Why could a computer that does not exist yet already threaten every bank account on earth?

The cryptographic time bomb:

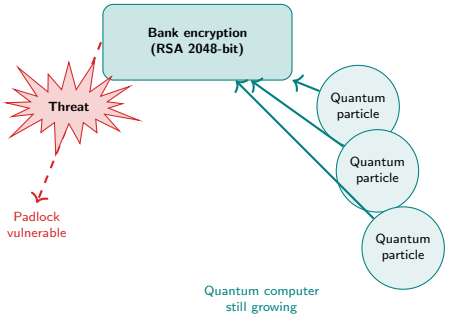
- Every online banking session, every credit card payment, every blockchain transaction depends on cryptography
- That cryptography assumes certain mathematical problems are impossibly hard to solve
- Quantum computers will make those problems easy
- We do not know exactly when quantum computers will arrive, but we know they are coming

Why this matters today, not tomorrow:

- Adversaries are collecting encrypted financial data right now
- They plan to decrypt it once quantum computers become available
- Data with a shelf life beyond ten years is already at risk
- Migrating cryptographic infrastructure takes a decade
- If you wait until quantum computers arrive, you are already too late

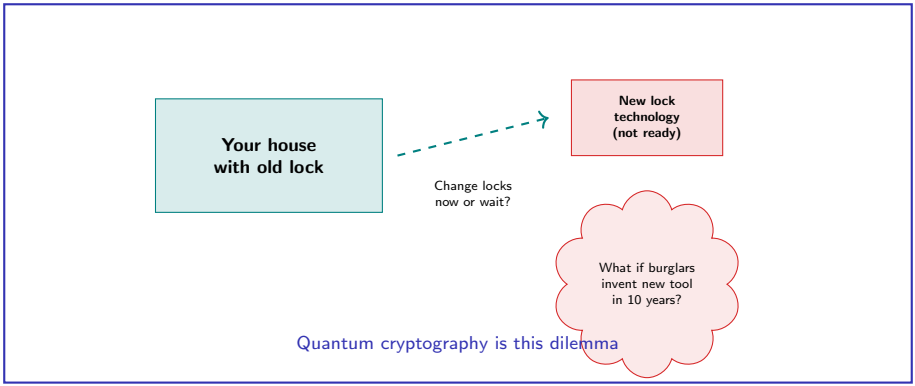
The timeline paradox:

- Quantum computing is uncertain in timing but certain in outcome
- Acting too early wastes resources; acting too late exposes data
- Financial institutions must begin migration now



Core tension

Have you ever changed the locks on your house because a new key technology was coming – before the technology existed?



Pause and reflect

Financial institutions face the same question: spend resources now to migrate cryptography before the threat materializes, or wait and hope the timeline is long enough.

The quantum threat is unique: you must act before the danger arrives, because once it does, your encrypted data from the past is already compromised.

What are the key differences between classical and quantum computing for cryptography?

Classical computing:

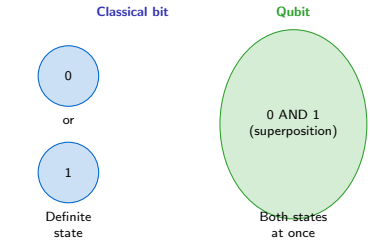
- Bits are either 0 or 1 at any given moment
- Operations are sequential or parallel across many bits
- Cryptography relies on problems that take billions of years to solve by exhaustive search
- Example: factoring a 2048-bit number into two primes is computationally infeasible

Quantum computing:

- Qubits exist in superposition: simultaneously 0 and 1 until measured
- Entanglement allows qubits to coordinate operations in ways classical bits cannot
- Certain algorithms exploit this to solve specific problems exponentially faster
- Example: Shor's algorithm can factor large numbers efficiently

Cryptographic implication:

- RSA and elliptic curve cryptography depend on the hardness of factoring and discrete logarithms
- Quantum computers break these assumptions
- Symmetric encryption (AES) and hash functions (SHA-256) are weakened but not broken



Classical: try all combinations (slow)

Quantum: explore many paths

How does a quantum algorithm break the cryptographic assumptions that protect financial transactions?

Shor's algorithm (1994):

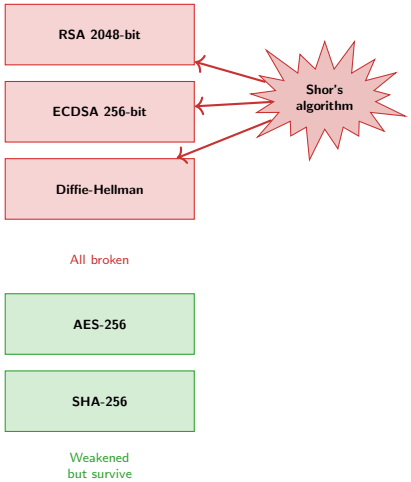
- Mathematician Peter Shor proved that a quantum computer can factor large numbers exponentially faster than any known classical algorithm
- Factoring a 2048-bit number takes billions of years classically; Shor's algorithm can do it in hours on a sufficiently large quantum computer
- The same algorithm solves the discrete logarithm problem, which underpins elliptic curve cryptography

What this breaks:

- RSA encryption and signatures (used in TLS, email, code signing)
- Elliptic curve digital signatures (used in Bitcoin, Ethereum, and most modern systems)
- Diffie-Hellman key exchange (used in VPNs and secure messaging)

What survives:

- AES-256 symmetric encryption (weakened but usable)
- SHA-256 hash functions (weakened but usable)
- Post-quantum algorithms based on different hard problems



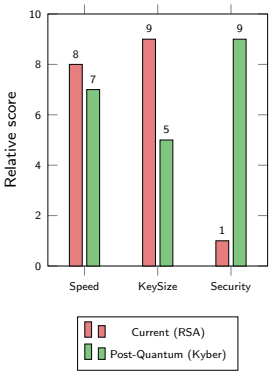
Cryptographic catastrophe

How do current and post-quantum cryptographic architectures compare?

Property	Current	Post-Quantum
Algorithm	RSA, ECDSA	Kyber, Dilithium
Hard problem	Factoring, DLP	Lattice, Hash
Key size	256-4096 bits	800-1600 bytes
Signature size	Small	Larger
Performance	Fast	Comparable
Quantum security	None	High
Maturity	Decades	New

Trade-offs:

- Post-quantum algorithms have larger key and signature sizes
- Performance is comparable to RSA for most applications
- Lattice-based algorithms offer the best balance
- Hash-based algorithms have highest security confidence but largest signatures



Post-quantum algorithms trade larger key sizes for quantum resistance.

Necessary trade-off

Post-quantum cryptography requires larger keys and signatures in exchange for protection against quantum attacks. The performance cost is acceptable.

What happens if an institution starts migrating too late and quantum computers arrive early?

Harvest now, decrypt later (HNDL):

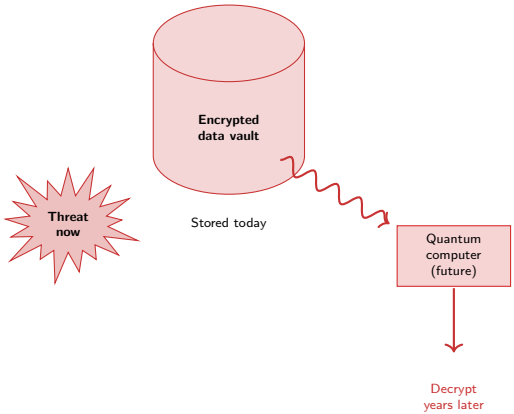
- Adversaries intercept and store encrypted financial data today
- They cannot decrypt it with current computers
- They wait for quantum computers to become available
- Once quantum arrives, they decrypt years of historical data

What data is at risk right now:

- Bank transactions and account details
- Mortgage applications and loan documents
- Corporate financial records and trade secrets
- Government financial communications
- Any data with a confidentiality requirement beyond ten years

Why late migration is catastrophic:

- Data encrypted today with RSA will be exposed retroactively
- There is no way to re-encrypt data that has already been intercepted
- Financial institutions that wait will face a data breach affecting years of historical records
- Regulatory penalties and reputational damage will be severe



Retroactive exposure

Where are financial institutions in their quantum readiness journey?

Readiness phases and current status:

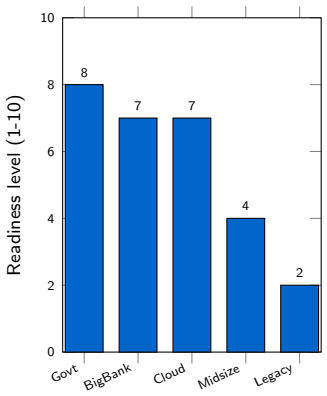
- **Phase 1: Awareness (complete):** Industry recognizes the quantum threat
- **Phase 2: Inventory (ongoing):** Cataloging cryptographic dependencies
- **Phase 3: Hybrid deployment (starting):** Testing post-quantum algorithms in non-critical systems
- **Phase 4: Full migration (future):** Replacing all classical cryptography

Who is leading:

- Government agencies: mandated migration timelines
- Large banks: active research and pilot programs
- Cloud providers: offering post-quantum services

Who is lagging:

- Small and mid-size financial institutions
- Legacy core banking systems
- Embedded systems with long replacement cycles



Government and large institutions lead; mid-size and legacy systems lag behind.

Readiness gap

Government and large institutions are actively migrating, but the majority of the financial sector remains in early phases

Who is most vulnerable to quantum threats and who is best prepared?

Most vulnerable:

- Financial institutions with long-lived encrypted data (mortgages, pensions)
- Blockchain networks using ECDSA signatures (Bitcoin, Ethereum)
- Legacy systems with hard-coded cryptography
- Organizations that have not inventoried cryptographic dependencies
- Small institutions with limited resources for migration

Best prepared:

- Government agencies with mandated migration timelines
- Cloud providers offering post-quantum services
- Financial institutions with crypto-agile architectures
- Organizations that have completed cryptographic inventories
- Systems designed with algorithm negotiation built in

Key differentiator:

- Crypto agility: the ability to swap algorithms without redesigning systems
- Organizations with hard-coded cryptography face complete rewrites
- Organizations with abstracted cryptography can migrate incrementally

Three questions to assess an institution's quantum preparedness

The Quantum Readiness Checklist:

Question 1: Has the institution inventoried all cryptographic dependencies?

- Can you list every system, protocol, and certificate using RSA or ECDSA?
- Do you know which vendor systems and hardware security modules depend on specific algorithms?
- Have you identified data with confidentiality requirements beyond ten years?

Question 2: Are post-quantum algorithms being tested in non-critical systems?

- Have you deployed hybrid certificates (classical plus post-quantum) in any environment?
- Are vendor roadmaps for post-quantum support documented?
- Is there a test environment for evaluating post-quantum performance?

Question 3: Is there a migration roadmap with milestones?

- Does the roadmap include phases for inventory, hybrid deployment, and full migration?
- Are there budget allocations for cryptographic updates?
- Is there executive sponsorship and governance?

Criterion	Yes/No
Inventory complete	_____
Long-lived data identified	_____
Vendor roadmaps known	_____
PQC testing started	_____
Hybrid deployment live	_____
Migration roadmap exists	_____
Budget allocated	_____
Executive sponsorship	_____
Total Yes	_____

Scoring guide:

- 0-2: Critical gap, urgent action needed
- 3-5: Lagging, accelerate efforts
- 6-8: On track, maintain momentum

Your Challenge

You are a bank CISO. Create a quantum readiness roadmap.

Scenario: Your bank has 500 applications, 200 vendor integrations, and tens of millions of customer records encrypted with RSA and ECDSA. The board asks for a quantum readiness plan. Estimates suggest quantum computers may arrive between 2030 and 2040.

Your task:

1. What do you inventory first and how do you prioritize systems?
2. What do you migrate first: external-facing systems or internal systems?
3. What is your timeline: when do you start inventory, hybrid deployment, and full migration?
4. How do you handle vendor dependencies for core banking and hardware security modules?
5. How do you balance the cost of migrating now versus the risk of waiting?

Constraints:

- Migration budget is limited; you cannot replace everything at once
- Some legacy systems cannot be updated and must be replaced entirely
- Vendors have varying levels of post-quantum readiness
- Regulatory mandates may impose deadlines before 2035
- Harvest now, decrypt later means historical data is already at risk

Deliverable: A three-phase roadmap with start dates, milestones, and prioritization criteria for each phase.

Think strategically

Quantum readiness is not just a technology project. It is a risk management program that requires executive sponsorship, vendor coordination, and long-term budget commitment.