk and opportunity assessment

Define a common language and structured risk landscape so that SBF members and their stakeholders operate from the same baseline – covering both the threats to existing infrastructure and the strategic opportunities for those who act early.

2. Make regulatory signals actionable

FINMA's Guidance 05/2026 confirms that quantum risk management is now a supervisory issue for Swiss financial institutions, explicitly including distributed ledger technologies. This Paper translates that signal into orientation relevant to blockchain-specific actors.

3. Provide role-specific first action steps

Different actors – protocol teams, key management providers, digital asset custodians and traditional financial institutions – face a variety of risk exposures. This Paper identifies those risks, puts them into context for each of the actors' categories and points each group toward a concrete starting point.

4. Define SBF's role

The Swiss Blockchain Federation positions itself as coordinator and standard setter for the Swiss blockchain ecosystem: developing shared frameworks, engaging with regulators and policymakers, and ensuring the industry moves as a coordinated whole rather than in uncoordinated, fragmented individual efforts.

5. Position Switzerland internationally as a first mover

The Crypto Valley's unique concentration of blockchain organizations, foundations, and protocol developers creates a natural opportunity to establish Switzerland as a global reference point for quantum-safe digital assets and distributed ledger protocols.

3.3 Scope and Limitations

This paper focuses on the Swiss blockchain and digital asset ecosystem. It does not constitute legal, regulatory, financial, or investment advice. The risk dimensions identified are illustrative and non-exhaustive – the threat landscape evolves continuously, as demonstrated by the significant revision of resource estimates in 2026 alone.

For detailed technical guidance, readers are referred to the Applied Quantum PQC Migration Framework (Ivezic, 2026) [Q20] and the NIST post-quantum standards (FIPS 203 / 204 / 205).

4 Risk Landscape

The quantum threat to distributed ledger technologies (DLT) and digital assets is neither a distant nor a theoretical concern any longer – it is actively unfolding across technical, market, and regulatory dimensions.

To establish a common language and baseline across the industry, this section structures the quantum threat into five interconnected risk dimensions: (i) Technical Vulnerabilities, (ii) Market & Systemic Risks, (iii) Timeline & Migration, (iv) Role-Specific Profiles, and (v) Performance, Governance & Geopolitics. These dimensions must not be viewed in isolation: technical vulnerabilities amplify market risks, unaligned governance delays necessary upgrades, and performance bottlenecks threaten protocol adoption. The first two dimensions are discussed in this chapter. The remaining three are considered in chapter 7 (Key Areas for Action).

Technical Deep-Dive & Implementation Reference: This section provides strategic decision-makers with high-level orientation. For technical implementation guidance, see the references in section 3.3.

(i) Technical Vulnerabilities Across the Blockchain Stack

The cryptographic stack securing digital assets exhibits fundamental vulnerabilities against quantum algorithms (primarily Shor's algorithm and, to a lesser degree, Grover's algorithm) across multiple layers:

- **Digital Signatures (Most Critical Vulnerability):** Elliptic-curve signature schemes (ECDSA, Schnorr as used in Bitcoin's Taproot, EdDSA such as Ed25519, and the BLS signatures used by Ethereum validators) used for transaction signing and validator consensus offer no resistance against private key derivation via Shor's algorithm.
- **Exposed Public Keys & Wallets:** Depending on the protocol used, a blockchain address that has initiated an outgoing transaction has permanently exposed its public key on-chain. On networks like Bitcoin, millions of coins (estimated ~6M BTC[3]) reside in exposed addresses (structural or operational exposure), making them primary targets for CRQC.

[3] https://research.glassnode.com/measuring-bitcoins-quantum-exposed-supply/

- **Systemic Consensus Threats:** In Proof-of-Stake networks, compromising validator signature keys directly threatens the integrity of the entire ledger, presenting a far more catastrophic, systemic threat than individual wallet breaches. Bitcoin's Proof-of-Work consensus is not affected in this way.
- **Zero-Knowledge Proofs:** Zero-knowledge systems relying on elliptic curves (e.g., pairing-based SNARKs such as Groth16 or KZG-based schemes) must transition to quantum-safe alternatives like hash-based SNARKs and STARKs or lattice-based proofs.
- **Infrastructure & HSMs:** Institutional custodians rely on Hardware Security Modules (HSMs). Several current HSM product lines already receive ML-DSA and ML-KEM support through firmware updates [Q21], but older HSM generations may require hardware replacement. Multi-Party Computation (MPC) schemes used by institutional custodians are not directly broken by quantum algorithms – however, the underlying signature schemes they rely on are. In addition, many threshold-ECDSA protocols use Paillier encryption and elliptic-curve-based building blocks, so their protocol messages are exposed to "harvest now, decrypt later". MPC providers must therefore migrate both their signing standards and these protocol building blocks.
- **Weak Entropy Threats:** The issue of weak entropy (or randomness) in cryptographic wallet generation has been a longstanding issue and debate in blockchain. Pseudo-Random Number Generators (PRNG) may have been seeded with predictable data, allowing for brute-force algorithm attacks. This is not a quantum-related vulnerability, and a properly seeded cryptographically secure random number generator is sufficient. Quantum Random Number Generators (QRNG) can serve as an additional, certifiable entropy source.

(ii) Market and Systemic Risks

Technical vulnerabilities translate directly into market dynamics that cannot be resolved solely through protocol patches:

- **"Trust Now, Forge Later" vs. "Harvest Now, Decrypt Later":** On-chain data is public, not encrypted, so nothing on-chain is "decrypted retroactively". The relevant risk for blockchains is that public keys already exposed on-chain allow private-key

derivation and signature forgery once a CRQC exists (sometimes called “trust now, forge later”). This applies to Bitcoin and Ethereum alike, since both expose public keys when funds are spent. “Harvest now, decrypt later” (HNDL) in the strict sense applies to encrypted off-chain data: TLS and API traffic, custody communication, backups, KYC and other client data, and MPC protocol messages. Such data can be intercepted today and decrypted once a CRQC exists, so this part of the threat is already active right now. It applies to all operations of the players in the blockchain ecosystem and is not specific to protocol developers and network participants.

- **The Compliance & Migration Gap:** FINMA’s Guidance 05/2026 establishes quantum risk management as a supervisory expectation for Swiss financial institutions. Internationally, leading standards bodies and regulators – including the European Commission and the NIS Cooperation Group, as well as the US standards body NIST – set PQC migration deadlines. Most of these are recommendations or drafts; only CNSA 2.0 sets binding dates, for US National Security Systems, and Switzerland has no legal PQC requirement yet. Where decentralized networks may require years to coordinate protocol-level upgrades, a dangerous compliance gap emerges where institutions must comply with evolving legal requirements before public blockchains are technically capable of supporting them.
- **Systemic Trust Shock & tokenized Real-World Assets (RWAs) Exposure:** Failing to secure tokenized Real-World Assets (RWAs — not to be confused with Risk-Weighted Assets in the banking context) and institutional custody solutions creates severe liability exposure. A breach at Q-Day could trigger an industry-wide liquidity shock and loss of investor confidence.
- **Orphaned Tokens:** Dormant wallets, lost keys, or unmanaged legacy accounts may miss migration deadlines. Once classical cryptography is broken, these assets, depending on the protocol, can become permanently frozen or stolen, potentially distorting circulating token supplies and market prices.
- **Vendor Dependency Risk:** A critical but often overlooked dimension of the quantum risk landscape is the dependency chain between institutional actors and their technology providers. Digital Asset Custodians and Traditional Financial Institutions do not control their own cryptographic infrastructure – they depend on Key Management

Technology providers (e.g. Taurus, Fireblocks, DFNS, Copper, Ledger, etc.) who in turn depend on Protocol Layer upgrades. This creates three specific risks:

- **Readiness gap:** Providers may not be PQC-ready on time – or may not communicate their status transparently.
- **Cost risk:** PQC migration may be positioned as a billable upgrade rather than a contractual obligation.
- **Verification gap:** Institutions have limited ability to independently validate whether a provider's PQC implementation is correct and complete.

Digital Asset Custodians and Traditional Financial Institutions should therefore treat vendor PQC readiness as an active risk management obligation – not a passive assumption – by demanding formal attestation, contractual migration milestones, and independent audit rights from all technology and service providers.

5 Excursus: Mosca's Theorem or Why the Clock Is Already Ticking

When does an organization need to begin its migration to post-quantum cryptography? Michele Mosca provided an uncomfortably simple answer as early as 2015 [Q22]. It requires only three variables. How long must the data remain confidential (X)? How long will migration to quantum-safe cryptography take (Y)? And when will a CRQC become available (Z)? If **X + Y > Z**, migration has started too late and the data is at risk: data harvested today can be stored and decrypted after Q-Day while it still has value. This is the essence of the **"Harvest Now, Decrypt Later"** principle. For confidential data, the threat therefore does not begin on Q-Day.

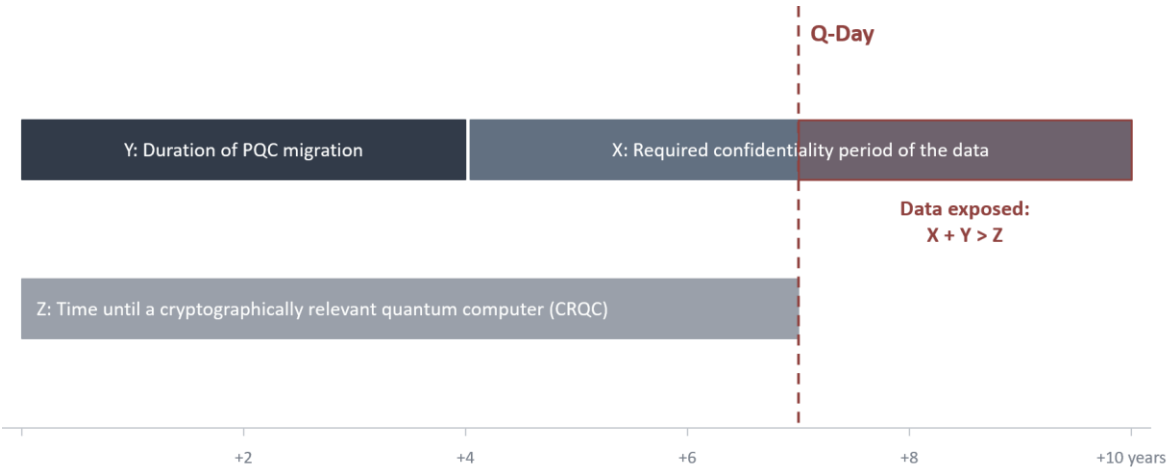


Figure 2: Mosca's Theorem - It's too late if X+Y > Z

What is concerning is that all three variables are currently evolving to the disadvantage of defenders. The trend is most visible for Z. In 2021, around 20 million noisy qubits were still estimated to be required to factor a 2048-bit RSA key. By 2025, Gidney had reduced this estimate to fewer than one million [Q23], [Q24]. In March 2026, another significant step followed, this time concerning secp256k1, the elliptic curve of relevance to blockchain systems. Google Quantum AI revised the resource estimate for solving the discrete logarithm problem to 1,200 logical qubits, corresponding to fewer than half a million physical qubits on a superconducting architecture. This is roughly a twentyfold reduction compared with the previous estimate by Litinski [Q25] of around nine million physical qubits on a photonic architecture, although the two figures refer to different hardware platforms [Q1].

Other hardware platforms may lower the threshold even further. Recent research indicates that Shor's algorithm could operate at cryptographically relevant scales on reconfigurable

atomic qubits with around 10,000 physical qubits. A P-256 discrete logarithm could be solved within days on a 26,000-qubit machine, albeit considerably more slowly than on superconducting systems [Q2]. This is consistent with annual expert surveys that increasingly project shorter remaining lifetimes for today's encryption standards [Q4], as well as with major technology providers such as Google, Microsoft, and Cloudflare targeting 2029 for completion of their own PQC migrations [Q3].

For conventional public blockchains, Mosca's equation becomes particularly critical because of the two remaining variables. **X can effectively become unlimited for cryptographic information permanently recorded on a public ledger.** Once a public key or other security-relevant information has been exposed on-chain, it can be copied and retained indefinitely, even if the blockchain itself later removes or obfuscates it. In this context, traditional "harvesting" is not even necessary because the relevant information is already publicly accessible.

This does not apply equally to all DLT architectures. Systems that never expose reusable public keys, minimize data persistence, use one-time cryptographic credentials, or employ privacy-preserving architectures can reduce long-term exposure. Ultimately, however, protection against quantum attacks on transaction authorization requires migration to quantum-safe cryptographic schemes rather than relying on data deletion or obfuscation alone.

Y, meanwhile, is exceptionally long. Decentralized networks require technical and socioeconomic consensus on protocol changes as well as the active participation of individual asset holders, potentially extending migration timelines to several years (see "Governance & Chain Splits" in chapter 7).

For keys already exposed on-chain, the conclusion is therefore simple: their risk window opens on Q-Day, whenever that is, and the only remedy is to migrate the affected funds before then. Given how long **Y is, waiting for certainty about Z** is not an option.

6 Regulatory Environment of Quantum Technology

So far, Switzerland has no specific “quantum laws”; however, the new technology is covered by various existing regulations.

The most prominent legal challenge is to be seen in data protection law. Based on Art. 13 of the Constitution requiring protection against misuse of personal data, the revised Data Protection Act (DPA) of 2023 requires a data protection impact assessment where the processing of personal data is likely to entail a high risk (Art. 22). The provision is technology-neutral, but quantum-enabled processing can fall under it. Furthermore, appropriate technical and organizational measures must be built into the systems to comply with the privacy-by-design and the privacy-by-default obligations (Art. 7). Quantum-enabled profiling or automated decision-making would require compliance with Art. 5 and Art. 21 DPA. In addition, what counts as state-of-the-art encryption will change: encryption itself remains, but the quantum-vulnerable algorithms will have to be replaced by post-quantum algorithms, for which standards (FIPS 203 / 204 / 205) already exist [Q15].

Whether quantum-enabled software is protected by the Swiss Patent Act is uncertain because this Act does not clearly define the term “invention”. Similar problems as in case of computer-implemented inventions and in case of algorithms or mathematical-methods occur since the patentability depends on a technical application. The requirements could be fulfilled by quantum-enabled control systems or quantum-hardened cryptographic transmission protocols.

In financial markets, quantum-enabled infrastructures must comply with the requirements of the Financial Market Infrastructure Act (FMIA) and the Information Security Act (ISA). Relevant aspects are safe operations, information security and cyber risks; concerned operators are trading venues, central counterparties, and central securities depositories. Ultimately, the protection of critical infrastructures is at stake.

In FINMA Guidance 05/2026, the Swiss Financial Market Supervisory Authority recommends a PQC roadmap by mid-2027 and a board-approved PQC strategy. That is currently the single most actionable regulatory date in Switzerland.

However, international timelines increasingly converge around 2030–2035 as the critical window for completing the transition to Post-Quantum Cryptography (PQC). NIST plans, in its draft IR 8547, to deprecate or phase out quantum-vulnerable cryptography from 2030

onwards, with broad removal by 2035 [Q26]. The EU's 2025 coordinated roadmap recommends that Member States start their transition by the end of 2026 and targets high-risk systems for migration by 2030, with the broader transition extending towards 2035 [Q27]. For US National Security Systems, CNSA 2.0 moves even faster: new products and services are expected to support the new standards from 2027, non-compliant equipment should be replaced by 2030, and CNSA 2.0 becomes mandatory across relevant systems from 2031, subject to defined exceptions [Q28].

These timelines are also relevant for Swiss companies operating internationally. Swiss firms serving customers abroad, participating in international supply chains, providing technology to regulated or critical infrastructures, or operating subsidiaries in the EU or US may become subject to these requirements directly or through customer, procurement and contractual requirements. Consequently, quantum readiness is not only a future Swiss regulatory issue, but increasingly a market-access and international competitiveness requirement.

Finally, as the inquiry into Crypto AG several years ago has shown, the control over cryptographic device security is a sensitive issue. In view of the Goods Control Act (GCA) and its Ordinance (also covering dual-use goods), the export of certain cryptographic goods, which are classified as dual-use goods, requires a license; this could become relevant for Swiss providers of quantum-safe cryptography that export their products.

7 Key Areas for Action

(iii) Timeline Dimension & Phased Migration Roadmap

Recent research demonstrates that the resources required to break 256-bit elliptic curve cryptography are significantly smaller than previously estimated. Expert opinion on the timing of a CRQC still varies widely [Q4]. This Paper uses 2029–2033 as its planning horizon, i.e. the period from which a CRQC can no longer be ruled out.[4]

Because migrating decentralized systems is uniquely complex, the transition must follow a structured, multi-year roadmap. It is important to note that the increased focus on PQC and the advances in cryptanalysis methods (e.g. machine-assisted cryptanalysis) result in an unprecedented rate of change in the fields of cybersecurity and applied cryptography. Specifically, new attacks are being discovered much more quickly, even on cryptographic algorithms that were considered promising PQC candidates, as the breaks of SIKE and Rainbow in 2022 showed [Q29], [Q30]. Even long-studied schemes such as Classic McEliece remain the subject of active cryptanalysis[5].

Combined with rapid advances on both the engineering and theoretical sides of Quantum Computing development, it is prudent to expect that the PQC migration is not going to be a one-time effort and that even before CRQCs become available, some of the new PQC algorithms might be broken or weakened significantly by classical attacks. Our recommendation, therefore, is to establish a continuous program that monitors the latest developments, assesses risks and targets achieving cryptographic agility, that is an ability to continuously migrate to safer cryptographic methods and systems.

Even though the blockchain and digital asset ecosystem faces challenges that affect all stakeholders, it is important to differentiate between possible actions and their outcomes for the two distinct groups: 1) Protocol Ecosystems and Key Management Technology providers (Layers A and B) and 2) extended ecosystem players such as Digital Asset Custodians and Traditional Financial Institutions (Layers C and D). This is due to a very specific dependency between these two groups and the nature of their respective legal responsibilities.

[4] Resource estimates (not timeline forecasts): see [Q1] and https://www.ionq.com/blog/the-first-full-stack-blueprint-for-breaking-256-bit-elliptic-curve-signatures

[5] As of the time of writing, it has not been broken. However, significant progress is being made e.g. https://eprint.iacr.org/2026/1630

We provide our recommendations as four interrelated roadmaps, one for each layer, followed by a common roadmap for all ecosystem players.

Layer	Actors	Core Dependency
A – Protocol Layer	Bitcoin, Ethereum, Solana, Cardano and other L1/L2 protocol teams	Must upgrade on-chain cryptographic rules — the most complex migration due to decentralized governance; all downstream layers depend on this
B – Key Management Technology	Taurus, Fireblocks, DFNS, Copper, Ledger, MetaMask	Build and operate key management infrastructure — direct cryptographic responsibility for PQC migration
C – Digital Asset Custodians	AMINA, Sygnum, InCore, Bitcoin Suisse, Swissquote, ZKB, Luzerner KB	Licensed institutions operating their own digital asset infrastructure — act as primary crypto gateway; PQC exposure depends directly on their technology providers
D – Traditional Financial Institutions	Julius Bär, Vontobel, PostFinance, Maerki Baumann, Kantonalbanken and others without own DLT infrastructure	Carry full client-facing regulatory and fiduciary liability despite being furthest from the cryptographic layer

Roadmap A – Protocol Providers and Ecosystems - *Bitcoin, Ethereum, Solana, Cardano, and other L1/L2 protocols*

Phase	Timeframe	Focus & Core Actions
Phase 1: Provide clear guidance on risks and vulnerabilities; establish mitigation roadmap	Immediate	Clearly document which technical vulnerabilities exist where and how they affect various players of the ecosystem/protocol. Establish a dedicated task force that drives the resolution forward and regularly updates the progress. Emphasize consensus building and aim for transparency in decision making, while focusing on achieving a specific deadline. If a fork is unavoidable, provide clear communication.

Phase 2: start mitigation project(s) and provide progress updates	By 2027	Clearly document the chosen approach, including the selected PQC signature scheme and transition mechanism. Create dedicated channels to showcase and communicate progress. Provide regular progress updates and emphasize test environments for evaluations, feedback and interoperability. If multiple alternatives are developed, clearly communicate how and when the final choice is to be made.
Phase 3: signal ecosystem consensus and migration start	2028–2029	Communicate the target (agreed) technical changes and focus on achieving production readiness. Update timelines and communicate progress. Establish, track and communicate the start of the migration milestone.
Phase 4: finish migration	2029 onwards (multi-year)	Start the migration, track progress and communicate the results. Migrating user funds will take several years after activation (BIP-361, for example, foresees around five years until legacy signatures are restricted [Q19]), so activation should be targeted for 2029 at the latest. Coins whose public keys are already exposed remain at risk until legacy signatures are restricted, i.e. potentially beyond the 2029–2033 planning horizon; this residual risk should be communicated explicitly. Clearly document and provide guidance on what happens to the assets, accounts, etc. for the ecosystem players, including the end-users.

Roadmap B - Key Management Technology - Taurus, Fireblocks, DFNS, Copper, Ledger, MetaMask and others

Phase	Timeframe	Focus & Core Actions
Phase 1: **Assess and communicate PQC readiness**	Immediate	Conduct internal audit of all cryptographic dependencies across products and infrastructure. Publish a clear PQC roadmap for institutional clients. Engage with Protocol Layer teams to monitor upgrade timelines.

Phase 2: **Develop and test PQC-capable products**	By 2027	For on-chain signing: monitor protocol-level PQC decisions and prepare infrastructure to support the chosen standard once finalized. For internal systems and client-facing infrastructure: follow the Common PQC Migration Roadmap — initiate PQC-capable signing for APIs, HSMs, and communication channels independently of protocol timelines. Provide test environments for institutional clients to evaluate PQC readiness.
Phase 3: **Release PQC-ready products and support client migration**	2028–2029	Release production-ready PQC versions of custody and key management products. Actively support Digital Asset Custodian clients through migration — tooling, documentation, and dedicated migration support.
Phase 4: **Full PQC migration**	After protocol migration	Deprecate classical signing support for internal systems and, for on-chain signing, once the respective protocols support PQC signatures. Ensure all clients have migrated. Communicate completion to regulators and institutional clients.

Roadmap C - Digital Asset Custodians - AMINA, Sygnum, InCore, Bitcoin Suisse, Swissquote, ZKB, Luzerner KB and others

Phase	Timeframe	Focus & Core Actions
Phase 1: **Inventory & Crypto-Agility**	Immediate	Conduct full-stack cryptographic audits (wallets, HSMs, bridges). Design wallet and custody architecture for crypto-agility and track protocol proposals that enable it (e.g., the draft Ethereum proposal EIP-8141 on account abstraction [Q31]). Demand formal PQC roadmap and annual attestation from all technology providers. Include audit rights in provider contracts.
Phase 2: **Hybrid Cryptography**	By 2027	Prepare hybrid signing (combining classical schemes like Ed25519 with PQC like ML-DSA/FN-DSA) in internal systems now and on-chain wherever the protocol supports it, to mitigate mathematical risks of newer PQC algorithms. Upgrade HSM firmware, or initiate hardware replacement for older HSM generations.
Phase 3: Signing Infrastructure & User Migration	2028–2029	Upgrade signing infrastructure. Execute coordinated end-user and institutional asset migration campaigns to PQC-native wallets, where supported by the protocol, prior to Q-Day.

Phase 4: **Full migration & regulatory confirmation**	After protocol migration	Complete migration of all client assets and internal infrastructure. Document PQC compliance and report to FINMA where supervised.

Roadmap D - Traditional Financial Institutions - Julius Bär, Vontobel, PostFinance, Maerki Baumann, Kantonalbanken and others without own Digital Asset Custody infrastructure

Phase	Timeframe	Focus & Core Actions
Phase 1: **Map exposure & demand accountability**	Immediate	Map all digital asset exposures and identify Digital Asset Custodian providers. Request formal PQC roadmaps and annual attestation from all service providers. Include PQC-readiness as a vendor due diligence criterion in line with FINMA Guidance 05/2026.
Phase 2: **Contractual & governance preparation**	By 2027	Incorporate PQC migration milestones into service agreements with Digital Asset Custodian providers. Brief boards and risk committees – quantum vendor risk is a fiduciary issue, not an IT issue.
Phase 3: **Monitor & validate provider migration**	2028–2029	Actively track migration progress of Digital Asset Custodian providers. Validate PQC compliance claims via independent review. Prepare client communication strategy.
Phase 4: **Confirm full chain compliance**	By 2030; on-chain after protocol migration	Confirm PQC readiness across the full provider chain. Document and report compliance to FINMA.

Common PQC migration recommendations for all ecosystem players

Besides the specific risks and action items related to the functioning of the protocols and related technical infrastructure (e.g. HSMs, Wallets, etc.), the overall security posture of any organization also depends on the timely PQC migration for all business systems.

We propose the following roadmap to ensure that organizations approach their PQC related risks holistically.

Phase	Timeframe	Focus & Core Actions
Phase 1: **Inventory & Crypto-Agility**	Immediate	Conduct a survey of all IT systems and identify applications and hardware that is potentially vulnerable to QC attacks (i.e. create Cryptographic Bill Of Materials - CBOM). Ensure that disaster recovery relevant systems, e.g. backup storage are also included in the survey. Prioritize the results by the criticality of the business processes the systems support and whether they are exposed to the Internet. Systems exposed to HNDL (harvest now, decrypt later), even internally, should be addressed first. Ensure that all external endpoints (web, APIs, SSH, etc.) use PQC key exchange now. For HTTP endpoints ensure TLS 1.3 only and hybrid PQC key exchange algorithms are used by default. Demand formal PQC roadmap and annual attestation from all technology providers. Include audit rights in provider contracts. Ensure that vendors and internal developers are planning for cryptographic agility.
Phase 2: **PQC migration starts and extended readiness**	By 2027	Deploy dual-signing mechanisms (combining classical schemes like Ed25519 with PQC like ML-DSA/FN-DSA) on business artifacts to mitigate mathematical risks of newer PQC algorithms. Initiate hardware replacements for devices that don't support software upgrades (e.g. HSMs, network devices, etc). Monitor development and deployment status of the new PQC-first version of the Web PKI Certificates (e.g. Merkle Tree Certificates) and plan for automation required to roll them out when the standard is ready. For the internal systems, ensure that the private Certificate Authorities (CA) are ready to support PQC signatures. Continuously update CBOM and the migration roadmap. Identify systems and hardware that have to be phased out due to lack of an upgrade path.
Phase 3: **Finalize migration**	2028–2029	Finalize migration of the business-critical systems. Replace the hardware and systems that can't be upgraded. Monitor PQC guidance and best practices published by IETF, NIST, ENISA and ETSI, etc. Revisit cryptographic agility plans.
Phase 4: **Full migration & regulatory confirmation**	By 2030	Document PQC compliance and, where supervised by FINMA, report to FINMA. Continuously update CBOM and the migration roadmap.

(iv) Role-Specific Risk Profiles

Risk exposure and operational imperatives vary significantly across the different actor layers:

- **Layer A – Protocol Teams & Foundations:** Bear the technical burden of PQC upgrades without centralized authority to enforce adoption — fork risk and coordination failure are their primary exposures.
- **Layer B – Key Management Technology Providers:** Carry direct cryptographic responsibility — delayed PQC readiness creates liability toward institutional clients.
- **Layer C – Digital Asset Custodians:** Face direct regulatory and fiduciary liability. Long HSM procurement and certification cycles mean action must start immediately.
- **Layer D – Traditional Financial Institutions:** Furthest from the cryptographic layer but fully exposed through their Layer C providers — vendor dependency is their primary and most overlooked risk.
- **Retail Users:** Most vulnerable due to information asymmetry — without proactive campaigns, inactive users risk total asset loss.

(v) Performance, Governance, and Geopolitics

- **Performance & Transaction Costs:** PQC signatures are roughly 40 to 70 times (ML-DSA) and more than 100 times (SLH-DSA) larger than classical 64-byte signatures [Q15], potentially increasing transaction fees significantly unless mitigation techniques (such as signature aggregation with *leanXMSS and leanVM,* or ZK-aggregation) are integrated.
- **Governance & Chain Splits:** Lack of consensus within decentralized communities during PQC upgrades introduces the severe risk of uncoordinated hard forks, creating split liquidity and operational chaos.
- **Geopolitical Asymmetry:** The quantum race is heavily funded by nation-states. A CRQC may be deployed without public disclosure, heightening risks for major financial hubs like Switzerland's Crypto Valley.

Transition to Strategic Recommendations

The interconnected nature of these risks demonstrates that isolated, individual efforts are insufficient. To establish Switzerland as a leading quantum-safe jurisdiction for digital assets (Objectives 4 & 5), swift and coordinated action is imperative.

The concrete initiatives led by the Swiss Blockchain Federation — centered on the establishment of the semi-annual **SBF Quantum Readiness Report** to provide global market transparency — are detailed in the following section.

8 Recommendations

8.1 For the Swiss Blockchain Federation (SBF) and its members

To position Switzerland globally as a pioneer in **quantum security for digital assets**, the SBF should take a proactive leadership and coordination role:

The "SBF Quantum Readiness Report" (Central Industry Monitor): The SBF establishes and maintains a structured, publicly accessible overview of all relevant blockchain protocol stacks:

- *How it works:* Blockchain organizations and development teams provide information to the SBF on their current progress towards quantum-safe migration, including the status of hybrid signatures, HSM compatibility, hash algorithms, and other relevant components.
- *Publication:* The SBF publishes a comprehensive report every six months.
- *Value:* Market participants, banks, and institutional investors can use the report to assess the technological risks associated with individual blockchain stacks, and consequently the tokens and RWAs built on them, as well as whether their quantum-readiness roadmaps are progressing according to plan. **This would give Switzerland a leading role in establishing a transparent, industry-wide standard for assessing quantum risks in DLT ecosystems. To address the verification gap described in chapter 4, self-reported information should be complemented by independent review where possible.**

Awareness and Best Practices: The SBF establishes a dedicated task force to develop practical guidelines and playbooks for its members, particularly crypto custodians, exchanges, and wallet developers. The objective is to make **cryptographic agility a design standard** for every new project emerging from Crypto Valley.

Development of Recovery Standards: The SBF should initiate industry-wide standards for dealing with **"orphaned tokens"**, meaning digital assets belonging to users who fail to migrate to new PQC-secure wallets within the required migration period.

8.2 For Financial Infrastructure Providers, Regulators, and Research Institutions

Crypto Custodians and Swiss Banks

Institutions must continuously assess their IT security frameworks for quantum resilience. This applies particularly to **Hardware Security Modules (HSMs)**. Upgrading to PQC-capable firmware, or replacing older HSM generations, is essential so that signing keys can move to PQC schemes once protocols support them. **"Harvest now, decrypt later"** is relevant for the encrypted channels, backups and client data around these systems, not for the signing keys inside the HSM. Institutions using Multi-Party Computation (MPC) for custody are equally affected (see chapter 4): their signature schemes and, depending on the protocol, some building blocks are quantum-vulnerable, so a careful assessment and migration is required.

Competent Authorities, including FINMA

Given the principles-based approach of Swiss supervisory law, there is currently no compelling need for rigid new regulation. However, supervisory authorities should integrate the findings of the proposed **SBF Quantum Readiness Report** into their regular industry dialogue to continuously assess the **quantum readiness and risk management capabilities** of supervised institutions.

Universities and Technology Partners

As quantum-safe signatures are significantly larger, leading Swiss research institutions such as **ETH Zurich**, **EPFL**, and other Swiss universities should focus on ZK-STARKs, signature aggregation approaches such as Ethereum's leanVM and leanXMSS, and efficient hybrid cryptographic systems. Only if transaction costs, including gas fees, remain economically viable despite the introduction of PQC can the Swiss financial sector continue to fully benefit from blockchain technology.

9 Sources

[Q1] R. Babbush et al. (Google Quantum AI), «Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations», arXiv:2603.28846, March 2026.

[Q2] M. Cain et al., «Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits», arXiv:2603.28627, 2026.

[Q3] Google: "Google's timeline for PQC migration", 25 March 2026; Microsoft Quantum Safe Program update, 30 June 2026 (critical products and services by 2029); Cloudflare PQC roadmap 2029.

[Q4] M. Mosca, M. Piani, «Quantum Threat Timeline Report 2025», Global Risk Institute, 2026.

[Q5] Swiss Quantum Commission, «Swiss Quantum Strategy», SCNAT, 2026.

[Q6] SERI, «Swiss Quantum Initiative», sbfi.admin.ch, accessed October 2026.

[Q7] Fondation Inartis, «The era of Quantum» incl. the map «Quantum in Switzerland», The New Now – Technologist No. 24, special edition produced in partnership with SATW, February 2024, ISBN 978-2-9701660-9-2, https://republic-of-innovation.ch/wordpress/wp-content/uploads/2024/02/Quantum_en-web-2.pdf.

[Q8] IonQ, «IonQ Completes Acquisition of ID Quantique», press release, May 2025.

[Q9] ZuriQ, seed financing round of USD 25.5 million, July 2026.

[Q10] Quantum Design, acquisition of Qnami AG, June 2026.

[Q11] SATW, «Kick-off for the Swiss Quantum Industry Network SQIN», news, October 2024.

[Q12] Swiss Bankers Association, «Quantum Computing in Banking: How it works, areas of application, and recommendations for Swiss banks», expert report, November 2024.

[Q13] FINMA, Guidance 05/2026 (quantum risk management), 9 July 2026.

[Q14] D. Aggarwal et al., «Quantum attacks on Bitcoin, and how to protect against them», arXiv:1710.10377, 2017.

[Q15] NIST, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), August 2024.

[Q16] A. Fenton, «SHRINCS BIP is published: quantum-secure Bitcoin comes with a catch», Cointelegraph, 27 August 2026.

[Q17] W. A. Vitale, «Migration Is the Hard Part», Bitcoin Suisse Industry Blog, 16 July 2026.

[Q18] S. D. Lerner, «The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius» (“Patoshi” pattern analysis), Bitslog blog, April 2013.

[Q19] Bitcoin Improvement Proposals BIP-360 (P2MR, February 2026) and BIP-361 (assigned February 2026, merged May 2026).

[Q20] M. Ivezic, «Applied Quantum PQC Migration Framework», Applied Quantum / PostQuantum.com, April 2026.

[Q21] Entrust, «Entrust nShield HSMs Post Quantum Cryptography Algorithms Achieve Validation from the NIST Cryptographic Algorithm Validation Program» (nShield 5

firmware v13.8.0 with ML-DSA, ML-KEM and SLH-DSA), press release, 10 September 2025.

[Q22] M. Mosca, «Cybersecurity in an era with quantum computers: will we be ready?», IACR ePrint 2015/1075, 2015.

[Q23] C. Gidney, M. Ekerå, «How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits», Quantum 5, 433, 2021.

[Q24] C. Gidney, «How to factor 2048 bit RSA integers with less than a million noisy qubits», arXiv:2505.15917, 2025.

[Q25] D. Litinski, «How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates», arXiv:2306.08585, 2023.

[Q26] NIST, IR 8547 (Initial Public Draft), «Transition to Post-Quantum Cryptography Standards», November 2024.

[Q27] NIS Cooperation Group, «A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography», June 2025.

[Q28] NSA, «Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)», 2022, with subsequent FAQ updates.

[Q29] W. Castryck, T. Decru, «An efficient key recovery attack on SIDH», IACR ePrint 2022/975, 2022.

[Q30] W. Beullens, «Breaking Rainbow Takes a Weekend on a Laptop», IACR ePrint 2022/214, 2022.

[Q31] Ethereum Improvement Proposal EIP-8141 (draft), eips.ethereum.org.