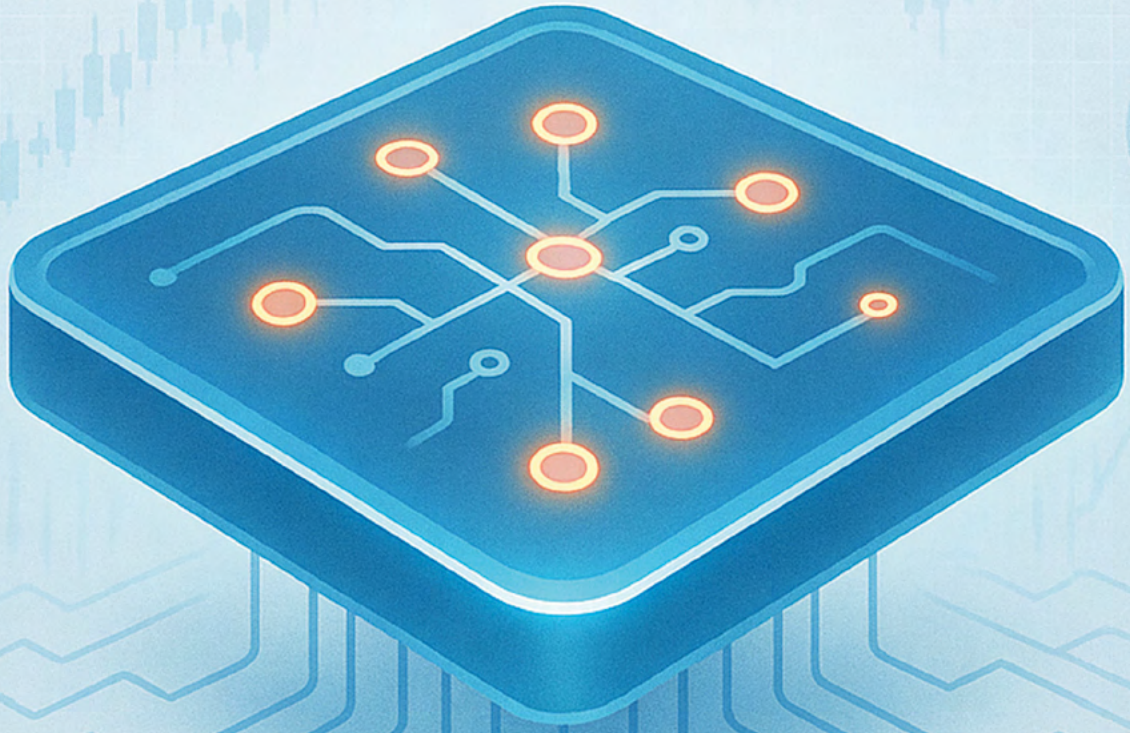
YOUR FIRST 100 QUESTIONS ON QUANTUM COMPUTING– ANSWERED



OSWALDO ZAPATA, PhD

RiskMathics
FINANCIAL INSTITUTE

YOUR FIRST 100 QUESTIONS ON QUANTUM COMPUTING—ANSWERED

Oswaldo Zapata, PhD

Introduction

Recently, I've been invited to give an increasing number of webinars to finance professionals interested in quantum computing.

After a few of these sessions, I began to notice that many of the questions were quite similar.

Rather than trying to recall them from memory, I turned to ChatGPT and asked it to generate "100 questions that finance professionals might ask after a talk on quantum computing and cryptosecurity."

To make the content more accessible, ChatGPT grouped the questions into 10 themed categories.
Initially, I believed I could answer all of them in a single weekend.

In reality, it took much longer!
Some questions required deeper research, as I realized my first responses were either incomplete or slightly inaccurate.

Another reason it took so much time was the editing process.

As always, I aimed to present the answers in a clear, accurate, and engaging manner.

I hope you find these answers both useful and enjoyable to read—as much as I enjoyed writing them.

Do not hesitate to reach out if you need additional help:

https://www.linkedin.com/in/oswaldo-zapata-phd-quantum-finance/

Oswaldo, May 2025.

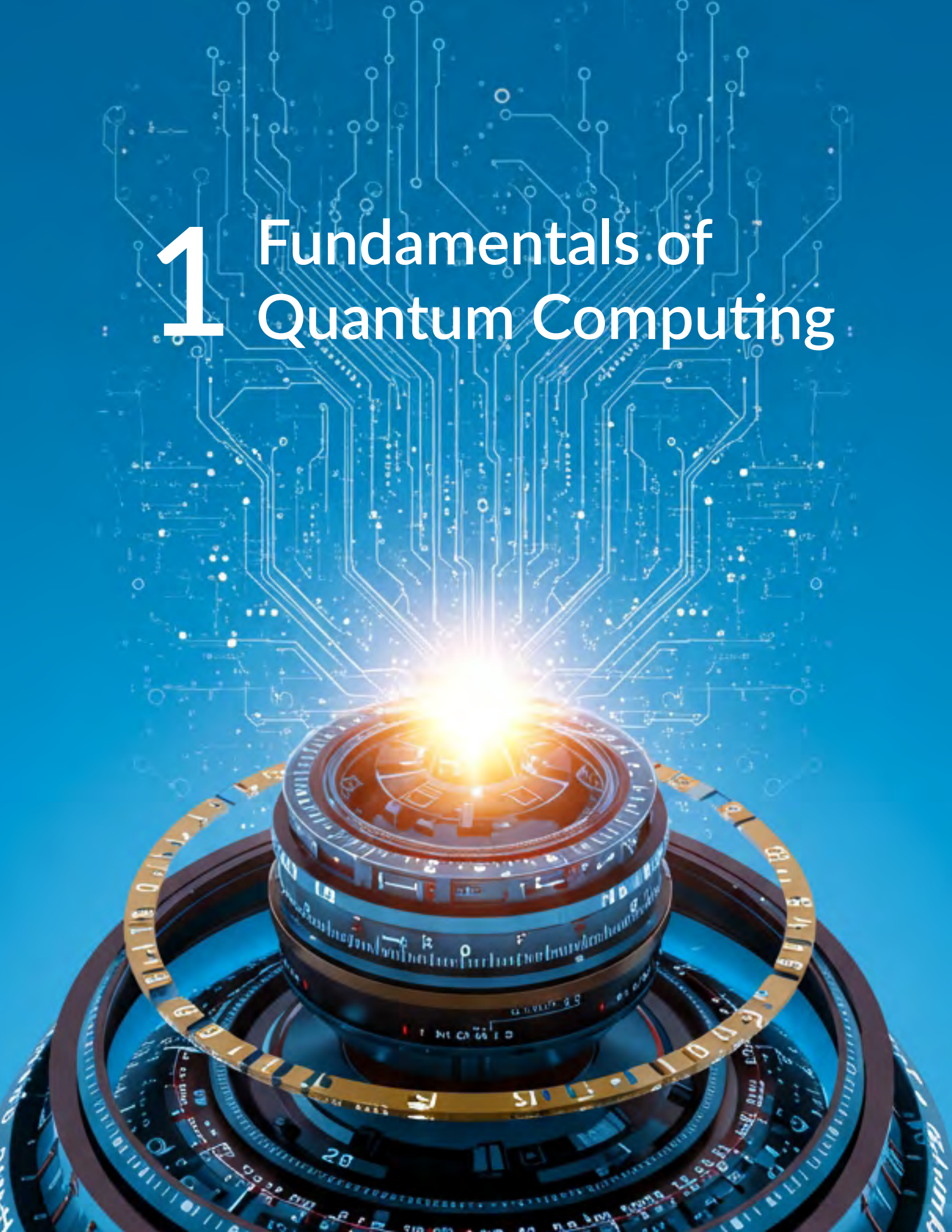
Acknowledgements

I would like to thank the colleagues who provided valuable feedback on the first draft of this eBook — in particular Greg Pitz, Jonathan Olson, Melissa Hernandez, Olga Mamlyga, Pushkar Kumar, and Wasim Mushtaq,.

Of course, all opinions expressed here are my own.

Table of Contents

1 Fundamentals of Quantum Computing



What is a quantum computer, really?

Quantum computers are devices that operate differently from the standard classical computers most of us have at home.

As the name suggests, quantum computers are based on the principles of quantum physics.

Instead of relying on conventional electric currents and electronic components, they use "quantum currents" and "quantum electronic components" to process information.

In quantum computing, the "quantum currents" are called *qubits*, and the "quantum electronic components" are known as *quantum gates*.

Experts believe that quantum computers can solve certain problems much faster than classical computers.

How does a qubit differ from a classical bit?

This is a bit technical, and honestly, understanding these concepts is not necessary to grasp the impact of quantum computing on sectors such as finance or on society at large.

A qubit is a concept from quantum mechanics, and it's well known that quantum physics is extremely difficult to understand.

The challenge arises because we are more familiar with macroscopic physics, where our intuition about nature helps us understand concepts like mass, force, velocity, and electric current.

In contrast, quantum mechanics—and particularly the concept of a qubit—can be quite counterintuitive.

However, if you're curious, here is a simplified definition of a qubit:

A classical bit is a physical system that can exist in only one of two states, which are mutually exclusive—such as black or white, on or off, 0 or 1.

A qubit, on the other hand, is a physical system that can also be measured in two exclusive states, but before measurement, the system is in a mathematical superposition of those states.

Of course, there are more details to this, but it gives a general idea.

Some people say that "a qubit is 0 and 1 at the same time," but that's wrong! The mathematical description just mentioned has nothing to do with physical reality.

Why are quantum computers so hard to build?

Even though a quantum computer is a macroscopic object, its internal quantum components are extremely tiny and highly sensitive to the external world and to undesirable interactions among themselves.

The challenge here is that, for the quantum computer to function properly, its internal components must be isolated from external influences and uncontrollable internal interactions.

For example, if a computation is running and heat or electromagnetic waves penetrate the system, the internal components—the qubits and the quantum gates—can be affected by these external factors.

Similarly, unpredictable interactions between qubits can also impact the output of the computation.

These kinds of effects can destroy the delicate quantum properties of the system, ultimately corrupting the results of the computation.

This is one of the reasons why some quantum computers need to be kept at extremely low temperatures—often hundreds of times colder than intergalactic space.

In physical terms, temperature is a measure of the average kinetic energy of particles in a system—how much they move and interact.

Lowering the temperature reduces this motion, thereby limiting unwanted energy exchanges that could disturb the fragile quantum states.

This is just one example. Other quantum hardware systems have their own challenges.

What's quantum superposition in simple terms?

Quantum superposition is a mathematical concept that is better understood without trying to interpret it physically.

The issue is that we naturally tend to apply our macroscopic understanding of the world to all physical phenomena, but this approach doesn't hold in the quantum realm.

Quantum mechanics tells us that if you can measure a system in different states—such as a quantum bit being 0 or 1—then the state just before measurement can be described as a linear superposition of these possible states.

Moreover, the linear coefficients are, in general, complex numbers.

However, this is a mathematical description, and it has no direct physical interpretation. It's incorrect to say that the cat is both dead and alive at the same time, or that a qubit is both 0 and 1 simultaneously before the measurement is made.

The superposition only tells us how the two measurable states are related and the probability of measuring each one.

What is quantum entanglement, and how is it useful?

Entanglement is one of those quantum concepts that many people use, sometimes without fully understanding its meaning.

In fact, entanglement is much more difficult to grasp than superposition, which is already a concept prone to many misinterpretations.

Let's say you have two isolated quantum systems.

In quantum mechanics, each of these systems is described by a vector, so you have two separate vectors, one for each system.

Now, suppose these two systems interact.

After this interaction, they are no longer described by two independent vectors; instead, they are described by a single vector that represents the combined system.

When you separate these two systems—taking them far apart—the description of each system no longer corresponds to the individual vectors we had in the beginning.

Instead, each physical system now contains information about the interaction it had with the other system.

This is what we mean by entanglement: the two systems are no longer isolated, and their states are intertwined.

The entangled system contains more information than the two isolated systems.

In quantum computing, this is useful because it allows us to entangle the information carried by different qubits and correlate the measurements of each of them.

What's the current status of real quantum hardware?

There are different types of quantum hardware, and various companies are developing them, so progress in this technology is not uniform.

For example, companies like IBM and Google are focusing on superconducting qubits, while Microsoft is working on a different approach called topological qubits.

Other types of hardware include photonic qubits, where properties of light, such as polarization, are used to encode quantum information, and trapped ions, where ions are controlled using lasers.

Currently, superconducting technology is the most advanced.

This has enabled Google and research groups in China to demonstrate quantum supremacy—proving that quantum solutions are faster than classical computers—on two separate occasions each.

The Chinese researchers have also shown quantum supremacy once using photonic technology.

These milestones highlight the growing potential of quantum computing, although significant challenges remain in scaling these systems.

Can quantum computers replace classical computers?

For certain tasks, yes; for others, I don't think so.

Classical computers have proven to be very effective at solving many complex problems, and it is expected that, for at least the next few decades, classical computers will continue to be used for these types of tasks.

For instance, in one hundred years, your computer at home or your phone will most likely still be classical computers.

However, for other challenging problems where classical computers struggle to find solutions within a reasonable amount of time, quantum computers will take the lead. This includes areas like accelerating machine learning processes or solving complex optimization problems.

That said, experts today are convinced that, in the near future, computers will likely be hybrid—combining both classical and quantum components.

These systems will work in tandem, with the classical components handling the parts of the problem they are efficient at, while the quantum components tackle the more complex and computationally intensive aspects.

What's quantum decoherence, and why is it a problem?

Decoherence is a process by which a quantum system loses or modifies the quantum properties—such as superposition or entanglement—that were initially assigned to it.

The causes of decoherence are varied and can include factors such as tiny temperature fluctuations, interactions with electromagnetic waves, or coupling to external environments.

Essentially, when a quantum system interacts unpredictably with its environment or other systems, it can cause the delicate quantum state to become entangled with the external systems, leading to a loss of coherence and the collapse of the quantum state into a classical one.

Decoherence is one of the major challenges in building stable quantum systems for practical use.

Why do quantum computers require such low temperatures?

Not all quantum computers require low temperatures.

However, superconducting qubits, the most advanced and widely known type of quantum hardware, need low temperatures to function properly.

Superconductivity is a physical phenomenon that occurs only at very low temperatures.

When temperatures are too high, the material loses its superconducting properties and cannot conduct electricity without resistance.

This is one of the reasons you often see large, complex cooling systems in most images of quantum computers.

The required temperature is extremely low—just a fraction of the temperature of intergalactic space.

But low temperatures are not required solely for superconductivity.

In fact, they are also essential for reducing thermal noise, which can interfere with the quantum properties of qubits.

For example, ion traps require low temperatures to minimize the motional noise of the ions.

Another technology that requires low temperatures is the topological qubits being developed by Microsoft.

However, other quantum technologies, such as trapped ions and photonic qubits, do not require such low temperatures to operate effectively.

What does “quantum gate” mean?

Suppose a standard electronic circuit.

For the circuit to operate, current flows through a series of electronic components, and at the end, current exits the circuit.

Each of these components, which perform specific functions, is called a gate.

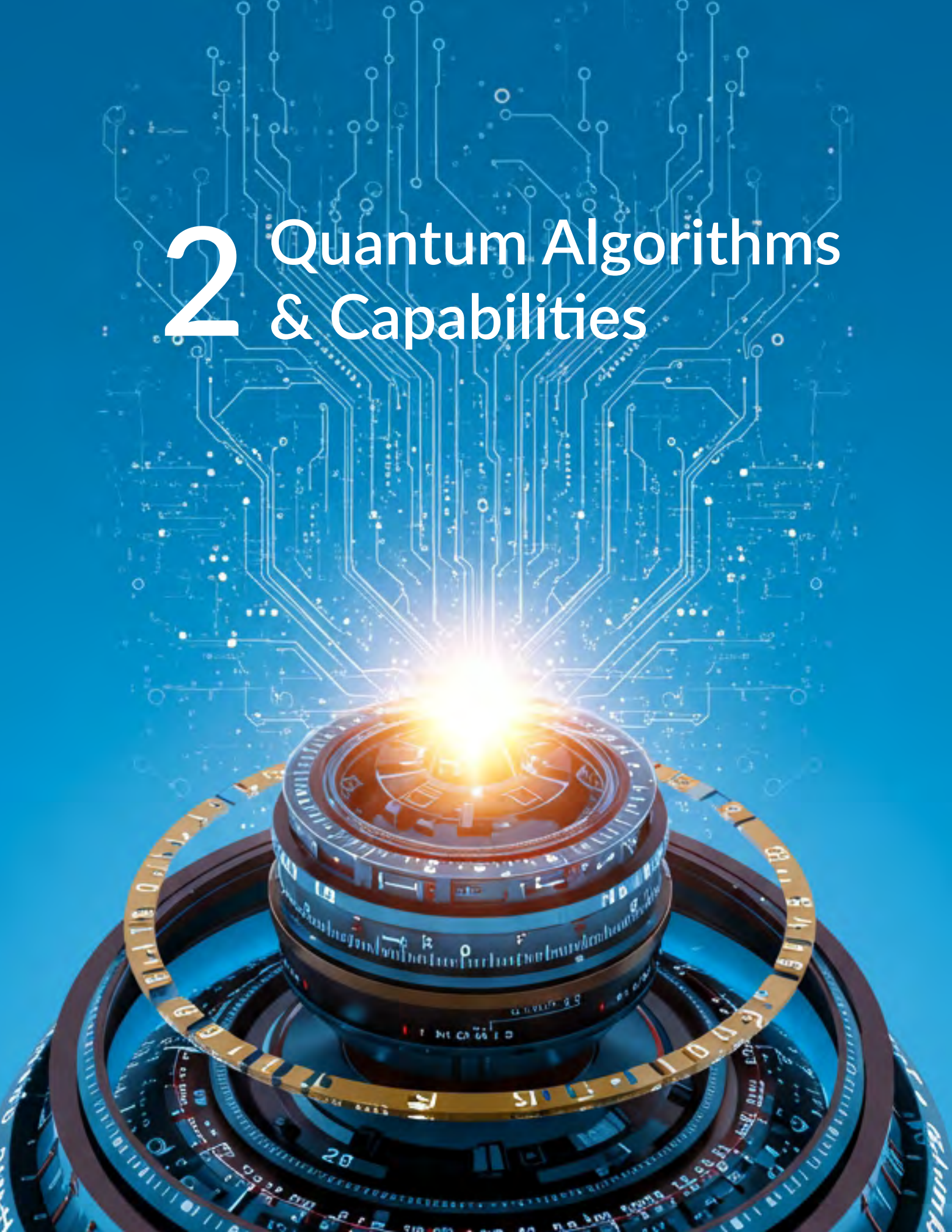
For example, a gate might simply block the current that arrives.

In the gate model of quantum computing, we have a similar situation.

There are quantum gates that determine how the quantum state of qubits should be modified.

A series of qubits, quantum gates, and measurements form what we call a quantum circuit, which is the quantum computing equivalent of a classical circuit.

2 Quantum Algorithms & Capabilities



What makes a quantum algorithm powerful?

In practical terms, an algorithm is a set of instructions given to a machine to perform a specific task.

Instead of building an entire computer from scratch to perform a single function, you can design a circuit that physically implements the algorithm for that task.

Each time you execute the algorithm, you get a result.

For classical algorithms, this result is always the same.

That's because classical computers operate under deterministic physics: given the same input, they will always produce the same output.

(While there are also non-deterministic classical algorithms, we'll set those aside for now.)

Quantum algorithms, however, behave differently.

Quantum mechanics is inherently probabilistic, not deterministic.

When you input data into a quantum circuit, you might get different results across different runs.

But the algorithm is designed so that the correct result appears more frequently when you repeat the process many times.

In some cases—though multiple runs may still be required—quantum algorithms can be more efficient than any classical algorithm tackling the same problem.

They may need fewer steps, less time, to reach a solution.

Why is that?

The advantage comes from two fundamental properties of quantum systems: superposition and entanglement.

The quantum algorithm is built in such a way that incorrect answers are suppressed while the correct ones are amplified.

This is the general principle behind many quantum algorithms.

What is Shor's algorithm, and why is it scary?

There are two sides to Shor's algorithm: the technical details and its practical implications. The core concept is relatively easy to grasp.

Suppose someone asks you to find the two prime numbers that multiply to give 15.

You'd quickly answer 3 and 5.

For 77, the answer is 7 and 11.

This seems like a simple task.

However, taking a large number like 3,127 and figuring out which two prime numbers were multiplied to get it—is much harder.

As the primes get larger, this factoring problem becomes exponentially more difficult for classical computers.

Shor's algorithm, developed by Peter Shor in the mid-1990s, is a quantum algorithm that can factor large numbers exponentially faster than the best-known classical algorithms.

At first glance, this might seem like an abstract mathematical breakthrough with little practical impact.

But that couldn't be further from the truth—and it's exactly why Shor's algorithm is so significant.

Modern encryption systems, such as RSA, rely on the assumption that factoring large numbers is computationally infeasible.

The concern is that once scalable quantum computers become available, malicious actors could use Shor's algorithm to break these encryption schemes, potentially gaining access to sensitive data from governments, financial institutions, and private organizations.

This looming threat is one of the main reasons behind the global effort to develop quantum-safe cryptography—encryption methods that can withstand attacks from both classical and quantum computers.

How does Grover's algorithm speed up searches?

Suppose you have to find an item within N items.

In a classical search, you have to check each item one by one and verify if it is the item you are looking for.

The number of tries it takes to find it is proportional to the number of items.

This is denoted by O(N).

Grover's algorithm is a quantum algorithm that speeds up this search.

It provides a quadratic speedup over classical search algorithms.

That is, instead of, say, 100 steps, it only needs about 10.

For large datasets, Grover's algorithm can significantly speed up the search process. For example, instead of 1 million steps, it only needs about 1 thousand.

This is denoted by O(√N).

Grover's algorithm utilizes the quantum properties of qubits and quantum gates to create entangled states that, when measured, give the result much faster.

Are there quantum algorithms for finance-specific tasks?

Quantum algorithms used in finance were not originally developed specifically for financial applications.

Instead, they were created in more general contexts and later adapted to financial problems.

For example, the *Quantum Approximate Optimization Algorithm (QAOA)* was initially developed to solve combinatorial optimization problems such as the Max-Cut problem.

It has since been applied to financial use cases like binary portfolio optimization.

Similarly, quantum-enhanced Monte Carlo methods—used to accelerate risk analysis and option pricing—were first developed in a broader computational context before being applied to finance.

Finally, quantum machine learning algorithms were not designed specifically for finance either.

However, finance has emerged as a prominent area for their application and further development, given its demand for high-dimensional data analysis and prediction.

Can quantum algorithms learn like AI/ML models?

Let us consider machine learning (ML) models for simplicity.

Classical ML models learn by finding the optimal values of their parameters through standard optimization techniques—such as gradient descent, for example.

Quantum machine learning (QML) processes, on the other hand, are different.

They exploit quantum properties like superposition and entanglement to enhance data processing.

However, current research in QML is still in its early stages, and it's not yet clear how these quantum models will match or exceed the performance of classical learning algorithms in real-world applications.

What is quantum annealing vs. gate-based quantum computing?

Gate-based quantum computing, also known as the quantum circuit model, is analogous to the classical circuit model. In this model, quantum information enters a circuit, is manipulated by a sequence of quantum gates, and is ultimately measured to produce an output.

These systems are referred to as universal quantum computers because, in principle, they can solve any computational problem given the appropriate quantum algorithm—much like classical universal computers.

Quantum annealing, by contrast, is based on a different physical mechanism and does not follow the gate-based model.

It is not considered a universal quantum computing model. Instead, quantum annealers work by minimizing an energy function, typically represented as an *Ising Hamiltonian or a QUBO (Quadratic Unconstrained Binary Optimization)* problem, which corresponds to finding the ground state of a system.

Quantum annealers are actively being developed for portfolio optimization, as the portfolio optimization problem can be mapped onto an Ising Hamiltonian.

One of the main challenges quantum annealers face is mitigating noise.

This is why, although some systems boast thousands of qubits, the coherence and fidelity of these qubits are generally lower than those found in gate-based quantum systems, such as those using superconducting qubits or trapped ions.

Qubit quality is essential for performing reliable and accurate quantum computations.

This concern over coherence and error rates is one reason why some experts remain skeptical about the long-term potential and practical achievements of quantum annealers.

Are quantum algorithms really faster than classical ones?

At present, quantum computing remains largely at the research stage.

A substantial body of work has been developed, and several quantum algorithms have demonstrated solid theoretical and experimental results—particularly in showing computational speedups over classical algorithms for specific problems.

However, much of the discussion surrounding quantum computing practical applications still involves speculation about its transformative potential.

This is why phrases like “quantum computing has the potential to transform…” or “quantum computing is expected to revolutionize…” are common in both academic and popular discussions.

One key area of debate is the performance of hybrid quantum-classical algorithms.

Despite their prominence in near-term quantum computing (often referred to as the Noisy Intermediate-Scale Quantum, or NISQ, era), it is still unclear whether these hybrid approaches consistently outperform the best classical methods.

This remains an open and active area of research.

Can quantum computers solve NP-complete problems?

That's a question nobody has yet been able to answer conclusively.

This question falls within the realm of complexity theory.

Complexity theory is the framework that allows mathematicians and computer scientists to determine whether a problem can be solved, and if so, how efficiently, using fundamental models of computation.

An NP-complete problem is one whose solution is difficult to find (no known polynomial-time algorithm), but if a solution is given, it can be verified in polynomial time.

It is a class of problems that appears to be unsolvable efficiently by classical computers.

However, so far, no one has been able to prove that quantum computation—the model used by quantum computers—can solve these problems efficiently either.

It remains an open question.

How do quantum circuit simulators differ from quantum computers?

A quantum circuit simulator is not a quantum computer.

It is a classical computer program designed to simulate the behavior of a quantum computer.

It performs quantum computations by classically emulating the evolution of quantum circuits and, in some cases, provides an estimate of how long it would take a real quantum computer to perform the same computation.

Quantum circuit simulators are important during this early stage of quantum hardware development because they allow researchers to evaluate the feasibility, performance, and scalability of quantum algorithms under realistic conditions.

Given the high cost and limited availability of quantum hardware via the cloud, individuals and small startups often choose to run their computations on quantum circuit simulators.

In some cases, companies first run their computations on a simulator and only promote those that meet certain performance or resource criteria to actual quantum hardware. This approach helps filter out less promising computations before using the more expensive and constrained resources of real quantum computers.

These simulators also help firms train internal teams, build quantum expertise, and prepare IT infrastructure.

Finally, quantum simulators are often used in combination with hybrid quantum-classical workflows, enabling financial institutions to tackle complex problems incrementally as the technology matures.

What's the difference between quantum speedup and quantum advantage?

Quantum speedup, usually referred to as quantum supremacy, is different from quantum advantage.

The former refers to demonstrating that a quantum computer can solve a specific problem faster than any known classical computer, regardless of whether the problem has practical significance.

In contrast, *quantum advantage* requires that the quantum computer solves a problem of practical relevance more efficiently than classical methods.

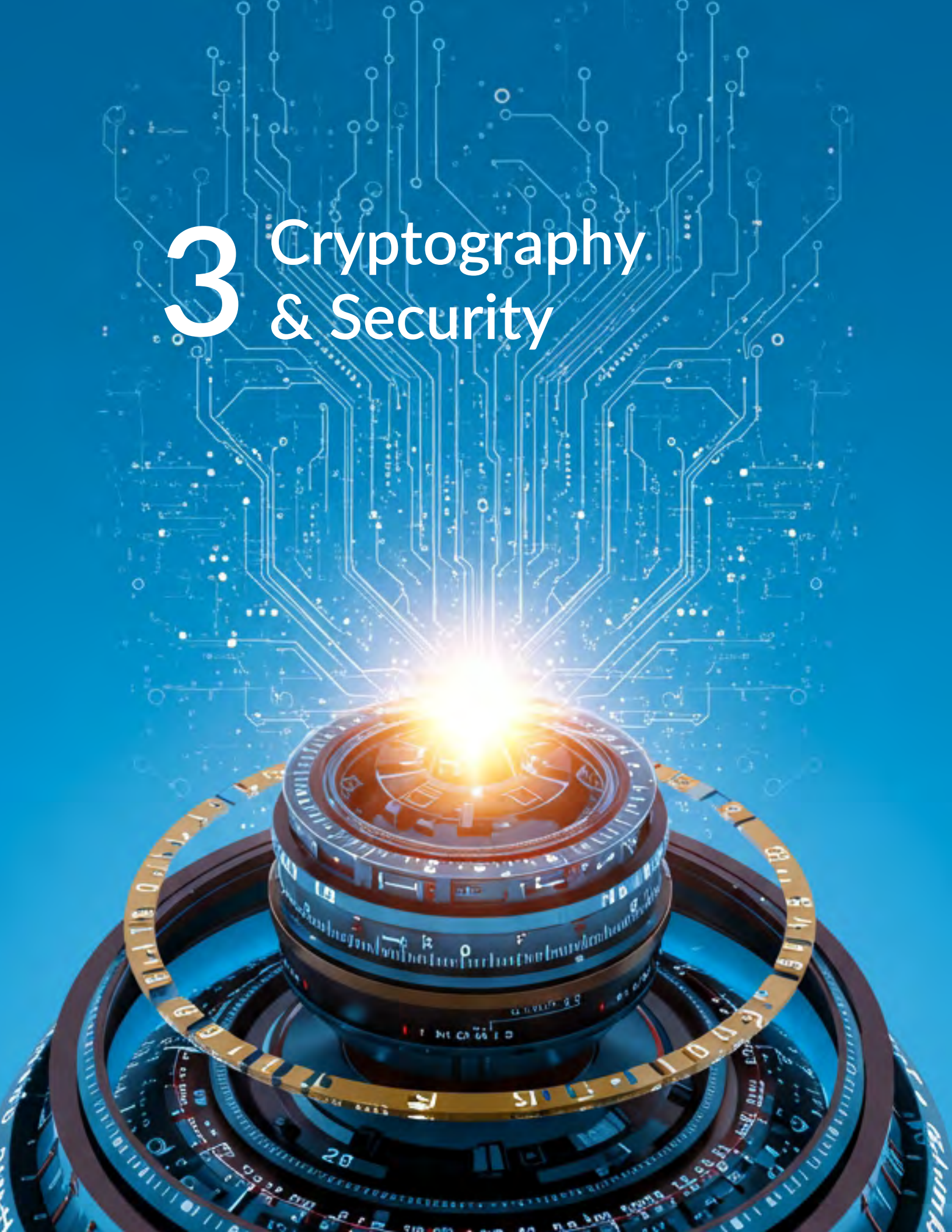
For example, in the problems solved by Google in 2019 and 2024, the tasks were mathematically well-defined but had no known practical use.

Therefore, the result is referred to as quantum supremacy, not quantum advantage.

While quantum supremacy has arguably been demonstrated, no one has yet experimentally proven that quantum computers are faster than classical computers on problems with real-world applications—such as those in biochemistry, logistics, or finance.

Achieving this would mark a major milestone in the development of quantum computing.

3 Cryptography & Security



Which encryption standards are most vulnerable?

An *encryption standard* is a method used to transform information into a form that can´t easily be connected back to the original.

We call the original *plaintext* and the transformed version *ciphertext*.

Most contemporary digital encryption standards are based on mathematical problems that are difficult for classical computers to solve.

The standards most vulnerable to quantum computing are those based on mathematical problems that quantum algorithms will be able to solve efficiently in the near future.

For example, *RSA*, widely used to secure digital data over the internet, relies on the difficulty of integer factorization, and *ECC* (Elliptic Curve Cryptography) is based on the discrete logarithm problem.

The problem is that *Shor's algorithm* can break both!

The day a sufficiently large quantum computer becomes available, it will be able to break these encryption systems in a relatively short period of time, making them some of the most vulnerable standards in the quantum era.

It is expected that this could happen within the next 5 to 10 years.

How long until RSA can be broken by quantum computing?

This is difficult to predict, but some experts estimate that it could be achieved within the next 5 to 10 years.

Of course, this timeline depends heavily on advancements in quantum hardware.

Some experts have estimated that breaking RSA encryption using Shor's algorithm would require a fault-tolerant quantum computer with millions of physical qubits—something we are still far from achieving.

However, given the rapid pace of research, particularly in quantum error correction and qubit coherence, this milestone could be reached sooner than expected.

Additionally, not all companies or governments disclose their full research efforts to the public, making accurate predictions even more difficult.

Is ECC more or less vulnerable than RSA?

Yes, ECC (Elliptic Curve Cryptography) is actually more vulnerable than RSA when it comes to quantum attacks.

While Shor's algorithm can break both RSA and ECC, ECC uses significantly smaller key sizes, which means it requires fewer physical qubits to break.

Approximately 10 million qubits for RSA and only 1 million qubits for ECC.

This makes ECC a more accessible target for future quantum computers and is one of the reasons why organizations are starting to move away from it in preparation for the quantum era.

ECC is currently used in many systems, including popular cryptocurrencies like Bitcoin and Ethereum.

Is AES encryption still safe in a quantum world?

Let's first highlight a key difference between RSA and ECC on one hand, and AES on the other.

RSA and ECC are *asymmetric encryption methods (public-key cryptography)*, relying on two keys: a public key to encrypt and a private key to decrypt. These keys are mathematically linked.

In contrast, *AES (Advanced Encryption Standard) is a symmetric encryption algorithm*, meaning the same key is used for both encryption and decryption.

This key must be securely shared between parties.

Symmetric algorithms like AES are more resistant to quantum attacks than asymmetric ones.

Shor's algorithm can completely break RSA and ECC, but it can't break AES!

There is another algorithm called *Grover's algorithm*, which can speed up brute-force key searches in symmetric systems.

However, it would take approximately 2^{256} operations to brute-force AES-256 on a classical computer, and about 2^{128} operations using a quantum computer with Grover's algorithm—which is still considered strong.

As a result, AES is expected to remain a fundamental part of post-quantum cryptographic systems.

What does "quantum-safe" encryption mean?

Quantum-safe encryption refers to encryption methods that are secure against both classical and quantum attacks.

These methods are designed—unlike RSA and ECC—around mathematical problems that are currently considered hard for both classical and quantum computers to solve.

This concept is closely related to *post-quantum cryptography*, which refers to the initiative to develop cryptographic algorithms designed to ensure data remains secure even against powerful quantum computers capable of running algorithms like Shor's and Grover's.

What is post-quantum cryptography (PQC)?

Post-quantum cryptography (PQC) refers to the creation, and increasingly the implementation, of a set of cryptographic algorithms designed to be secure against the capabilities of quantum algorithms running on quantum computers.

These new algorithms are based on mathematical problems that are not known to be

solvable efficiently by quantum algorithms like Shor's and Grover's.

Examples of such problems include lattice problems, multivariate polynomials, code-based schemes, and hash-based signatures.

Due to the threat that quantum computers pose to sensitive data, such as military and financial data, in December 2024 the National Institute of Standards and Technology (NIST) standardized several PQC algorithms to supplement or completely replace existing cryptographic systems.

NIST has established that by 2030, federal agencies should consider current standard encryption methods vulnerable, and by 2035, they are expected to be disallowed.

Banks haven't yet established a timeline for transitioning to post-quantum cryptography.

Will all existing encrypted data be compromised?

Potentially, yes.

The concern is that not only could future data be compromised, but data that is transferred or stored today could also be decrypted by quantum computers in the future.

In fact, malicious actors may already be collecting encrypted data with the intention of decrypting it once quantum computing capabilities become available.

Although there is no concrete evidence that this is currently happening, it remains a plausible threat.

This is why it is critical for organizations handling long-term sensitive data to begin transitioning to *quantum-resistant encryption methods*.

What are hybrid cryptosystems, and should we use them?

Transitioning to a fully quantum-safe infrastructure—especially for institutions like banks—is costly and may take many years to complete.

To begin moving in that direction, experts recommend adopting *hybrid cryptosystems*, which combine traditional (classical) encryption algorithms—less expensive and faster to implement—with quantum-resistant algorithms, which may require new types of technology and infrastructure.

This combination provides protection against both classical and future quantum attacks and is particularly useful during the transition phase.

Is Quantum Key Distribution (QKD) a realistic option?

Quantum Key Distribution (QKD) is considered one of the most secure methods of encryption because it relies not on complex mathematical problems, but on the fundamental laws of physics.

Information exchange is protected by principles of quantum mechanics—most notably, the no-cloning theorem and the fact that measurement inherently disturbs the system being observed.

While QKD offers strong theoretical security, its practical implementation is currently limited by high costs, the need for specialized hardware, and distance constraints.

As a result, QKD is best suited for niche applications—such as in government or high-security financial sectors—that can afford dedicated infrastructure. For most businesses, including most banks, it is not yet a broadly scalable solution.

Are blockchain-based systems at risk?

Yes, blockchain systems—especially those that rely on elliptic curve cryptography (ECC) for digital signatures, such as Bitcoin and Ethereum—are vulnerable to quantum attacks. A sufficiently powerful quantum computer running Shor's algorithm could, in theory, derive private keys from exposed public keys.

This would enable an attacker to forge signatures and potentially take control of wallets or validate fraudulent transactions.
While the underlying data structure of blockchains—the distributed ledger itself—is relatively robust and tamper-resistant, the cryptographic primitives that secure identities and transactions are not quantum-safe.

To ensure the continued security, integrity, and trust of these systems, blockchain platforms will need to transition to quantum-resistant cryptographic algorithms.

This transition poses significant challenges due to the decentralized nature of these networks, but it is increasingly recognized as a necessary step for long-term resilience.

4 Financial Sector Threats

How will quantum computing impact financial transactions?

Currently, financial transactions are secured using cryptographic systems such as *RSA and ECC (Elliptic Curve Cryptography)*.

However, Shor's algorithm—a quantum algorithm designed to efficiently factor large integers—poses a serious threat to these systems.

Once sufficiently powerful quantum computers become available, which many experts anticipate within the next decade or so, Shor's algorithm could effectively break the cryptographic foundations of RSA and ECC.

These encryption methods protect the integrity and confidentiality of sensitive financial data, including transaction details and stored records.

A quantum-capable adversary could, in theory, intercept encrypted financial transactions and manipulate them—altering the amount, recipient, or even the sender—potentially leading to large-scale financial fraud and systemic risk.

That is one of the key reasons why financial institutions and cybersecurity experts are actively developing and beginning to adopt quantum-resistant cryptographic algorithms to ensure long-term data security in a quantum future.

What about quantum attacks on banking infrastructure?

Banks protect customer data using a range of security technologies.

They implement internal authentication and authorization systems, as well as *Virtual Private Networks (VPNs)*.

To connect to third-party services, they use secure *Application Programming Interfaces (APIs)*, typically protected by *Transport Layer Security (TLS)*.

The issue with these protection systems is that they rely on classical cryptographic algorithms such as RSA, ECC, and Diffie–Hellman.

While these algorithms are considered secure against today's threats, they are not resistant to quantum attacks.

Once large-scale quantum computers become available—within a decade, as most experts estimate—they could break the mathematical foundations of these cryptosystems.

This quantum vulnerability poses a significant risk to the backbone of modern banking infrastructure, and banks should be actively preparing for it.

Could quantum computing undermine digital signatures?

Digital signatures are used to verify transactions, validate contracts, and ensure the authenticity of software and digital communications.

Trust in the financial system and the technology industry relies on them.

However, digital signature algorithms such as *RSA*, *DSA (Digital Signature Algorithm)*, *and ECDSA (Elliptic Curve DSA)* are vulnerable to large quantum computers capable of running Shor's algorithm.

The implications are serious: trust in financial transactions, legal documents, identity systems, and software integrity could all be compromised.

Addressing this threat is a major challenge for the future of cybersecurity.

That is why efforts are underway to develop and standardize quantum-resistant digital signature schemes.

Will smart contracts need reworking for quantum safety?

A smart contract is a program that lives on a blockchain and enforces rules automatically once the conditions of an agreement are met, without the need for intermediaries.

Many blockchains use *elliptic curve cryptography (ECC)* for validating transactions and verifying signatures associated with smart contracts.

If these cryptographic keys are exposed, a quantum attacker could potentially forge signatures, enabling unauthorized actions or contract manipulation.

Because of this threat, smart contracts—and the blockchains they operate on—will require substantial updates to maintain security.

Future smart contracts must integrate post-quantum signature schemes to remain secure as quantum-safe standards are developed and adopted.

Can current authentication protocols survive quantum threats?

An *authentication protocol* is a set of rules and procedures that verify the identity of a user, device, or system before granting access to resources or services.

Most current authentication protocols—such as *OAuth 2.0*, *SAML (Security Assertion Markup Language)*, *and FIDO2/WebAuthn* used in banking—rely on cryptographic algorithms built on mathematical problems that are vulnerable to quantum computing.

The key exchanges and digital signatures they use could be broken by sufficiently powerful quantum computers.

Without upgrades, these protocols may become ineffective against quantum-level adversaries within the next 10 years, according to some estimates.

Transitioning to hybrid or fully quantum-resistant versions of these protocols is crucial to ensure that authentication remains reliable in the coming decade.

Are SWIFT and interbank systems ready for this shift?

SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a global messaging network used by banks and financial institutions.

It does not move money itself but transmits secure messages related to financial transactions.

Other interbank messaging systems operate in a similar manner.

Since these systems rely on digital signatures for authentication and integrity, they are not currently resistant to the threat posed by large quantum computers.

To remain secure, they will need to be updated with quantum-resistant cryptographic protocols.

Will cryptocurrencies need to fork to remain secure?

A fork is essentially a significant update or change to a blockchain's underlying protocol used by a cryptocurrency.

Given the threat posed by quantum computers, most major cryptocurrencies—especially those using ECC for wallet addresses and transaction verification—will likely need a hard fork to integrate quantum-safe cryptographic algorithms.

Without this, quantum attackers could derive private keys from public keys, which in turn could lead to stealing funds or impersonating signatures.

Some blockchain projects are already exploring post-quantum upgrades, but widespread adoption will require careful planning and community consensus.

Could quantum computing cause a financial "zero day"?

A zero-day refers to the sudden exploitation of previously unknown vulnerabilities—in this case, related to quantum computing—before defenses are in place.

If quantum computing reaches a critical capability before financial institutions are adequately prepared, the risk becomes very real.

Such an event could result in massive theft, fraud, or a collapse of trust in digital financial systems.

How should hedge funds think about secure storage?

Hedge funds handle highly sensitive information and must make data security a top priority.

If the budget permits, they should begin by auditing their current data storage practices through the lens of emerging quantum computing risks.

Protecting client information—both past and present—as well as transaction records, intellectual property, and other confidential data is essential.

This protection must account for the potential of quantum computing to compromise both the integrity and secrecy of stored information.

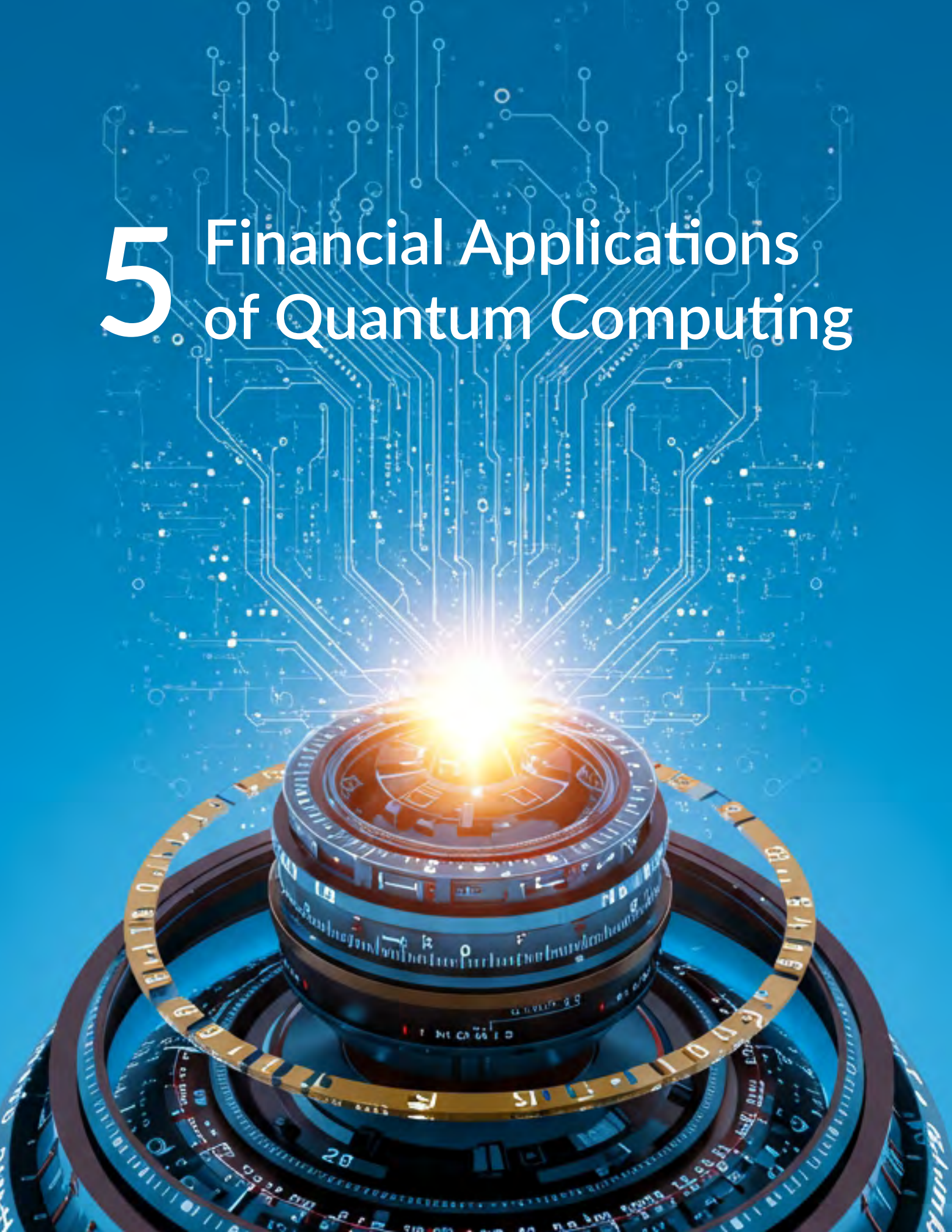
What should custodians do today to protect digital assets?

Due to the threat posed by large quantum computers—potentially emerging within the next 5–10 years—custodians of digital assets should ideally begin adopting hybrid classical and quantum-resistant cryptographic models.

The most effective approach is to stay informed about technological developments in the field, including both the theoretical foundations and practical implementations of quantum-resistant algorithms, as well as ongoing efforts such as NIST's standardization of post-quantum cryptography.

Custodians should also evaluate the quantum resilience of their wallet technologies, transaction signing mechanisms, and secure communication channels to ensure their platforms can transition smoothly as quantum capabilities evolve.

5 Financial Applications of Quantum Computing



Can quantum computing improve risk modeling?

Estimating risk in financial scenarios is a complex task, and traditional methods often struggle with large datasets and intricate dependencies, leading to slow or approximate results.

Quantum algorithms have the potential to significantly enhance risk modeling by enabling more efficient computation of complex, high-dimensional scenarios.

Algorithms such as *Quantum Amplitude Estimation (QAE)* can offer a quadratic speedup over classical Monte Carlo simulations, which are widely used to calculate key risk metrics such as *Value-at-Risk (VaR)* and expected shortfall.

Other techniques—including *Quantum Monte Carlo*, *variational quantum algorithms*, *and quantum machine learning*—are being actively explored to better capture non-linear risk factors, correlations, and extreme events.

As quantum hardware matures and algorithm research advances, these methods are expected to more accurately model and compute realistic risk scenarios, offering a significant improvement over current approaches.

Will portfolio optimization be transformed?

Portfolio optimization is one of the holy grails of finance, and many in the field believe quantum computers have the potential to outperform classical approaches.
However, we are not there yet.

It is well known that classical algorithms struggle with large, complex datasets and constraints in portfolio optimization.

Experts in quantum computing for finance believe that quantum methods can eventually enhance or accelerate these calculations.

There is some early evidence to support these expectations.

For instance, algorithms like the *Quantum Approximate Optimization Algorithm (QAOA)* have shown promise in addressing binary optimization problems—specifically, *Quadratic*

Unconstrained Binary Optimization (QUBO) problems—which are notoriously difficult for classical computers to solve efficiently.

As quantum algorithms continue to evolve, they may become capable of solving increasingly complex optimization tasks that are currently intractable.

In particular, hybrid quantum-classical algorithms and quantum annealing could offer faster or more efficient solutions, potentially leading to improved asset allocation strategies.

Can we use quantum tools for arbitrage opportunities?

Arbitrage involves exploiting price discrepancies across markets, which requires the ability to quickly process large datasets and identify patterns.

Quantum computers, with their ability to process vast amounts of data far more efficiently than classical computers, could offer a faster and more effective way to evaluate market conditions.

This could potentially uncover arbitrage opportunities that would be difficult, if not impossible, for classical computers to detect.

Such advancements could give traders a significant edge in executing profitable trades in real-time.

However, this remains a possibility that is still under active research, and the full potential of quantum computers in this area will become clearer as hardware and algorithms continue to develop.

Over the next 3 to 5 years, it should become more apparent how quantum computing can specifically enhance arbitrage strategies.

Could it make pricing derivatives faster or better?

Pricing complex derivatives, such as options, is one of the core challenges in finance, involving sophisticated models based on stochastic processes.

These models often require significant computational resources to produce accurate pricing, particularly when dealing with numerous variables.

In theory, quantum computing could make derivative pricing both faster and more accurate.

For example, quantum algorithms like *Quantum Monte Carlo (QMC)* could dramatically reduce the time required to simulate various pricing scenarios and calculate the fair value of derivatives.

By leveraging quantum speedups, financial institutions could enhance pricing accuracy, particularly in volatile market scenarios.

What role might it play in stress testing?

Stress testing refers to the evaluation of the performance of financial instruments or institutions under extreme but plausible adverse scenarios.

Traditional stress testing can be computationally expensive and time-consuming due to the complex interdependencies of risk factors.

Quantum computers, in theory, could enable faster simulations of various worst-case scenarios.

If realized, they would provide quicker and more accurate assessments of financial systems under stress, offering better tools for risk managers to prepare for potential systemic shocks.

As of now, though, quantum computing for stress testing is still largely in the research phase.

Is quantum Monte Carlo different from classical Monte Carlo?

Yes.

Quantum-enhanced Monte Carlo—often referred to as *quantum Monte Carlo (QMC)—differs from classical Monte Carlo (MC)* methods.

Classical Monte Carlo relies on random sampling to approximate solutions to complex problems.

QMC leverages a quantum algorithm called amplitude estimation, which can significantly accelerate the convergence of results.

In theory, this can provide a quadratic speedup over classical Monte Carlo, making QMC especially promising for computationally intensive tasks such as pricing complex financial derivatives or simulating large-scale financial systems.

However, while the theoretical speedup is well established, practical implementation of QMC is highly complex.

Challenges related to noise, error correction, and algorithm design mean that it's still uncertain whether QMC can consistently outperform classical Monte Carlo in real-world applications—at least with current quantum hardware.

How might quantum computing benefit credit risk analysis?

Credit risk involves a nuanced trade-off between potential financial returns and the probability of borrower default.

The intricate interdependencies among financial instruments, counterparties, and market conditions make credit risk modeling computationally intensive and analytically complex. While classical models remain the backbone of current risk assessment frameworks, quantum computing may offer future advantages by accelerating specific tasks such as portfolio optimization, high-dimensional simulations, and probabilistic inference—areas where classical methods often struggle with scalability.

Although practical applications of quantum computing in finance are still in the early stages, research suggests that quantum algorithms could eventually enhance the speed and scope of credit risk simulations—for example, by improving machine learning processes through quantum acceleration.

However, realizing these benefits depends on continued advances in quantum hardware and the development of suitable hybrid quantum-classical algorithms.

Can quantum speed up macroeconomic simulations?

Traditional economic models—such as Monte Carlo simulations—require substantial computational resources to simulate and forecast macroeconomic indicators like GDP growth, inflation, and unemployment rates, particularly when incorporating global interdependencies.

Quantum computers have the potential to accelerate specific tasks such as stochastic sampling and optimization, which are central to many economic models.

This could lead to more accurate and timely forecasts, enabling better policy decisions and more adaptive economic planning.

Realizing this potential will depend on advances in quantum hardware and the development of compatible algorithms and software.

Nonetheless, both government institutions and private financial organizations are actively exploring these technologies to meet the future demands of the industry.

Will high-frequency trading (HFT) be revolutionized?

High-frequency trading (HFT) involves executing a large number of trades at extremely high speeds to capitalize on small, short-term price movements in financial markets.

It relies heavily on real-time data analysis and the ability of the trading system to process data and respond as quickly as possible to gain a competitive edge.

Quantum computing, with its expected ability to perform complex calculations at unprecedented speeds, has the potential to transform HFT by analyzing market data more efficiently and uncovering patterns that are difficult or impossible for classical systems to detect in real-time.

Quantum algorithms could also improve signal detection, enabling more sophisticated and timely trading strategies.

Are there practical tools for financial analysts yet?

Major quantum computing companies, such as IBM and D-Wave, are developing quantum software frameworks for finance-related applications, including optimization and risk analysis.

However, these tools are still in the early stages of development.

While quantum algorithms have been demonstrated in research environments, there is not yet widespread access to ready-to-use software for financial analysts.

As quantum hardware continues to mature, the software is expected to become more accessible and practical for everyday use by financial professionals.

6 Strategic Planning & Risk Management

When should firms start preparing for post-quantum risks?

Some institutions and organizations are more vulnerable to quantum threats than others, depending on their sector.

For example, *government bodies*—such as defense departments, intelligence agencies, and electoral systems—store highly sensitive data.

Telecommunications and *tech giants* are at risk due to the vast amounts of private data and communications they handle.

Financial institutions are also critical targets, as they manage transactions and client data essential to the financial stability of nations and regions.

These sectors should begin preparing for post-quantum risks as soon as possible. Although practical quantum computers capable of breaking current cryptographic systems do not yet exist, their arrival is inevitable and the transition to quantum-resistant encryption will take years.

Early preparation allows organizations to assess vulnerabilities and begin updating their cryptographic infrastructure.

Ideally, businesses should have transitioned to PQC solutions within the next three to five years to ensure mid-term security.

However, this timeline is widely considered overly optimistic, and most institutions are unlikely to meet it without significant effort and coordination.

Should we audit our current cryptography now?

This depends on the size and nature of your organization.

If you're in one of the high-risk sectors—such as telecommunications, finance, or government—auditing your current cryptographic systems is essential.

Understanding the vulnerabilities in your existing encryption is a critical first step in planning the transition to quantum-safe alternatives.

A thorough audit helps identify which systems are at risk and supports informed decision-making about necessary upgrades.
This may include implementing *hybrid solutions*, where both classical and quantum-resistant algorithms are used together to minimize potential security gaps during the transition phase.
Ultimately, the long-term goal is to fully transition to *quantum cryptographic methods*, with no reliance on classical algorithms, to ensure data remains secure well into the future.

How do we identify quantum vulnerabilities?

Identifying quantum vulnerabilities requires a thorough assessment by experts of the cryptographic algorithms currently used across a company's information systems.

Systems that rely on public-key cryptography, such as RSA and ECC, are particularly vulnerable to quantum threats.

After conducting these vulnerability scans, the organization must stay updated on research related to quantum-safe algorithms and begin implementing them.

Transitioning to post-quantum cryptographic protocols is crucial for mitigating these risks and ensuring that the organization's data remain secure against future quantum threats.

Should CISOs be developing post-quantum migration plans?

CISO stands for *Chief Information Security Officer*.

These are senior executives within an organization responsible for overseeing and managing the organization's information and cybersecurity strategy.

Given their role and the threat posed by future large-scale quantum computers, it is clear that they must educate themselves about the risks quantum computing poses to their organization's data security.

With their expertise, and after educating themselves about the quantum threat, they should determine whether their organization requires an audit.

Based on the results of the audit, they may need to consider—and, in some cases, begin—implementing post-quantum migration plans.
Preparing for this transition should be treated as a strategic priority.

Is there an enterprise-wide roadmap for quantum readiness?

For large companies, this is a complex but often essential undertaking.

Regardless of industry or company size, the first step is to build awareness of the quantum threat within the information security team.

In some cases, a thorough audit may be necessary.

Following the audit, the organization can begin designing a roadmap that includes staff training and updates to its encryption technologies.

In addition to internal planning, the organization will likely begin collaborating with third-party vendors to ensure comprehensive readiness.

Given that quantum threats are expected to grow over time, developing a quantum readiness strategy should be a priority—especially for industries that collect sensitive data.

What is the "harvest now, decrypt later" threat?

The "harvest now, decrypt later" threat refers to the risk that cybercriminals may be intercepting and storing encrypted data today, with the intention of decrypting it in the future—once quantum computers capable of breaking current encryption standards become available.

While there is no concrete evidence that this is happening yet, the possibility that it may be occurring now or in the near future is particularly concerning for long-term sensitive information, such as financial or classified military data, which may retain value for years or even decades.

Because of this future threat, some financial organizations—particularly large firms—are beginning to plan the encryption of their data using quantum-resistant methods.

How do we prioritize systems for quantum protection?

Prioritizing systems for quantum protection requires balancing the sensitivity of the data with the vulnerability of the encryption in use.

Systems handling the most sensitive information—such as client data or data critical to business operations—should be prioritized.

At the same time, some existing systems are more resistant to quantum threats than others, so the relative strength of the cryptographic protections must also be considered. Therefore, prioritization should be based on factors such as data sensitivity, system criticality, and the expected timeframe in which quantum threats may become a reality.

What's the role of third-party vendors in this transition?

Most organizations that collect data—for example, in the financial sector—have information security teams.

However, many of them lack the in-house capability to audit cryptographic systems and make decisions about how to address the quantum threat.

That's why third-party vendors are essential to the transition to post-quantum cryptography.

Their role is to perform audits, provide solutions and products, and offer the expertise needed to help organizations implement quantum-safe protocols.

These vendors integrate quantum-resistant technologies into their offerings, including hardware, software, and cloud services.

Organizations rely on them to upgrade encryption methods and to support hybrid cryptosystems that bridge classical and quantum-safe cryptography.

Will there be insurance products for quantum risk?

It is worth noting that such insurance products do not yet exist.

However, as quantum threats become more imminent with advances in quantum hardware and software, it is likely that insurance products covering quantum risk will emerge.

Insurance companies may offer policies that cover damages resulting from quantum-enabled cyberattacks.

What role should the board play in quantum risk strategy?

Regarding the quantum threat, the board of a company should take an active role in ensuring that it is integrated into the overall risk management and cybersecurity frameworks.

Board members should collaborate closely with senior leadership, especially CISOs, to ensure that adequate resources—both human and financial—are allocated for the transition to quantum-safe encryption.

It is critical for the board to support proactive, long-term strategies that protect the organization's data, assets, and reputation.

7 Industry Landscape & Players

Which tech firms are leading quantum hardware development?

There are various types of quantum hardware, and different companies are developing them.

Google, *IBM*, and *Rigetti* are developing superconducting quantum computers. Most experts consider this technology to be the most advanced quantum hardware.

Another approach is trapped ion technology, pursued by companies such as *IonQ* and *Quantinuum*.

Trapped-ion technology is another promising approach to building quantum computers, often ranked alongside superconducting qubits as a leading candidate.

Photonics, which uses quantum properties of light to encode information, is being developed by companies like *PsiQuantum*.

Additionally, cold atom technology is under development by companies such as Xanadu and *Pasqal*.

Photonics and cold atom quantum technologies are definitely promising, but currently, they are generally considered less mature compared to superconducting qubits and trapped ions.

Microsoft is working on topological qubits, where quantum information is encoded within the global properties of certain materials.

Finally, quantum annealers are a distinct category, with D-Wave as the primary company in this field.

Are there startups worth watching in quantum cybersecurity?

Yes, several startups in quantum cybersecurity are gaining attention as quantum computing advances.

They focus on bridging the gap between current cryptographic standards and the need for post-quantum resilience.

Many are developing *post-quantum cryptography* solutions and quantum key *distribution* systems to address emerging threats.

Some of these companies are more established, while others are still in early stages. Together, they are key players to watch in the cybersecurity space as quantum technology continues to evolve.

How far ahead are IBM, Google, and Microsoft?

There appears to be a global consensus within the quantum computing community that *IBM* and Google are currently leading the charge in the field.

Both companies are developing superconducting qubit systems and have made significant progress in hardware and software.

IBM is advancing its quantum infrastructure and has also made strides in quantum-safe cryptography.

Google made headlines with its claim of *"quantum supremacy"* in 2019 using its Sycamore processor, and again in 2024 with its newer system, Willow.

Microsoft, meanwhile, is focused on developing topological qubits and has built an extensive quantum development ecosystem.

In 2025, it made headlines with its announcement related to *Majorana-based qubits*.

All three companies are pushing the boundaries of quantum computing, though practical, fault-tolerant quantum machines remain a goal still under active development.

Is there a "standard stack" emerging for quantum development?

In computer science, a "standard stack" is a commonly used set of tools and technologies to build, deploy, and run applications.

Since quantum computing is still an emerging field, a fully standardized stack has not yet been established.

However, a standard stack for quantum development is beginning to take shape.

For example, several quantum programming languages and frameworks—such as Qiskit (IBM), Cirq (Google), and Q# (Microsoft)—are gaining traction among quantum developers. Additionally, access to quantum hardware through cloud platforms like IBM Quantum, Azure Quantum, and Google Cloud Quantum is becoming increasingly common.

As quantum hardware, software, and algorithms continue to evolve, the industry is likely to see further movement toward standardization.

Are banks currently piloting quantum applications?

Yes, several major banks are investing significant resources—not only in terms of funding but also dedicated personnel—into quantum research and development.

Key areas of focus include risk analysis, portfolio optimization, and cryptography.

Banks such as *JPMorgan Chase*, *HSBC*, and *Wells Fargo* are collaborating with quantum computing companies like IBM and Rigetti to enhance computational efficiency and data security.

Although these initiatives are still in the early stages, the goal is to identify areas where quantum computing can provide a meaningful advantage over classical approaches—particularly for tasks involving large datasets and complex simulations.

What's the status of quantum adoption in Asia/Europe?

Across Europe and Asia (and also in North America), quantum adoption is steadily advancing, driven by strong investment in research, development, and public–private collaboration.

In Europe (as in North America), governments and industries have made significant commitments to quantum technologies, with applications spanning cybersecurity, finance, and healthcare.

In Asia, countries such as China, Singapore, South Korea, and Japan have also allocated substantial resources to quantum research.

Among them, China stands out as particularly advanced, taking an aggressive approach to developing nationwide quantum communication infrastructure and quantum cryptography.

While commercial adoption of quantum computing remains in its early stages globally, these regions are positioning themselves as future leaders in the quantum landscape.

Who's leading in quantum-related patents?

IBM, Google, and Microsoft are among the leaders in quantum computing across hardware, software, and algorithms.

The same holds true for quantum-related patents.

At the time of writing, IBM holds approximately 2,500 patents, Google around 1,500, and Microsoft about 1,200.

These three firms hold a significant portion of the intellectual property associated with quantum technologies.

IBM, in particular, has a large portfolio focused on quantum hardware, software, and cryptography, positioning it as a front-runner in the field.

In addition, startups and academic institutions are contributing to the growing body of patents related to quantum computing.

The increasing number of quantum-related patents signals the rapid pace of innovation and commercialization in this emerging field.

Are any financial services firms using quantum simulators?

A quantum simulator—more accurately referred to as a quantum emulator—is a classical computing system that mimics the behavior of a quantum computer.

It allows users to develop and test quantum algorithms without requiring access to physical quantum hardware.

In the financial sector, firms such as *JPMorgan Chase*, *HSBC*, and *Goldman Sachs* are actively using quantum simulators to explore potential applications of quantum computing, including portfolio optimization, market trend analysis, credit scoring, and fraud detection.

Are cloud-based quantum platforms secure?

Like most reliable internet services, cloud-based quantum platforms use strong encryption and access controls to ensure data security.

However, they are not secure against future threats posed by large-scale quantum computers running Shor's algorithm, which could break today's encryption standards.

This is why major cloud providers such as IBM, Microsoft, and Amazon are actively working to integrate post-quantum cryptography into their quantum services.

They must guarantee that clients' data remains protected at all times—during transmission, storage, and computation.

How do you compare IonQ, Rigetti, and D-Wave?

These are well-known companies in the quantum computing space, particularly in hardware development.

IonQ uses trapped-ion technology, which is known for its stability and precision in quantum operations.

However, like many quantum systems, it faces challenges related to scalability.

Rigetti focuses on building superconducting quantum computers and offers a hybrid quantum-classical platform, enabling more practical solutions for cloud-based quantum computing.

Superconducting qubits are considered by many experts to be the most mature quantum hardware technology at the time of writing, and possibly the first to achieve quantum advantage for solving real-world problems.

D-Wave, on the other hand, specializes in quantum annealing—a type of quantum computing that is not gate-based and is particularly effective for solving optimization problems.

Although D-Wave has been active in the field longer than some of its peers, some quantum computing experts remain skeptical about the actual achievements and long-term potential of its technology.

In contrast, the *gate-based approaches* used by IonQ and Rigetti are generally considered more versatile and scalable, making them better suited for executing a broader range of quantum algorithms.

8 Investing in Quantum Technology

Are there public companies to invest in quantum?

Yes, in addition to private entities investing in quantum ventures, there are also public companies in which individuals can invest.

For example, IBM, Google, Amazon, and Microsoft are all well-known public companies that are investing heavily in quantum computing research and development and are publicly traded.

Other publicly traded companies working on quantum technologies include Rigetti, IonQ, and D-Wave.

Given that quantum technology is still in the research and development phase, these stocks tend to be highly volatile.

What about venture capital activity in this space?

Venture capital activity in the quantum computing space is growing rapidly.

Firms like *Quantum Coast Capital* in the U.S., *Quantum Exponential* in the U.K., and *Quantonation* in France, are making notable early-stage investments in quantum technology companies.

These investments span all three key areas of quantum technology: quantum computation, quantum communication, and quantum sensing.

With practical applications of quantum sensing and quantum communication expected in the near future, interest in these domains is increasing significantly.

The influx of venture capital reflects strong confidence not only in the long-term potential of quantum computing but also in its near-term opportunities.

As a result, many startups are now scaling up thanks to this wave of private investment.

Are there ETFs focused on quantum technologies?

An *Exchange-Traded Fund (ETF)* is an investment fund traded on stock exchanges, similar to individual stocks.

Some ETFs invest in companies involved in quantum computing, quantum encryption, and other related technologies.

These ETFs provide investors with a diversified way to gain exposure to the quantum technology sector without having to pick individual stocks.

Notable ETFs include the *Defiance Quantum ETF (QTUM)* and the *Global X Future Tech ETF (QUBT)*, each with approximately $1.1 billion in assets under management (AUM).

How should we analyze quantum startups?

Analyzing quantum startups shares many aspects with evaluating other tech startups but also requires unique considerations due to the specialized and cutting-edge nature of quantum technology.

Common metrics include the technical capability of the team and established partnerships with academic institutions or large tech companies.

It's important to assess the stage and scalability of the quantum hardware or software the startup uses or develops, as well as their roadmap for transitioning from theoretical research to practical, scalable applications.

Another key factor is the strength of the startup's *intellectual property (IP)* portfolio.

Finally, how well the startup integrates with the broader quantum ecosystem can be a strong indicator of its potential for growth and adoption.

In addition to these factors, business-oriented startup metrics remain critical, including the ability to secure funding and a well-defined go-to-market strategy.

What's the M&A activity like in quantum tech?

Mergers and acquisitions (M&A) refer to the process by which two companies either combine into one or one is acquired by the other.

As quantum technology develops, tech companies are increasingly seeking to acquire or merge with promising quantum startups.

Since many quantum startups are still at an early stage and not yet mature, large companies are typically more interested in acquiring smaller ones rather than merging with them. That said, mergers have occurred.

The most notable example is *Quantinuum*, formed in 2021 through the merger of *Honeywell Quantum Solutions* (a hardware-focused company) and *Cambridge Quantum Computing* (a quantum software company).

This merger created one of the largest and most integrated quantum computing companies in the world, combining hardware, software, and algorithm development under one roof. The M&A trend is expected to continue as quantum computing becomes a more commercially viable and competitive industry.

Are there SPACs related to quantum computing?

Traditionally, a private company becomes publicly traded on a stock exchange by offering shares to the public.

The first offering and pricing of the stock is called an Initial Public Offering (IPO).

For example, *Quantinuum*, a quantum hardware company developing trapped-ion technology, is planning to go public through an IPO in the next couple of years.

The preferred method for quantum startups to go public, though, has often been through SPACs.

SPAC stands for *Special Purpose Acquisition Company*.

Here's how it works:

A company with no commercial operations is created and goes public with the sole purpose of acquiring or merging with an existing private company—in this case, a quantum company.

Several quantum companies have gone public through this process.

For example: *Rigetti* (superconducting qubits), *IonQ* (trapped-ion technology), and *D-Wave* (quantum annealing).

There are two clear advantages to this process:

1. It allows the startup to raise capital in about half the time it would take through a traditional IPO.
2. It provides investors with an opportunity to invest in quantum computing through a publicly listed vehicle.

While SPACs are an appealing option for quantum startups looking to raise capital, they can carry risks due to the speculative nature of quantum technology at its current stage.

How do quantum patents contribute to company valuation?

Quantum patents—in areas like hardware, software, algorithms, or encryption—are a key factor in assessing the value of quantum technology companies.

Beyond protecting innovation, a well-developed patent portfolio signals technical expertise and provides a strong competitive advantage.

For example, patents can generate revenue through licensing agreements.

In mergers, acquisitions, or strategic partnerships, a strong intellectual property position can significantly boost a company's negotiating leverage and overall market valuation.

Can we value early-stage quantum companies reliably?

Quantum computing remains largely in the research phase, and there is naturally a high level of uncertainty regarding the timelines for bringing quantum technologies to market.

As a result, valuing early-stage quantum companies can be challenging.

Traditional valuation methods may not be applicable in this context.

However, investors can focus on assessing several key factors: the state of the technology being developed, the team's expertise, the intellectual property portfolio, funding raised, market potential, and strategic partnerships.

Comparisons with similar past public deals can also be useful.

Additionally, market trends in the quantum technology sector are important for estimating a company's valuation.

What's the typical revenue model for a quantum startup?

The revenue model for quantum startups varies widely depending on the application area and the maturity of their technology.

One common approach for quantum software companies is licensing their intellectual property—particularly proprietary software platforms, tools, or implementations related to quantum algorithms and frameworks.

These may include simulators, hybrid quantum-classical integrations, and error mitigation techniques.

Another important revenue model is *Quantum Computing* as a Service (QCaaS).

In this model, quantum hardware providers offer remote access to quantum computers via the cloud, much like cloud computing services operate today.

Quantum software companies often build on top of this infrastructure to deliver domain-specific applications.

Because quantum computers are extremely expensive and complex to maintain, QCaaS provides a practical and scalable way for users to run quantum programs without owning the hardware.

Clients are typically charged based on quantum processing time, API access, or through subscription-based pricing plans.

In the cybersecurity space, quantum startups generate revenue by offering quantum-safe encryption solutions, particularly through post-quantum cryptography.

A smaller subset of startups also develops Quantum Key Distribution (QKD) systems, though these are typically more hardware-intensive and capital-demanding.

Additionally, many early-stage quantum startups provide consulting and training services to help organizations explore how quantum computing could be applied to industries such as finance, pharmaceuticals, logistics, and materials science.

As the technology matures, we can expect more diverse and sophisticated business models to emerge—adapting to both technical advancements and the evolving needs of different sectors.

How can quantum breakthroughs affect entire sectors?

It is unlikely that quantum computing will transform entire sectors; however, it will significantly impact key areas within them.

For example, in finance, quantum technology could revolutionize portfolio optimization, market trend analysis, credit scoring, and fraud detection.

Other financial activities, however, are likely to remain largely unaffected, such as most customer service operations and day-to-day accounting and bookkeeping.

In cybersecurity, quantum-safe encryption may change how sensitive data is protected. Still, in the financial sector, implementing quantum-based protection for all data storage—at least in the near term—may be too costly.

In such cases, post-quantum cryptography will likely offer a more practical solution.
In conclusion, while quantum technology may not overhaul entire industries, it is expected to transform substantial portions of their operations.

9 Policy, Regulation & Standards

What is NIST doing about post-quantum cryptography?

The threat posed by future large-scale quantum computers running Shor's algorithm can be addressed through two main approaches:

1. Developing new cryptographic algorithms based on mathematical problems that quantum computers cannot efficiently solve.
   This is the objective of *post-quantum cryptography (PQC)*.
2. Implementing fully quantum solutions, such as *quantum key distribution (QKD)*, whose security is based on the fundamental laws of quantum mechanics.

The *National Institute of Standards and Technology (NIST)* is leading global efforts to standardize PQC algorithms. In 2016, NIST launched a public competition to evaluate and select algorithms that are resistant to quantum attacks.

In 2024, after years of rigorous evaluation, NIST announced a set of new quantum-safe cryptographic standards that U.S. government agencies are now required to begin adopting.

Will regulation require companies to adopt PQC?

At the time of writing, since the National Institute of Standards and Technology (NIST) is a non-regulatory agency, it does not require the private sector to comply with the *post-quantum cryptography (PQC)* standards announced in December 2024.

Currently, only federal agencies and institutions such as government offices and military organizations are mandated to begin adopting PQC.

Other critical infrastructure sectors—such as finance, healthcare, and transportation—are expected to follow suit in the future.

However, the cost, complexity, and time required to implement these new cryptographic standards present significant challenges.

Some experts suggest that, over time, companies that fail to transition to quantum-safe standards may face increased legal, regulatory, or compliance risks.

Is there guidance from the NSA or other agencies?

As the government agency responsible for the collection and processing of information for intelligence and counterintelligence purposes, the *NSA (National Security Agency)* is also tasked with protecting this information.

Consequently, it leads national efforts in cybersecurity, including securing data systems and communications.

Recognizing the emerging threat of quantum computing, the NSA has urged both government and private sector organizations to begin preparing for quantum readiness—particularly for systems that require long-term confidentiality.

This aligns with broader federal efforts, including *NIST's* standardization of post-quantum cryptographic algorithms.

Will quantum readiness be part of cybersecurity audits?

As future large-scale quantum computers pose new risks to standard cryptographic systems, auditors will need to evaluate an organization's preparedness for transitioning to quantum-safe encryption.

This includes assessing whether companies have updated their cryptographic protocols (for example, by following guidance from NIST), identified potential quantum vulnerabilities, and developed a tailored roadmap for adopting post-quantum cryptography.

Going forward, audits will also examine whether organizations are complying with regulations related to quantum security.

Are there international standards being developed?

In addition to the *National Institute of Standards and Technology (NIST)*, other regional and international organizations are actively developing quantum-safe cryptographic standards.

Since quantum threats are a global concern, bodies such as the *European Telecommunications Standards Institute (ETSI)* and the *International Organization for Standardization (ISO)* are working, in coordination with NIST, to establish global standards for quantum-resistant encryption.

These efforts aim to ensure that quantum-safe technologies are adopted worldwide to protect the international transfer of sensitive information, such as cross-border data exchanges and military communications.

Is legislation around data privacy quantum-aware?

Currently, most data privacy legislation does not explicitly address quantum threats. For example, in the financial sector, the *Gramm-Leach-Bliley Act (GLBA)* in the United States and the *General Data Protection Regulation (GDPR)* in the European Union do not take into account the risks posed by large-scale quantum computers.

However, as quantum computing technology advances, it is likely that legislators and regulators will begin incorporating quantum-awareness into data privacy frameworks. This presents a significant challenge, as it will require data-collecting organizations—such as Big Tech firms and financial institutions—to upgrade their encryption protocols.

This transition will demand both time and substantial investment, making it a complex process for widespread implementation.

Will financial regulators issue their own frameworks?

Given the potential impact of quantum computing on the financial sector, it is likely that financial regulators will start issuing dedicated regulatory frameworks.

Since the threat quantum computers pose to data encryption is expected to be one of the earliest effects of quantum technology on finance, the first regulatory frameworks will almost certainly focus on quantum security.

Regulatory bodies such as the U.S. *Securities and Exchange Commission (SEC)*, which is responsible for enforcing federal securities laws and protecting investors, and the *European Central Bank (ECB)*, which oversees monetary policy and financial stability in the euro area, may develop guidelines specifically aimed at ensuring quantum resilience in data storage.

These initial regulations will likely encourage—or even require—the financial industry to adopt quantum-safe encryption.

Could noncompliance with quantum standards become a liability?

Quantum security standards have not yet been enacted.

However, once they are approved—and as quantum threats become more tangible—noncompliance could become a significant liability.

Regulators are likely to impose legal consequences for failing to adopt quantum-safe cryptographic measures, particularly in industries that handle sensitive data, such as finance and government.

Based on past experience, we can expect that noncompliant organizations—banks, for example—could face regulatory fines, legal action, or reputational damage if their systems are compromised due to outdated or vulnerable encryption.

In the future, maintaining compliance with quantum security standards may become essential for both legal protection and operational resilience.

Are current compliance tools adaptable to quantum transition?

Many of today's compliance tools, such as the software platforms *RSA Archer and MetricStream*, focus on managing risks related to classical systems.

Since they are designed primarily for non-quantum environments, these tools may require significant adaptation to address the challenges posed by the quantum transition.
Such adaptation could involve integrating quantum-safe cryptographic standards into existing compliance platforms.

The goal is for compliance tools to evolve alongside advances in quantum technology, ensuring effective quantum risk management throughout the transition.

How will Basel III/IV interact with quantum security frameworks?

Basel III and Basel IV are regulatory frameworks developed by the Basel Committee on *Banking Supervision* to strengthen regulation, supervision, and risk management within the banking sector.

At present, the Basel III/IV frameworks do not incorporate quantum security considerations.

However, given the emerging quantum threat, these frameworks will likely need to include quantum security requirements in the future—particularly concerning the protection of financial data storage.

Consequently, financial institutions will need to adopt quantum-safe cryptography to remain compliant with updated Basel standards and to mitigate systemic risks.

10 The Future & Big Picture

Could quantum computing cause systemic financial risk?

Yes, quantum computing has the potential to affect the entire financial system.

Because they can break widely used cryptographic methods, quantum computers could compromise the security of stored financial data and digital transactions worldwide.

If financial institutions are unprepared, this may lead to widespread breaches, financial instability, and a loss of trust in the integrity of digital assets.

Beyond cryptographic risks, quantum computing could also disrupt financial models that rely on classical computational assumptions.

Institutions that fail to prepare for the quantum transition could face these risks directly—making it essential to begin migrating toward quantum-safe technologies.

How does quantum computing compare to AI in impact potential?

Let's be cautious about predictions.

However, it may be that the potential of quantum computing to transform society is much greater than that of artificial intelligence (AI).

Two limitations of AI that quantum computing may overcome are:

1. AI relies on classical algorithms, so the correlations it uncovers from data are classical in nature.
   Quantum computers, however, can reveal correlations beyond classical computation—insights that standard computers simply cannot detect.
2. The energy consumption and physical miniaturization limits of classical computers constrain the capabilities of current AI systems.

Quantum computers have the potential to surpass these limitations and tackle complex problems in fields such as biochemistry, materials science, and finance.

Quantum computing researchers are also exploring the possibility that quantum computers may consume significantly less energy compared to the ever-increasing

energy demands of traditional computers running complex AI algorithms.

For example, it is estimated that generating a high-quality image with AI models like ChatGPT consumes energy roughly equivalent to fully charging a mobile phone—an unsustainable trend.

Quantum computing could help alleviate such energy burdens.

Are we looking at another dot-com moment or a paradigm shift?

The quantum computing revolution is expected to be far more impactful than the internet revolution.

While the internet has transformed almost every aspect of modern society—from education to banking, and transportation to medicine—the potential impact of quantum computing could be even greater.

Quantum computers may not only accelerate processes that classical computers currently handle, such as discovering new treatments for diseases like cancer or Parkinson's, but they are also expected to solve problems that classical computers fundamentally cannot. At present, this remains speculative, and there is no definitive proof that quantum computers will achieve such levels of performance.

However, many experts are confident that this could become a reality in the not-too-distant future.

Mastering quantum technologies will represent a radical paradigm shift in technical capabilities.

Additionally, numerous new questions and challenges will emerge once this technology becomes accessible.

Could quantum computing democratize finance or create inequality?

Quantum computing has the potential to do both—and it likely will.

On one hand, quantum computers could enable better, more affordable financial services, especially benefiting people in developing countries where many still lack access to banking.

On the other hand, the investments required for quantum technologies—both financial and human—are substantial, and not all countries or companies can afford them.

This could widen the gap between industrialized and developing countries.

Even within industrialized nations, smaller companies may struggle to adopt quantum technologies, similar to what has been observed with AI, where larger firms gain the most advantage, potentially increasing inequality.

Only time will tell, but like AI, quantum computing raises significant ethical and societal concerns.

How will quantum influence fintech and neobanks?

That's difficult to predict with certainty.

The fintech ecosystem is highly dynamic and receptive to technological transformations. One fascinating possibility is Big Tech capturing market share from traditional financial institutions.

Big Tech companies not only collect vast amounts of data that can be leveraged to provide financial services to their users, but they are also at the forefront of developing future quantum computing technologies.

For example, Google has access to data from hundreds of millions of users across its various platforms.

Additionally, Google is a leader in quantum computing research.

This powerful combination of Big Data and quantum technology positions Big Tech to potentially create emerging financial organizations in the near future.
At stake are trillions of dollars!

Is there a risk of a "quantum arms race" among institutions?

Private organizations and public institutions—especially in sectors like pharmaceuticals, finance, defense, and information security—are already competing to develop and deploy quantum technologies that offer a strategic advantage.

This race could result in unequal access to quantum capabilities, with certain institutions or countries gaining advantages in securing data, performing high-speed computations, or breaking traditional encryption methods.

Such competition may, for example, lead to increased tensions between countries or regions, and potentially deepen global divides.

For this reason, there will likely be a need for international collaboration and regulation to ensure the responsible development and use of quantum technologies.

Will quantum computing disrupt trading algorithms?

Quantum computing researchers in finance are actively exploring ways to accelerate and enhance trading algorithms.

The focus is on developing quantum algorithms for tasks like portfolio optimization, risk analysis, and Monte Carlo simulations—problems that are computationally intensive on classical machines.

Quantum advantage in these areas could lead to new trading strategies and significant shifts in market dynamics.

However, this remains largely in the research and experimental stage.

If realized in the future, the integration of quantum computing into trading systems could fundamentally alter how financial markets function—creating both opportunities for innovation and challenges for oversight and regulation.

What educational resources should investment professionals explore?

Quantum physics, and quantum computing in particular, are difficult conceptual and highly mathematical subjects.

To think that a finance student or professional will be able to understand quantum computing by itself in the short term is delusional.

There are some online resources, some of them free, that can be used.

Their efficacy, though, is disputable.

The best way for someone with a finance background to learn quantum computing is to hire a professional knowledgeable in the subject and take private lessons.

Not all individuals are the same, of course, and a tailored solution should always be sought.

But in general, buying a formal textbook on quantum computing or watching YouTube videos is not a good use of time.

You will likely just waste your time.

For most finance professionals, the best approach is to take private lessons with an experienced quantum expert.

How can firms develop internal quantum literacy?

Quantum education is one of the most urgent priorities for private organizations today.

Many firms raise strong objections to adopting quantum computing, with the most common being that their current systems are efficient and quantum computers aren't imminent.

As a result, many believe they can safely ignore quantum computing for now.

However, this view is inaccurate and carries significant risks.

Larger firms are certainly more vulnerable, but most companies should begin considering the implications of quantum computing sooner rather than later.

There are several ways firms can start building quantum literacy.

They can, for example, hire experts to provide targeted training or bring in quantum computing professionals who can raise quantum awareness within existing teams, thereby laying the groundwork for more advanced implementations in the future.

What's the biggest myth about quantum computing?

Perhaps the biggest myth about quantum computing is that quantum computers will replace classical computers.

This simply isn't true—at least, there's no reason to believe so today.

For example, you'll most likely never own a quantum mobile phone.

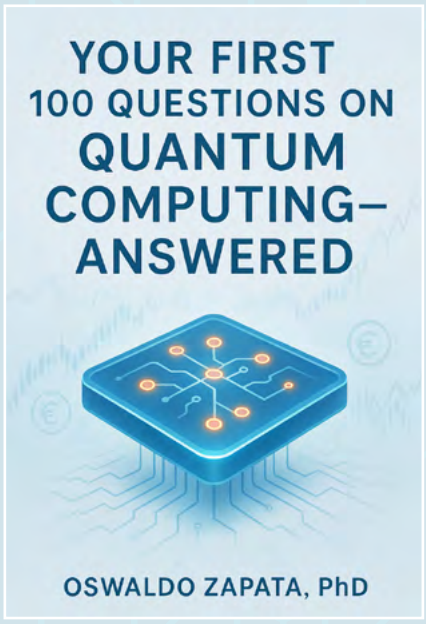
In fact, it's widely believed that classical and quantum computers will coexist, working together rather than in isolation.

Quantum computers will handle specific problems that are difficult or impossible for classical machines, while classical computers will continue managing everyday tasks.

So don't expect classical computers to disappear anytime soon—or maybe ever.

It's like using your fingers to add simple numbers: there's no need to grab your phone for that.

Classical computers will remain essential for a long time.



What's Next?

I hope you've found this practical book helpful—and that you'll come back to it as you continue along your quantum journey.

As quantum technologies mature, it's essential for financial professionals to stay ahead of the curve and understand the impact these advances will have on the industry.

The shift from classical to quantum systems won't be simple, that's for sure—but those individuals and institutions who start preparing now will be the ones leading the way in the years to come.

Wishing you all the best as you continue exploring the quantum world.

If you'd like to connect or learn more, don't hesitate to reach out to me on LinkedIn:

https://www.linkedin.com/in/oswaldo-zapata-phd-quantum-finance/

RiskMathics
FINANCIAL INSTITUTE