QUANTUM COMMUNICATION

QUANTUM RESISTANCE BY QKD AND PQC

WHY – TECHNICAL FACTS

QUANTUM COMPUTING WILL BREAK ENCRYPTION !

WHAT BREAKS



Public-key cryptography

RSA · Diffie-Hellman · ECC

Secures key exchange and digital signatures – HTTPS, VPN, online banking, e-ID, PKI, Crypto coins,...

WILL BE BROKEN

WHY IT BREAKS



Shor's algorithm

Cracks the maths of RSA, DH, ECC

Exponential

speed-up - longer keys won't help

WHAT SURVIVES



Symmetric encryption

AES

Grover's algorithm halves the key strength
AES-256 still provides 128 bits.

WEAKENED – NOT BROKEN

Bottom line: replace RSA, DH & ECC with quantum-safe methods (PQC, QKD) – and use AES-256.

XBC

Sources: P. W. Shor (1994); L. K. Grover (1996).

§

REGULATORY FACTS

Compliance: EU PQC deadlines

THE LEGAL BASIS

EU Recommendation 2024/1101
Apr 2024 · plan the PQC switch

EU PQC Roadmap (NIS CG)
Jun 2025 · one EU timeline

NIS2 amendment, Art. 7(2)(k)
Jan 2026 · proposed: PQC policies

Cyber Resilience Act
Dec 2027 · duties for digital products

EU TIMELINE FOR THE PQC TRANSITION



START
National PQC roadmaps
Inventory & risk analysis
First pilots

HIGH RISK DONE
High-risk systems migrated
RSA/ECC no longer alone
Quantum-safe updates

COMPLETE
Medium-risk migrated
Low-risk where feasible
Same target in US & UK

What counts as high risk?

Data that must stay secret 10+ years ("store now, decrypt later")

Long migrations (8+ years), e.g. software updates

Is it binding?

The roadmap is a recommendation, but NIS2 will require national **post-quantum cryptography** policies.

Management is accountable (NIS2, DORA).

No-regret steps

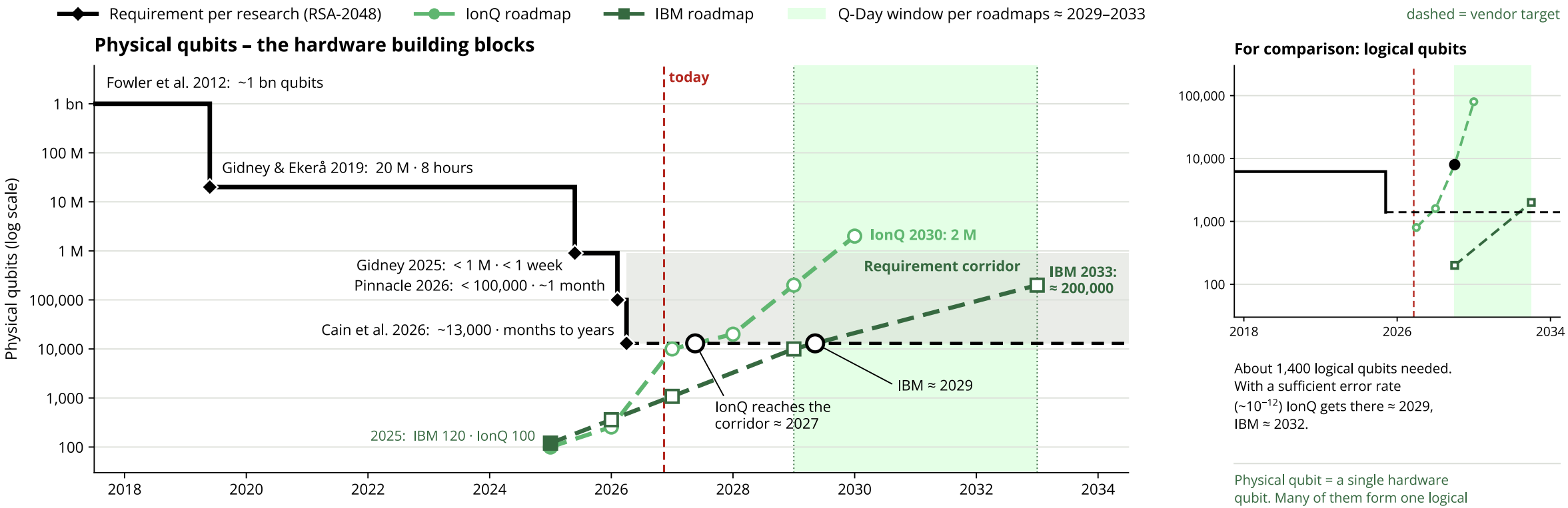
- Crypto inventory & dependencies
- Quantum risk analysis
- Ask suppliers for their PQC plan
- Start with high-risk systems

XBC Sources: Recommendation (EU) 2024/1101 · NIS CG EU PQC Roadmap v1.1 (2025) & FAQ (2026) · COM(2026) 13 (NIS2 amendment, proposal) · Regulation (EU) 2024/2847 (CRA)

DEVELOPMENTS

When will quantum computers break RSA-2048?

The physical-qubit requirement has fallen by four to five orders of magnitude since 2012 – vendor roadmaps reach it from ≈ 2027.



About 1,400 logical qubits needed. With a sufficient error rate (~10^{-12}) IonQ gets there ≈ 2029, IBM ≈ 2032.

Physical qubit = a single hardware qubit. Many of them form one logical qubit through error correction.

Requirements fall faster than expected

From ~1 bn (2012) to 13,000–100,000 physical qubits (2026) – purely through better algorithms and error correction.

More qubits = shorter attack time

~13,000 qubits: months to years · ~100,000: about a month · < 1 M: under a week. The grey corridor shows this range.

Action must start today

"Store now, decrypt later": data intercepted today can be read later. EU roadmap: start PQC migration by end of 2026, critical infrastructure by 2030.

Sources: Fowler et al., Phys. Rev. A 86 (2012) · Gidney & Ekerå, arXiv:1905.09749 · Gidney, arXiv:2505.15917 · Webster et al. (Pinnacle), arXiv:2602.11457 · Cain et al., arXiv:2603.28627 · IonQ and IBM roadmaps 2025 · EU NIS Cooperation Group, PQC roadmap 2025.

Notes: Requirement figures rest on different hardware assumptions (e.g. neutral atoms, non-local connectivity) and are not directly comparable. Roadmaps are non-binding vendor targets; IBM physical counts 2029/33 estimated. As of November 2026.

IMPACT

IMPACT

Bitcoin: one third of all coins exposed

6.9 M BTC

≈ one third of all bitcoin

Public key already visible on the blockchain
≈ €0.67 trillion · Project Eleven, Feb 2026

Why are these coins exposed?



- **Address re-used** – key revealed by an earlier payment
- **Address type** shows the key (old P2PK, Taproot)

hours – days

to derive a private key

Shor's algorithm on a CRQC would break
ECDSA (secp256k1) – the signature behind every BTC

Largest exposed wallets

Binance cold wallet	`34xp4v…4Twseo · P2SH re-use`	**249k BTC** ≈ **€24 bn**
Robinhood cold wallet	`bc1ql49y…98859v2 · P2WPKH re-use`	**141k BTC** ≈ **€14 bn**

Harvest now, steal later: the public keys are already on-chain – a future CRQC would just need to read them.

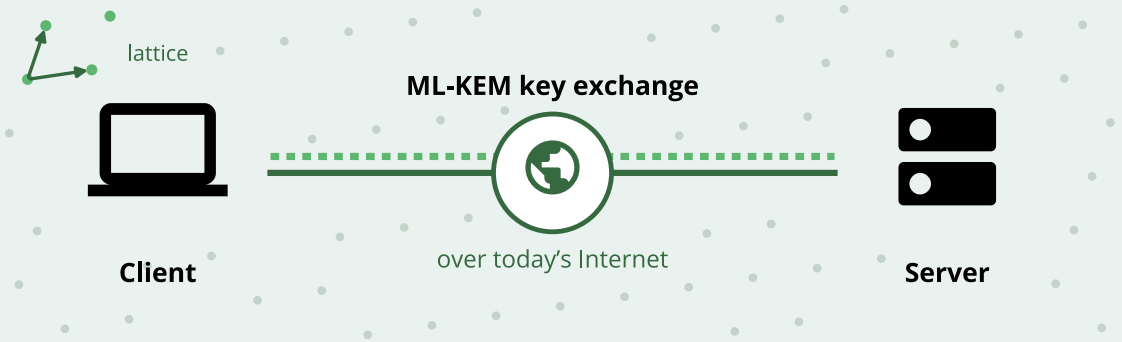
XBC

Sources: Project Eleven – Bitcoin Risq List & quantum threat report (block 936,882, Feb 2026) · Chaincode Labs – Bitcoin and Quantum Computing · Deloitte – Quantum computers and the Bitcoin blockchain · € at ~€96,500/BTC

Quantum Cryptography



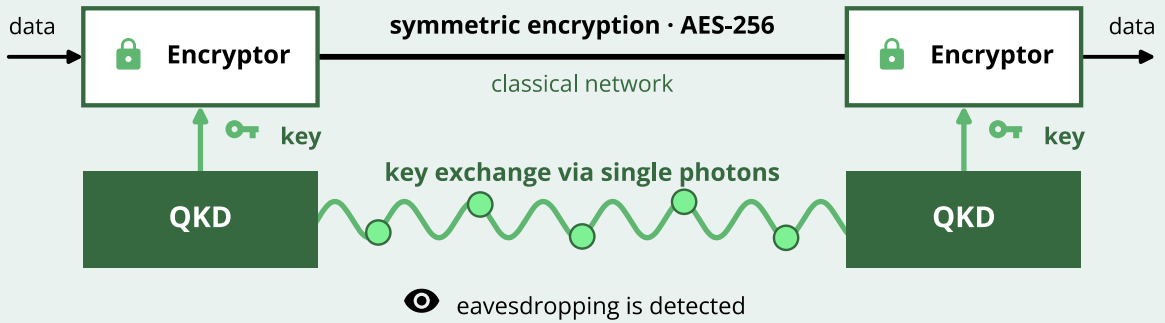
PQC — Post-Quantum Cryptography — = mathematics



Encryption	Signatures	Based on
ML-KEM HQC	ML-DSA · SLH-DSA FN-DSA	lattices · hashes codes

- ✓ Software only – runs on existing networks
- ✓ NIST standards since 2024, already in use
- ✗ Security relies on mathematical assumptions

QKD — Quantum Key Distribution — = physics



Protocols	Based on	Reach
DV · CV entanglement	no-cloning · measurement	~100 km fibre satellite beyond

- ✓ Physics-based – safe against any future computer
- ✓ Eavesdropping is physically detectable
- ✗ Dedicated hardware and fibre, limited reach

PQC + QKD = hybrid

Both keys are combined – the link stays secure as long as one of the two holds.

QKD Types

QKD | Types & Vendors



Entanglement-based QKD

pairs of linked photons

- **0/3 – zero third** — AT
- **Quantum Optics Jena** — DE

DV-QKD

discrete variables: single photons

- **IDQ – ID Quantique** — CH/US
- **ThinkQuantum** — IT
- **Falqon Systems** — NL
- **QTI** — IT
- **Toshiba** — JP

CV-QKD

continuous variables: laser light, telecom parts

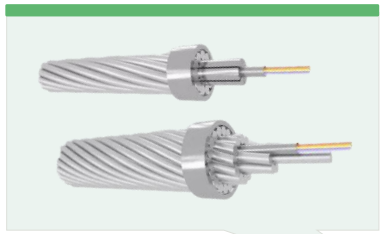
- **KEEQuant** — DE
- **LuxQuanta** — ES



USE CASES

USE CASE · CRITICAL INFRASTRUCTURE / ENERGY

PoC: QKD for the energy grid



Optical Ground Wire (OPGW) ≈ 52 km

quantum channel in the OPGW

QKD system

QKD system

IDQ

Teleprotection

Voice

Data

Substation

Hitachi Energy
XMC20 / FOX615
SECU1/SENC1 + QRNG

fibre optical cables

Power plant

Hitachi Energy
XMC20 / FOX615
SECU1/SENC1 + QRNG

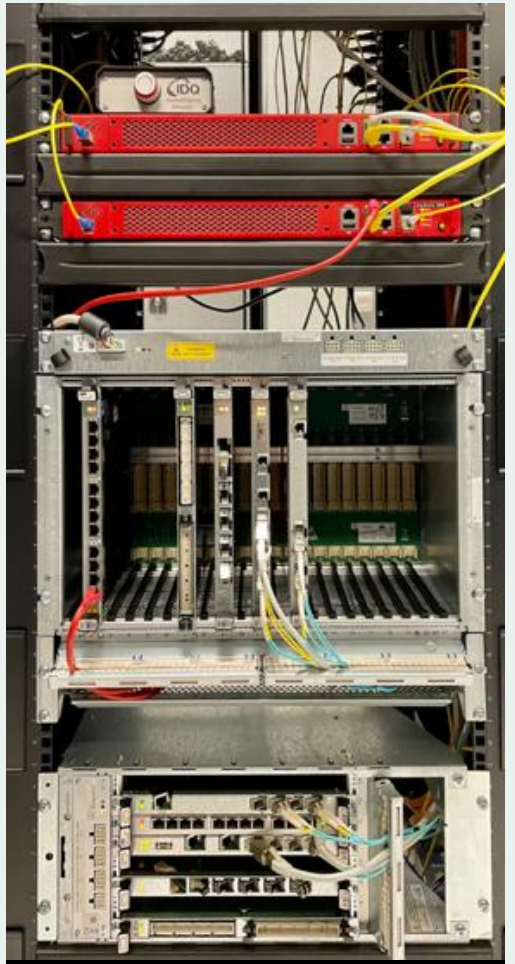
Teleprotection

Voice

Data

private & public wireless networks

Hitachi Energy



Real setup
IDQ QKD + Hitachi Energy FOX615

What is protected

Grid control traffic (teleprotection), voice and data between substations.

Why it works here

The quantum channel uses fibre already in the power line (OPGW).

Source: www.idquantique.com/random-number-generation/qrng-use-cases/hitachi-qrng-use-case/ · photo: real PoC setup

THANK YOU!

QUANTUM RESISTANCE BY QKD AND PQC

quantum@xbc-digital.com