Quantum Computing and the coming Financial Security Crisis

Kapila Dodamgoda

Abstract

In our interconnected digital landscape, the security of personal and professional data—protected by traditional passwords and encryption methods—is facing an unprecedented threat from the rise of quantum computing. Unlike classical computers, quantum computers leverage qubits, allowing them to perform complex calculations at exponentially faster rates. As companies like Google and IBM advance quantum technology, traditional cryptographic algorithms like RSA and ECC, which safeguard systems in banking, secure messaging, and blockchain, could be compromised. This article examines the looming risks quantum computing poses to current cybersecurity frameworks, particularly in finance and cryptocurrency, and underscores the urgent need for transitioning to quantum-resistant encryption. It highlights the potential for quantum computers to disrupt encryption infrastructure and outlines strategic precautions that organizations must implement to defend against this emerging threat.

Introduction

We live in an intricately connected digital world. From the moment we wake up, we interact with systems and platforms that define our personal and professional lives—banking apps, messaging platforms, cloud storage, social media, trading platforms, enterprise systems, ERPs, CRMs, accounting software, and payment gateways. Every one of these requires a login, typically secured with a username and password.

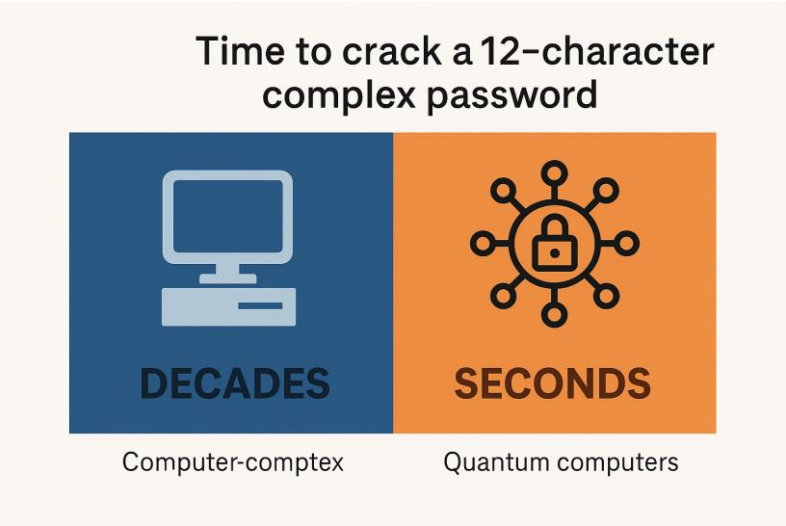
We trust these credentials to protect our most valuable assets: our identity, finances, transactions, client data, and company secrets. But the digital world is on the brink of disruption, and the most powerful threat isn't a hacker with a laptop—it's quantum computing.

How Traditional Passwords Work—And Why They've Been "Good Enough"

Most conventional systems use passwords in combination with hashing algorithms and encryption. Strong passwords—those with a mix of uppercase, lowercase, numbers, and symbols—are difficult to crack by brute-force due to the computational limits of current machines.

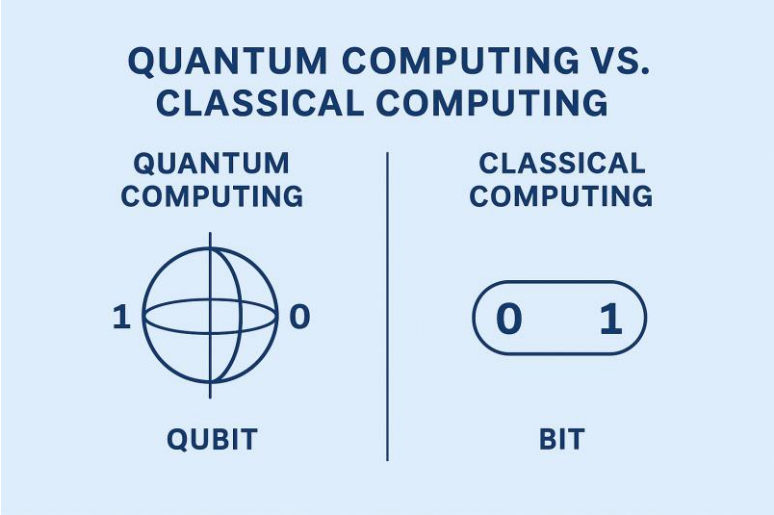
For example, a 12-character complex password might take decades to break using brute-force attacks with today's computing power. Encryption standards like RSA (Rivest–Shamir–Adleman) or AES (Advanced Encryption Standard) rely on the assumption that factoring large numbers or solving specific math problems is time-consuming and resource-intensive for classical computers.

But what if a machine could do in seconds what would take today's fastest supercomputers centuries?



What Is Quantum Computing?

Quantum computing isn't just a faster version of today's computers—it's a completely new paradigm. Instead of using bits (0s and 1s), quantum computers use qubits, which can represent 0, 1, or both simultaneously due to a property called superposition. These qubits can also link together in a phenomenon called entanglement, allowing for powerful parallel processing.
The result? An exponential leap in computational power—capable of solving problems that even the best supercomputers can't touch.



Are Quantum Computers Real?

Yes—quantum computers are real and functioning. Companies like Google and IBM have already built experimental machines—Google's "Willow" chip and IBM's "Osprey"—that have performed calculations beyond the reach of any classical supercomputer.

These machines have demonstrated quantum advantage, proving they can outperform traditional systems on specific tasks. Backed by billions in global investment, their success validates the physical reality of quantum computing and confirms decades of quantum theory.

The Alarming Risk: Quantum and Cybersecurity

Here's where it gets terrifying: once quantum computers reach sufficient maturity, they'll be able to break the encryption that underpins financial systems, national security, medical records, and more. Many of today's digital systems—especially in banking, online payments, cloud transactions, and secure messaging—are protected by cryptographic algorithms such as:

- **RSA**: Used widely for secure data transmission
- **DSA (Digital Signature Algorithm)**: Secures digital signatures
- **ECC (Elliptic Curve Cryptography)**: Popular for mobile, blockchain, and IoT security

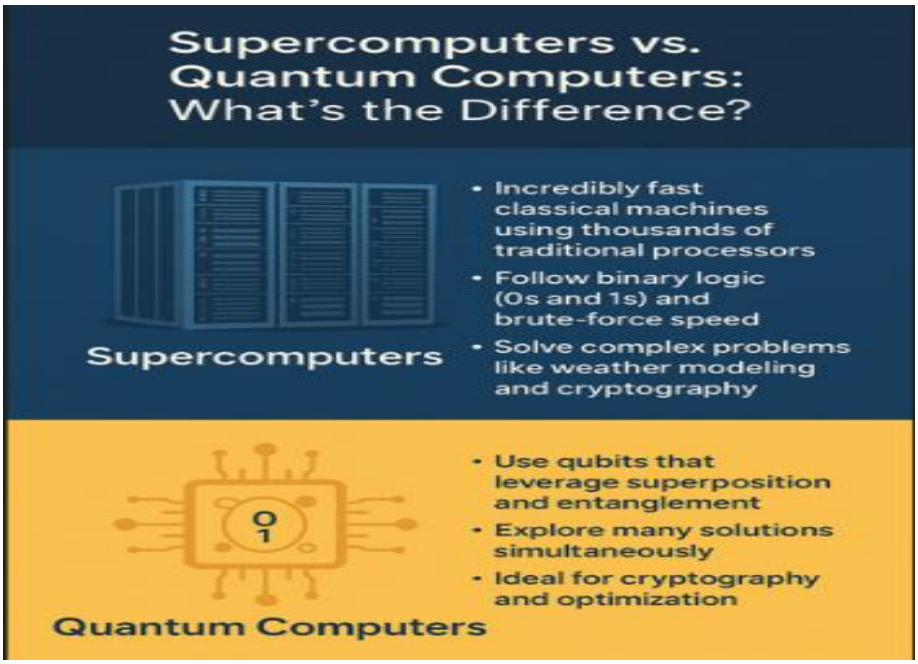
These algorithms rely on the mathematical difficulty of certain problems (like factoring large numbers) to keep data safe.

But **Shor's Algorithm**, a powerful quantum method, can factor large numbers exponentially faster than traditional methods. This means that a sufficiently powerful quantum computer could potentially break RSA, DSA, or ECC encryption in minutes, rendering them useless—and exposing sensitive financial data.

Encryption Type	Algorithm	Quantum Safe?	Usage
RSA-2048	RSA	❌ No	Web, email, banking
ECC (secp256k1)	ECC	❌ No	Bitcoin, Blockchain
AES-256	Symmetric Cipher	✅ Partially	General encryption
Kyber	PQC (NIST finalist)	✅ Yes	Future communications
Dilithium, Falcon	PQC Signatures	✅ Yes	Digital identity

Supercomputers vs. Quantum Computers: Why is the Case Different?

Supercomputers are incredibly fast classical machines used for complex calculations—weather modelling, molecular simulations, cryptography, and more—by harnessing thousands of traditional processors in parallel. They follow binary logic (0s and 1s) and rely on brute-force speed to solve problems. Quantum computers, on the other hand, use qubits—quantum bits that can represent multiple states simultaneously thanks to superposition and entanglement.



This enables them to explore many solutions at once, making them ideal for solving problems that even the fastest supercomputers would take centuries to crack. In short: supercomputers are powerful; quantum computers are exponentially powerful for specific tasks, especially in cryptography and optimization.

Will Quantum Computing Improve Bitcoin Mining?

Yes, quantum computers could theoretically speed up Bitcoin mining using Grover's algorithm, which offers a faster way to solve the brute-force computations behind Proof-of-Work. However, this remains hypothetical—today's quantum machines aren't yet powerful or cost-effective enough. Even if they were, the Bitcoin network would self-adjust its mining difficulty, rebalancing the advantage. The greater concern lies elsewhere: quantum computing's potential to break Bitcoin's encryption, threatening the very foundation of its security.

Is Quantum Computing a Threat to Bitcoin and Crypto?

Yes—but not immediately.

A powerful quantum computer could, in theory, crack the encryption that protects Bitcoin wallets, allowing attackers to derive private keys from exposed public keys and steal funds. The greatest risk lies in older or reused addresses where public keys have already been revealed.
While the risk isn't immediate, the crypto community is already preparing. Quantum-resistant blockchain algorithms are being developed. Still, the broader implication remains: the entire internet's encryption infrastructure, including HTTPS, VPNs, and secure logins, could be affected.

Is the Quantum Threat Immediate?

Not quite—but **we are in the warning phase**.

Today's quantum computers remain experimental and aren't yet capable of breaking real-world encryption. But research is advancing rapidly. Experts suggest that within 10–15 years, quantum computers may reach the scale required to challenge today's encryption.
The danger is also retrospective: attackers can "harvest now, decrypt later"—stealing encrypted data today and decrypting it once quantum capabilities catch up. This puts archived financial data, old emails, contracts, and backups at long-term risk.

Precautions: What You Can—and Must—Do Now

1. Transition to Quantum-Resistant Encryption: International standards bodies like NIST are already finalizing post-quantum cryptography (PQC) algorithms. Financial institutions must begin migration now, especially for long-term archives and core systems.

2. Audit Your Cyber Exposure: Work with IT to assess which systems use traditional encryption. Focus on systems handling:

- Personally Identifiable Information (PII)
- Financial statements and audits
- Client portfolios and sensitive transaction data

3. Educate Teams and Clients: Cyber risk isn't just for IT teams. Finance, legal, audit, and operations staff must understand quantum risk—and embed it into risk assessments and vendor evaluations.

4. Secure Archived Data: Even if your data seems safe today, it could be decrypted tomorrow. Re-encrypt old backups and long-term data using quantum-resistant methods.

A Call to Finance Professionals

The age of quantum disruption is no longer distant—it's already unfolding. For finance professionals, this is more than a technology issue. It's a strategic, operational, and fiduciary challenge that calls for immediate attention and long-term planning.

Traditionally, the role of CFOs, controllers, auditors, and risk managers has been to manage capital, ensure compliance, and protect value. But in the quantum era, your role expands to include a new kind of asset: digital trust. If encryption collapses, so does the integrity of everything finance touches—transaction records, audit trails, payment systems, and investor confidence.

This is a call to move from **passive awareness** to **proactive defense**. Finance leaders must work with IT, cybersecurity, and compliance teams to:

- Map **digital exposure**, especially in areas handling sensitive or regulated data
- Upgrade **legacy systems** to prepare for **post-quantum encryption**
- Allocate budgets for **quantum-risk mitigation technologies**
- Lead **board-level discussions** on long-term cyber risk

Don't assume this is "IT's problem." When a breach happens, it's finance that faces the scrutiny—from regulators, shareholders, and the public.

The era of quantum computing won't wait. It's **knocking on our firewalled doors**, testing our systems, and quietly harvesting our encrypted archives.

Finance must lead—not follow—in preparing for a future where security is measured not just in passwords, but in foresight.

Conclusion

The advent of quantum computing is reshaping the landscape of digital security, posing significant challenges that extend beyond technological domains into strategic and operational realms, particularly for finance professionals. As quantum computers approach maturity, the potential to break conventional encryption threatens the integrity of transaction records, audit trails, and overall investor confidence. The finance sector is called to proactively address these risks by transitioning to quantum-resistant encryption, auditing cyber exposure, and educating teams across departments. This transition demands strategic foresight and collaboration between finance, IT, and cybersecurity teams to safeguard sensitive data against future vulnerabilities. As the era of quantum computing unfolds, finance leaders must spearhead efforts to secure digital trust, ensuring that security is not only about robust passwords but also about preparedness and foresight in the face of technological evolution. By leading these efforts, finance professionals can ensure resilience in a future where traditional safeguards may no longer suffice.

In recent years, artificial intelligence (AI) has emerged as a transformative force across various industries, offering the potential to revolutionise how businesses operate and engage with consumers. One such application of AI is in the realm of pricing strategies, where companies like Delta Air Lines are moving towards individualised pricing models to enhance profitability. This approach involves the use of AI to dynamically set prices based on a variety of factors, moving away from traditional static pricing models. While the potential for increased revenue and operational efficiency is significant, this strategy also raises concerns about privacy, fairness, and the ethical implications of such practices.