SCBX QUANTUM OUTLOOK 2026:
The Unfiltered Truth of Quantum

SPECIAL EDITION
NOVEMBER 2026





Foreword

We stand at the precipice of a new computational era. For decades, the global economy has been driven by the continuous advancement of classical computing and, more recently, the explosive growth of Artificial Intelligence. Yet, as our challenges in finance, logistics, and scientific discovery grow increasingly complex, some of these problems are growing beyond what even the most powerful classical computers can handle in practice.

Quantum computing is not merely an upgrade; it is a fundamental paradigm shift. The question is no longer if scalable quantum computing will be realized, but when—and who will be prepared to harness its potential.

Whether you are an enterprise leader seeking competitive advantage, an investor evaluating the landscape, or simply a curious mind eager to understand the future of technology, this report is designed to equip you with the clarity needed to transition from quantum curiosity to quantum readiness.

Contents

CHAPTER 1
Summary

Page **4-7**

- **a.** Executive Summary
- **b.** The Question that Catalyzes Quantum Thinking: What if a tech giant announces usable, scalable quantum computing tomorrow?
- **c.** Quantum Readiness
- **d.** Realistic Opportunities for Quantum Computing

CHAPTER 2
Quantum Computing For Laypeople

Page **8-11**

- **a.** Common Misconceptions
- **b.** What is a quantum computer?
- **c.** Quantum Algorithms: The Engines of Innovation

CHAPTER 3
Progress Towards Quantum Advantage

Page **12-22**

- **a.** What is the Quantum Advantage?
- **b.** Towards Fault-Tolerant Quantum Computing
- **c.** Algorithm development and Resource Requirements
- **d.** Use cases versus actual quantum advantages
- **e.** Potential Applications in Finance
- **f.** Quantum AI: Promise and Reality

CHAPTER 4
Post-Quantum Cryptography Update (2026)

Page **23-25**

- **a.** Why organizations are preparing now
- **b.** Migration deadlines are closer
- **c.** Q-Day might be closer than we thought and Risk-associated with it is quite certain
- **d.** From standards to implementation
- **e.** What the financial sector is already learning
- **f.** Regional direction is becoming clearer
- **g.** Preparing for the implementation phase

CHAPTER 5
Global Investment Landscape And The Effort To Build Quantum Computers

Page **26-30**

- **a.** Landscape: from research ecosystem to quantum supply chain
- **b.** Economic impact projections: how to read the numbers carefully

CHAPTER 6
Thailand Positioning

Page **31-34**

- **a.** National Strategic Pivot
- **b.** Siam Quantum Square (SQ^2)
- **c.** Key players from industrial sector
- **d.** A Distributed Thai Quantum Research Ecosystem
- **e.** Moving forwards together

Ending Remarks:
The Quantum Imperative

Page **35**

Appendix

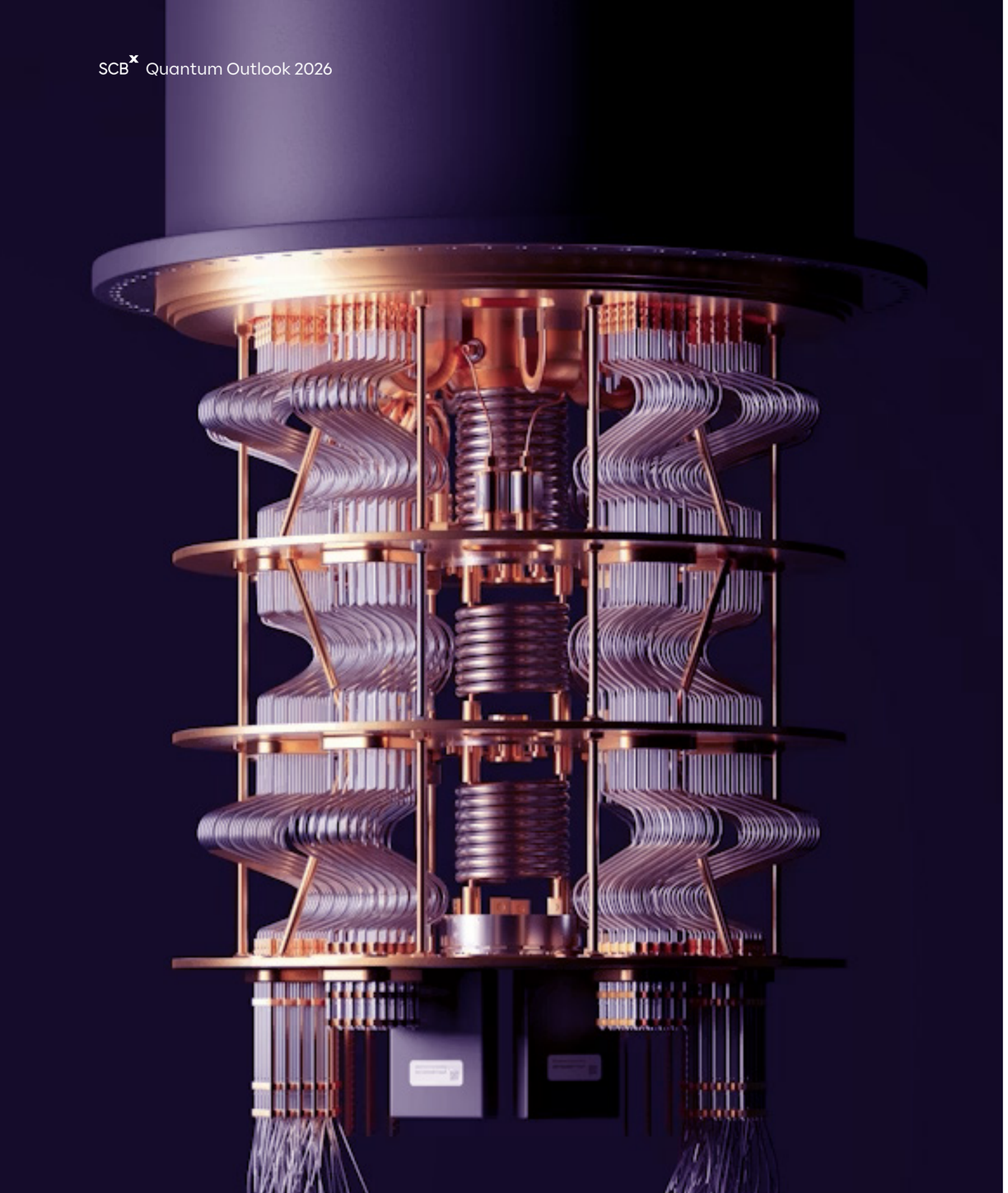
Page **36-37**

1. **Appendix A**: Glossary Of Terms
2. **Appendix B:** Technical Deep-Dive – SCBX Portfolio Optimization Research
3. **Appendix C:** The Quantum Readiness Checklist

CHAPTER 1

SUMMARY





1.1 Executive Summary

The global economy relies heavily on classical information processing. For decades, classical computing – and more recently Artificial Intelligence (AI) – has driven enormous technological and economic growth. Yet classical computing is built on a simple unit of information: the **bit**, which can take the value of either 0 or 1 but **never both at the same time.**

As industries attempt to solve increasingly complex problems—from climate forecasting, supply chains, drug discovery, material design, precision medicine, and ecosystem modeling—classical computers often struggle to scale to the size and complexity of these tasks within useful time and cost limits. Many of these problems grow **exponentially in difficulty** as the number of variables and problem size increases, making exact solutions computationally impractical even for the largest supercomputers and AI. This is why researchers and industry are exploring a new way of processing information based on the most fundamental laws allowed by nature: quantum **computation (QC)**, whose basic unit is the **qubit (quantum bit)**, which can represent 0 and 1 in a fundamentally different way, allowing the machine to transcend the limitations of classical computers.

The *previous SCBX Quantum Outlook: Post-Quantum Cryptography* (December 2025) [2] addressed the necessary defensive strategy for data protection and data encryption against future quantum computing threats. This outlook shifts the perspective to the **offensive strategic view: Quantum Readiness and Value Creation.** Quantum computing is transitioning from scientific curiosity toward a more realistic and more practical platform for enterprise innovation — shifting the question from "Is it possible to build one?" to "How soon must we be ready?" [1].

We have indeed moved far beyond Richard P. Feynman's original vision of quantum computing.

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical." [Feynman1982]

This document outlines the importance of quantum readiness, realistic cross-industry opportunities for quantum computing, explains the technology in accessible terms, and provides a foundation for how corporations can begin preparing to capture business value as quantum computing matures.

1.2 The Question That Catalyzes Quantum Thinking: What If A Tech Giant Announces Usable, Scalable Quantum Computing Tomorrow?

Imagine waking up tomorrow to the news that a major tech company has successfully deployed a fault-tolerant, scalable quantum computer, available through the cloud. Beyond the headlines, the most profound implication for global industry would be the sudden appearance of an insurmountable *information advantage.*

What kinds of information or solutions are still out of reach today without a useful quantum computer? In many important settings, industries face problems that grow explosively in complexity as the number of variables increases. Examples include accurately simulating molecular interactions for new drugs or materials, optimizing large supply chains with many changing constraints, or finding efficient routing across thousands of vehicles and destinations, to name a few. In such cases, classical computers often cannot check every possibility directly. They must rely on shortcuts, approximations, and heuristics.

Without a useful quantum computer, we are often limited in how close we can get to the best possible solution in extremely complex systems. For instance, precisely simulating all relevant molecular interactions on a classical computer can take an impractically long time [PNAS2017]. Furthermore, for large enterprises, even a marginal improvement in solution quality—such as a 2% gain (a very conservative estimation)—can yield a substantial return on investment in industries like finance, logistics, and materials science.

A useful quantum computer may help with some of these problems by processing certain kinds of complex information in a more natural way. Because it uses quantum-mechanical effects, it may make some previously impractical calculations more accessible. However, it is important not to overstate the case: quantum computers are not magic machines.

For some tasks, such as breaking widely used public-key cryptography with Shor's algorithm, quantum computers offer an enormous, well-established speedup over the best methods known today [Shor]. But for many real-world optimisation problems, the picture is more complicated. Some problems are so difficult that no known method—classical or quantum—can guarantee the perfect answer efficiently as the problem size grows [Kempe2006]. In practice, this means quantum computing may offer major benefits in selected areas, but it is unlikely to solve every hard optimisation problem automatically. Whether quantum algorithms will deliver a practical and disruptive edge across broad classes of business problems remains an active area of research [Preskill2018], and this report discusses those expectations in a realistic way.

1.3 Quantum Readiness

The central question for organizations today is no longer whether quantum computers will eventually be built, but rather who will be ready when they arrive. For most industries, the greatest strategic risk is not technological failure—it is strategic delay.

- **It takes time to be ready.** Becoming quantum-ready is not simply a matter of purchasing hardware once it becomes available. It requires new expertise across physics, mathematics, computer science, and domain knowledge, as well as significant re-skilling of engineering teams. Unlike AI, which can often be integrated into existing software pipelines, quantum computing frequently requires reformulating problems from first principles and developing new quantum workflows. *Organizations that wait until large-scale hardware arrives risk facing a significant competency gap.*
- **Valuable quantum applications are still being discovered.** Even within the global scientific community, it remains unclear which problems will ultimately deliver the greatest economic advantage. Identifying the right use cases requires experimentation and early engagement. *Organizations that begin exploring quantum applications today are not merely testing a new technology—they are discovering where real value may lie and developing proprietary algorithms tailored to their industry.* These innovations can be protected as intellectual property and may become a meaningful competitive advantage once large-scale quantum hardware becomes available.
- **Hardware access can be limited.** Another often overlooked factor is access to quantum hardware itself. In the early years of fault-tolerant quantum computing, large-scale processors will likely remain scarce and expensive. Access will be mediated through cloud providers and research partnerships. Organizations already engaged with hardware providers will naturally move to the front of the queue when new systems become available. *Those who wait may discover that access to the most advanced systems is limited, delayed, or prohibitively expensive.*
- **The window is narrowing.** Only a few years ago, many credible projections placed useful fault-tolerant quantum computers in the late 2030s or even the 2040s. However, rapid progress in hardware engineering, error correction, and algorithmic optimisation has significantly compressed these timelines. Several industry roadmaps now suggest the possibility of useful quantum advantage emerging between the late 2020s and the early 2030s for selected applications. Organizations whose plans still assume a late-2030s arrival are pacing themselves against a forecast that is already obsolete.



Executive TL;DR: The greatest strategic risk in quantum computing is not that the technology arrives too late, but that it arrives suddenly—and your organization is not ready. Quantum computing cannot be adopted overnight; it requires new expertise, new algorithms, and a workforce capable of thinking in fundamentally different computational models. Building this capability takes years. Institutions that begin only when large-scale quantum hardware becomes available will face a severe competency gap, while early movers will already possess the talent, intellectual property, and operational experience needed to deploy the technology immediately. Moreover, early access to cutting-edge quantum hardware will likely be limited, and those already engaged in the ecosystem will move to the front of the queue. In this sense, delaying preparation does not simply postpone investment—it creates a real **opportunity loss**, where the most valuable knowledge, partnerships, and competitive advantages are captured by others first.

1.4 Realistic Opportunities For Quantum Computing

Quantum computers are not universal replacements for classical computers. When it comes to problem solving, they are better understood as highly specialised accelerators for certain kinds of tasks. According to the World Economic Forum (WEF), practical applications are already emerging through hybrid quantum-classical approaches across several important sectors with projected economic value reaching hundreds of billions of dollars by 2035 by quantum computing alone [WEF1].

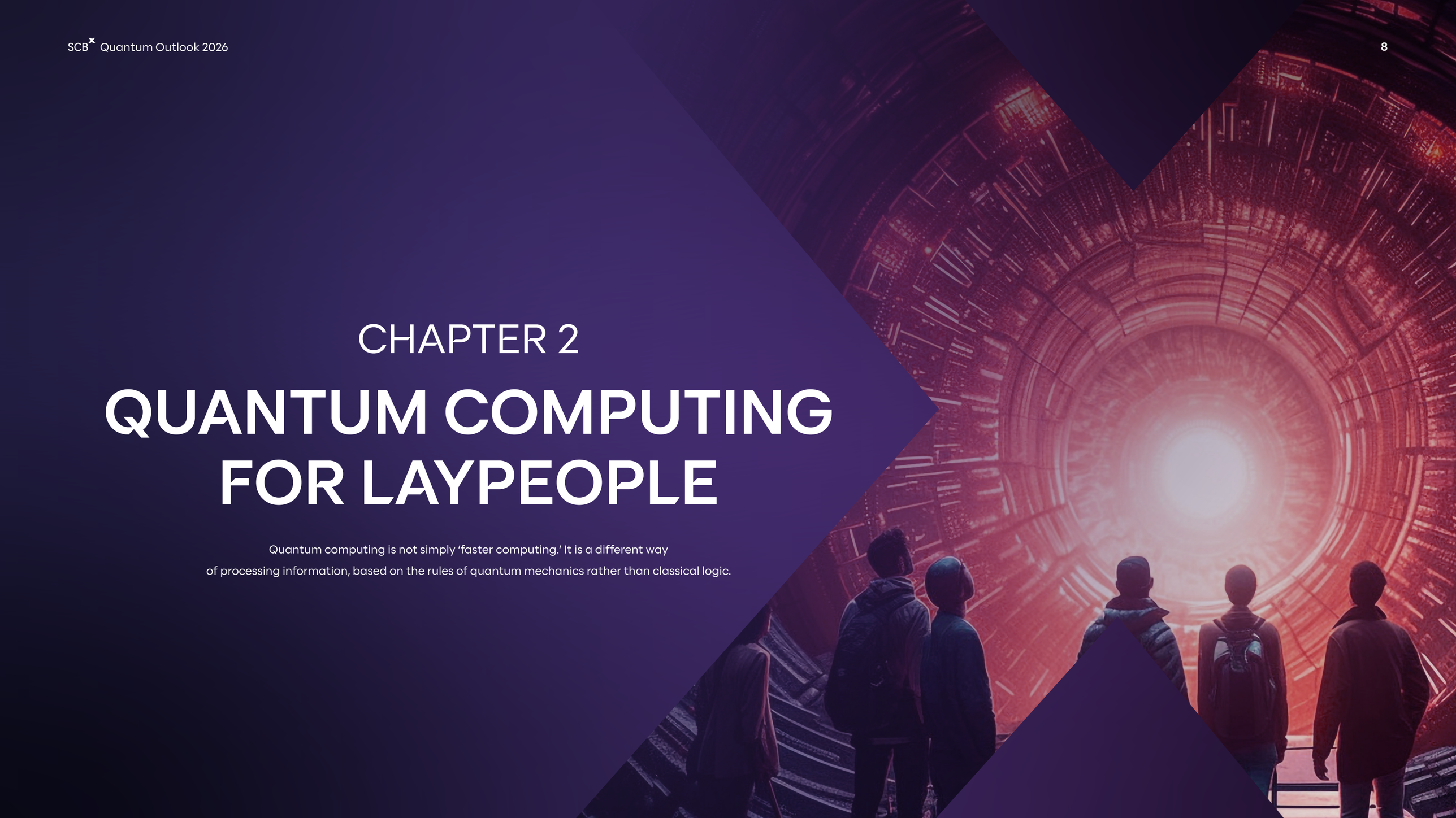
Key realistic cross-industry opportunities include:

- **Combinatorial Optimization (Logistics and Operations):** Finding the most efficient schedule, route, or allocation in a changing environment is often very difficult for classical systems. The Port of Los Angeles recently piloted hybrid quantum optimisation for cargo-handling scenarios, reducing crane travel distance by around 30%, thereby improving operational productivity [WEF2]. Similarly, Ford Otosan used hybrid computing to optimise production scheduling, reducing scheduling time to under five minutes [WEF2].
- **Advanced Chemical Simulation (Materials and Healthcare):** Classical computers face major difficulties when trying to simulate large quantum systems accurately, including molecules and materials. Quantum computers are especially promising here because chemistry is already quantum-mechanical at its core. This could help accelerate the discovery of better batteries, sustainable materials, and pharmaceuticals. For instance, Moderna is partnering with IBM to predict how mRNA sequences fold into functional shapes. These are still early, small-scale experiments, but they show how quantum methods might one day model such molecules with fewer simplifications than classical tools require [WEF3].
- **The Financial Sector Imperative:** Among all industries, financial services may be one of the clearest early beneficiaries of quantum computing. Finance depends heavily on complex modelling, simulation, optimisation, and pattern detection. The World Economic Forum projects that quantum computing use cases in financial services could generate up to $622 billion in value by 2035 [WEF4]. Leading institutions are already moving beyond theory into proofs of concept. For example, Turkish bank Yapı Kredi piloted quantum annealing to analyse cascading financial risks in a subset of 4,297 corporate clients drawn from a network of more than 600,000, reporting a seven-second computation for that pilot scenario [WEF4]. In addition, institutions such as Intesa Sanpaolo and Santander are piloting quantum and quantum-inspired methods for fraud detection and dynamic bond-hedging optimisation [WEF4]. Used in this way—as a specialised accelerator for mathematically intensive tasks—quantum computing could become a meaningful competitive tool for financial institutions.

CHAPTER 2

QUANTUM COMPUTING FOR LAYPEOPLE

Quantum computing is not simply ‘faster computing.’ It is a different way of processing information, based on the rules of quantum mechanics rather than classical logic.



2.1 Common Misconceptions

Before discussing the opportunity, it is important to clear away some of the noise surrounding the technology. Understanding what quantum computers cannot do is just as important as understanding what they may eventually do well.

Misconception 1: **"Quantum computers can solve any problem."**

Reality**:** While quantum computers can solve certain problems far more efficiently than their classical counterparts, they are not "magic genies". Post-quantum cryptography (PQC) comprises classical cryptographic methods designed to resist attacks by classical and quantum computers. No efficient quantum attacks are currently known against the underlying problems of the selected schemes. it uses mathematical problems for which no efficient quantum computations are currently known [1].

Misconception 2: **"Quantum computers find the best solution by trying every option at once."**

Reality: While "Superposition" allows a quantum computer to explore multiple solution paths at the same time, the challenge is that one cannot simply read off all those solutions at once under the rules of quantum mechanics. When we look at the result, the system "collapses" into a single answer due to "Quantum Measurement." If we are not careful about the algorithmic design, that answer is random. The 'art' of a quantum algorithm is not just exploring all paths, but cleverly using 'quantum interference' to make the right answer much more likely to appear than the wrong ones. Like overlapping ripples on a pond, a quantum algorithm must choreograph probability waves so incorrect answers cancel out, while the correct answer amplifies into a large, measurable crest. Engineering this precise quantum interference across thousands of variables is exceptionally difficult, making the discovery of useful quantum algorithms a profound challenge.

Misconception 3: **"The only number that matters is the number of Qubits."**

Reality: Quantity does not equal quality – a simple fact. Having 1,000 "noisy" or "low-quality" qubits is like having a massive workforce where everyone is whispering and making mistakes; the work never gets done. The real milestone is **error correction** — using many physical qubits together to create **'Logical Qubits'** that are stable and reliable enough to perform meaningful computation. Despite being aware of logical qubits, one needs to pay attention to the details when reading the big announcement from quantum companies. This is a teaser, and we elaborate more on this in the later section [see **Section 3.2**].

Misconception 4: **"Scientists already know the full potential of these machines."**

Reality: Think about when the very first classical computer "ENIAC" was introduced in the 1940s. No one then predicted the existence of the Internet, AI, or social media as we see everywhere today. We are in the 'ENIAC era' of quantum computing — the fundamental machine exists and works, but we are still years away from the reliable, scalable systems that will transform industries and integrate into our daily lives seamlessly. We know the technical and scientific tools, but the disruptive innovations will come from the creative synergy between quantum science and business — an exploration we must begin today.

2.2 What Is A Quantum Computer?

The prevailing narrative suggests that quantum computers are merely a fundamentally different alternative to the classical machines we use today. While accurate, this description understates the reality. In the physical sciences, classical mechanics is actually a constrained, simplified subset of the broader laws of **Quantum Mechanics.**

Consequently, a quantum computer should not be viewed as a separate species of technology, but as a more **universal and general computational model.** It possesses the inherent capacity to simulate classical computation and, for selected tasks, perform calculations much more efficiently than the best known classical methods. Ultimately, quantum computers are built from the most fundamental units of information called **Qubits**, which utilize the key concepts of superposition, interference, entanglement, and measurement:

Superposition (The Power of "And"): A qubit isn't just a 0 or a 1. It can exist in a state of both simultaneously. Imagine a coin spinning on a table: while it's spinning, it is both heads and tails at once. This allows the computer to hold and manipulate many states simultaneously — though extracting a useful answer from those states requires carefully engineered algorithms, as described in the misconception above.

Quantum Measurement (The Bottleneck): This is the moment we 'stop the coin' to see the result — and once measured, the quantum state is gone. This irreversibility is one of the central constraints that quantum algorithms must be designed around.

Entanglement (The Invisible Correlation): Entanglement links two qubits so that measuring one instantly determines the state of the other, regardless of distance. This is not a communication channel — no information travels between them — but it creates correlations that have no equivalent in classical computing. By enabling these correlations, quantum computers can solve some classically-hard problems.

By harnessing these properties, the Qubit serves as a powerful generalization of the classical Bit—expanding the binary backbone of today's digital technology into a vastly more complex quantum computational paradigm.



2.3 Quantum Algorithms: The Engines Of Innovation

Quantum hardware alone creates no value. The bridge between the quantum physics described above and real-world business impact is the **Quantum Algorithm** — a set of mathematical instructions that exploits superposition, entanglement, and interference to solve specific classes of problems in ways no classical program can match.

To navigate this landscape, it helps to think in three layers:

- **Algorithm (The Engine):** The specific pattern or set of instructions the quantum computer follows.
- **Problem (The Task):** The mathematical hurdle the engine is designed to clear (e.g., "Find the prime factors of this giant number").
- **Application (The Impact):** The real-world situation where that speedup of solving problems may translate into competitive or strategic value.

Examples Of Well-Known Quantum Algorithms (In The Fault-Tolerant Era)

The algorithms highlighted below represent the definitive benchmarks of the fault-tolerant era [further details in **Section 3.3**]. Their theoretical performance is rigorously established under specified assumptions, while the size of the advantage depends on the problem, input preparation, required output, and classical comparison method. However, realizing these advantages in practice requires mature hardware—specifically, quantum computers equipped with stable *logical qubits* capable of executing millions of *high-fidelity operations* without compounding physical errors. While the hardware required to run them at a commercially disruptive scale is still being engineered, practical advantage must be assessed for each application.

Algorithm	The Mathematical "Problem"	Potential Real-World Impact
Shor's [2]	Factors large numbers into their prime components in polynomial time — an exponential speedup over the best classical methods.	**Cybersecurity:** The reason we must upgrade our national encryption standards today.
Quantum Phase Estimation (QPE) [3]	Extracts the energy levels of a quantum system — the fundamental property that determines how molecules behave, react, and bond — with very high precision—something that becomes impractical for classical computers beyond fairly small molecules	**Pharma & Materials:** Precisely simulating the active sites where drug molecules bind to biological targets; designing new battery cathode materials; and elucidating complex catalytic mechanisms—such as how the biological FeMoco cluster enables room-temperature nitrogen fixation, which could revolutionize industrial fertilizer production [5]. QPE is the algorithm underpinning the most scientifically credible, long-term quantum chemistry advantage.
Harrow–Hassidim–Lloyd [4]	Solves very large systems of linear equations — the mathematical backbone of simulation, optimisation, and machine learning — with a potentially exponential speedup, but only under specific conditions	**Finance & Engineering:** Accelerating portfolio risk calculations, optimising large-scale logistics networks, and speeding up machine learning model training tasks that reduce to solving linear systems.

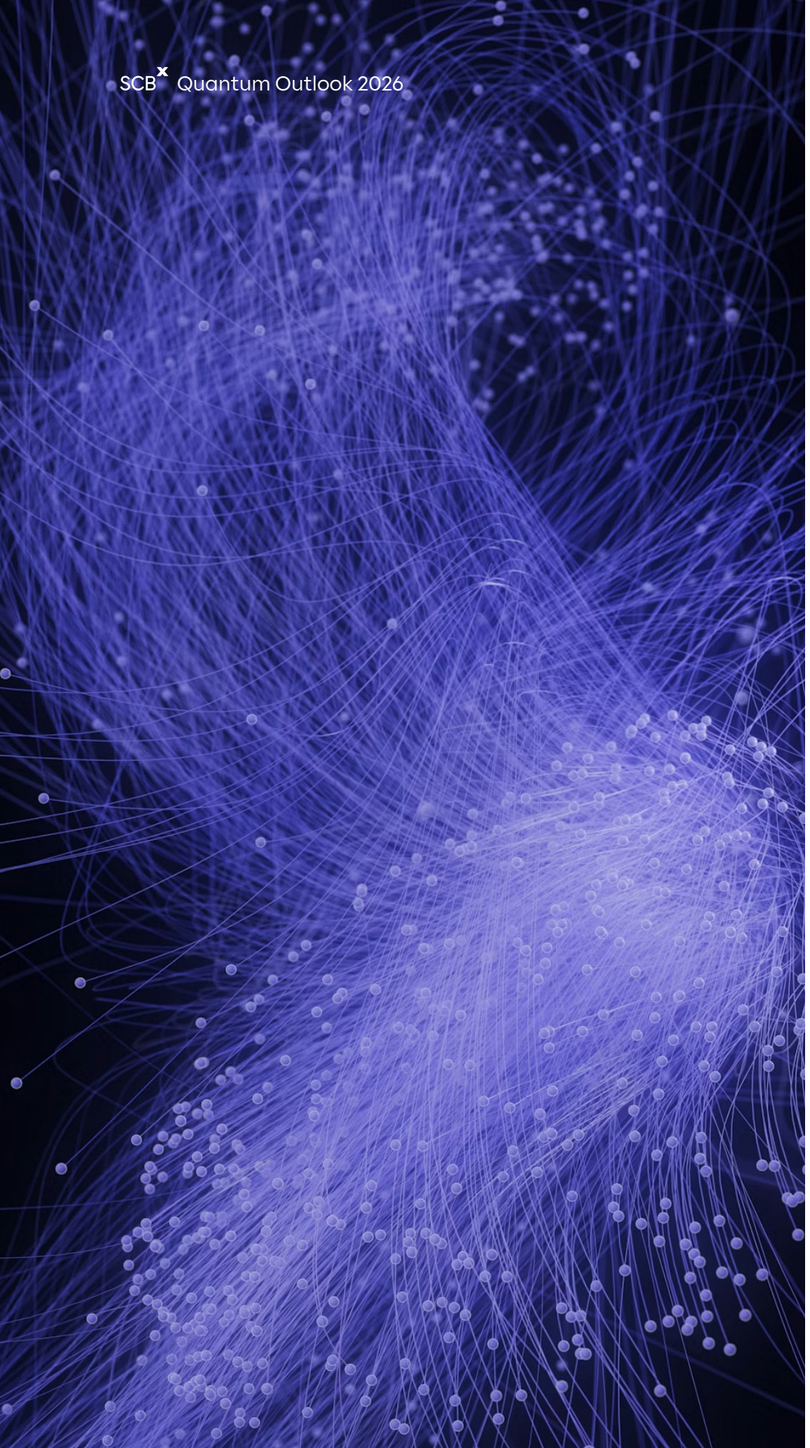
The Expanding Frontier Of Quantum Algorithmic Discovery

While Shor's, QPE, and HHL serve as the foundational pillars of quantum computer science, the broader landscape of quantum software is rapidly evolving. Drawing on the earlier analogy, every new algorithm must discover a unique way to choreograph computational "probability waves" for a specific new problem. The continuous discovery of these algorithms remains one of the most active and exciting frontiers in the field today, constantly broadening the horizon of what quantum computers will eventually be able to solve. This ever-growing catalog of theoretical breakthroughs and known quantum speedups is actively tracked by the scientific community in resources such as the Quantum Algorithm Zoo [6].

CHAPTER 3

PROGRESS TOWARDS QUANTUM ADVANTAGE





While the expanding catalog of quantum algorithms provides the theoretical blueprints for potential quantum computational advantage, an algorithm alone is merely a mathematical concept. Translating these quantum algorithms into tangible economic value requires bridging the gap between theoretical science and applied physical engineering in hardware development.

Quantum computing aims to provide solutions to high-impact, complex problems that can potentially reshape the global economy and technology, as mentioned above. Realizing this potential is a dual-track challenge, requiring simultaneous breakthroughs in the physical hardware capable of manipulating delicate quantum states and the specialized software required to process them. While currently in a pre-commercial phase, the industry is advancing rapidly. Waiting passively for the technology to fully 'arrive' is a strategic error; the pace of current development suggests that the transition from laboratory experiment to market disruption will be abrupt, disproportionately rewarding organizations that prepare in advance.

3.1 What Is The Quantum Advantage?

In the journey toward a quantum-enabled economy, it is vital to distinguish between scientific milestones and tangible business value. Not all "advantages" are created equal, and understanding the three distinct levels of progress is essential for setting realistic investment expectations.

- **Quantum Supremacy (Level 1: The proof-of-concept milestone):** This represents a key technical achievement where a quantum device completes a specific computational task in a much faster time scale compared to the world's most powerful supercomputers (i.e., the order of minutes versus many years – placing it beyond any practical classical reach). Google first claimed this milestone in 2019, and subsequent demonstrations by other quantum companies and research institutes have progressively strengthened the evidence [2][4]. Interestingly, classical researchers later found far faster methods for Google's original 2019 task, shrinking its famous "10,000 years" estimate dramatically—a useful reminder that such claims are a moving target. While these experiments prove that quantum hardware today is physically capable of solving classically intractable tasks at scale, the tasks themselves lack direct commercial utility. They are a necessary proof-of-concept—evidence that the strange rules of quantum physics work—but not yet commercially deployable products.

- **Quantum Utility (Level 2: The first glimpse of real-world value):** This occurs when a quantum computer can perform a calculation with a level of accuracy and complexity that exceeds the capacity of "existing" classical algorithms, providing reliable data that scientists and engineers can actually use and verify. In this phase, we don't necessarily care if the quantum computer is faster than a supercomputer (that's Level 3 Quantum Advantage). We care that the quantum computer is accurate enough to be a trusted tool for exploring relevant problems that classical computers can only guess at or approximate. The term was popularised by IBM in 2023 [5].

As of October 2026, the field is in a transition period. In July 2026, IBM and the University of Chicago reported a computation on 70 error-protected ("logical") qubits that they say is beyond leading classical simulation methods, with a built-in way to check that the answer can be trusted [6]. Within weeks, other researchers showed that a large GPU cluster could keep pace—illustrating how quickly classical methods fight back [7]. Google's "Quantum Echoes" experiment (2025) is another verifiable demonstration on a scientific task. However, the industry has not yet achieved broad commercial quantum utility for general-purpose, large-scale applications.

- **Quantum Advantage (Level 3):** This is the ultimate inflection point. It occurs when a quantum computer solves a commercially relevant problem—such as simulating a complex drug molecule that classical computers cannot accurately model, or optimizing a global logistics network beyond classical reach—faster, cheaper, or more accurately than any known classical method. The most credible near-term Level 3 candidates, supported by published resource estimates with specific qubit counts, are in quantum chemistry and materials (e.g., FeMoco, drug molecule simulation)[8]. Breaking cryptography (e.g., RSA-2048 via Shor's algorithm) has equally well-studied estimates, but it is a security threat rather than a source of business value (see Section 3.3.2).

In our view, the field is now entering Level 2, and the roadmaps of the leading hardware companies make Level 3 for selected problems plausible within a decade. It is crucial to stress that Level 2 is not a single moment but a widening zone, and organisations that dismiss it as a mere stepping stone risk missing the early signals that will determine which companies are positioned to capture Level 3 value when it arrives.

3.2 Towards Fault-Tolerant Quantum Computing

To realize a commercial quantum advantage, we require a system that is not only large but structurally stable and can reliably operate. The 'Holy Grail' for quantum hardware is known as a **Fault-Tolerant Quantum Computer (FTQC)**—a machine capable of identifying and correcting its own errors in real-time, and is capable of running any expected operation as commanded.

While quantum hardware is developing at a fast pace, the current hardware does not achieve this yet, and the race for building the first FTQC is on. To fully understand the hardware development side, it is necessary to grasp these following concepts. They may sound intimidating but logically things flow quite smoothly. It will greatly enhance us to be aware when reading press releases from quantum companies.

While hardware is advancing at an exponential pace, we have not yet reached the FTQC era. The global race to build the first reliable machine is now an engineering marathon. For leadership, understanding the following hierarchy is essential for evaluating the "breakthrough" headlines often seen in the press.

3.2.1 What Are Fault-Tolerant Quantum Computers?

A single Physical Qubit (the raw hardware unit — a superconducting circuit, a trapped ion, a neutral atom) is inherently "noisy." Even the best-engineered qubits occasionally fail to perform as commanded. To overcome this, we use a strategy known as **Quantum Error Correction.**

We can categorize the development of an FTQC through a business-organizational analogy:

- **The Physical Qubit (The Individual Worker):** An individual worker may be highly skilled, but they are human and prone to occasional errors. If your entire operation relies on one person never making a mistake, the system will eventually fail.
- **The Logical Qubit (The High-Performing Team):** A "Logical Qubit" is a group of high-quality physical qubits working in unison. Like a professional team, they check each other's work and correct errors as they happen. For this to work, the "individual workers" must reach a minimum level of competency; if the individuals are too prone to error, adding more of them only creates more chaos.

- **The FTQC (The Working Company):** Having a few good teams is a start, but it doesn't make a functional bank. A **Fault-Tolerant Quantum Computer** is like a large-scale company where hundreds of "teams" (logical qubits) work together coherently. They are supported by an infrastructure (universal gates) that allows them to execute complex, long-term projects without the entire organization collapsing due to a single mistake.

Current Status: We are now transitioning from the era of "Individual Workers" to the "Logical Teams". The next 5 years will be defined by how well we can integrate these teams into a "Working Company".

3.2.2 Strategic Milestones: What To Monitor

For executives tracking progress in quantum hardware, five milestones serve as the clearest signal of genuine advancement. These are not marketing metrics — they are the specific engineering and technological challenges that must be cleared, in roughly this order, before fault-tolerant computation becomes possible.





Milestone 1: Physical Error Rates Below The Fault-Tolerance Threshold

Executive TL;DR: This is the "break-even" point. Below this, adding more qubits actually makes the computer smarter rather than noisier.

What it means: Every quantum operation — qubit preparation, single-qubit gates, two-qubit gates, and measurement — must be performed with an error rate below the threshold of the chosen error-correction code. For the most widely used approach (surface codes), this threshold is approximately 1% per operation. Below this threshold, adding more qubits actively helps. Above it, adding more qubits makes things worse. In practice, engineers aim for error rates around 0.1% which is comfortably below the threshold, so that error correction does not require an unmanageable number of extra qubits.

Milestone 2: Below-Threshold Logical Qubits (Error Suppression With Scale)

Executive TL;DR: This confirms the theory is working. It proves the machine is scalable and not just a one-off laboratory fluke.

What it means: Demonstrating that logical error rates decrease exponentially as more physical qubits are added to the error-correcting code. This is the definitive proof that quantum error correction is working as theory predicts — that the system is operating below the fault-tolerance threshold in a scalable way, not just on a single carefully tuned device.

Milestone 3: A Universal Fault-Tolerant Gate Set

Executive TL;DR: This is the bridge to software. Without this, the computer can only solve niche problems; with it, it can run any algorithm (like Shor's or HHL).

What it means: Demonstrating that every type of quantum operation needed for universal computation can be performed with active error correction running throughout — including the notoriously difficult non-Clifford gates (specifically the T-gate), which cannot be performed in the same simple, protected way as other operations in the most common error-correction schemes, and are therefore usually produced via a resource-intensive process called magic state distillation or magic state cultivation.

Milestone 4: Magic State Distillation / Cultivation At Scale

Executive TL;DR: In early designs, most of a machine's qubits were expected to be spent just producing "magic states." Milestone 4 is about making the machine efficient enough to be commercially viable.

What it means: Producing high-quality "magic states" — the special quantum resource states required to implement fault-tolerant T-gates — efficiently enough that the physical qubit overhead does not dominate the entire machine. In current surface-code architectures, magic state distillation consumes the majority of physical qubits in a fault-tolerant system: early estimates suggested that, for RSA-breaking computations, the large majority of physical qubits would be devoted purely to producing magic states rather than to the computation itself. Newer techniques such as magic state cultivation (2024) have already reduced this burden significantly.

Milestone 5: Sustained Fault-Tolerant Operation At Industrially Relevant Scale And Runtime

Executive TL;DR: This is where we achieve the ultimate goal where quantum computers are ready for the commercial quantum advantage (Level 3).

What it means: A machine simultaneously satisfying all of: (1) enough logical qubits for a target algorithm — currently estimated at ~1,400 for RSA-2048 and ~1,000–2,500 for FeMoco chemistry, depending on the method (see Section 3.3.3); (2) logical error rates low enough for the required circuit depth — approximately 10^{-12} for Shor's algorithm; (3) sustained continuous operation for the full runtime — hours to days; and (4) a classical control system fast enough to decode errors and apply corrections in real time without falling behind the qubit error rate.

We now provide the hardware timeline for some key players in the field. Note that the list of quantum companies may not be exhaustive here.

Company	M1 — Physical Error Below Threshold	M2 — Below-Threshold Logical Qubits	M3 — Universal FT Gate Set	M4 — Magic state Production At Scale	M5 — Sustained FT At Useful Scale
IBM Superconducting	Achieved Heron r2/r3: ~0.1–0.3% two-qubit error rate	(Almost) Achieved qLDPC codes and fast real-time decoding demonstrated; Loon test chip (Nov 2025) integrates key FT components. Below-threshold scaling with qLDPC codes not yet published.	Partial Clifford gates demonstrated; T-gate via distillation in progress. July 2026: 468 logical T gates run on 70 logical qubits (small error-protection codes)	Partial 10× decoding speedup achieved; distillation at scale targeted 2026–2027	Not yet Starling (2029): ~200 LQ, 100M ops. Blue Jay (2033+): ~2,000 LQ
Google Superconducting	Achieved Willow: sub-0.5% two-qubit error rate across full chip	Achieved Willow (Dec 2024): first demonstration of exponential error suppression with scale. Published in Nature.	Partial Clifford operations below threshold shown; protected T-gate (non-Clifford) techniques still at an early, small-scale stage	Partial Magic state cultivation (a cheaper alternative to distillation, developed by Google) not yet shown at useful scale	Not yet Target: useful error-corrected QC by 2029. Estimated ~1M physical qubits required. Also building neutral-atom hardware since Mar 2026.
Quantinuum Trapped ion	Achieved Helios: >99.9% two-qubit gate fidelity — Quantinuum reports 99.921% average two-qubit gate fidelity across the commercially available Helios system (November 2025)	(Almost) Achieved 48 error-corrected logical qubits on Helios at ~2:1 ratio using small codes; near-"five-nines" logical fidelity reported (Aug 2026). Errors falling as codes grow not yet shown at scale.	Achieved First fully error-corrected universal gate set including T-gate (June 2025), at small code size. T-gate error below native physical rate.	Partial Magic state injection demonstrated at small scale; scaling to hundreds of LQ targeted in Sol (2027)	Not yet Apollo (2029): first fully FT machine. Thousands of physical qubits, commercially relevant LQ count. Sol (2027) trap chip now in validation.
Microsoft Topological	Disputed Majorana 1 (Feb 2025) and Majorana 2 (Jun 2026) announced; independent physicists dispute whether a working topological qubit has been shown. Near-term hedge: "Magne" neutral-atom machine with Atom Computing (late 2026).	Not yet Below-threshold logical operation not yet publicly demonstrated. Roadmap Stage 3 targets this.	Not yet Universal gate set via topological braiding is the theoretical promise; not yet demonstrated experimentally	Not yet Much lower overhead than surface codes is the design promise; not yet validated	Not yet Now targets a scalable quantum computer by 2029 (announced Jun 2026). Designed for 1M qubits on a single chip; in DARPA's final evaluation stage.

M = Milestone | LQ = Logical Qubits | FT = Fault-Tolerant | Sources: company roadmaps and public announcements as of the third quarter of 2026. M3 partial credit requires Clifford gates demonstrated fault-tolerantly; full credit requires T-gate confirmed below physical error rate.

Company	M1 — Physical Error Below Threshold	M2 — Below-Threshold Logical Qubits	M3 — Universal FT Gate Set	M4 — Magic state Production At Scale	M5 — Sustained FT At Useful Scale
IonQ Trapped ion	Achieved Barium platform: >99.9% two-qubit fidelity; 99.99% reported in 2025 using Oxford Ionics technology	Partial Error correction experiments ongoing; below-threshold at scale not yet published	Partial Individual FT gate demonstrations; full universal FT gate set not yet confirmed	Not yet Magic state infrastructure targeted in 2027 chip (~10K physical / ~800 LQ)	Not yet 2028 target: ~1,600 LQ across two chips. Depends on Oxford Ionics + Lightsynq integration.
QuEra Neutral atom	Achieved Harvard-MIT-QuEra 2025: below-threshold error correction on arrays of up to 448 atoms	Achieved Harvard-led 2025 (Nature): below-threshold logical performance; algorithms run on up to 96 logical qubits. Separate Harvard-MIT result: 3,000-qubit array run continuously for 2+ hours.	Partial Magic state distillation demonstrated (2025); full universal FT gate set not yet confirmed at scale	Partial Magic state distillation demonstrated 2025 — ahead of most competitors on this specific milestone	Not yet 2026–2027: 100 LQ / ~10K physical qubits (Gen 3). ~1,000 LQ targeted by 2030 with photonic networking. Compact ~2:1 encodings for quantum memory reported (Apr 2026).

M = Milestone | LQ = Logical Qubits | FT = Fault-Tolerant | Sources: company roadmaps and public announcements as of the third quarter of 2026. M3 partial credit requires Clifford gates demonstrated fault-tolerantly; full credit requires T-gate confirmed below physical error rate.

A few things worth highlighting from this cross-company view:

Quantinuum is the clear scientific leader on milestones 1–3. It was the first company to demonstrate a complete, error-corrected universal gate set (M3), albeit at small scale, and it reports the highest two-qubit gate fidelities of any platform. Its compact 2:1 encodings on Helios are efficient, but they use small codes; the next test is whether errors keep falling as the codes grow. Neutral-atom teams (Harvard/QuEra) have since reported similarly compact encodings.

Google and QuEra are the leaders on M2. Both have published peer-reviewed evidence of exponential error suppression with scale — the most important theoretical validation that fault-tolerant quantum computing is physically achievable. QuEra's two-hour continuous operation result is the strongest runtime demonstration to date. The Harvard–MIT two-hour continuous operation of a 3,000-atom array (with QuEra as a close partner) is the strongest runtime demonstration to date.

Microsoft is the wildcard. On paper, its topological architecture offers the most efficient path to M4 and M5 — dramatically lower error-correction overhead would be transformative. But it is the furthest behind on demonstrated milestones, and its February 2025 results are still under independent verification. Its Majorana 1 (2025) and Majorana 2 (June 2026) results remain disputed by independent physicists, even as Microsoft now targets a scalable machine by 2029. If the architecture works as claimed, Microsoft could leapfrog everyone; if it does not, it is years behind.

IBM has the most credible and detailed path to M5. Its roadmap is the most granular and most consistently delivered upon. Starling (2029) and Blue Jay (2033+) give concrete performance targets that no other company matches in specificity. IBM reinforced this in May 2026 with a plan to invest more than $10 billion in quantum over five years, including a new US quantum-chip foundry (Anderon) backed by the US Department of Commerce [16].

The gap that matters most is M4. Every company is partially demonstrated at best on magic state production at scale — and this is the milestone that dominates physical qubit overhead. Progress here in 2026–2027 will be the strongest leading indicator of which company actually crosses M5 first.

3.3 Algorithm Development And Resource Requirements

Focusing on hardware alone provides only half of the strategic picture. The "Quantum Gap"—the distance between current machine power and the requirements for high-value applications—is being closed by two converging forces: building more powerful machines (Hardware) and writing more efficient instructions (Software).

3.3.1

3.3.1 State-of-the-Art Experiments (as of the third quarter of 2026)

The following milestones represent the shift from laboratory curiosity to industrial utility

Experiment	Organization / Hardware	What Was Demonstrated	Key Result	Strategic Significance	Source
Random Circuit Sampling (RCS) – Re-establishing Quantum Supremacy	Google Quantum AI – Willow processor (105 qubits)	Random circuit sampling benchmark completed on a 105-qubit processor	Task completed in ~5 minutes that would take classical supercomputers ~10^{25} years	Confirms the processor operates in the quantum regime at scale. RCS is not useful computation but a hardware validation benchmark tracking progress toward scalable quantum processors	Google Quantum AI Willow announcement (Dec 2024)
Quantum Echoes Algorithm – First Verifiable Advantage on a Useful Algorithm	Google Quantum AI – Willow chip	Implementation of the Quantum Echoes (OTOC) algorithm to study quantum dynamics	~13,000× faster than the best classical estimate for this specific measurement (Nature, Oct 2025). A separate, smaller proof-of-concept applied the technique to two real molecules.	Represents a transition from benchmark problems to scientifically meaningful algorithms, suggesting early Level-2 quantum utility	Google Quantum AI announcement (Oct 2025); collaboration with University of California, Berkeley
Universal Fault-Tolerant Gate Set	Quantinuum – H-series trapped-ion hardware	Full error-corrected universal gate set demonstrated, including Clifford gates and T-gate via magic-state injection, with real-time error detection	T-gate error rate below physical error scale; continuous mid-circuit measurement and feed-forward correction implemented	Demonstrates the last major scientific prerequisite for fault-tolerant quantum computing. Remaining challenge is engineering scale-up (more logical qubits, longer runtime)	Quantinuum technical paper & blog (June 2025)
Sustained Neutral-Atom Operation With Qubit Replenishment	Harvard University – Massachusetts Institute of Technology collaboration (supported by QuEra Computing)	Neutral-atom array with 3,000 qubits operated continuously for >2 hours while replenishing atoms lost from traps	Continuous operation for over two hours. (In separate 2025 papers, Harvard/QuEra teams ran algorithms on up to 96 logical qubits with below-threshold performance and demonstrated logical magic-state distillation.)	Addresses a key engineering bottleneck in neutral-atom systems: atom loss during long computations, enabling sustained runtimes required for industrial algorithms	Nature (2025), several papers
Hybrid Quantum –HPC Workflow For Biomolecular Simulation	RIKEN (Fugaku supercomputer) + Quantinuum (Reimei quantum computer)	First integrated workflow combining a top-tier classical supercomputer with a quantum processor to study biomolecular chemistry	Real scientific workflow exploring chemical reactions in biomolecules	Demonstrates the most likely near-term deployment model: quantum processors as co-processors within HPC pipelines for chemistry, materials science, and pharmaceuticals	RIKEN–Quantinuum collaboration (2025)
Verified Quantum Advantage On Logical Qubits	IBM + University of Chicago – IBM Heron processor	A structured (non-random) circuit on 70 error-protected logical qubits, with a built-in way to check how trustworthy the answer is	~15 minutes on the quantum computer; 2,415 logical two-qubit operations and 468 logical T gates; logical errors ~10× lower than physical. A large GPU cluster later matched it in ~37 minutes	Shows how advantage claims are now made—and contested—in public via IBM's open "Quantum Advantage Tracker"; combines scale, error protection and verifiability	IBM Newsroom (Jul 2026); arXiv preprint

3.3.2 Closing The Gap By Better Design Of The Algorithms

As discussed above, the quantum resources required to execute major algorithms can decrease dramatically over time as researchers discover more efficient implementations. Improvements may come from better circuit constructions, more efficient arithmetic, improved error-correction codes, or entirely new algorithmic techniques.

The key strategic insight is that **hardware progress is not the only driver of quantum capability.** Advances in algorithm design and error correction can reduce the number of required qubits by orders of magnitude. In other words, the effective "distance" between current hardware and commercially useful quantum applications can shrink rapidly as software and theory improve.

Over the past decade, this pattern has already been observed repeatedly. The resource requirements for several flagship quantum algorithms have fallen dramatically as new techniques were introduced. A particularly instructive example is **Shor's algorithm** for integer factorization.

Case Study: **Resource Evolution For Breaking RSA-2048**

Why It Matters: **RSA-2048 is one of the most widely deployed public-key cryptosystems, used for example in digital certificates and signatures. Together with elliptic-curve cryptography (ECC), which secures most internet connections and virtually all cryptocurrencies, it protects a vast portion of the global digital infrastructure.**

A sufficiently powerful quantum computer running Peter Shor's algorithm could factor RSA-2048 keys efficiently, rendering this widely used cryptographic system insecure.For this reason, the resource requirements for executing Shor's algorithm have been studied intensively over the past decade. The results illustrate a striking trend: rapid reductions in the estimated number of qubits required.

Year	Study	Estimated Resources	Key Insight
2012	Surface-code analysis by Austin Fowler and collaborators	~1 billion physical qubits	Early fault-tolerant estimates assumed conservative error -correction overheads
2019	Study by Craig Gidney and Martin Ekerå (published in Quantum, 2021)	~20 million noisy physical qubits; runtime ~8 hours	Major improvements in modular arithmetic circuits reduced the resource cost dramatically
2025	Updated analysis by Craig Gidney at Google Quantum AI	<1 million noisy physical qubits and ~1,400 logical qubits; runtime <1 week	Innovations include approximate residue arithmetic, yoked surface codes, and magic-state cultivation
2026	"Pinnacle" architecture by Iceberg Quantum, a Sydney start-up (preprint, revised May 2026)	<100,000 physical qubits (about a month of runtime); ~150,000 qubits for about a week	Uses qLDPC error-correction codes instead of surface codes; assumes 0.1% error rates and very fast operations; harder to engineer because distant qubits must be connected
2026 (ECC)	Google Quantum AI with Ethereum Foundation & Stanford (white paper, Mar 2026) – target: 256-bit elliptic curves	<1,200–1,450 logical qubits; <500,000 physical qubits; runtime of minutes	Roughly 10× cheaper than earlier ECC estimates. Google withheld the attack circuits and published a zero-knowledge proof instead, so outsiders can verify the claim without learning the attack

Alignment With Industry Hardware Roadmaps: Interestingly, the latest algorithmic estimates now fall within the scaling targets announced by several quantum hardware companies:

- IonQ has publicly projected systems with roughly **1,600 logical qubits by around 2028**. It now says it expects to reach logical-qubit counts relevant to RSA-2048 in 2028–2029.
- IBM's longer-term **Blue Jay** architecture (target early-2030s) aims for **~2,000 logical qubits**, which would exceed the estimated requirement.

A word of caution: logical-qubit counts are not directly comparable between companies, because each company's logical qubits have different error rates—and breaking RSA also needs extremely low error rates and long, stable runs. IBM's Starling (2029, ~200 logical qubits), for example, is still well short of the ~1,200–1,400 logical qubits that the latest RSA and ECC estimates require.

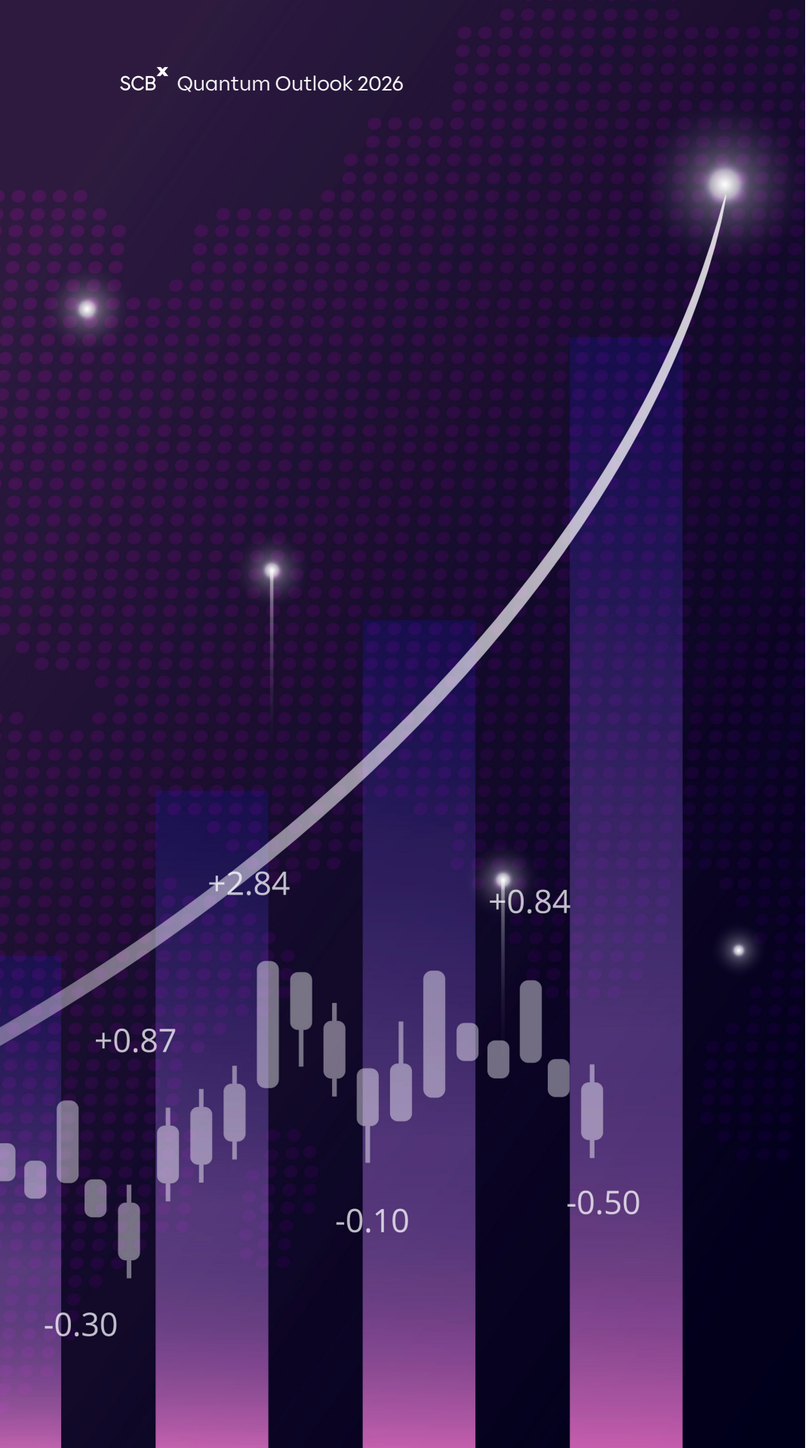
Taken together, currently published roadmaps suggest that — without requiring any additional fundamental scientific breakthroughs beyond those already known by the mid-2020s — the capability to break RSA-2048 could plausibly emerge in the **early-to-mid 2030s.** For context, a 2026 survey of 26 experts by the Global Risk Institute put the chance of a cryptographically relevant quantum computer within 10 years at 28–49% [12], and Google (March 2026) and Microsoft (June 2026) have both set 2029 as the deadline for moving their own systems to post-quantum cryptography.

3.3.3 Resource Requirements Of The Current Day

We highlight some current resource requirements of some known quantum algorithms to solve practical problems.

Note that these are published estimates for future fault-tolerant machines, not today's hardware, and they keep changing as techniques improve.

Algorithm	Targeted Problem	Practical Implication	Est. Logical Qubits	Estimated Run Time
Shor's Algorithm	RSA-2048 Factoring / 256-bit ECC	Cybersecurity: Rendering current global encryption standards (RSA/ECC) obsolete.	~1,200–1,450 (ECC); ~1,400 (RSA)	Minutes (ECC) to < 1 week (RSA), on ~0.1–1 million physical qubits
Quantum Phase Estimation (QPE)	FeMoco Molecular Simulation	Sustainability/ESG: Catalyst discovery for high-efficiency fertilizer and carbon capture.	~1,000 – 2,500 (method-dependent)	Hours to days (one widely cited 2021 estimate: ~4 days) [8]
Quantum Amplitude Estimation	Monte Carlo pricing of complex derivatives	Faster derivative pricing and risk calculations [14].	~8,000–11,500 [14].	~1 second is the target for advantage, requiring ~54–82 million sequential T-gate layers per second—far beyond today's hardware [14].
Grover's Algorithm	Unstructured Data Search	Intelligence/Data: Quadratic speedup for brute-force search problems; in practice, error-correction overheads may cancel much of this gain [13].	Problem-dependent	Often slower than classical alternatives at realistic problem sizes.



3.4 Use Cases Versus Actual Quantum Advantages

Many of the "use cases" appearing in quantum computing research today are best understood as exploratory demonstrations rather than examples of true quantum advantage. In most cases, the same problems can still be solved entirely using classical computers. Consequently, these demonstrations should not be interpreted as evidence that quantum computers are already outperforming classical systems.

This naturally raises a question that executives often ask: *"If the machine is not yet better, why should we use it now?"*

The answer lies in **Quantum Readiness** (see again Sec 1.3)

Today's quantum experiments are typically hybrid workflows, where a classical computer performs the majority of the computation while a quantum processor executes a small, specialized subroutine. The goal is not to outperform classical supercomputers today, but rather to prepare systems, algorithms, and teams for the moment when scalable quantum hardware becomes available.

In this sense, current projects function primarily as proof-of-concept development. Organizations use quantum simulators or small-scale hardware to redesign parts of their computational pipelines so that they are compatible with future quantum processors. When large-scale machines — for example, processors with thousands of high-quality qubits — become available, institutions that have already developed this expertise will be able to integrate the technology rapidly.

Equally important is the development of human capital. Quantum computing requires a fundamentally different way of thinking about computation, combining ideas from physics, mathematics, computer science, and domain-specific expertise. Building this capability within an organization takes time. In many respects, the transition may be more disruptive than the adoption of AI, because it requires rethinking how certain computational problems are formulated and solved.

3.4.1 Case-Study: Portfolio Optimization With Constraint At SCBX

One example of quantum readiness initiatives is our ongoing research on portfolio optimization, a problem widely studied by global financial institutions. The objective is to construct investment portfolios that balance expected returns against risk while satisfying a variety of practical constraints.

Our current research focuses on designing more efficient quantum circuits for this class of optimization problems. In particular, we study methods for embedding real-world constraints — such as budget limitation or asset allocation rules — directly into the quantum operations themselves. The goal of this work is not immediate performance gains over classical optimization algorithms. Rather, it is to develop quantum-native formulations of financial optimization problems, ensuring that once larger and more reliable quantum processors become available, the algorithms and workflows required to utilize them are already in place.

3.5 Potential Applications In Finance

Quantum computing is frequently cited in the media as having transformative potential for the financial sector. However, from a scientific perspective, **rigorous research in quantum finance is still relatively limited**, and many proposed applications remain at an early exploratory stage.

This creates a significant opportunity for financial institutions to engage in **serious, foundational research** that could shape the future use of quantum technologies in finance. Several application areas are widely considered promising [3]:

1. Risk Management (Monte Carlo Simulations): Many financial risk calculations rely on **Monte Carlo simulations**, which estimate the probability distribution of possible market outcomes. These simulations are computationally expensive and are often used to compute metrics such as Value-at-Risk (VaR). Quantum algorithms for amplitude estimation may, in principle, accelerate certain Monte Carlo calculations, potentially reducing computation times from hours to near real-time, although published estimates suggest this will require large and very fast fault-tolerant machines [14]. If realized at scale, this could significantly improve the speed and responsiveness of risk assessment systems.

2. Fraud Detection: Another potential application lies in quantum machine learning, where quantum algorithms are used to analyze large datasets and detect complex patterns. In financial systems, such techniques could assist in identifying subtle anomalies in transaction data that may indicate fraudulent activity or systemic risk. Although still largely theoretical, this area represents an intersection of data science, cybersecurity, and quantum computing that warrants further investigation. A practical hurdle is that loading large amounts of classical data into a quantum computer is itself slow, which can erase the expected speedup.

3. Asset Pricing: Pricing complex financial derivatives often requires solving large systems of differential equations or performing high-dimensional numerical integrations. Quantum algorithms for linear systems and quantum simulation may offer new approaches to solving these problems with improved numerical precision. While practical demonstrations remain limited, such techniques could eventually improve the accuracy and efficiency of derivative pricing models.

4. Portfolio Optimization remains one of the most widely studied financial applications of quantum computing. However, the relevance of this problem varies significantly across institutions depending on their business strategies. At SCB, for example, our research focuses primarily on risk-aware portfolio construction rather than high-frequency trading optimization. In this context, the objective is not necessarily to compute solutions faster than competitors, but to explore how additional information — such as transaction data or alpha signals — can be integrated into the optimization process while maintaining controlled risk exposure. Quantum algorithms may eventually provide new methods for incorporating these constraints and signals into large-scale optimization models.

Recent industry pilots illustrate both the promise and the need for caution. In 2025, HSBC and IBM reported that a hybrid quantum workflow improved predictions of whether corporate bond trades would be filled, using real production-scale trading data [15]. Results like this are encouraging, but they have not yet been shown to beat the best classical methods in general.

3.6 Quantum AI: Promise And Reality

"Quantum AI" has become one of the most talked-about phrases in technology, and it now appears in national strategies, research-centre missions and product launches, including in Thailand (see Sections 6.1–6.2). It helps to separate two very different ideas hiding behind the same label. The first is **quantum for AI**: using quantum computers to speed up or improve machine-learning tasks such as classification, pattern recognition or generative modelling. The second is **AI for quantum**: using today's AI to help build and operate quantum computers themselves.

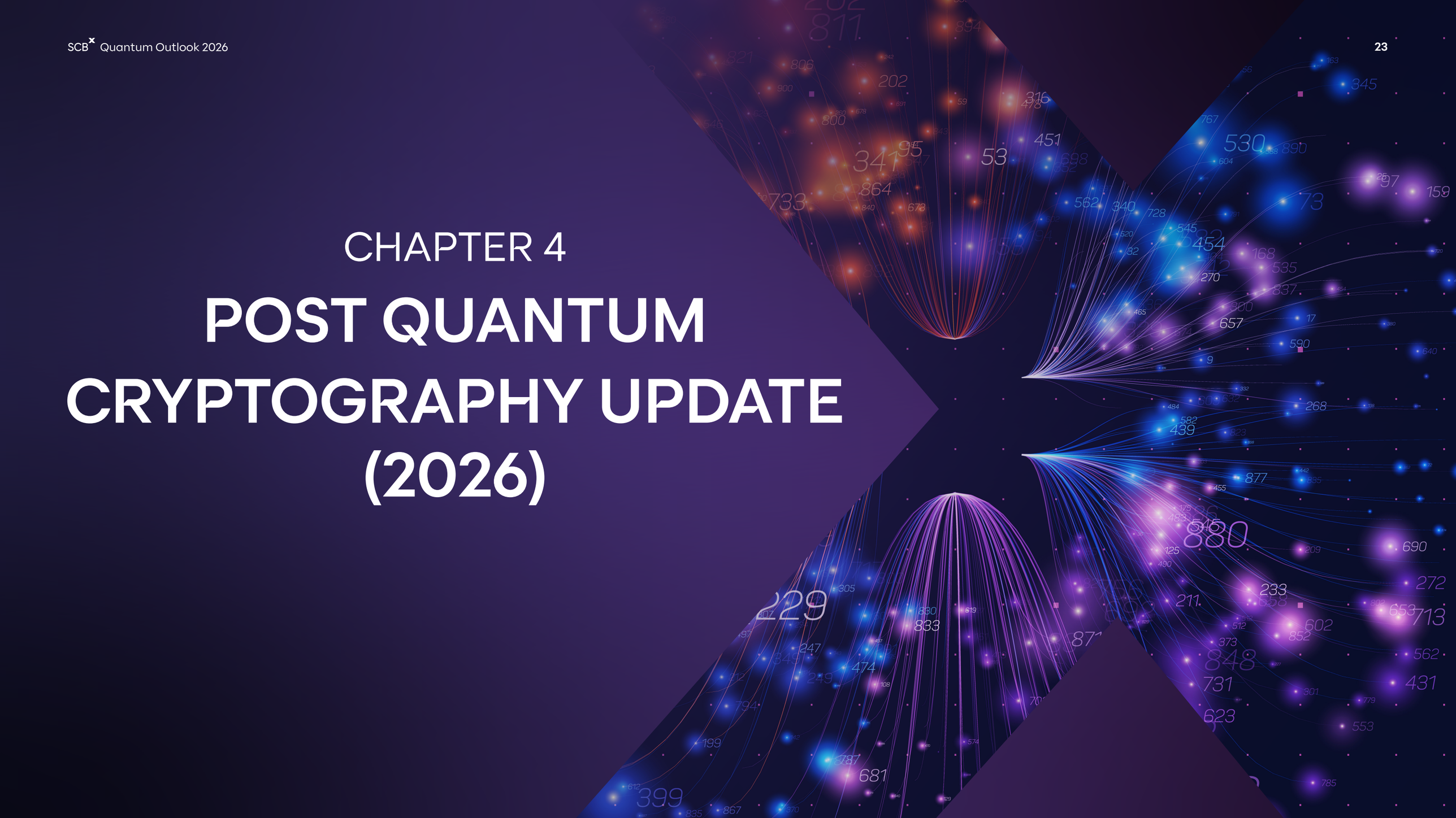
Perhaps surprisingly, the second direction is where the clearest results are today. AI models are already used to calibrate qubits, to help design chips and materials, and to spot errors in real time. Google DeepMind's AlphaQubit, for example, showed that a neural network can identify errors in a quantum processor more accurately than conventional methods [17], and Microsoft says it used AI tools to help redesign the materials in its Majorana 2 chip [18]. In other words, AI is helping to speed up the arrival of useful quantum computers which is one of the reasons the two technologies are increasingly discussed together.

The first direction (quantum computers making AI better) is promising but still largely unexplored at practical scale. Two hurdles matter most. First, today's AI runs on enormous amounts of classical data, and loading that data into a quantum computer is itself slow, which can cancel out the expected speedup. Second, several early claims of quantum machine-learning speedups were later matched by clever classical algorithms that borrow quantum ideas [19]. Quantum computers are therefore unlikely to replace GPUs for training large language models. Their more realistic role is narrower: working on problems where the data is itself quantum in nature (such as molecules and materials), generating training data that classical computers find hard to simulate, or acting as specialised components inside larger, mostly classical AI pipelines. Hardware makers are already positioning for this—Quantinuum, for instance, launched its Helios system in 2025 with a focus on what it calls "generative quantum AI" [20].

For SCBX, the practical message is to treat Quantum AI as a research frontier rather than a near-term product. Our work with SQ² on quantum approaches to problems such as fraud detection (Section 3.5) follows this spirit: building expertise, testing ideas carefully against strong classical baselines, and being ready to move quickly if genuine advantages emerge.

CHAPTER 4

POST QUANTUM CRYPTOGRAPHY UPDATE (2026)



4.1 Why Organizations Are Preparing Now

Modern digital services rely on cryptography to keep information private, verify identities and confirm that transactions are genuine. A large part of this trust depends on public-key cryptography - methods used to secure digital connections and create digital signatures. A sufficiently powerful quantum computer is expected to weaken some of the public-key methods widely used today. Post-quantum cryptography (PQC) refers to newer cryptographic methods designed to remain secure against that future capability. [1]

No publicly known quantum computer can break these methods at the scale required for real-world attacks today. The challenge is time. Replacing cryptography across a large organization can take years, and some sensitive information must remain confidential for many years. Information captured now could therefore still be valuable if it becomes possible to decrypt later. Preparation has to begin before the threat becomes operational.

Key idea: **the quantum threat is real even though its exact timing is unknown; the time needed to prepare is already measurable.**

4.2 Migration Deadlines Are Closer

The clearest 2026 change is that governments are putting dates around migration even though the arrival of a cryptography-breaking quantum computer remains uncertain. In the United States, Executive Order 14412 requires high-value and high-impact federal systems to use post-quantum methods for establishing encryption keys by the end of 2030 and for digital signatures by the end of 2031. A follow-on federal implementation plan extends the broader migration programme through 2035. [5,6]

Executive Order 14413, issued at the same time, aims to accelerate U.S. quantum research and commercialization. Read together, the two Orders show a deliberate policy choice: continue advancing quantum capability while reducing dependence on cryptography that future quantum systems could threaten. [7]

For organizations outside the U.S. federal system, the main effect is likely to come through technology suppliers and industry practice rather than direct legal reach. Cloud, security, identity, network and software providers that serve regulated or government customers will increasingly need to support post-quantum requirements. Similar planning is visible elsewhere: Australia is targeting completion of its transition by the end of 2030, while Singapore is moving from general guidance toward measurable readiness expectations for financial institutions. [8-10]

For decision-makers, 2030 is therefore becoming a useful planning horizon for high-priority systems. It should not be read as a forecast of when current cryptography will fail.

4.3 Q-Day Might Be Closer Than We Thought And Risk-Associated With It Is Quite Certain

The policy timetable is becoming clearer; the technology timetable is not. Research continues to refine estimates of how much quantum computing power would be needed to break widely used public-key cryptography. These studies are theoretical and depend on different assumptions about hardware, error correction and operating speed, so their numbers should not be treated as a single forecast.

One recent example is a May 2026 study by Tian Xue and Jacob Covey. It modelled how an attack on RSA-2048 - a commonly used form of public-key cryptography - could be distributed across a modular system of about 500,000 qubits, the basic units of quantum computation. The study did not demonstrate an actual attack. Its importance is that new methods of designing and organizing quantum systems can change the estimated resources required. [3]

Planning implication: **organizations should not tie migration to one qubit count or one predicted date. Data lifetime, system criticality and the time needed to change should drive preparation.**

4.4 From Standards To Implementation

The U.S. National Institute of Standards and Technology (NIST) has finalized its first post-quantum cryptography standards and continues to encourage organizations to begin migration. This removes an important source of uncertainty: usable standards now exist. The remaining challenge is to introduce them into real systems without disrupting the services that depend on those systems. [1]

In a large organization, cryptography is spread across websites, digital certificates, identity systems, secure connections, payment services, devices and third-party platforms. Migration therefore requires more than replacing one algorithm. Organizations need to know where vulnerable cryptography is used, which business services depend on it, which products can be upgraded, and where suppliers control the timetable.

Organizations should also plan for future change. Crypto-agility means the ability to replace cryptographic methods without rebuilding the whole business system. NIST's updated guidance treats this as an architectural and operational capability rather than a one-time technology upgrade. In practical terms, systems, contracts and operating processes should make later cryptographic changes manageable. [2]

4.5 What The Financial Sector Is Already Learning

Evidence from the financial sector supports this systems view. The Bank for International Settlements (BIS) Innovation Hub tested post-quantum digital signatures in an operational payment environment through Project Leap Phase 2. The main lessons were broader than the algorithm itself: different systems and products had to work together, performance had to remain acceptable, and organizations had to coordinate changes across the service. A later BIS project, FuSSE, similarly treated quantum readiness and the ability to change cryptography as design requirements for future settlement infrastructure. [11,12]

For banks and other financial institutions, this is particularly relevant because critical services often depend on long-lived infrastructure and external providers. A technology supplier may be broadly "post-quantum ready" while a specific product version, certificate service or payment component is not. Readiness therefore depends on evidence at the level of the actual service, not only on a supplier statement or an algorithm name.

4.6 Regional Direction Is Becoming Clearer

Singapore provides a useful regional example of how preparation is becoming more structured. In 2026, the Cyber Security Agency of Singapore (CSA), GovTech and IMDA issued a final Quantum-Safe Migration Handbook and Quantum Readiness Index, giving organizations a common way to assess progress. The Monetary Authority of Singapore (MAS) has also stated that it aims for financial institutions to become quantum-resilient - able to maintain security as quantum technology advances - before the end of the decade. [9,10]

Thailand is earlier in the policy cycle, but the direction is also becoming clearer. The National Cyber Security Agency (NCSA) opened the draft Quantum Security Framework 2026-2035 for public consultation from 15 to 29 July 2026. The draft Quantum Security Transition Master Plan proposes phased implementation: readiness assessment and cryptographic inventory in 2026-2027, pilots and technical validation in 2027-2030, and broader migration through 2035. These are proposed planning milestones in draft policy-development material, not adopted regulatory obligations. [13-15]

For financial institutions, the practical message is consistent across these developments. Quantum readiness is becoming a technology-risk discipline: organizations need to understand where vulnerable cryptography is used, which systems matter most, whether suppliers can support the transition, what has been tested, and who is responsible for the next decision.

Readiness is moving from awareness to evidence: **visibility, prioritization, supplier readiness, testing and clear ownership.**

4.7 Preparing For The Implementation Phase

Organizations do not need to wait for final regulatory requirements to begin foundational work. Thailand's draft Quantum Security Framework and draft Quantum Security Transition Master Plan follow a sequence also seen internationally: understand the current environment, prioritize by risk, test before scaling, and keep evidence of progress. The documents remain draft, but they offer a useful domestic reference for how implementation may be structured. [13,14]

An early priority is visibility. Organizations should identify where vulnerable cryptography is used, which systems depend on it and who owns those systems. A cryptographic inventory is simply a record of where encryption, digital signatures and related security mechanisms are used. It does not need to be perfect on day one; it needs to be good enough to show what may have to change. Prioritization can then focus on long-lived sensitive information, identity, payments, key management and other critical services, while considering how difficult each system is to change and how dependent it is on suppliers. The practical implication is to direct limited time and resources first to systems where delayed migration would create the greatest business or security risk. [13,14]

Supplier readiness and practical testing come next. Banks and other large organizations should ask key providers what post-quantum support is available, when upgrades are expected and how long older methods will remain supported. Before migration is expanded, organizations should test a real service from end to end rather than an algorithm in isolation. The aim is to confirm that applications, certificates, key-management services, network components and operating processes continue to work together with acceptable performance and reliability. BIS Project Leap provides a useful example of why system-level testing matters. [11,14]

Finally, quantum readiness should become part of normal technology-risk governance. Organizations should keep the inventory current, track supplier progress, assign clear ownership, record remaining risks and review readiness periodically. The objective is not to predict exactly when quantum computing will become a practical threat to cryptography. It is to make the transition controlled, evidence-based and timely enough that organizations are not forced into disruptive change later.

CHAPTER 5

GLOBAL INVESTMENT LANDSCAPE AND THE EFFORT TO BUILD QUANTUM COMPUTERS





5.1 Landscape: From Research Ecosystem To Quantum Supply Chain

The global quantum ecosystem is moving from a research-led phase into an early stage of commercial industrialization. That does **not** mean the industry is mature: most quantum technologies are still at an early stage of commercialization. But the structure of the field is changing. Instead of a single company trying to do everything—from hardware physics to end-user applications—an increasingly segmented supply chain is emerging, with specialized firms operating at different abstraction layers. Several recent analyses explicitly compare this trajectory to the historical evolution of the semiconductor industry, where long-run scale came from specialization rather than full vertical integration [1]

This shift is visible not only in company formation, but also in policy and capital flows. OECD and EPO report that more than 30 countries have introduced tailored quantum policies, including 18 OECD countries with comprehensive national strategies [4]. In the United Kingdom, the government has committed a ten-year £2.5 billion programme for quantum research and innovation [5]. The European Commission's Quantum Technologies Flagship is a ten-year initiative with an expected €1 billion EU budget [6]. In the United States, federal quantum R&D budgets have risen substantially since 2019 under the National Quantum Initiative, and in late 2025 the Department of Energy announced $625 million to renew its five National Quantum Information Science Research Centers [7-8]

Private and public investors are also scaling up. According to McKinsey's Quantum Technology Monitor 2026, investment in quantum-technology start-ups jumped to about $12.6 billion in 2025—roughly 6.3 times the 2024 level—with around 60% concentrated in the ten largest deals [15]. Strikingly, the public share of start-up funding fell from about one-third in 2024 to just 3% in 2025, as stock-market listings and private capital took over. Major corporate commitments followed in 2026: IBM announced plans to invest more than $10 billion in quantum over five years, and Quantinuum raised $1.7 billion in its stock-market listing [16][19]. OECD's ecosystem analysis (December 2025) notes that public support nonetheless remains important for the field's research base [4].

For financial institutions, the strategic implication is important: the quantum economy is no longer just about owning hardware. It is becoming a layered ecosystem in which most enterprises will participate near the top of the stack—through cloud access, workflow integration, sector-specific algorithms, and internal capability building—rather than through fabrication of qubits or operation of cryogenic systems [1]. For quantum computing, the supply chain is structurally stratified as follows:

Supply Chain Layer	Functional Description	Representative Companies / Leaders
1. Materials and equipment	This is the enabling physical base: cryogenic systems, lasers, vacuum systems, photonics, control electronics, specialized materials, and fabrication tools.	Bluefors, Oxford Instruments, Applied Materials, and other suppliers whose products are often shared with adjacent deep-tech and semiconductor ecosystems.
2. Qubit fabrication and hardware	The creation of the actual physical processors. This layer is highly diversified, exploring various quantum modalities to mitigate the risk of technological dead-ends. Competing hardware modalities include superconducting circuits, trapped ions, neutral atoms, photonics, spin qubits, and annealing-based systems.	IBM, Google, Atom Computing, IonQ, Pasqal, QuEra, Microsoft, PsiQuantum, D-Wave.
3. Middleware and control Systems	The critical classical-quantum interface. This involves the orchestration software, pulse control, microwave electronics, calibration stacks, and hybrid runtime infrastructure.	Quantum Machines, Emergence Quantum, Horizon Quantum, Conductor Quantum, Zurich Instruments, Keysight, Qblox, and NVIDIA (CUDA-Q / NVQLink).
4. Error correction, suppression, and runtime reliability	This is the layer that helps translate noisy physical qubits into more stable logical operations (logical qubits). It includes decoders, error-suppression tools, and hardware-efficient error-correction architectures.	Riverlane, QuEra, Alice & Bob, alongside in-house efforts from major hardware players.
5. Algorithms and software development	This layer abstracts away hardware complexity and focuses on useful methods for optimization, simulation, machine learning, and workflow design.	Phasecraft, QC Ware, Classiq, and Multiverse Computing.
6. Application and cloud access layer	This is where most enterprises will first engage: through quantum-as-a-service and hybrid cloud platforms that connect classical HPC and enterprise workflows to quantum processors.	IBM Quantum Platform, Amazon Braket, Microsoft Azure Quantum, Google Cloud, and Oracle Cloud (hosting Quantinuum's Helios) [19].

The Quantum Computing Supply Chain Stack



The quantum ecosystem has evolved into specialized abstraction layers. Financial institutions engage primarily at the Application and Cloud Access layers, leveraging the underlying innovations without needing to manage physical hardware.

For an organization such as SCBX, this layered structure means the most relevant investment is unlikely to be in hardware ownership. It is more likely to be in talent, partnerships, data readiness, use-case selection, hybrid workflow design, and the internal ability to evaluate when a quantum or quantum-inspired method is genuinely better than a classical baseline. That is a much narrower, and more realistic, strategic commitment than "building a quantum stack" from scratch.



5.2 Economic Impact Projections: How To Read The Numbers Carefully

The first point of discipline is that several different kinds of numbers are often mixed together in public discussions of quantum computing. These should be separated.

First, there is **capital invested into the sector**: venture funding, corporate funding, and government programmes. Second, there is **market revenue**: the amount quantum-technology vendors may earn by selling hardware, software, services, and infrastructure. Third, there is **economic value unlocked for users**: the additional revenue, cost savings, productivity gains, or risk reduction that quantum-enabled workflows may create for sectors such as finance, chemicals, healthcare, and logistics. These are not the same thing, and they should not be added together.

On the *market-size* side, McKinsey estimates that by 2035 the combined quantum-technology market could reach up to $97 billion in annual revenue worldwide, of which quantum computing could account for about $28 billion to $72 billion, quantum communication $11 billion to $15 billion, and quantum sensing $7 billion to $10 billion [10]. McKinsey presents these as ranges precisely because the outcome depends heavily on technology progress, adoption speed, and scaling assumptions. McKinsey's 2026 update revises this outlook to roughly $60–100 billion for the overall quantum-technology market by 2035, with quantum computing accounting for about $43–71 billion [15].

On the economic-value side, the numbers are larger because they refer to value created in downstream industries rather than supplier revenue. McKinsey estimates that quantum computing could unlock roughly $0.9 trillion to $2.0 trillion in economic value by 2035 across four major industry groups: global energy and materials, pharmaceuticals and medical products, financial services, and travel, transport, and logistics [11]. Within that broader picture, McKinsey's finance work estimates $400 billion to $600 billion in potential value for financial services by 2035 [12]. Its analysis gives $200 billion to $500 billion for pharmaceutical sector [13], and a similar $200 billion to $500 billion range in chemical sector [14]. These figures are best read as "value at stake under favorable adoption scenarios," not as guaranteed outcomes.

The rationale behind these estimates is usually straightforward, even if the exact numbers are uncertain. The value does not come from quantum computing being "faster" in the abstract. It comes from better answers to expensive computational problems: more accurate molecular simulation, better portfolio and risk calculations, improved routing and scheduling, faster design cycles, and improved decision quality in settings where even a small percentage improvement has meaningful financial consequences. In that sense, the strongest economic case for quantum computing is not broad automation; *it is targeted improvement in very costly decision problems.*

That said, these projections should be treated with caution for at least four reasons. First, the hardware path remains uncertain: the field has made real progress, but scaling reliable *logical qubits* is still the central bottleneck. Second, many early business applications will be **hybrid**, meaning that value may arrive gradually rather than through a single moment of universal "quantum advantage." Third, the ecosystem is still immature and unusually dependent on public funding and strategic partnerships. Fourth, sector estimates often rest on scenario analysis and may overlap conceptually, so they should not be aggregated too aggressively.

For SCBX, the right interpretation is therefore not that quantum computing will certainly produce a precise dollar amount of value by 2035. Rather, it is that several independent analyses now place finance among the sectors with the highest potential exposure—both upside and strategic risk—if the technology matures. The appropriate response is *not speculative overcommitment, but disciplined readiness:* build internal understanding, identify narrow high-value use cases, run hybrid pilots where sensible, and stay close enough to the ecosystem to move when the technology genuinely crosses the threshold from interesting to economically useful.

CHAPTER 6

THAILAND POSITIONING



6.1 National Strategic Pivot

Thailand's quantum push should be understood not as a single project, but as the early formation of a national capability stack. The country already has a formal policy foundation: the **Thailand Quantum Technology Roadmap 2020–2029**, issued under the Ministry of Higher Education, Science, Research and Innovation, which identified the whole quantum technologies as strategic pillars for long-term national development.

The Roadmap had been collaboratively written and pushed forward by **QTRic (Quantum Technology Research Initiative Consortium)**, which describes itself as a collaborative network of Thai quantum researchers who work on quantum technologies including not only quantum computing but also expanding to quantum simulation, quantum communication, and quantum sensing and metrology. In that context, the national objective is best framed not as immediate technological self-sufficiency, but as a gradual move up the value chain: from being primarily a user of imported digital technologies to building domestic talent, research infrastructure, and selected areas of technological ownership. Public policy, university programs, and early private-sector activity are beginning to align around that goal.

6.2 Siam Quantum Square (SQ²)

A recent institutional milestone was the launch of **Siam Quantum Square (SQ²)** at Chulalongkorn University on 26 January 2026. According to the university, SQ² is intended to serve as a **national quantum hub for quantum research, talent development, and cross-sector collaboration.**

The center focuses on several key areas including:

- Quantum computing and quantum algorithms
- Quantum Artificial Intelligence (Quantum AI), also known as Quantum machine learning
- Superconducting qubit systems and experimental quantum hardware

Its activities are supported by national research programs including the Reinventing University initiative and PMU-B under MHESI [3], as well as internal Chulalongkorn funding such as the CU Power Grant.

Expertise. SQ² combines **fundamental research, and industry-facing applied work.**

On the scientific side, the center conducts rigorous academic research into the physics and mathematics underlying **Quantum AI** and new classes of **Quantum Algorithms** capable of processing information in ways fundamentally different from classical computation.

Experimentally, SQ² is also developing expertise in **superconducting materials and thin-film fabrication**, supporting long-term research toward domestic quantum hardware capabilities.

Importantly, the center is also structured to work directly with industry. Collaborations with partners such as SCBX (formalised through an MoU in May 2026; see Section 6.3) allow researchers to explore how quantum computing might operate in real enterprise environments and what kinds of financial or industrial problems may ultimately benefit from quantum advantage.

SQ² also provides **consultation and readiness programs** for companies and government agencies interested in preparing for the quantum era. In addition, the center plans to release graduate quantum programs for university students.

Vision And Future Prospect. SQ²'s long-term mission extends beyond academic research. The center aims to serve as a strategic anchor for Thailand's emerging quantum ecosystem, focusing on several key objectives:

- Establish itself as a **globally visible research node** in quantum science and technology
- Build strong connections between academic research and industrial applications
- Support organizations in becoming **quantum-ready** through training and collaboration
- Cultivate the next generation of **quantum scientists, engineers, and developers**
- Contribute to the formation of a sustainable **national quantum innovation ecosystem**

In practical terms, this means building the infrastructure required for Thai researchers and engineers to translate **quantum physics into deployable technologies.** Through these efforts, SQ² aims to strengthen Thailand's **cognitive workforce**—equipping physicists, engineers, and data scientists with the advanced skills needed to participate in the global quantum technology economy.

International Connections. Crucially, to guarantee immediate integration into the highly segmented global quantum supply chain, SQ² secured high-level, strategic partnerships with international technology leaders. Collaborations with entities such as **IBM Thailand, Western Digital, South Korea's Qunova Computing**, and **Japan's National Institute of Advanced Industrial Science and Technology (AIST)** ensure that Thailand's domestic quantum ecosystem remains globally interoperable, commercially viable, and technologically synchronized with state-of-the-art advancements.



6.3 Key Players From Industrial Sector

Within the private sector, one main actor is the **Quantum Technology Foundation (Thailand) (QTFT)**, a Bangkok-based **consulting company focused on "quantum-ready" tools for modelling and optimizing complex enterprise networks.** The company emphasizes optimization use cases and enterprise readiness rather than hardware development, which makes it particularly relevant to industries such as logistics, energy, and financial services [2]. QTFT also plays a crucial role in catalyzing a secure and seamless national transition into the quantum era by proactively integrating quantum-resistant cybersecurity protocols (Post-Quantum Cryptography, or PQC) across corporate and governmental digital infrastructures.

Another notable industrial contributor is **SCBX**, which has begun investing in quantum technology exploration and is among **the first large Thai enterprises actively preparing for quantum readiness.** SCBX collaborates with SQ² to investigate potential applications of quantum computing in finance. This includes research into quantum algorithms for key financial problems such as portfolio optimization and fraud detection, as well as broader exploration of how quantum computing might eventually enhance financial modelling and risk analysis. In May 2026, SCBX and Chulalongkorn University formalised this partnership through a Memorandum of Understanding covering frontier research, ecosystem-building activities, and the co-development of this SCBX Quantum Outlook report [8].

Beyond its research efforts, SCBX is also contributing to the development of Thailand's broader quantum ecosystem from the industrial sector. Lastly, SCBX is working with QTFT on the implementation of **Post-Quantum Cryptography (PQC),** positioning the organization among the early adopters preparing financial infrastructure for the post-quantum security era.

Large Thai conglomerates are also entering the field. CP Group and True Corporation co-founded Quantum Club Thailand in 2026 and are using True Digital Park as a hub where local companies can test quantum-hybrid applications, with the stated ambition of positioning Thailand as ASEAN's quantum hub [6].

6.4 A Distributed Thai Quantum Research Ecosystem

Thailand's quantum activity is also geographically distributed. Rather than concentrating every capability in one institution, the ecosystem appears to be developing through a networked model in which different universities contribute different strengths. A useful coordinating mechanism here is **QTRic** which has been presented by Thai science diplomacy channels as part of a broader national investment in frontier science [4]. This creates a comprehensive, nationwide quantum ecosystem that industry can seamlessly tap into:

- **Central Region (Bangkok) – Chulalongkorn University:** Serving as the core of the national network in quantum computing and quantum algorithms, as well as housing SQ² – this hub focuses deeply on quantum computing theory, superconducting qubit technology, algorithmic development, and software engineering, alongside talent development and business-facing executive education. For sectors such as finance, this makes Bangkok particularly relevant as the point where research capability, enterprise training, and early use-case development can meet.

- **Northeastern Region – Suranaree University of Technology (SUT):** Hosting QTRic, SUT plays an important role in the national network through QTRic and through visible work in **quantum sensing**. Public SUT materials and conference records show activity around **NV-diamond magnetometry** and quantum sensing, including thesis work on magnetic-field imaging with quantum diamond sensors and conference programming on quantum diamond magnetometer technology. This positions SUT as a meaningful node in sensing and metrology-oriented quantum research [5].

In addition, **The Institute for Fundamental Study (IF) – Naresuan University** has started to work on Post Quantum Cryptography in collaboration with QTFT.

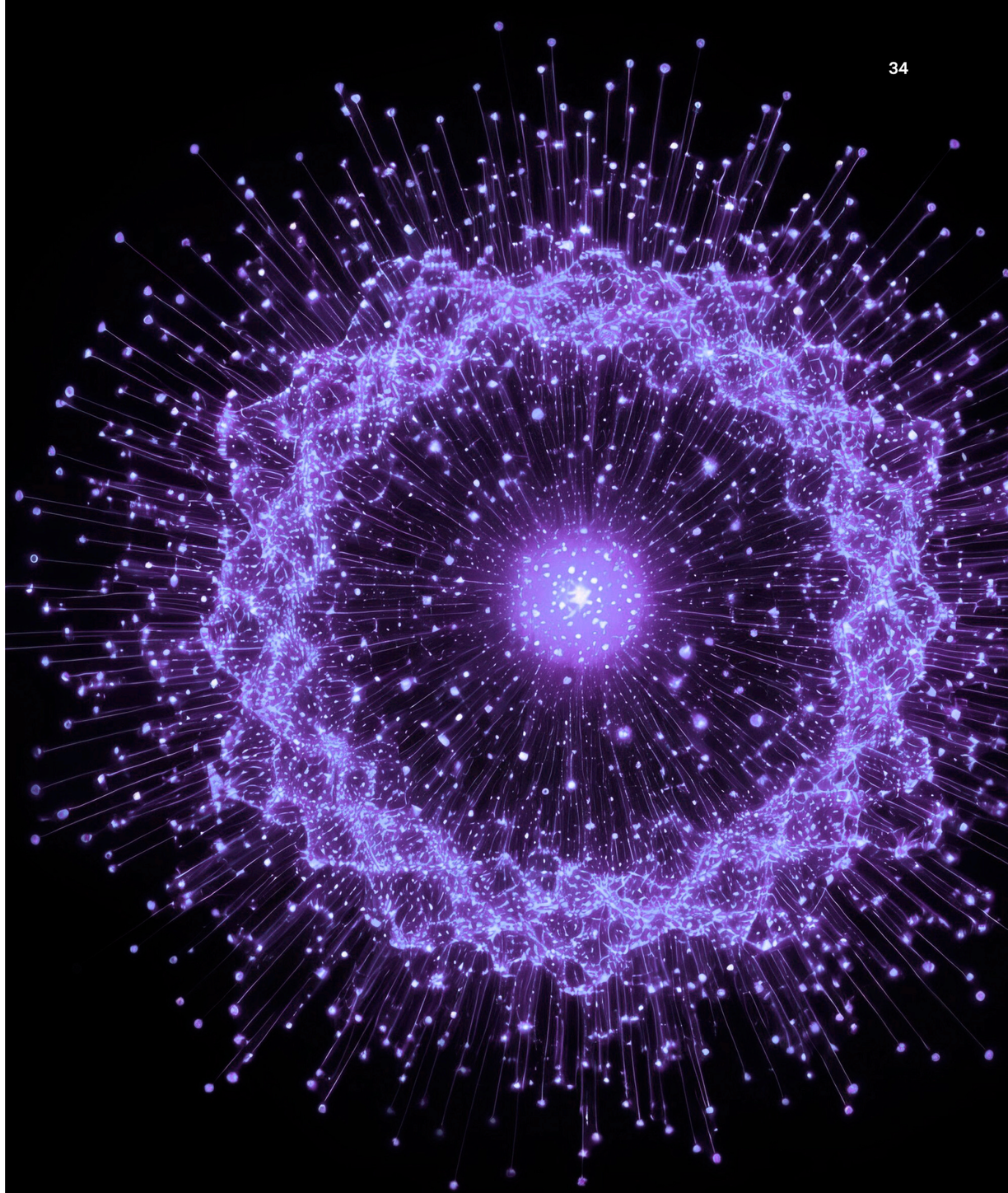
- **Northern Region – Chiang Mai University (CMU):** Leading the nation in experimental Quantum Simulation research, CMU utilizes highly advanced physical setups—such as neutral atom simulation experiments—with the goal of accurately modeling complex chemical, biological, and physical interactions. The platform can also be used to study exotic quantum phases.

- **Southern Region – Prince of Songkla University (PSU):** Taking charge of Quantum Communication research, PSU is pioneering critical experiments in Quantum Key Distribution (QKD) protocols. QKD can distribute cryptographic keys over specialized links, while post-quantum cryptography (PQC) provides a more broadly deployable route to protecting financial and governmental networks against quantum attacks.

6.5 Moving Forwards Together

Taken together, the distributed nature of these national initiatives suggests a highly pragmatic strategy: Thailand's comparative advantage will likely come less from trying to reproduce the capital-intensive, full quantum hardware stack of the largest global powers, and more from building a coordinated, specialized, and internationally connected ecosystem. This model ties directly back to the supply chain realities outlined in Section 5.1 Thailand does not need to own the entire quantum computing supply chain to participate in it meaningfully. By focusing on specific, high-value abstraction layers—such as algorithmic development, hybrid software integration, and strategic domestic niches like quantum sensing—the country can enter the global market where its domestic strengths are already emerging, gradually deepening its technological sovereignty and economic role over time.

Executing this strategy of smart specialization, however, requires a unified, cross-sector effort. Translating academic research into tangible economic value demands that industrial companies, government stakeholders, and quantum experts work coherently together. Public sector agencies must continue to provide the foundational digital infrastructure and supportive funding frameworks. Academic and research hubs, such as SQ² and QTRic, must remain focused on advancing applied science and cultivating a quantum-ready workforce. Crucially, forward-thinking industrial leaders and industry-bridging organizations—such as SCBX and QTFT—must act as the commercial catalysts. By defining high-value business use cases, providing complex real-world data landscapes, and piloting hybrid workflows today, the private sector creates the critical demand signal that accelerates the entire national ecosystem. Ultimately, moving forward together ensures that Thailand will not merely be a passive consumer of the coming quantum revolution, but a resilient, integrated, and value-generating contributor to it.



Ending Remarks:
The Quantum Imperative



The shift from classical to quantum computing is not simply another IT upgrade. It is a longer-term change in how difficult problems may be represented, simulated, optimized, and processed. Fully fault-tolerant, large-scale quantum computers are still under development, but the preparation phase is already underway—in global industry, in national policy, and increasingly in Thailand itself.

For enterprise leaders and national stakeholders, the practical message is not that quantum value is guaranteed tomorrow. It is that waiting until the technology is fully commoditized may create a costly capability gap. Achieving **quantum readiness** today is thus a strategic imperative.

The organizations most likely to benefit will be those that begin early in a disciplined way: building technical literacy, identifying narrow but high-value use cases, preparing data and security architectures, and forming the right research and industry partnerships. As with other exponential technologies, the penalty for falling behind is steep. The complex technical expertise required for mastery means that catching up will be a very slow process—even more so for quantum technologies than for AI.

In that sense, Thailand's goal should not be to imitate the largest quantum powers line by line. It should be to develop credible domestic strengths, connect them to global networks, and make sure that when quantum technologies become economically decisive in selected sectors, Thailand is prepared not only to adopt them, but to contribute to them.

Appendix

Appendix A:
Glossary Of Terms

To ensure clarity across all levels of the organization, the following definitions summarize the core concepts discussed in this report:

- **Qubit:** The fundamental unit of quantum information. Unlike a classical bit (0 or 1), a qubit can exist in a state of **superposition**, representing a combination of both 0 and 1 simultaneously.
- **Entanglement:** A quantum phenomenon where qubits become interconnected such that measurement results on them are correlated in ways that have no classical equivalent, regardless of distance. Entanglement does not send information instantly, but it is an essential resource for quantum algorithms and error correction.
- **Quantum Advantage:** The point at which a quantum computer solves a commercially relevant problem faster, cheaper, or more accurately than any known classical method (Level 3 in Section 3.1). The press often uses the term more loosely for any task where a quantum computer beats classical methods.
- **NISQ (Noisy Intermediate-Scale Quantum):** The current era of quantum hardware, where processors are large enough to perform complex tasks but remain sensitive to environmental "noise," leading to errors.
- **Fault-Tolerance:** The ability of a quantum computer to continue operating correctly even when individual components fail or errors occur, achieved through complex error-correction codes.
- **Physical vs. Logical Qubit:** A physical qubit is a single, error-prone hardware element. A logical qubit is a more reliable qubit built by combining many physical qubits with error correction—like a team that checks each other's work.
- **Quantum Error Correction (QEC):** Techniques that spread information across many physical qubits so that errors can be detected and fixed during a computation without destroying the quantum state.
- **Magic States / T-gate:** Special resources needed to perform the one type of operation (the "T-gate") that standard error-correction schemes cannot protect cheaply. Producing them efficiently is a major engineering challenge.
- **Post-Quantum Cryptography (PQC):** New encryption methods, standardised by bodies such as NIST, that run on today's computers but are designed to resist attacks from future quantum computers.
- **CRQC / Q-Day:** A cryptographically relevant quantum computer (CRQC) is one powerful enough to break today's public-key encryption; "Q-Day" is the day such a machine exists.
- **Variational Quantum Algorithm (VQA):** A hybrid approach that uses both quantum and classical computers to solve optimization problems, widely used in today's near-term experiments, although attention is shifting toward early error-corrected algorithms.

Appendix B:
Technical Deep-Dive – SCBX Portfolio Optimization Research

This section explains preliminary finding research conducted by the **SCBX** collaborative with **Chulalongkorn University** regarding "Portfolio Optimization with Constraint."

The Problem: Constraint Enforcement

In financial modeling, portfolios must adhere to strict rules (e.g., "invest exactly 100% of the budget" or "select exactly 5 assets"). Standard quantum approaches often explore "invalid" solutions, wasting computational time and reducing accuracy.

The Solution: The Preserving Mixer

The research introduced a specialized quantum circuit architecture known as a **Preserving Mixer**. This architecture mathematically restricts the quantum computer's search space to only include portfolios that meet all predefined constraints. It builds on the "Quantum Alternating Operator Ansatz" framework of Hadfield et al. (2019), which first proposed constraint-preserving mixers, and tailors it to realistic portfolio constraints.

Key Performance Benchmarks:

- **Training Stability:** Our methodology demonstrated a significantly higher **MaxProb ratio**, meaning the algorithm finds the optimal solution with much higher consistency. (MaxProb measures how likely the algorithm is to return the single best portfolio.)
- **Scalability:** By mitigating the **Barren Plateau** effect (where training signals disappear in large systems), this approach is expected to help the optimization remain trainable as problems grow beyond the 11-qubit experiments performed so far—a promising sign that still needs to be confirmed on larger problems and real hardware.

Appendix C:
The Quantum Readiness Checklist

Organizations can use this framework to assess their current position and prepare for the transition to quantum-enhanced operations.

1. Strategic Identification: Identify the top three "intractable" optimization or simulation problems within your core business units (e.g., risk modeling, supply chain, molecular discovery).

2. Quantum Champion: Designate a technical lead or "Quantum Champion" to monitor hardware milestones and maintain a roadmap.

3. Data Architecture: Ensure data pipelines are "clean" and capable of feeding into hybrid classical-quantum workflows.

4. Ecosystem Mapping: Identify potential academic and industrial partners (e.g., SQ²) for joint R&D initiatives.

5. Cryptography Audit: Evaluate the organization's long-term data security and begin planning for the transition to Post-Quantum Cryptography (PQC). With regulators now setting firm deadlines (e.g., US Executive Order 14412 of June 2026), start with an inventory of where vulnerable cryptography is used.

6. Milestone Watch: Track a short list of dated external signals—for example IBM's Kookaburra module, Microsoft and Atom Computing's "Magne" machine, Quantinuum's Sol, and independent verification of quantum-advantage claims—and agree in advance what action each would trigger.

7. Talent Pipeline: Assess the internal "AI-to-Quantum" transition path for current data scientists and engineers.

References:

CHAPTER 1: Summary

[1] https://physics.mit.edu/news/quantum-computing-reality-check-what-business-needs-to-know-now/#:~:text=Credit%3A%20Adam%20Glanzman,Credit%3A%20Adam%20Glanzman

[2] https://www.scbx.com/th/scbx-exclusive/scbx-quantum-outlook/

[Feynman1982] Feynman, R. P. (1982). "Simulating physics with computers." International Journal of Theoretical Physics, 21, 467–488

[PNAS2017] Reiher, M., Wiebe, N., Svore, K. M., Wecker, D., & Troyer, M. (2017). "Elucidating reaction mechanisms on quantum computers." Proceedings of the National Academy of Sciences (PNAS), 114(29), 7555-7560.

[Shor] Shor, P. W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings 35th Annual Symposium on Foundations of Computer Science (IEEE).

[Kempe2006] Kempe, J., Kitaev, A., & Regev, O. (2006). "The Complexity of the Local Hamiltonian Problem." SIAM Journal on Computing, 35(5), 1070–1097. DOI: 10.1137/S0097539704445226.

[Preskill2018] Preskill, J. (2018). "Quantum Computing in the NISQ era and beyond." Quantum, 2, 79.

[WEF1] World Economic Forum in collaboration with Accenture. (January 2025). Embracing the Quantum Economy: A Pathway for Business Leaders.

[WEF2] World Economic Forum in collaboration with Accenture. (October 2025). Quantum Technologies: Key Opportunities for Advanced Manufacturing and Supply Chains.

[WEF3] World Economic Forum in collaboration with Accenture. (December 2025). Quantum Technologies: Strategic Imperatives for Health and Healthcare Leaders.

[WEF4] World Economic Forum in collaboration with Accenture. (July 2025). Quantum Technologies: Key Strategies and Opportunities for Financial Services Leaders.

CHAPTER 2: Quantum Computing for Laypeople

[1] SCBX. (December 2025). SCBX Quantum Outlook: Post-Quantum Cryptography.

[2] Shor, P. W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings 35th Annual Symposium on Foundations of Computer Science (IEEE).

[3] Kitaev, A. Y. (1995). "Quantum measurements and the Abelian Stabilizer Problem." arXiv:quant-ph/9511026.

[4] Harrow, A. W., Hassidim, A., & Lloyd, S. (2009). "Quantum algorithm for linear systems of equations." Physical Review Letters, 103(15), 150502.

[5] Reiher, M., Wiebe, N., Svore, K. M., Wecker, D., & Troyer, M. (2017). "Elucidating reaction mechanisms on quantum computers." Proceedings of the National Academy of Sciences (PNAS), 114(29), 7555-7560.

[6] https://quantumalgorithmzoo.org/

CHAPTER 3: Progress towards quantum advantage

[1] Financial Services & Quantum: Making Big Decisions When Seconds Equal Money, Third Quarter 2023, https://www.vedp.org/news/financial-services-quantum-making-big-decisions-when-seconds-equal-money

[2] https://www.sciencenews.org/article/google-quantum-supremacy-claim-controversy-top-science-stories-2019-yir#:~:text=Google%20claimed%20quantum%20supremacy%20in%202019%20%E2%80%94%20and%20sparked%20controversy

[3] Herman, D. et. al. Quantum computing for finance, Nature Review Physics 2023 https://www.nature.com/articles/s42254-023-00603-1

[4] Arute, F. et al. (2019). "Quantum supremacy using a programmable superconducting processor." Nature, 574, 505–510.

[5] Kim, Y. et al. (2023). "Evidence for the utility of quantum computing before fault tolerance." Nature, 618, 500–505.

[6] IBM Newsroom (30 July 2026). "IBM and The University of Chicago Demonstrate Quantum Advantage, Establishing Trusted Quantum Computation on Logical Circuits."

[7] Replace or supplement with Manabe, H., Gu, H., & Pan, F. (13 August 2026). 'Classical Simulation and Design Frontiers for IBM's Doped Clifford Sampling Experiment.' arXiv:2608.13110.

[8] Lee, J. et al. (2021). "Even more efficient quantum computations of chemistry through tensor hypercontraction." PRX Quantum, 2, 030305.

[9] Gidney, C. (2025). "How to factor 2048 bit RSA integers with less than a million noisy qubits." arXiv:2505.15917.

[10] Webster, P. et al. (2026). "The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes." arXiv:2602.11457.

[11] Babbush, R. & Neven, H., Google Research (31 March 2026). "Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly."

[12] Mosca, M. & Piani, M., Global Risk Institute (March 2026). "Quantum Threat Timeline Report 2025."

[13] Babbush, R. et al. (2021). "Focus beyond quadratic speedups for error-corrected quantum advantage." PRX Quantum, 2, 010103.

[14] Chakrabarti, S. et al. (2021). "A threshold for quantum advantage in derivative pricing." Quantum, 5, 463.

[15] IBM (2025). "Quantum computing shows promising potential in finance." IBM Think.

[16] IBM Corp. Form 8-K (28 May 2026), Regulation FD disclosure on quantum investment.

[17] Bausch, J. et al. (2024). "Learning high-accuracy error decoding for quantum processors." Nature, 635, 834–840.

[18] Microsoft Source (2 June 2026). "Majorana 2, made more reliable with Microsoft Discovery agentic AI."

[19] Tang, E. (2019). "A quantum-inspired classical algorithm for recommendation systems." Proceedings of the 51st ACM Symposium on Theory of Computing (STOC), 217–228.

[20] Quantinuum (5 November 2025). "Quantinuum Announces Commercial Launch of New Helios Quantum Computer That Offers Unprecedented Accuracy to Enable Generative Quantum AI (GenQAI)."

CHAPTER 4: Post Quantum Cryptography Update (2026)

Primary sources and technical research used for the 2025-2026 update

[1] NIST - Post-Quantum Cryptography

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[2] NIST CSWP 39upd1 - Considerations for Achieving Crypto Agility

https://csrc.nist.gov/pubs/cswp/39/upd1/considerations-for-achieving-crypto-agility/final

[3] Xue & Covey - Factoring 2048-bit RSA integers with a half-million-qubit modular atomic processor, 5 May 2026

https://arxiv.org/abs/2605.03951

[4] DARPA - Quantum Benchmarking Initiative update, 10 Mar 2026

https://www.darpa.mil/news/2026/qbi-stage-a-qbit

[5] White House - Executive Order 14412

https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/

[6] OMB M-26-15 - Execution of the Migration to Post-Quantum Cryptography

https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf

[7] White House - Executive Order 14413

https://www.whitehouse.gov/presidential-actions/2026/06/ushering-in-the-next-frontier-of-quantum-innovation/

[8] Australian Signals Directorate - Planning for Post-Quantum Cryptography

https://www.cyber.gov.au/business-government/secure-design/quantum/planning-for-post-quantum-cryptography

[9] Singapore CSA - Quantum-Safe Migration Handbook and Quantum Readiness Index

https://www.csa.gov.sg/resources/publications/quantum-safe-handbook-and-quantum-readiness-index/

[10] MAS - Annual Report 2025/2026 remarks on quantum resilience

https://www.bis.org/speeches/20260817-remarks-mas-annual-report-20252026

[11] BIS Innovation Hub - Project Leap Phase 2

https://www.bis.org/publ/othp107.htm

[12] BIS Innovation Hub - Project FuSSE

https://www.bis.org/publications/project-fusse-exploring-flexible-scalable-and-secure-settlement-engines

[13] NCSA Thailand - Draft Quantum Security Framework 2026-2035, public-consultation revision, 2026

[14] NCSA Thailand - Draft Quantum Security Transition Master Plan 2026-2035, 2026

[15] Replace the URL with https://law.go.th/listeningDetail?survey_id=NzY0OURHQV9MQVdfRlJPTlRFTkQ%3D .
Keep the Framework title and 15-29 July 2026 dates. Alternatively relabel the existing URL as the Migration Master Plan and Action Plan consultation, 16-30 July 2026.

Note: The Thai Framework and Master Plan are cited as draft policy-development materials.
They are used to indicate the current direction of policy and implementation planning, not as binding regulatory requirements.

CHAPTER 5: Global Investment Landscape and the Effort to Build Quantum Computers

[1] The emerging quantum supply chain – Riverlane (2025), https://www.riverlane.com/blog/the-emerging-quantum-supply-chain

[3] Quantum 2.0 Market Report 2026: A Global $50 Billion Market https://www.globenewswire.com/news-release/2026/02/16/3238572/0/en/Quantum-2-0-Market-Report-2026-A-Global-50-Billion-Market-by-2036-Seismic-Technological-Shift-Unlocks-New-Capabilities-in-Industries-Like-Finance-Healthcare-and-Defense.html

[4] Mapping the global quantum ecosystem (December 2025): https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/mapping-the-global-quantum-ecosystem_47891dd2/20251217-0001.pdf

[5] Policy Paper on UK National Quantum Strategy (December 2023): https://www.gov.uk/government/publications/national-quantum-strategy/national-quantum-strategy-accessible-webpage

[6] European Quantum Technologies Flagship: https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship

[7] The U.S. National Quantum Initiative Supplement to the President's FY 2025 Budget, National Science & Technology Council (December 2024)

https://www.quantum.gov/wp-content/uploads/2024/12/NQI-Annual-Report-FY2025.pdf

[8] The U.S. Department of Energy https://www.energy.gov/articles/energy-department-announces-625-million-advance-next-phase-national-quantum-information?utm_source=chatgpt.com

[9] McKinsey. The quantum leap in banking: Redefining financial performance – McKinsey (2026), https://www.mckinsey.com/industries/financial-services/our-insights/the-quantum-leap-in-banking-redefining-financial-performance

[10] McKinsey. The Year of Quantum: From concept to reality in 2025 (June 23, 2025 Report) https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025

[11] McKinsey. Quantum Technology Monitor (June 2025) https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20year%20of%20quantum%20from%20concept%20to%20reality%20in%202025/quantum-monitor-2025.pdf

[12] McKinsey. Quantum communications and computing: elevating the banking sector (2026). https://www.mckinsey.com/industries/financial-services/our-insights/quantum-communication-and-computing-elevating-the-banking-sector

[13] McKinsey. The quantum revolution in pharma (2025). https://www.mckinsey.com/industries/life-sciences/our-insights/the-quantum-revolution-in-pharma-faster-smarter-and-more-precise

[14] McKinsey. Solving chemistry's toughest problems: the quantum computing advantages (2026). https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/solving-chemistrys-toughest-problems-the-quantum-computing-advantage?utm_source=chatgpt.com

[15] McKinsey. Quantum Technology Monitor 2026: A commercial tipping point (April 2026). https://www.mckinsey.com/capabilities/mckinsey-technology/our-insights/mckinsey-quantum-technology-monitor-2026-a-commercial-tipping-point

[16] IBM Corp. Form 8-K (28 May 2026) and Reuters (28 May 2026), "IBM to invest $10 billion for large-scale quantum computer by 2029."

[17] The White House. Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks" (22 June 2026); Executive Order 14413, "Ushering in the Next Frontier of Quantum Innovation" (22 June 2026).

[18] U.S. Department of Energy (17 September 2026). "DOE Launches Competition to Accelerate Development of World's First Fault-Tolerant Quantum Computer."

[19] Quantinuum Inc. (11 August 2026). "Quantinuum Reports Second Quarter 2026 Results."

[20] WisdomTree (June 2026). "The U.S. government became a quantum investor. Should you?"

CHAPTER 6: Thailand Positioning

[1] NXPO: Roadmap Whitepaper https://www.nxpo.or.th/th/wp-content/uploads/2021/11/TQT-Roadmap-Whitepaper-Rev4-21-Sep-2020.pdf

[2] https://www.qtft.org/

[3] https://www.chula.ac.th/en/news/288469/

[4] https://qtric.sut.ac.th/qtri2025/index.html

[5] https://sutir.sut.ac.th/jspui/handle/123456789/10268

[6] Quantum Computing Report (6 August 2026). "Thailand Launches 'Quantum Club Thailand' at True Digital Park to Build ASEAN Quantum Hub"; The Quantum Insider (5 August 2026).

[7] Quantum Computing Report (September 2026). "Chulalongkorn University and Qunova Computing Execute MoU to Advance Hybrid Quantum Algorithms for Industrial R&D."

[8] SCBX (8 May 2026). "SCBX Partners with Chulalongkorn University to Advance Quantum Technology."

[9] Qunova Computing (7 September 2026). "Chulalongkorn University Signs MoU with Qunova Computing for Cooperation on Quantum Technology & Research."

[10] The Quantum Insider (21 September 2026). "Chulalongkorn University and AIST Sign MoU on Quantum Technology."

Authors



Assistant Professor Thiparat Chotibut, Ph.D.
Tenure-track faculty member
at School of Physical and Mathematical Sciences,
Nanyang Technological University (NTU)



Supanut Thanasilp, Ph.D.
Tenure-track faculty member, Department of Physics,
Faculty of Science, Chulalongkorn University



Poompong Chaiwongkhot, Ph.D.
Co-Founder and Chief Technology Officer, QTFT



Kaweewut Temphuwapat
Chief Innovation Officer, SCBX
Chief Executive Officer, SCB 10X



Tutanon Sinthuprasith, Ph.D.
Head of R&D, SCBX



Nut Chukamphaeng
Senior Research Scientist, SCBX



Koravich Sangkaew
AI Engineer, SCB DataX

This publication was made possible through the collaboration of

SCB X

data X

SIAM QUANTUM SQUARE

Chula Chulalongkorn University

QTFT



www.scbx.com