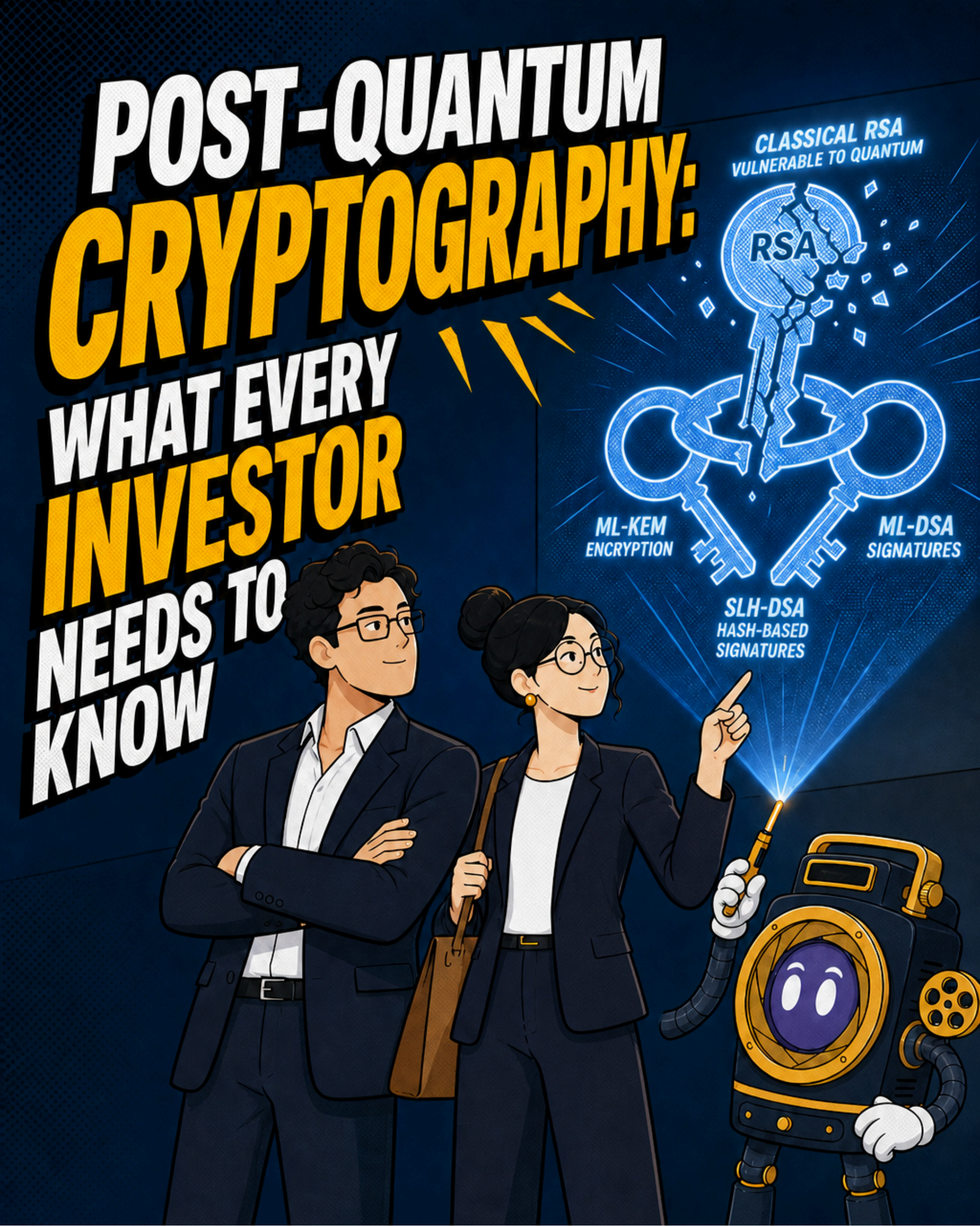
POST-QUANTUM CRYPTOGRAPHY: WHAT EVERY INVESTOR NEEDS TO KNOW



THE ENCRYPTION HOLDING YOUR DATA TOGETHER IS RUNNING OUT OF TIME

Today
You are secure with current encryption

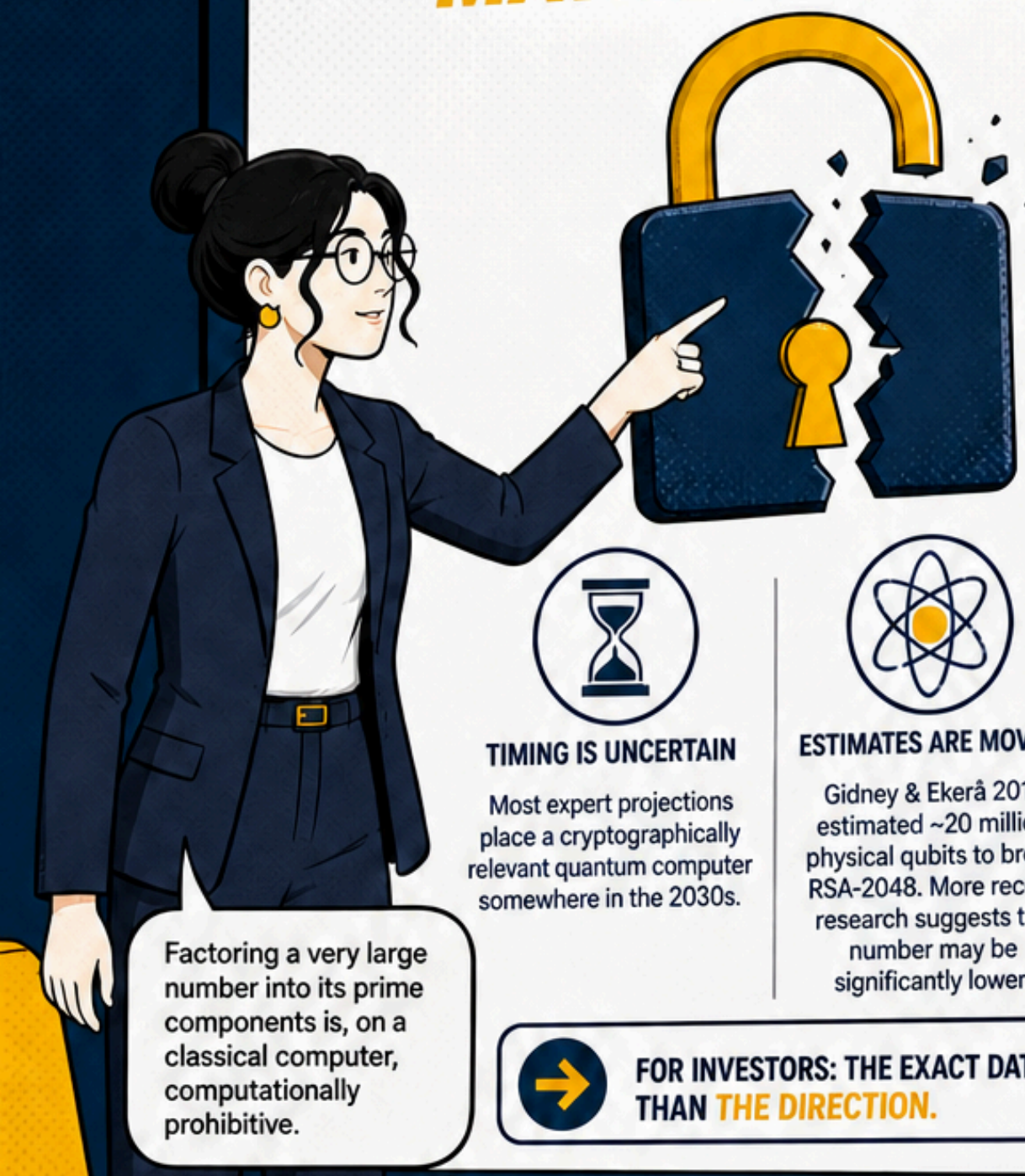
2025–2027
Governments set mandates. Standards take shape.

2028–2030
DEADLINE APPROACHING
Migrations must be underway

2030–2035
Post-quantum adoption accelerates

2035+
Quantum computers become practical

WHY THE ENCRYTION YOU RELY ON TODAY IS MATHEMATICALLY FRAGILE



61 × 61

37 × 37

53 × 53

71 × 71

Factoring a very large number into its prime components is, on a classical computer, computationally prohibitive.

TIMING IS UNCERTAIN

Most expert projections place a cryptographically relevant quantum computer somewhere in the 2030s.

ESTIMATES ARE MOVING

Gidney & Ekerå 2019 estimated ~20 million physical qubits to break RSA-2048. More recent research suggests the number may be significantly lower.

DIRECTION IS CLEAR

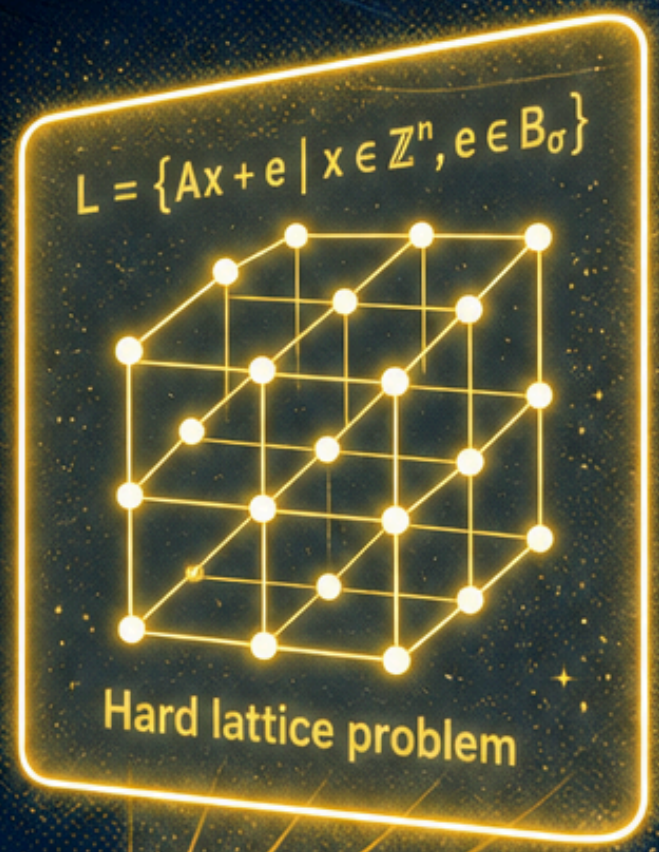
These estimates have generally moved downward, but the pace and endpoints remain uncertain.

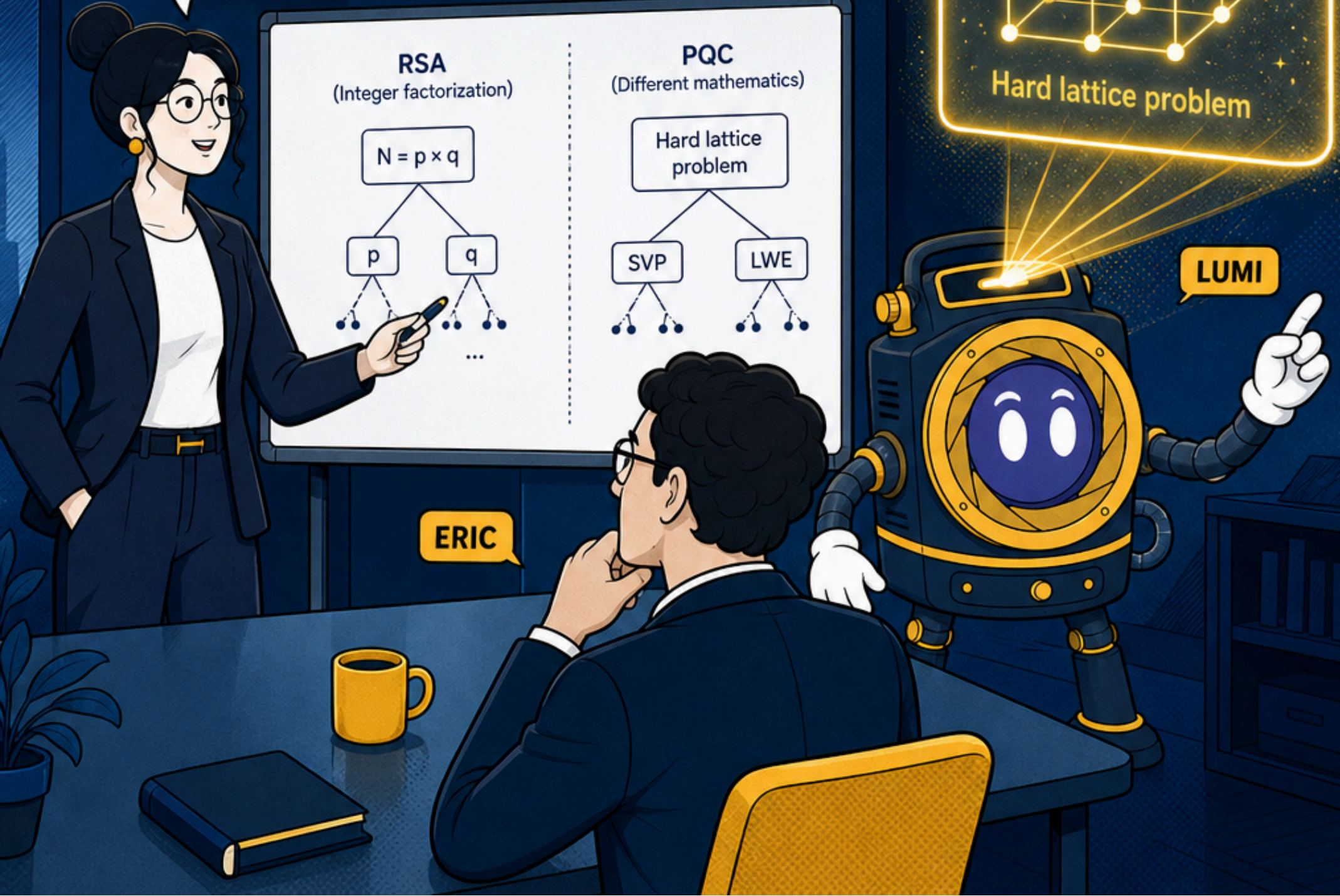
FOR INVESTORS: THE EXACT DATE MATTERS LESS THAN THE DIRECTION.

WHAT IS POST-QUANTUM CRYPTOGRAPHY?

Post-quantum cryptography (PQC) is a set of mathematical problems believed to be hard for **quantum computers** to solve — even using Shor's algorithm.

Where RSA relies on **integer factorization**, PQC is built on **entirely different mathematics** that Shor's algorithm simply can't touch.



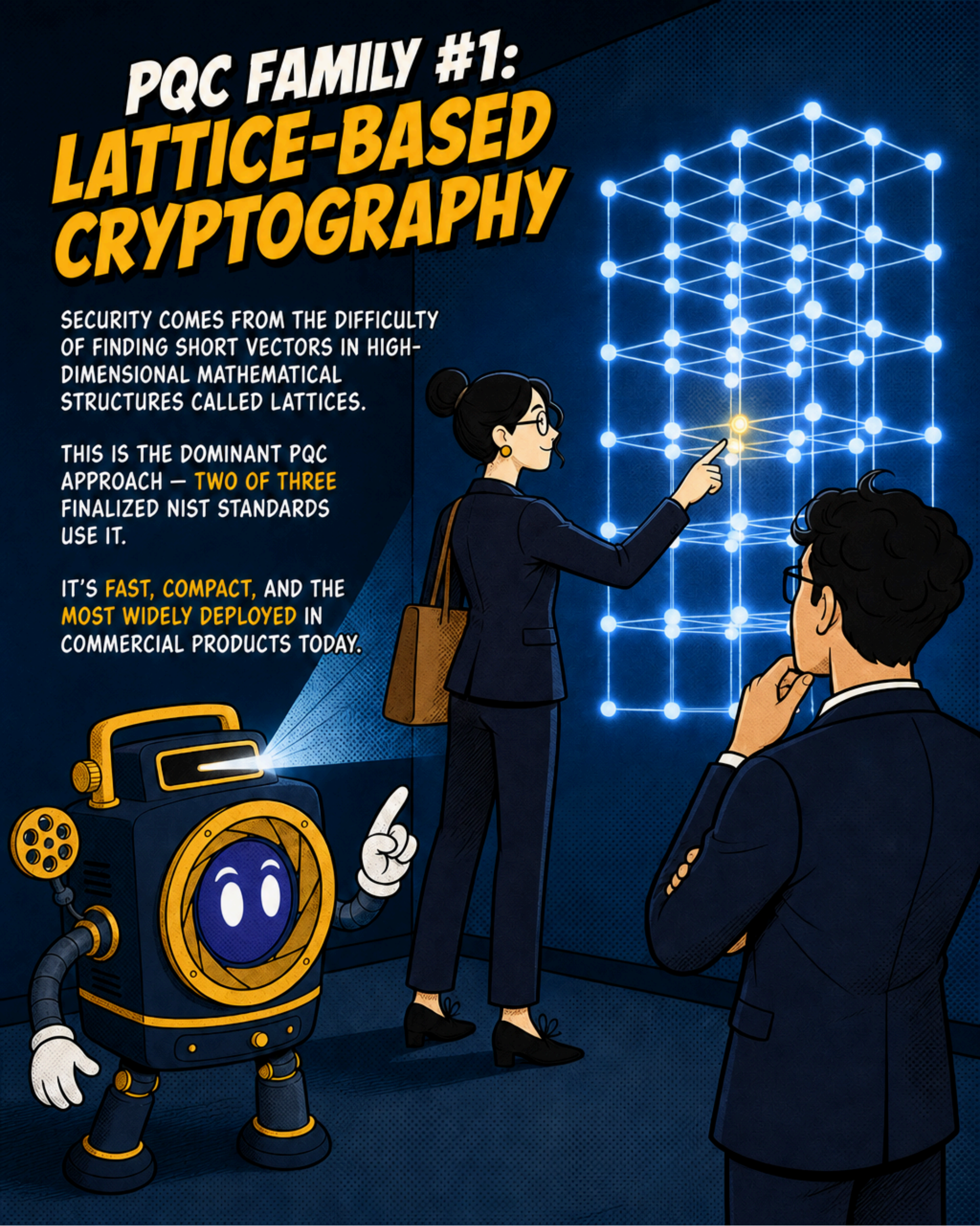


PQC FAMILY #1: LATTICE-BASED CRYPTOGRAPHY

SECURITY COMES FROM THE DIFFICULTY OF FINDING SHORT VECTORS IN HIGH-DIMENSIONAL MATHEMATICAL STRUCTURES CALLED LATTICES.

THIS IS THE DOMINANT PQC APPROACH — **TWO OF THREE** FINALIZED NIST STANDARDS USE IT.

IT'S **FAST, COMPACT,** AND THE **MOST WIDELY DEPLOYED** IN COMMERCIAL PRODUCTS TODAY.



PQC families 2 & 3:
Hash-based and code-based

HASH-BASED

- Security relies on one-way hash functions.
- Extremely conservative — no credible attack path exists.
- SLH-DSA (SPHINCS+) uses this; tradeoff is larger signatures.

CODE-BASED

- Built on decoding random error-correcting codes.
- Strong backup to lattice math, with NIST developing additional standards for diversification.

NIST FINALIZES ITS PRINCIPAL PQC STANDARDS AFTER AN 8-YEAR GLOBAL EVALUATION

THREE STANDARDS PUBLISHED:

ML-KEM (FIPS 203):
KEY ENCAPSULATION — ENCRYPTION, TLS, VPNS

ML-DSA (FIPS 204):
DIGITAL SIGNATURES — AUTH, CODE SIGNING, CERTIFICATES

SLH-DSA (FIPS 205):
HASH-BASED SIGNATURES — CONSERVATIVE FALLBACK

A FOURTH STANDARD, **FN-DSA (FALCON)**, WAS IN LATE-STAGE DRAFTING.

THE NIST RELEASE TRIGGERED BINDING MIGRATION TIMELINES WORLDWIDE

US FEDERAL AGENCIES:
Mandatory compliance timelines activated immediately

EU (21 MEMBER STATES):
Critical infrastructure migration deadline — **2030**

NSA CNSA 2.0:
PQC required for new classified systems by **2027**; full transition by **2035**

NIST STANDARDS

REMOVE THE LAST EXCUSE FOR INACTION

- There is now an **approved, auditable** standard to migrate to
- Organizations can no longer defer — **procurement requirements** are reshaping vendor contracts
- The only remaining question: **Has your organization started?**

THE STANDARDS ARE A REGULATORY STARTING GUN — NOT A DISTANT WARNING.

THE ATTACK THAT'S ALREADY HAPPENING:

HARVEST NOW, DECRYPT LATER

2026
Harvest / Collect

2030s
Decrypt / Exploit

ENCRYPTED DATA CAPTURED

ARCHIVED & STORED SECURELY

DECRYPTED & EXPLOITED

THE BREACH ISN'T VISIBLE WHEN THE DATA IS STOLEN.
IT BECOMES VISIBLE YEARS LATER,
WHEN THE ENCRYPTION COLLAPSES.

MOST EXPOSED

- GOVERNMENT COMMUNICATIONS
- FINANCIAL RECORDS
- HEALTHCARE DATA
- INTELLECTUAL PROPERTY
- LEGAL DOCUMENTS (MERGERS, CAPITAL RAISES)

**HNDL DOESN'T REQUIRE A QUANTUM COMPUTER TODAY—
JUST ACCESS, PATIENCE, AND TIME.**

MIGRATION TIMELINES ARE LONGER THAN MOST ORGANIZATIONS EXPECT

PQC MIGRATION FOR ENTERPRISES

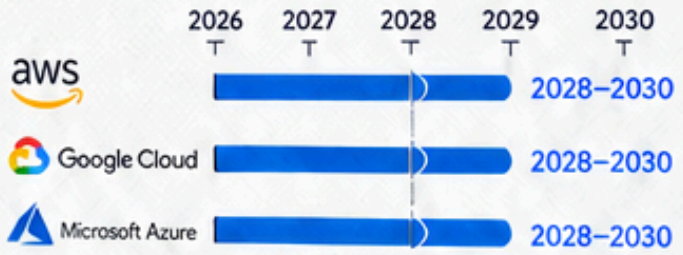
NIST PROJECTS 5–10 YEAR ADOPTION CYCLES FOR CRITICAL INFRASTRUCTURE

2027–2030

EARLY ADOPTERS IN FINANCIAL SERVICES AND GOVERNMENT TARGET COMPLETION BY 2027–2030

CLOUD PROVIDERS MOVING FASTER

HYBRID TLS SUPPORT ANNOUNCED; FULL PQC MIGRATION TARGETS



HYBRID APPROACHES LAYER PQC ALONGSIDE CLASSICAL ENCRYPTION FOR FORWARD SECRECY AND BACKWARDS COMPATIBILITY

GOVERNMENT GUIDANCE AND TIMELINES

UNDER NSA GUIDANCE

2025
SOFTWARE/FIRMWARE SIGNING & CLOUD SERVICES ADOPT QUANTUM-RESISTANT ALGORITHMS

→

2026
BROADER NETWORK INFRASTRUCTURE TRANSITIONS UNDER WAY

CISA NIST DHS

COMPLIANCE REALITY FOR LISTED COMPANIES

EU DORA
REQUIRES ACTIVE MONITORING OF QUANTUM RISK SINCE JAN 2025

U.S. FEDERAL AGENCIES MIGRATION DEADLINE PARTIALLY UNRESOLVED AS OF MID-2026, CREATING COMPLIANCE UNCERTAINTY

COMPLIANCE UNCERTAINTY FOR CONTRACTORS AND FINANCIAL INSTITUTIONS

→ **MIGRATION TAKES MANY YEARS** FOR MEDIUM/LARGE ENTERPRISES →

ORGANIZATIONS THAT DELAY ARE NARROWING THEIR MARGIN CONSIDERABLY

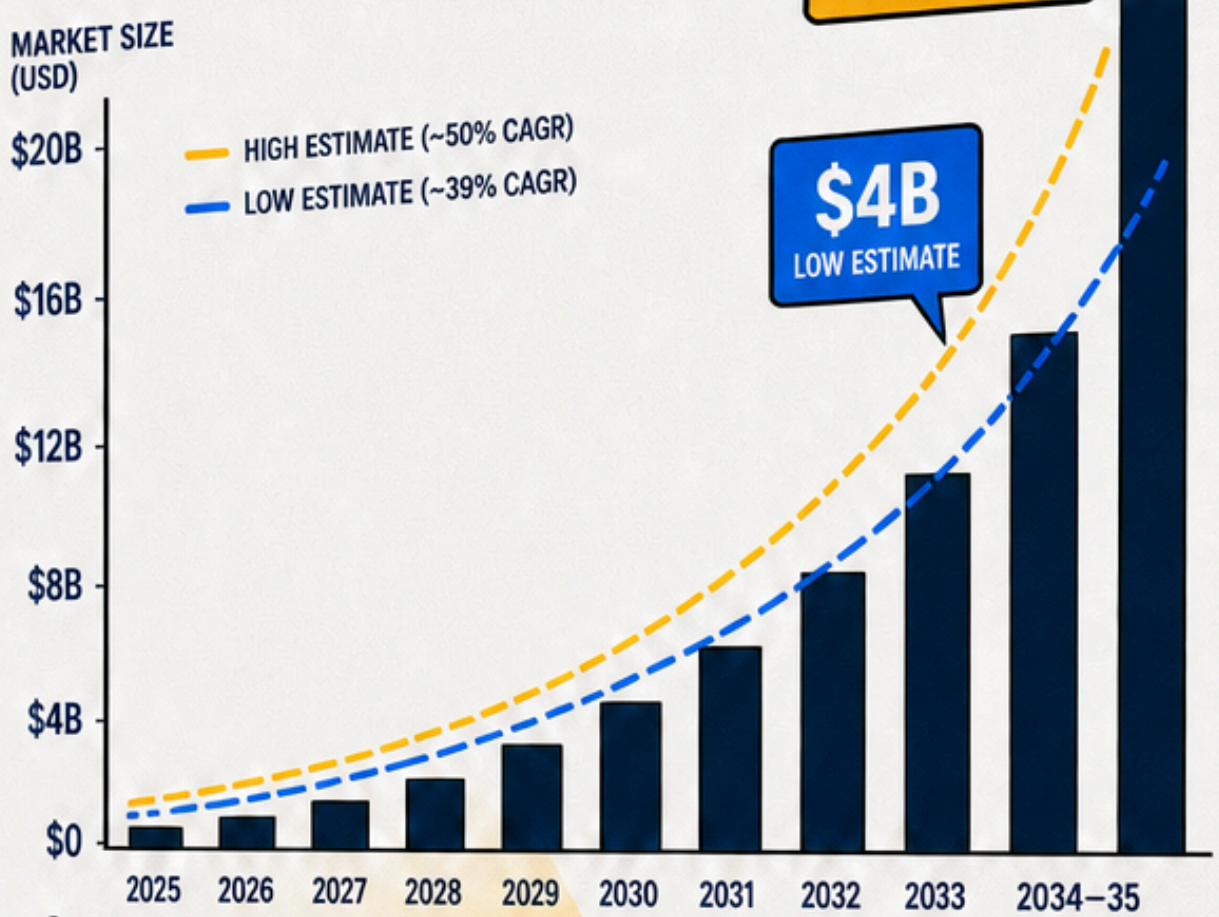
PQC MARKET SIZE: GROWTH TRAJECTORY

From hundreds of millions in 2025 to **$4B–$19B** by the early-to-mid 2030s.

CAGR estimates range from **~39%** to **~50%** depending on scope and methodology.

Wide variance reflects genuine **adoption uncertainty**—not a consensus signal.

Lattice-based schemes (ML-KEM, ML-DSA) expected to lead early commercial deployment as primary **NIST-standardised** algorithms.



GOVERNMENT TAILWINDS FOR PQC VENDORS

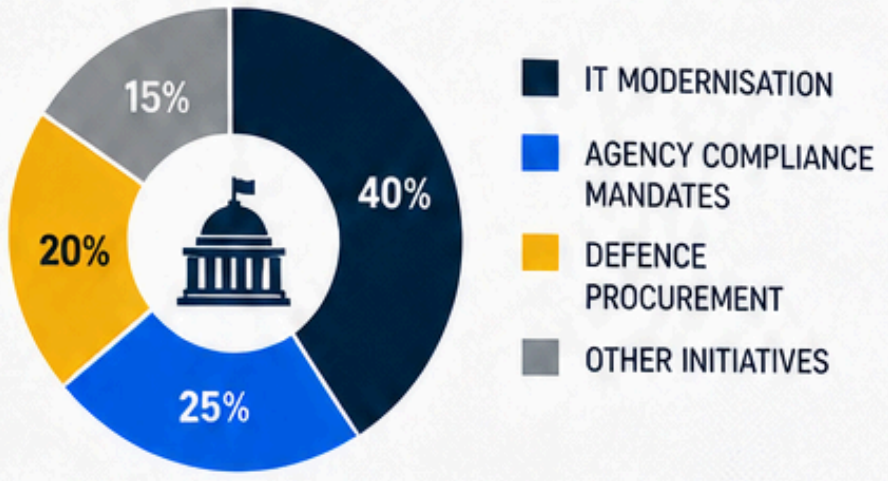
Federal cybersecurity budgets – spanning IT modernisation, agency compliance mandates, and defence procurement – represent a meaningful tailwind.

A precise dollar figure ring-fenced exclusively for PQC is not isolatable from public documents.

The direction of government commitment is clear; the exact quantum is harder to pin down.

Cloud-hosted PQC is tracking faster growth as hyperscalers embed quantum-safe services.

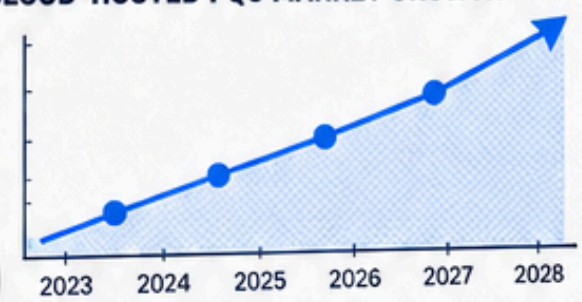
FEDERAL CYBERSECURITY BUDGET ALLOCATION



THE DIRECTION OF GOVERNMENT COMMITMENT IS CLEAR.

The exact quantum is harder to pin down.

CLOUD-HOSTED PQC MARKET GROWTH



HARDWARE AND PKI: THE REFRESH CYCLES

HSMs:

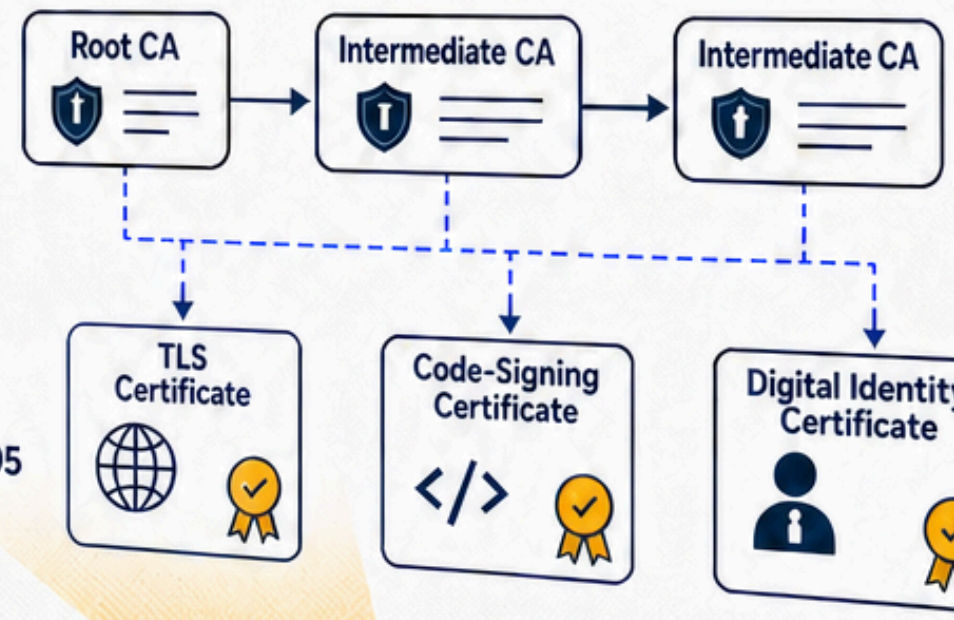
Every HSM in banking, payments, and securities infrastructure requires upgrade or replacement for PQC support — a predictable hardware refresh cycle.

HSM Gen 1 — HSM Gen 2 — HSM PQC-Ready

2022 Gen 1 (Legacy) — 2025 Upgrade Window — 2028+ PQC Standard

PKI and certificate management:

Every TLS cert, code-signing cert, [illegible] digital identity [illegible] to a public key [illegible]cture. Vendors [illegible] for FIPS 203–205 [illegible]-positioned.



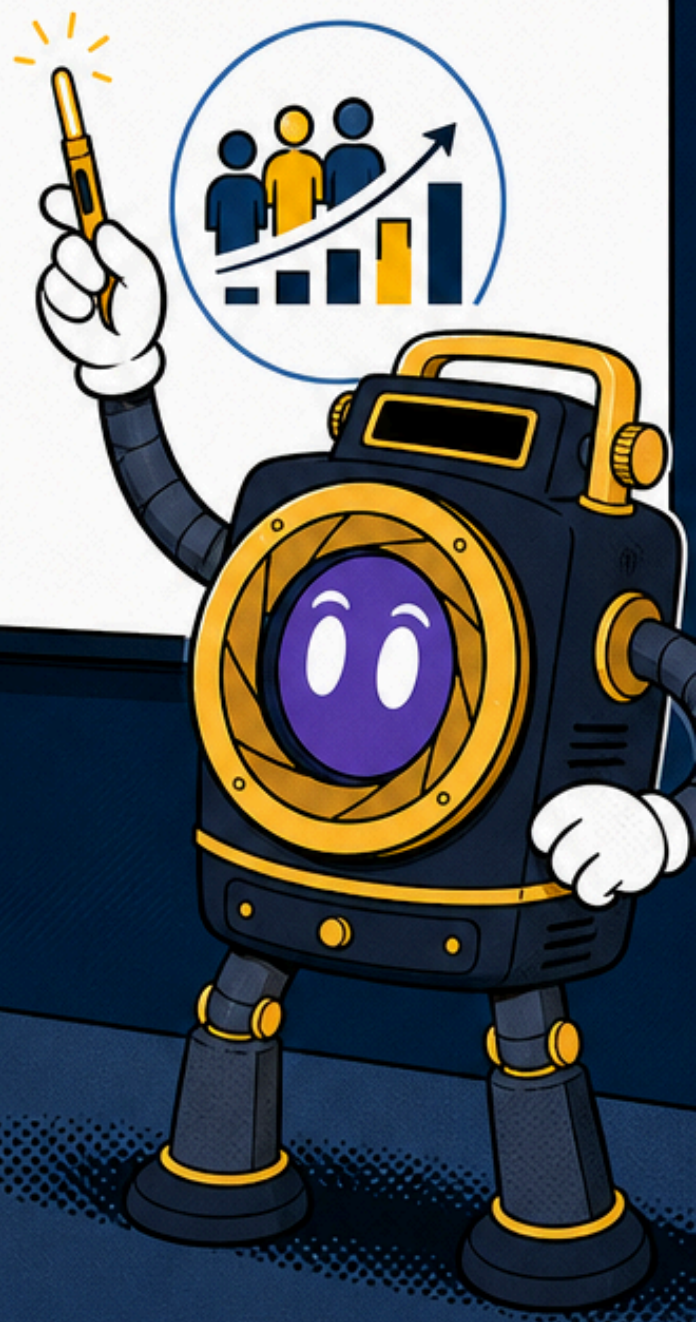
CLOUD KEY MANAGEMENT AND MIGRATION SERVICES

CLOUD KEY MANAGEMENT:

Hyperscalers embed PQC as managed services. Organisations without deep cryptography expertise will consume PQC via APIs, accelerating the cloud provider advantage.

CONSULTING AND MIGRATION SERVICES:

The skills gap is acute. External expertise is increasingly essential, making services a faster-growing segment than solutions alone.



WHAT THIS MEANS
IF YOU'RE EVALUATING A DEEP TECH OR FINTECH INVESTMENT

Four questions that belong in due diligence if the company handles sensitive data at scale:

1	**Has the company completed a cryptographic inventory?**	Most organisations don't know every place RSA or ECC appears in their stack. A company that can't answer this question hasn't started.
2	**Is there a documented migration roadmap with ownership?**	NIST standards are published. Migration timelines exist. A company with no roadmap is carrying undisclosed technical debt.
3	**What's the data retention profile?**	A company storing financial records, health data, or regulated IP for 10+ years faces HNDL exposure that begins today, not at Q-Day.
4	**Are cloud dependencies PQC-ready?**	If the company uses AWS, Azure, or GCP for key management, the hyperscaler's PQC roadmap directly affects the company's risk profile. Hybrid TLS support is available. The question is whether it's switched on.

None of this requires a company to have completed migration today. It requires evidence that the problem is understood and owned.

THE BOTTOM LINE

KNOWN VULNERABILITY

This is a mathematical fact.

PUBLISHED STANDARDS

NIST standards published Aug 2024.

HARVEST NOW, DECRYPT LATER

The clock starts today, not on Q-Day.

MIGRATION CYCLE ACTIVE

Timelines, growth, and regulations are in motion.

THIS IS A TRANSITION HAPPENING NOW.

infrairis

https://startups.infrairis.com