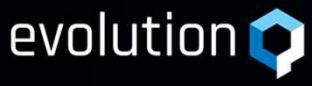
Cryptographic Risk Management in the Quantum Era: Threats, Resilience, and Complexity

Michele Mosca,
Co-founder and Programme Chair,
ETSI-IQC Quantum-Safe Cryptography Conference



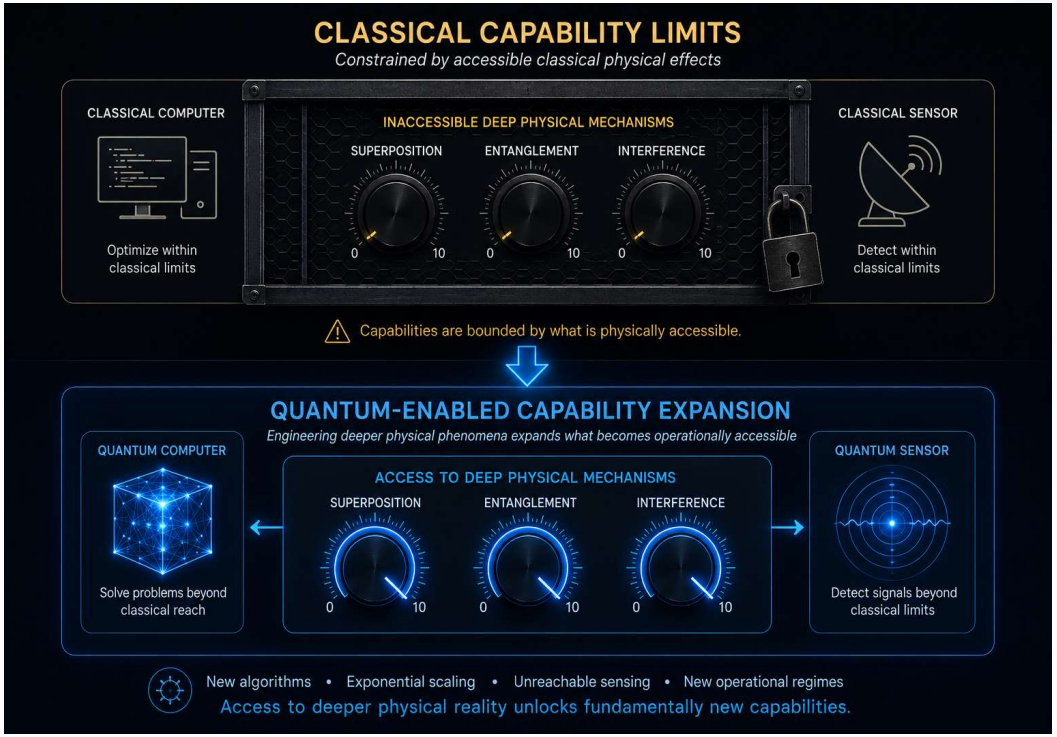
How Quantum is Different

Most technologies improve performance within the understood physical limits.

Quantum technologies may enable capabilities that are physically inaccessible to classical systems.

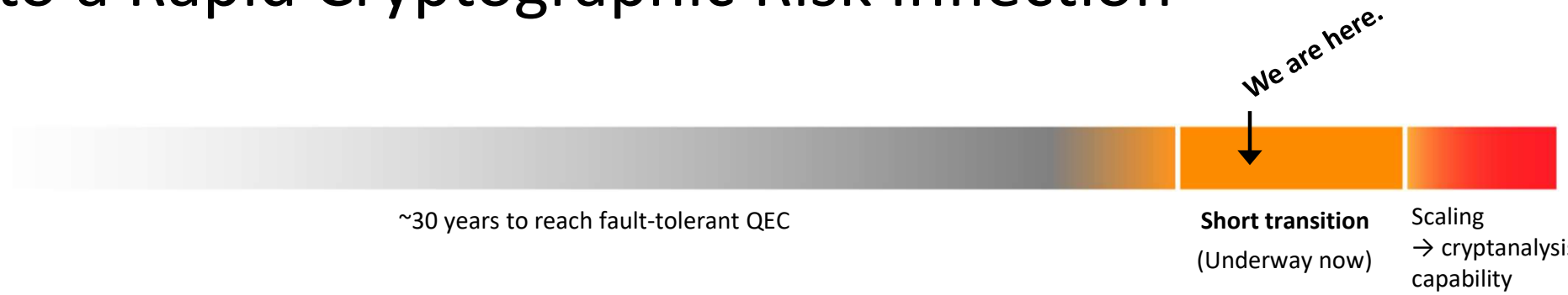
The impact distribution is unusually heavy-tailed:

- uncertain timing
- uncertain applications
- potentially extraordinary impact



© 2026 evolutionQ. All rights reserved.

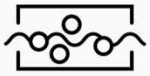
From 30 Years of Progress to a Rapid Cryptographic Risk Inflection



Multiple viable technology paths


Neutral atoms


Superconducting


Ion traps

Emerging: *Photonics, Silicon spins, Other spins*

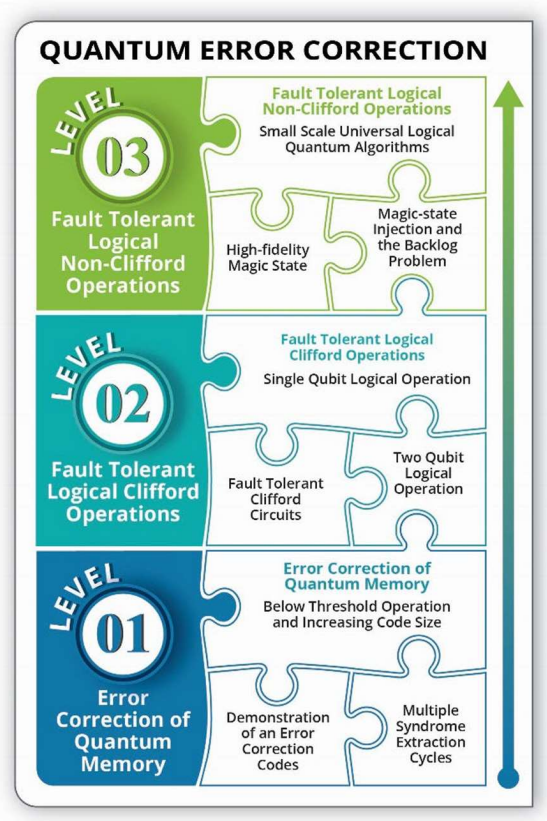
Non-linear risk:

Once fault tolerance is reached, relatively limited additional scaling can break today's cryptography.

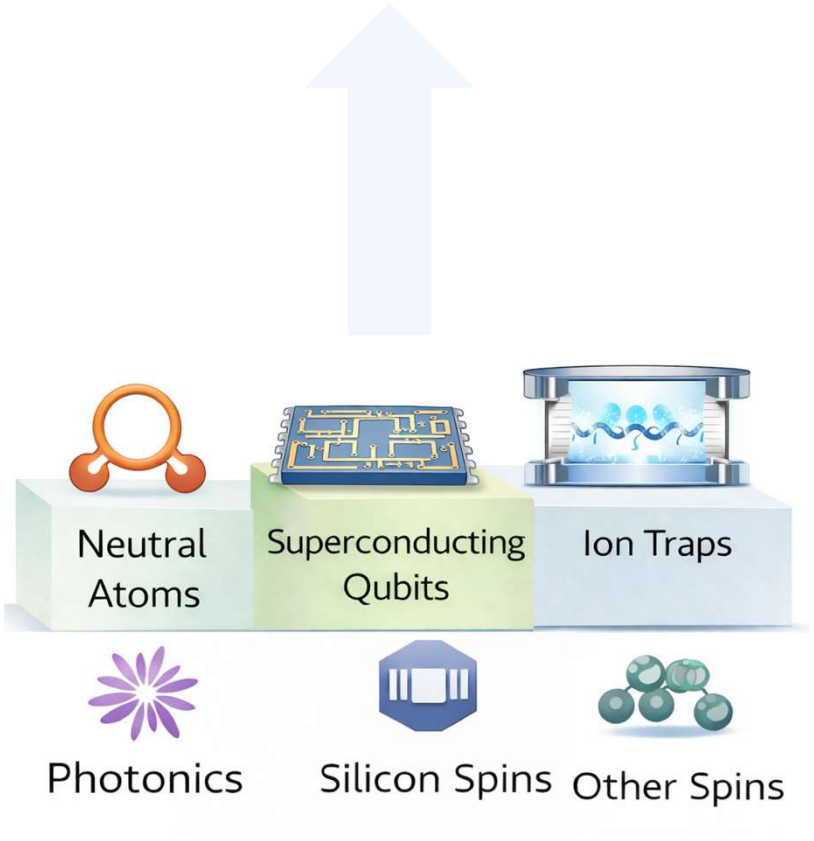
Implication: timelines are uncertain, and response time may be limited.

© 2026 evolutionQ. All rights reserved.

Meaningful Quantum Cryptanalysis Tracking

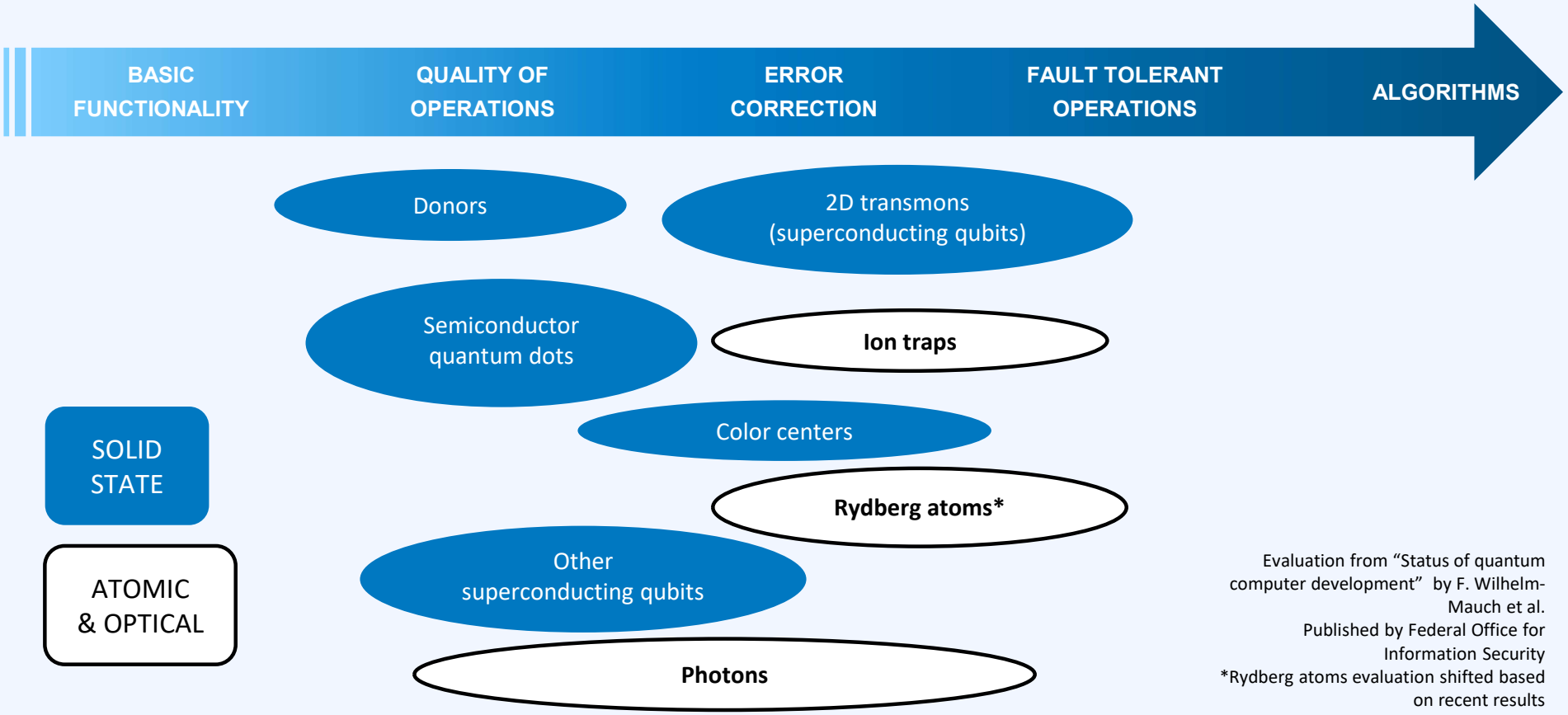


https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2025/why-quantum-computers-are-not-cracking-rsa-yet-final.pdf



© 2026 evolutionQ. All rights reserved.

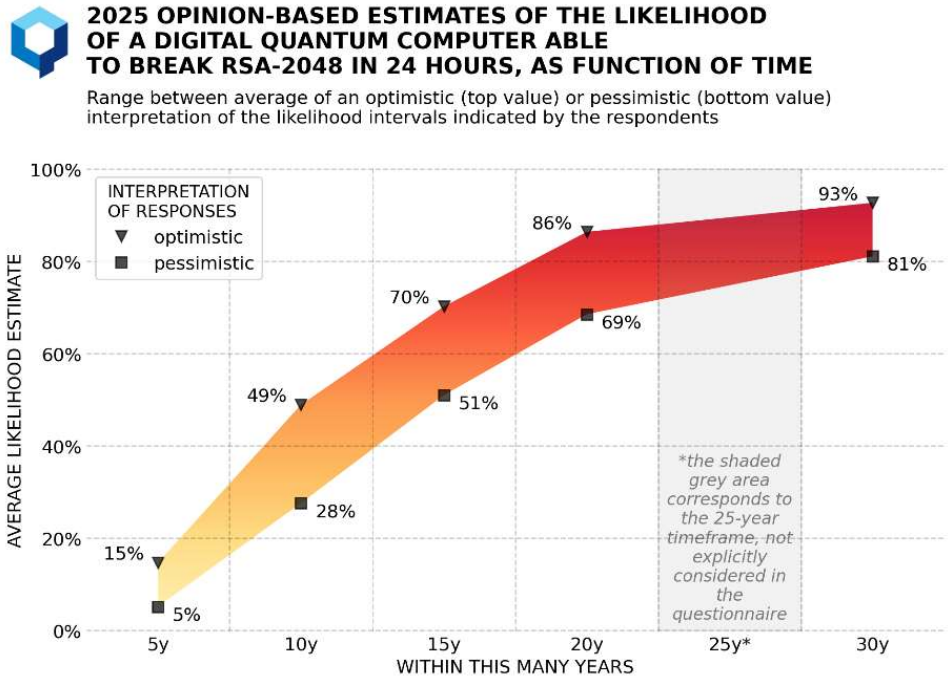
Status

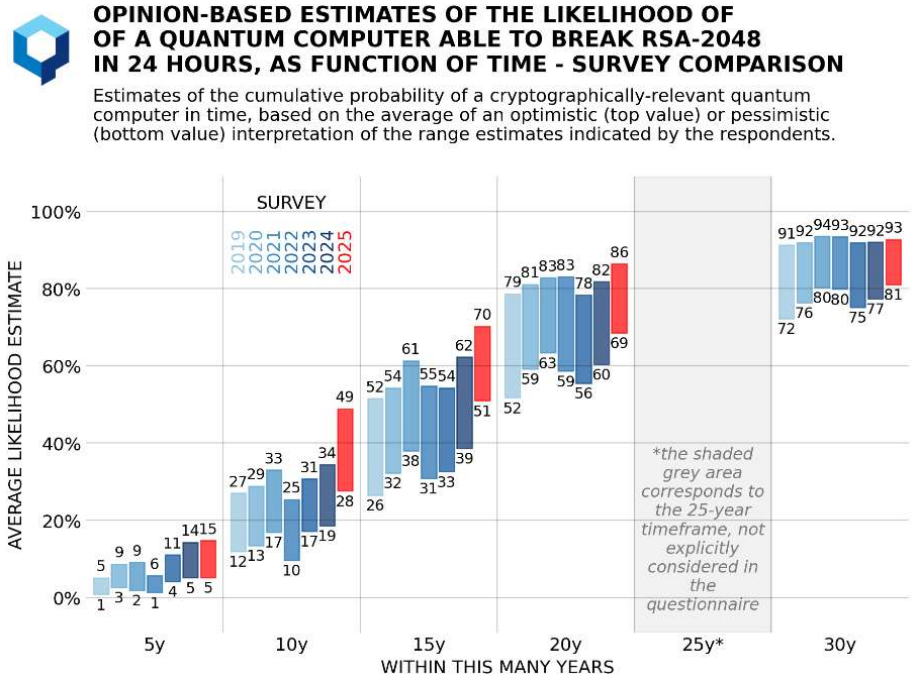


Evaluation from "Status of quantum computer development" by F. Wilhelm-Mauch et al.
Published by Federal Office for Information Security
*Rydberg atoms evaluation shifted based on recent results

© 2026 evolutionQ. All rights reserved.

Toward Quantum Factoring

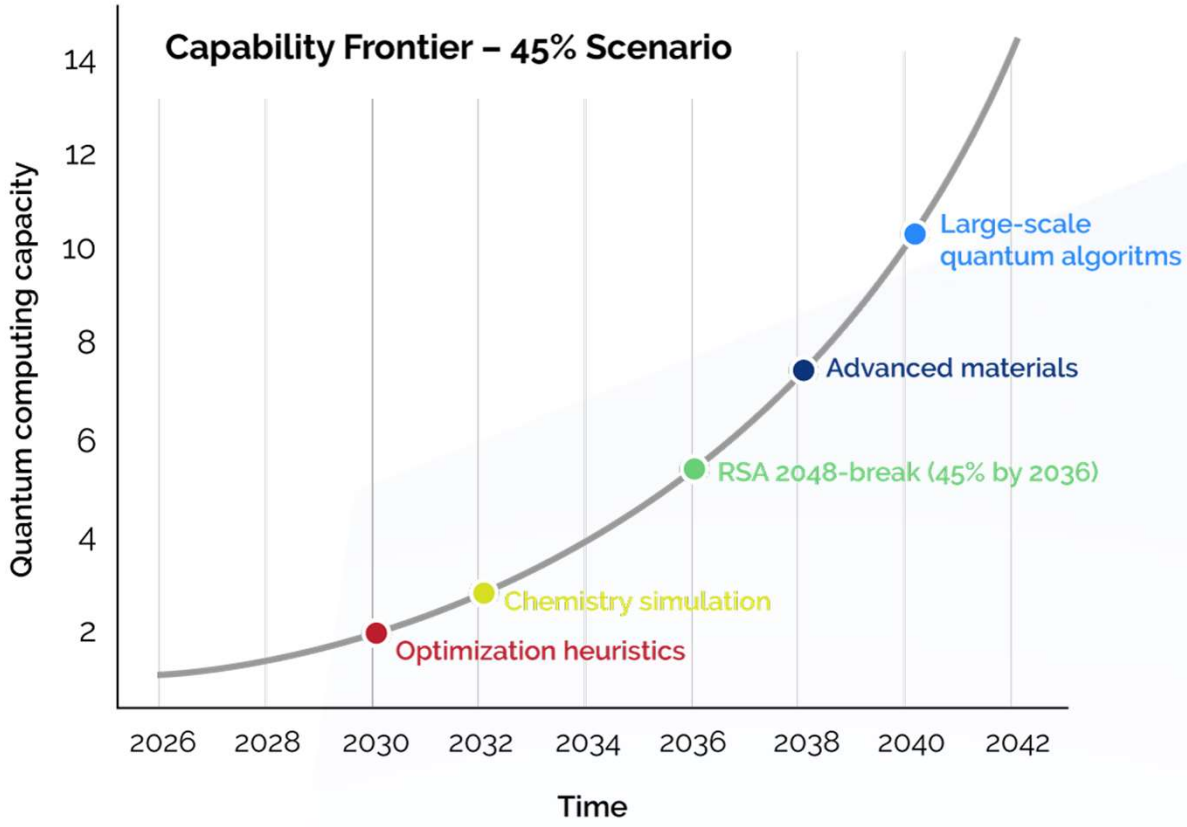




(2025 Quantum Threat Timeline, Global Risk Institute)

© 2026 evolutionQ. All rights reserved.

Other Quantum Computing Capabilities
(ILLUSTRATIVE DIAGRAM)



© 2026 evolutionQ. All rights reserved.

Quantum Computing Strategy for Enterprises

The goal is to reduce uncertainty about how quantum computing could change fundamental assumptions of your sector

Why this matters:

- The biggest risk is strategic surprise
- If quantum capabilities suddenly make certain problems easier to solve, competitors may move quickly
- Institutions that are unprepared could be disrupted

Biggest challenge:

- Finding the sweet spot between passive wait-and-see and innovation theatre

© 2026 evolutionQ. All rights reserved.

Potential Applications / Use cases

- Condensed matter physics
- Nuclear & particle physics
- Quantum chemistry
- Combinatorial & continuous optimization
- Finance
- Machine learning
- Cryptanalysis
- …

evolution

© 2026 evolutionQ. All rights reserved.

Likelihood of Early Quantum Computers

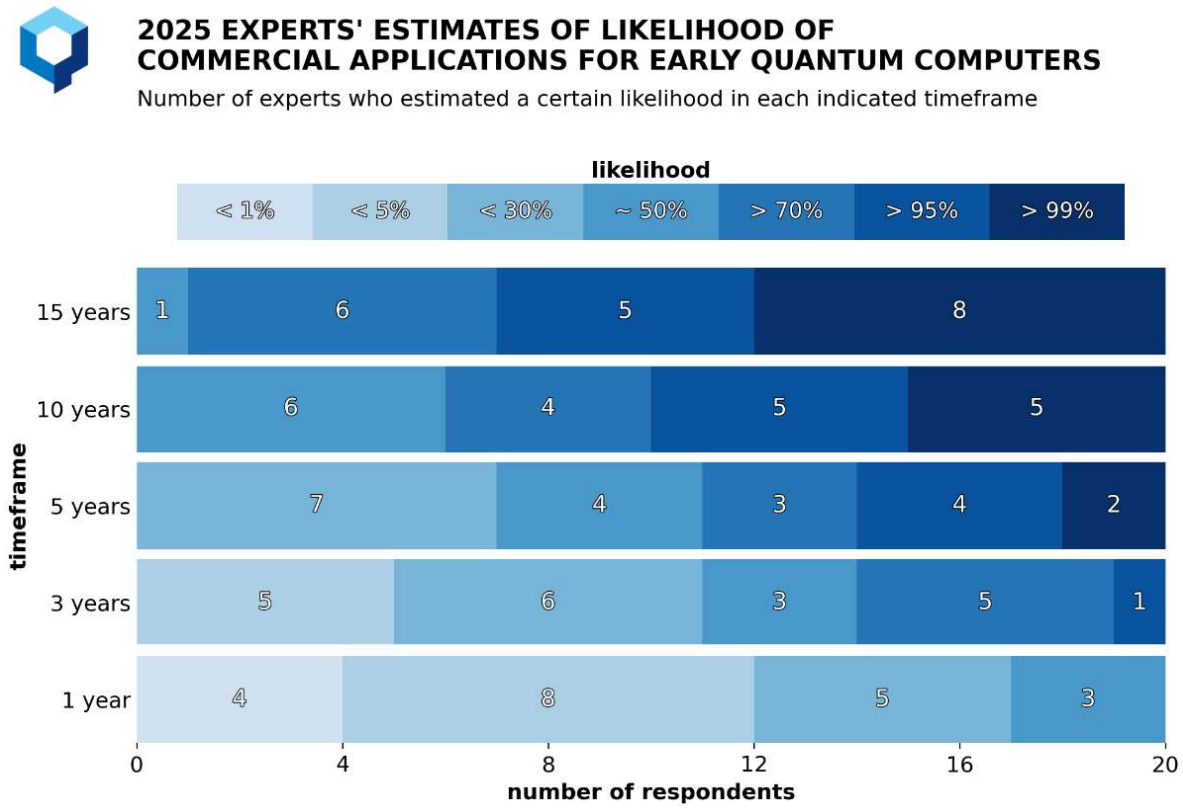


Figure 22 We asked the experts to indicate the likelihood for commercial applications of "early" quantum computers / quantum processors not yet powerful enough to be directly relevant from a cryptographic perspective. Not all experts expressed an opinion in this sense, but among those who did, more than half indicated a likelihood of about 50% or more within 5 years.

(2025 Quantum Threat Timeline, Global Risk Institute)

© 2026 evolutionQ. All rights reserved.

Two Parallel Tracks

Track 1:
The rocket is being built

- Quantum hardware continues improving globally

Track 2:
Mission planning

- Where should we fly the rocket? (financial use cases that could be transformed)
- How will we fly it? (algorithms, workflows, integration with existing systems)

© 2026 evolutionQ. All rights reserved.

Avoid the Wrong Focus

A common trap in emerging technologies:

- Chasing short-term 'wins' that are mostly demonstrations
- Creating theatre rather than lasting advantage

The real opportunity:

- Preparing now for the much larger capabilities that could arrive later
- Ensuring the enterprise is ready to mitigate risks and seize opportunities when the technology becomes mission-ready

© 2026 evolutionQ. All rights reserved.

Applications of Quantum Networks

Quantum computing

- Distributed quantum computation
- “Blind” quantum computation

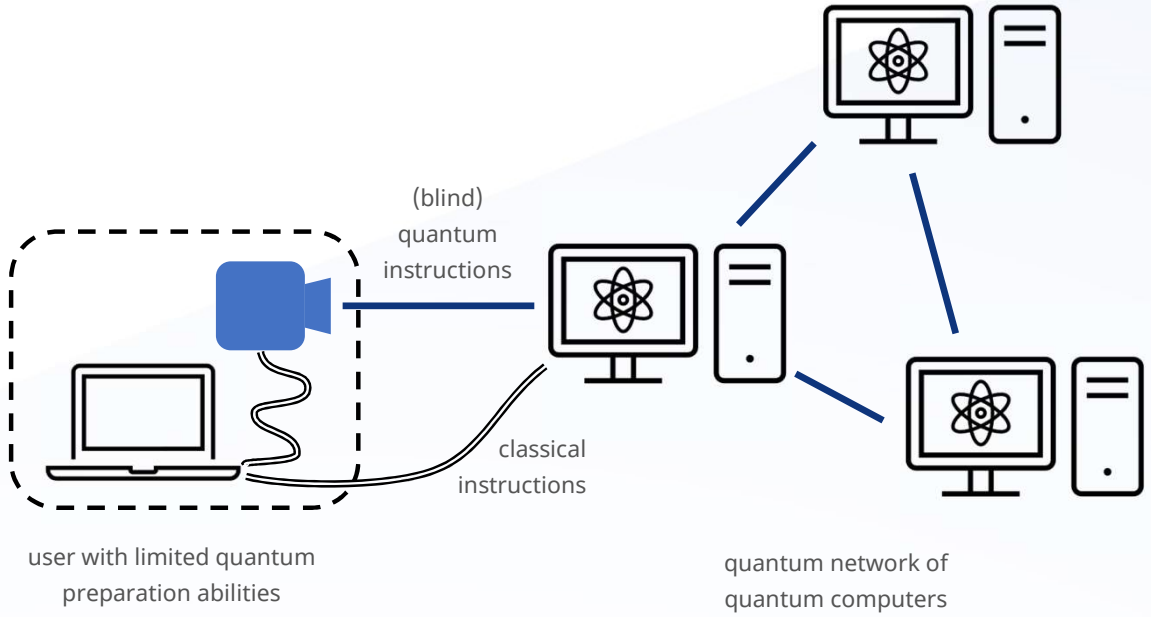
Fundamental science

- Tests of quantum properties

Quantum sensing

Quantum cryptography

...



© 2026 evolutionQ. All rights reserved.

Back to the “Quantum threat”…

Creating value by leveraging quantum, AI, etc, requires trustworthy foundations.

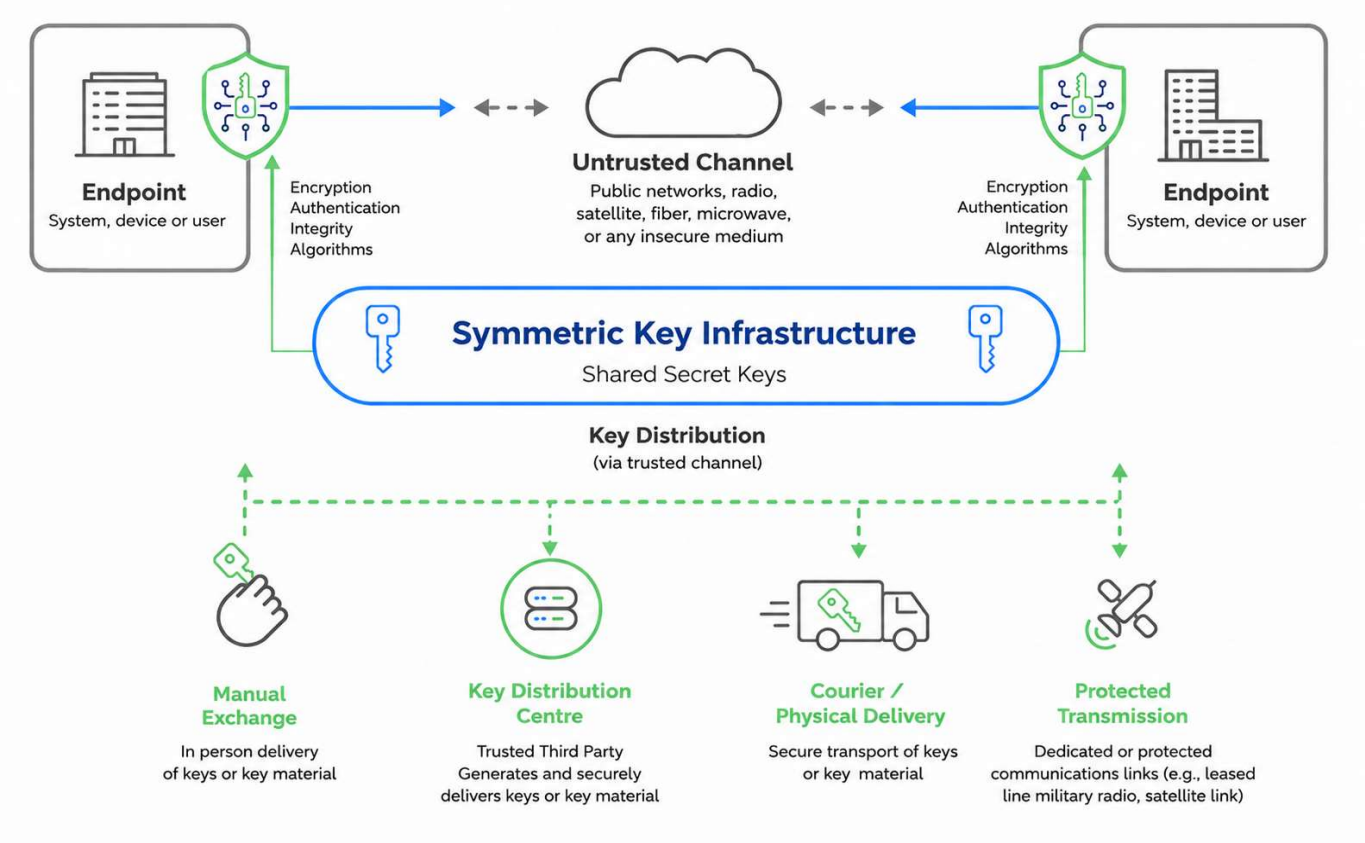
If they aren’t trustworthy then either:

- the capabilities aren’t trusted/used and less value is created
- if they are trusted nonetheless, we risk losing the value created

© 2026 evolutionQ. All rights reserved.

The Original Trust Architecture

SYMMETRIC KEYS AND OUT-OF-BAND TRUST



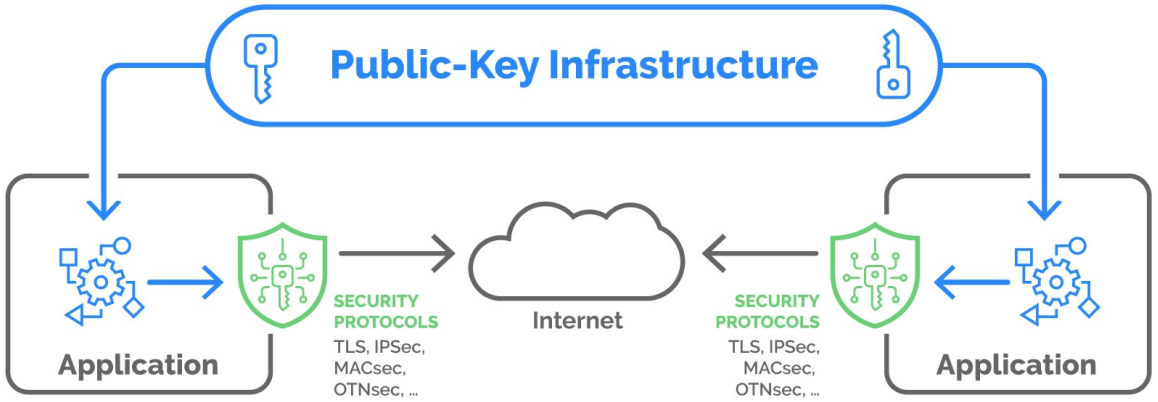
Principle:
Keys are established through trusted channels and then used to secure communications over untrusted channels.

This model has been used for centuries – from messengers and couriers to modern secure links.

© 2026 evolutionQ. All rights reserved.

The Public Key Revolution

AUTOMATING TRUST TRANSFER AND IN-BAND KEY EXCHANGE



- Scalable trust
- Open network security
- Global interoperability
- In-band key establishment
- Mathematical trust assumptions

© 2026 evolutionQ. All rights reserved.

Shared Assumptions Create Hyper-concentrated Risk

- We manage concentration risk across vendors and suppliers
- We vet and diversify platforms, providers, and infrastructure

But operational diversity does not eliminate shared trust dependencies

The same small set of cryptographic assumptions are re-used across identity, signatures, firmware validation, etc.

If one assumption breaks, that apparent diversity and trustworthiness collapses.

© 2026 evolutionQ. All rights reserved.

Cryptographic Fragility Amplifies Operational Risk

Modern operational resilience depends on:

- Trusted identity
- Software provenance
- Secure coordination
- Resilient communications

When shared assumptions fail:

- Operationally independent systems may fail together
- Recovery and coordination become harder
- Confidence in digital systems becomes harder to maintain

evolution

© 2026 evolutionQ. All rights reserved.

Luck isn’t a Strategy

- Shor’s algorithm revealed fragility. Adversaries also include AI and quantum enabled attackers
- Breakthrough timing is unpredictable

Must be ready for a true cryptographic zero-day

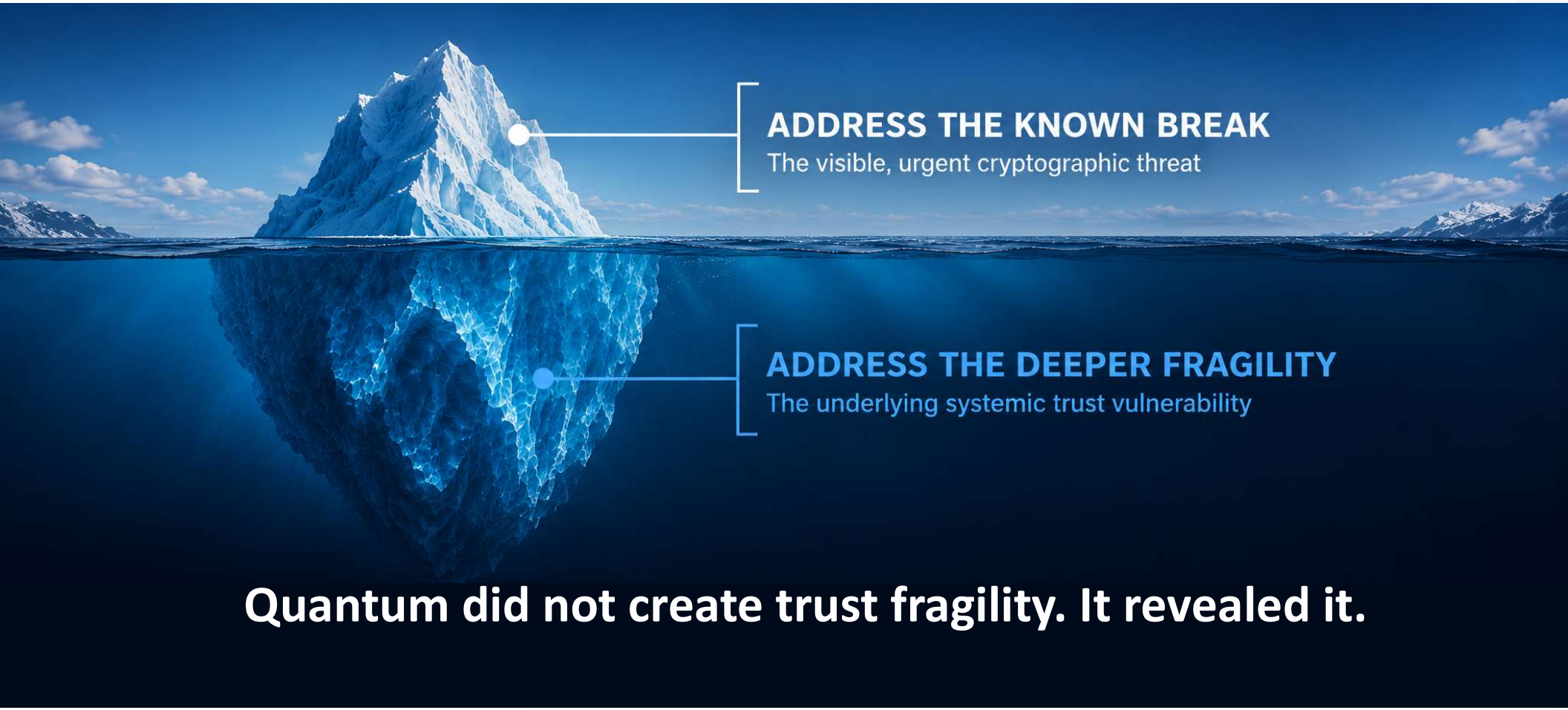
© 2026 evolutionQ. All rights reserved.

AI *Compresses* Response Time

- Faster exploitation
- Faster discovery
- Machine-speed cyber operations
- Reduced confidence in orderly adaptation
- Reduced defender reaction windows

© 2026 evolutionQ. All rights reserved.

Two Urgencies



Quantum did not create trust fragility. It revealed it.

Resilience Requires Surviving Failure —Not just Recovering from it

Agility enables adaptation
(effective when there is time and warning)

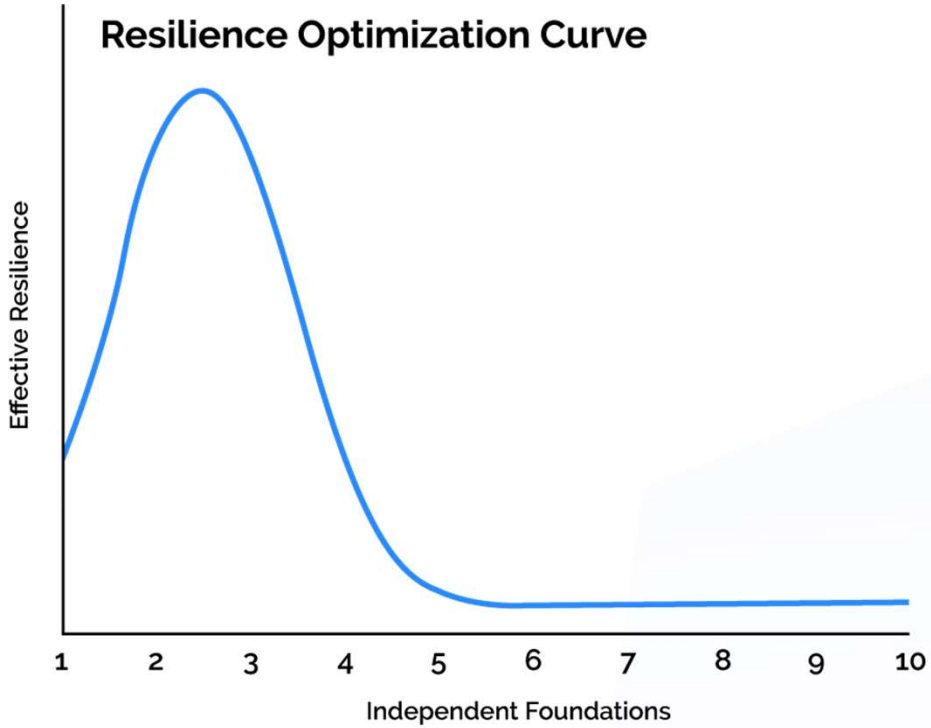
Defence-in-depth (e.g. MFA) enables survival
(for systems that cannot tolerate failure)

Diversity means safeguards don’t share the same underlying weaknesses

evolution

© 2026 evolutionQ. All rights reserved.

Resilience is an Optimization Problem



(only an illustration)

- One pillar → fragile
- Two or three (or so) independent pillars → resilience
- Too many foundations → complexity, cost, operational error

Resilience lies between concentration and chaos.

© 2026 evolutionQ. All rights reserved.

PQC is Necessary

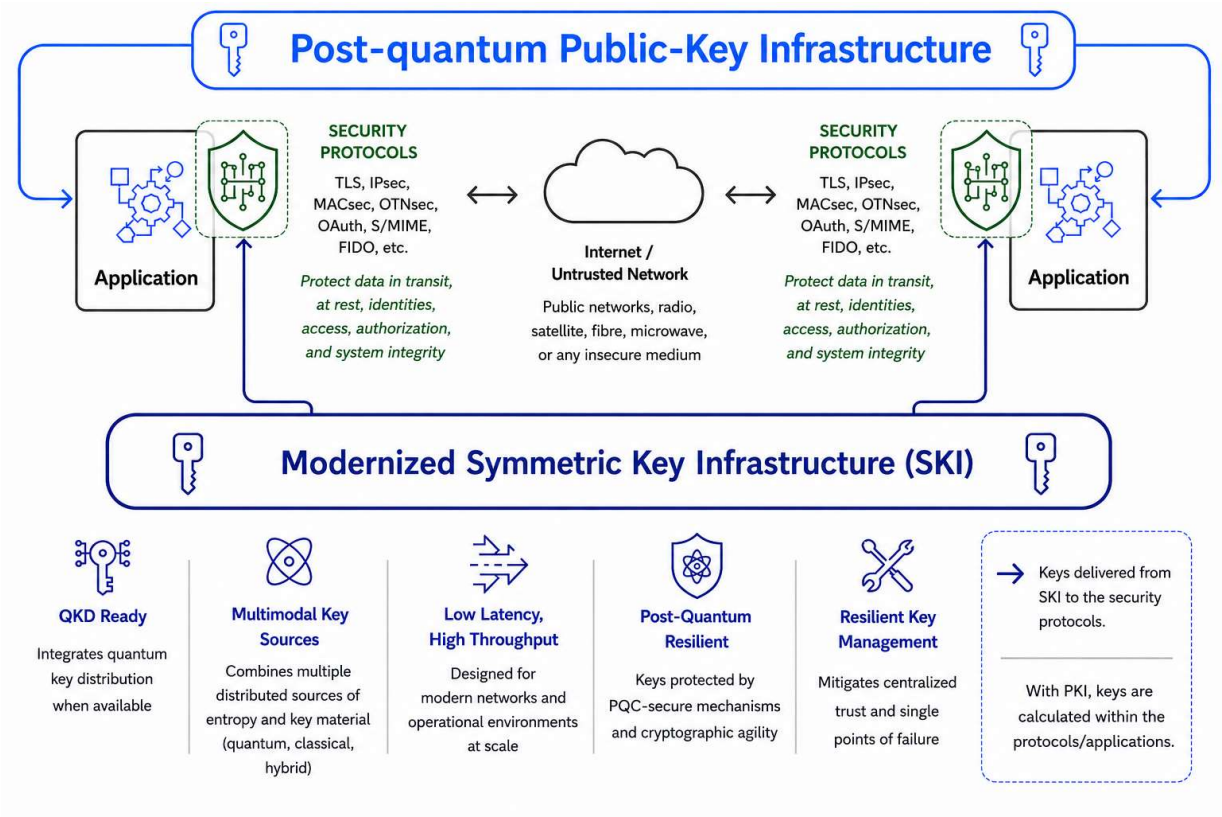
NIS CG	• Quantum Safe Roadmap by Dec. 31, 2026 • High-risk use cases transitioned by Dec. 31, 2030 • Medium-risk use cases transitioned by Dec. 31, 2035
BSI	• Recommendation to start migration now; • Protected against 'store now, decrypt later' attacks as soon as possible, latest by the end of 2030
NCSC	• By 2028- define migration goals • By 2031 – carry out highest priority PQC migration activities • By 2035 – complete migration to PQC
CCCS	• Quantum Safe Roadmap by April 30, 2026 • High priority systems migrated by 2031 • Medium priority systems migrated by 2036
NIST, NSA	• CNSA 2.0 guidelines: priority migrations by 2031, remainder 2035 • Deprecate RSA, ECC by 2030; Disallow by 2035

- Addresses known quantum attacks
- Leading cryptologic agencies mandate completion by 2030–2035

Timelines reflect realistic migration time — not guaranteed safety.

© 2026 evolutionQ. All rights reserved.

Enabling Cryptographic Resilience



Purpose:
Provide, protect, and manage high-assurance symmetric keys for today and tomorrow with **quantum readiness and multimodal key generation for long-term resilience.**

- **Reduced dependence on shared trust assumptions**
- **Operational resilience under cryptographic uncertainty**
- **Cryptographic agility and trust-layer evolution**

© 2026 evolutionQ. All rights reserved.

Why Symmetric Keys and Out-of-band Trust Matter

- Reduced dependence on shared assumptions
- Complementary trust foundations
- Quantum-resistant cryptographic primitives
- Flexible evolution of trust infrastructures
- Long-term resilience and agility

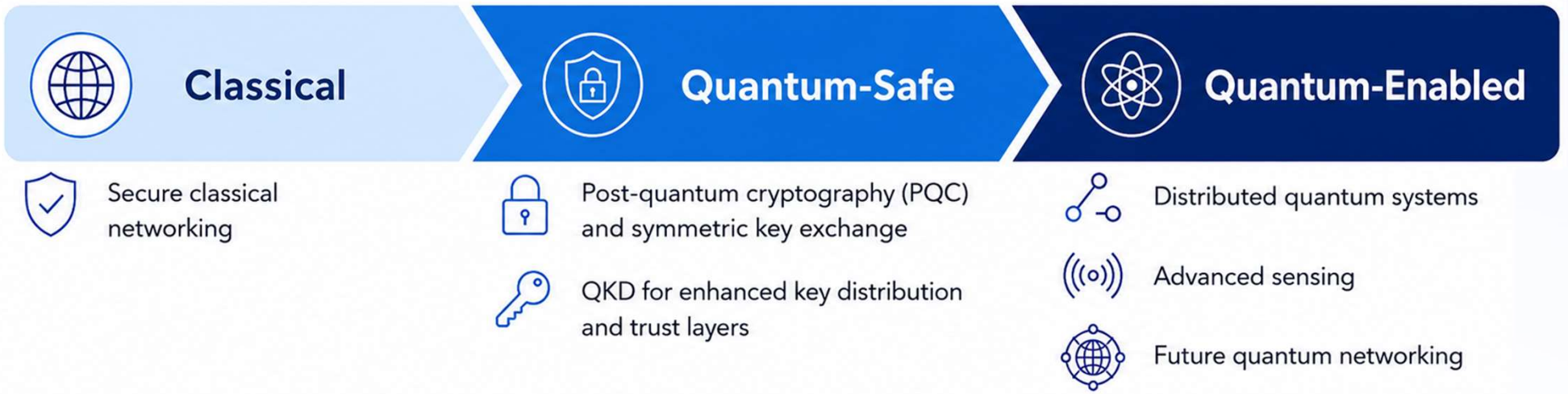
evolution

© 2026 evolutionQ. All rights reserved.

Networks as Trust Infrastructure

EVOLUTION, NOT DISRUPTION

- Trusted-node deployment today; reduced-trust architectures emerging
- Operational capability development today builds future trust infrastructure

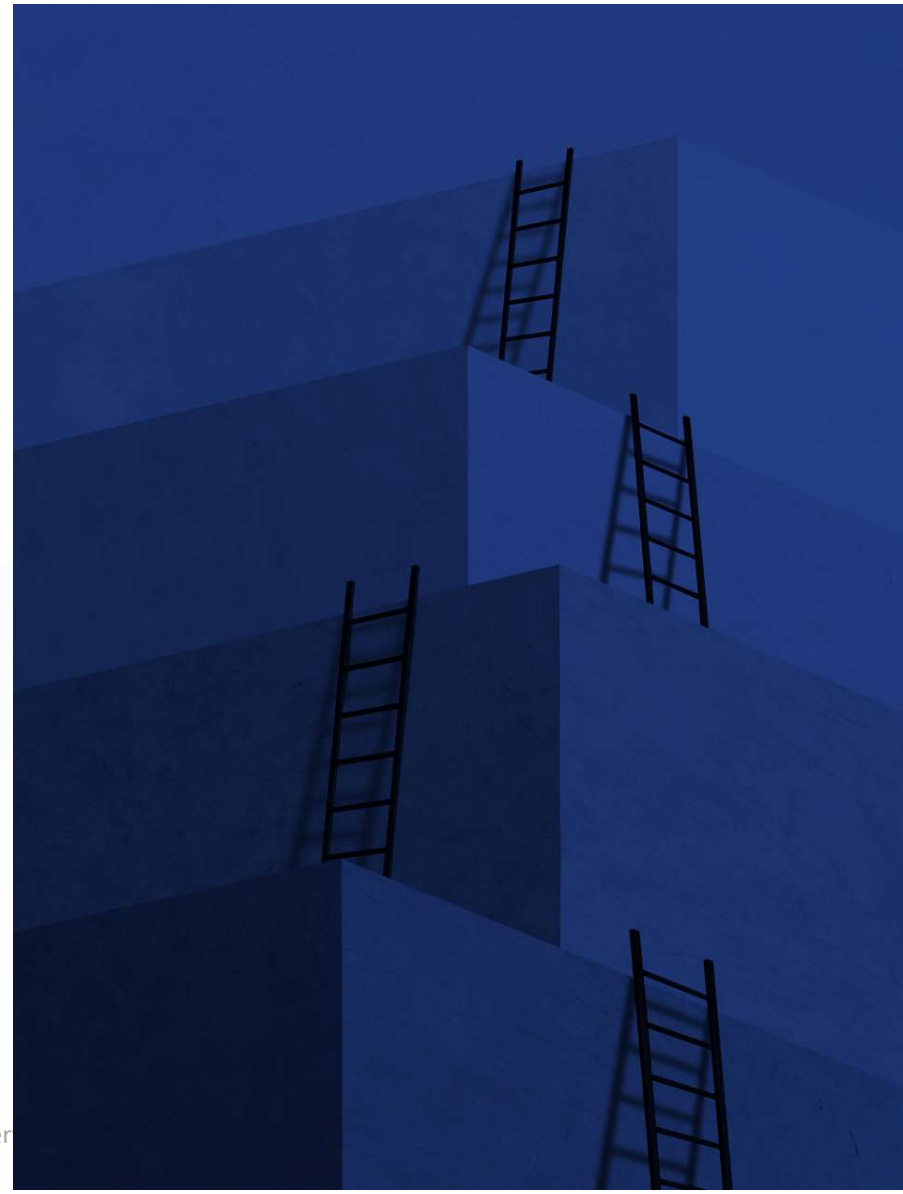


Networks increasingly participate in trust establishment and distribution

© 2026 evolutionQ. All rights reserved.

“What are the Biggest Obstacles?”

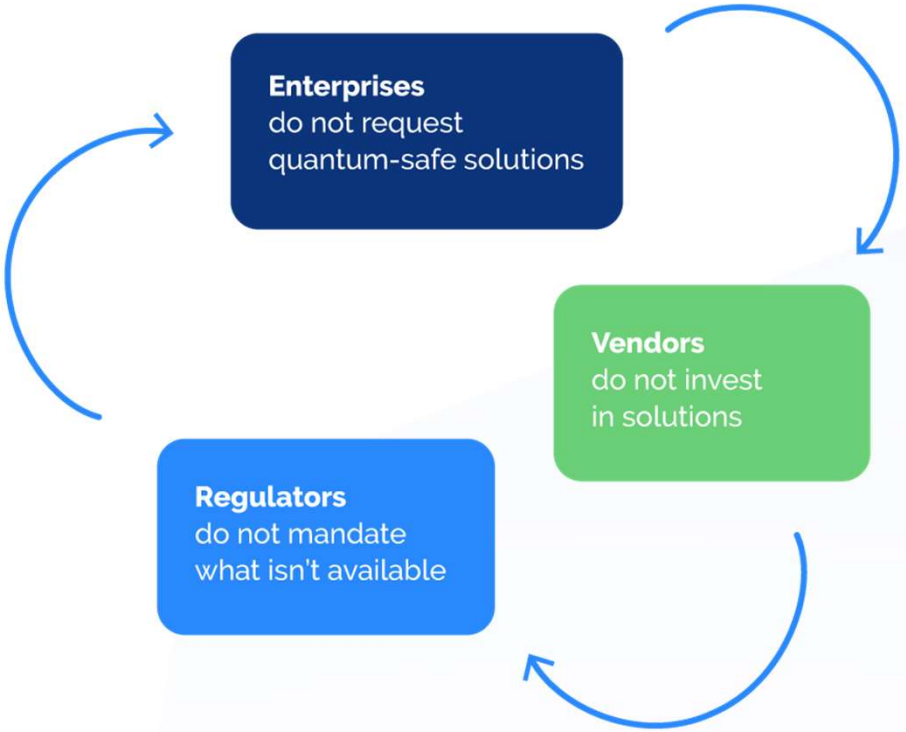
1) Not enough interest or willingness to be quantum-safe or cryptographically resilient
2) Significant gaps in solution space
3) Ecosystem coordination



evolution

© 2026 evolutionQ. All rights reser

Breaking the Quantum-resilience Coordination Trap



Vicious Cycle: No demand → No supply → No regulation → No demand → …

© 2026 evolutionQ. All rights reserved.

Do I Really Need to do This?

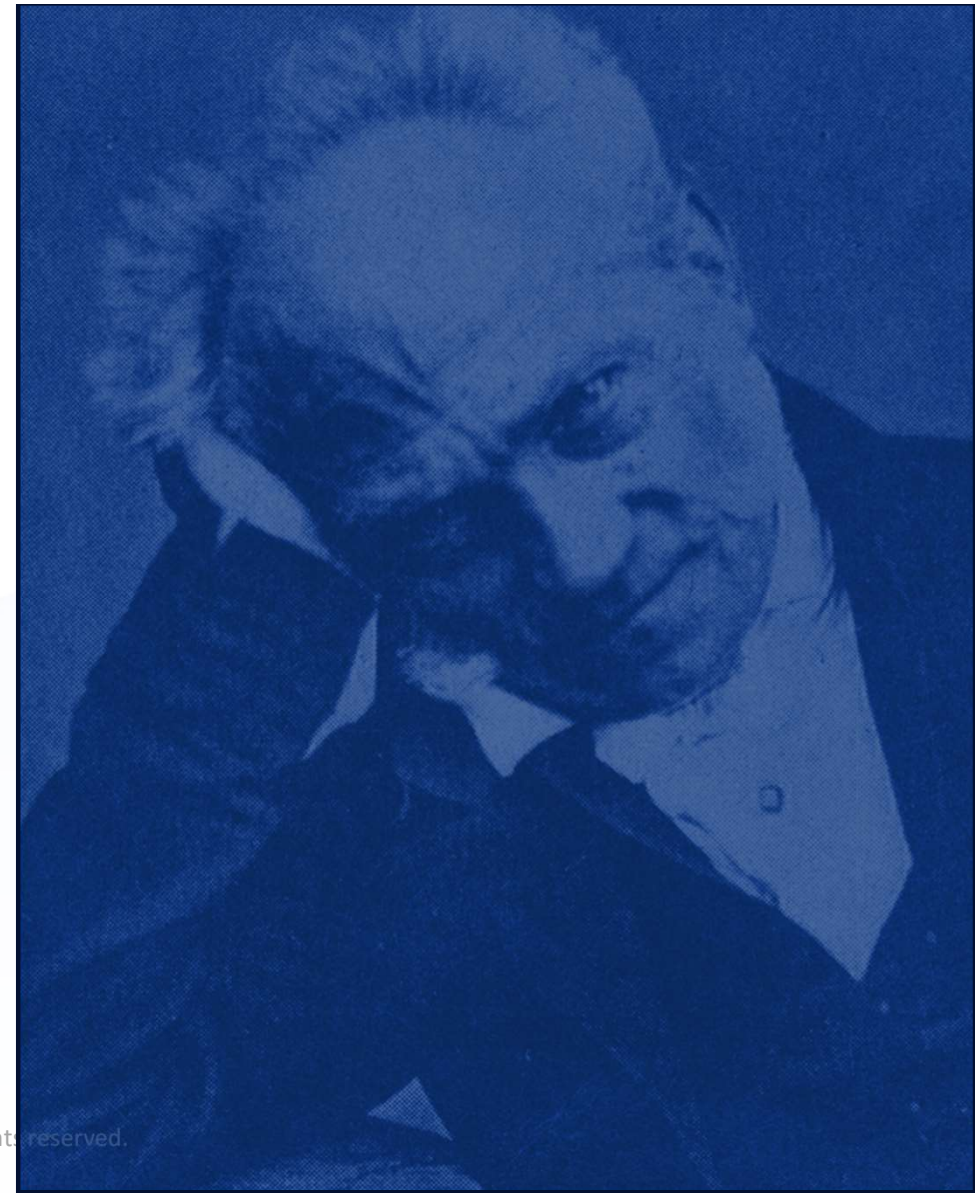
"All truth passes through three stages:

- First, it is ridiculed.
- Second, it is violently opposed.
- Third, it is accepted as being self-evident."

– Arthur Schopenhauer

"Fourth, those who ridiculed and opposed
ask why you're not ready yet."

– Manfred Lochter, BSI



evolution

© 2026 evolutionQ. All rights reserved.

Other Resources

Look for the latest reports by:

- Canadian Forum for Digital Infrastructure Resilience (CFDIR) Quantum Readiness Working Group (2026 edition to be out later this year)
- Quantum-Safe Financial Forum (QSFF)
- FS-ISAC
- CCCS, NCSC, etc.
- Dutch TNO
- World Economic Forum (WEF)
- Various ETSI groups

Thank you!

Michele Mosca
Co-founder and Professor,
Institute for Quantum Computing, University of Waterloo
CEO, evolutionQ Inc.
Geschäftsführer, evolutionQ GmbH