VTT

Quantum computing:

Practical guide to navigating the future

beyond the obvious

Quantum computing: Practical guide to navigating the future

Preface

In recent years we have been amazed many times by the rapid pace of technology development in a variety of fields. Even so, quantum computing stands out among all these exciting new technologies with its very large transformative potential. It promises to revolutionise industries and redefine computational limits in a scale not seen yet. As we approach this quantum era, it's crucial for business leaders, policymakers, and innovators to understand its profound implications.

This guide simplifies the complex world of quantum computing. It explains the basics, explores the current state of the technology, and offers a roadmap for organisations to prepare for a future where quantum capabilities become practical realities.

I am convinced that quantum computing's impact will be immense. It can solve complex problems and optimise systems with unmatched efficiency. Its applications span finance, pharmaceuticals, energy, and manufacturing, promising breakthroughs that could reshape our world.

Preparing for this quantum future is essential for staying competitive. This guide provides valuable insights into strategic considerations, potential applications, and practical steps organisations can take to lead in this technological revolution.

We have learned from past technology leaps, that during the early days of such development, it's important to be both excited and pragmatic. While the full potential of quantum computing is still on the horizon, the time to learn and prepare is now. By building knowledge, fostering partnerships, and investing in quantum-ready strategies, organisations can harness the power of quantum computing as it matures.

This guide is your first step towards quantum readiness. It equips you with the knowledge and tools to make informed decisions, develop effective quantum strategies, and navigate the challenges and opportunities ahead. Start preparing for a future where the impossible becomes possible.

Antti Vasara
CEO, VTT Technical Research Centre of Finland Ltd

0/ Why this book?

The book's purpose is to make you consider the importance of quantum computing for your company and how you should prepare for the quantum age. It provides a practical overview of the opportunities and challenges of quantum computing from a business perspective. Instead of diving deep into quantum physics, the focus is on how you can prepare your company for a future where quantum computing is commonplace.

You will learn which industries are most likely to encounter the transformative power of quantum computing and what competitive advantages it can offer. It provides practical tools for analysing your industry and planning your strategy while offering guidance on navigating this emerging technological landscape. Additionally, the book helps interpret media articles and news about the development of quantum technology, which are becoming increasingly frequent. You can also use this book as an ambassador for quantum computing within your organisation.

This book aims to help you navigate the extremes of quantum computing's narrative—cutting through the hype and avoiding the pessimism of those grappling with its most demanding challenges. After reading, you will gain a balanced, structured understanding of quantum computing's opportunities and challenges. This perspective will empower you with the knowledge to make informed, strategic decisions in this rapidly evolving field.

- ✓ **Recognise quantum computing's business impact**
- ✓ **Navigate the quantum age**
- ✓ **Empower informed decisions**

Exploring the "how" and "why"

In this book, you will discover ten essential questions that underscore the key considerations for stakeholders regarding quantum computing. We formulated these ten questions based on discussions and interviews with companies new to quantum computing or taking their first steps to learn more. The book is structured so that each chapter begins with a brief answer to the posed question, which is then elaborated upon in the subsequent paragraphs. While the chapters in this book are arranged to form a cohesive narrative, each chapter is also designed to stand alone. This allows you to delve into specific questions of interest without needing to read the entire book.

While we do not answer the question "WHEN", this book helps you define "HOW" you should prepare for the quantum age and "WHY".

Navigating information challenges

Understanding the developments in quantum computing can be challenging for those outside the field. This book was created to simplify the learning process, offering a clear introduction to quantum computing. Our goal is to provide a broad audience with a basic understanding of why it is crucial to stay informed about quantum computing advancements and how these developments could impact the future business and operational landscape across various sectors.

We sought answers to these questions through creative and thorough engagement with various sources. This task required considerable effort, including exploration of literary sources, conducting interviews, participating in industry events, and engaging in valuable discussions with academic experts. Along the way, we found that each communicator brought their own goals and perspectives to the conversation.

Some large management consulting firms list use cases[1] and give the impression that quantum applications are just around the corner[2]. Companies developing quantum technology and quantum computing software startups emphasise progress and publish ambitious technology roadmaps to accelerate investor and adopter companies' interest. Part of this communication involves launching new terms[3], making it even more challenging to follow the industry's development.

Scientific articles typically concentrate on specific aspects of quantum technology or the development of algorithms. Recently, this focus has shifted from physicists to engineers and software engineers as the technology evolves. For those unfamiliar with the field, keeping up with advancements through these scientific sources can be challenging due to the simultaneous progress in creating various types of qubits, as no single qubit design has emerged as the dominant one.

No single qubit technology has emerged as the dominant design.

On the other hand, researchers often take a cautious stance when discussing quantum computing's progress and potential advantages. Information obtained from quantum industry business events is also not yet primarily aimed at future users but rather at other players in the quantum ecosystem and investors.

We aimed to understand each communicator's goals and perspectives when compiling the material for the book's questions and answers. Additionally, we sought to discern the excess hype and evaluate the factors contributing to cautious estimates. However, we would like to emphasise the hope that the potential of quantum computing includes addressing some of humanity's most significant challenges. And because it is still uncertain when quantum computers will be ready to solve large-scale practical problems and what the best use cases might be, we try to help identify factors affecting the development of technology, potential applications, and broader societal impacts. At times, we highlight the current maturity of the technology and its near-term development, while in other sections, we look further into the future, particularly from the perspective of the opportunities quantum computing may bring.

Recent developments in generative AI, which surprised even the most seasoned AI experts with its rapid leap in capability, remind us how quickly transformative technologies can advance. This emphasises the need to monitor progress in quantum computing, even if breakthroughs seem distant. By staying vigilant, we can better anticipate the opportunities and challenges ahead.

Like the questions shaping the chapters of this book, the beliefs in the following table are drawn from common assumptions we encountered during our research. You can use this table for quick learning and to identify the sections of the book you want to explore first.

Table 1. Common beliefs and myths about quantum computing.

Belief	Reality	Read more
Quantum computers are distant future technology	Not true! Quantum computers are already today used around the world by scientists and companies to solve real problems	Chapter 4
Quantum computers are already faster than classical	Currently, no quantum application has yet demonstrated to be faster than best-in-class classical methods in practical settings.	Chapter 4
Speed is the only benefit of quantum computers	Quantum computers can also provide more accurate results and reduce energy consumption	Chapters 1&3
If my business doesn't need super computers, we don't need quantum	Not true! Quantum computers are designed for different purposes than (classical) supercomputers. They are not replacements but complements.	Chapter 2
Quantum computers evaluate all combinations at once (in parallel)	Not really! The answer requires a basic understanding of quantum mechanics, which this book is not about. However, you can start your journey here.	Chapter 2, Further reading
More qubits always mean better performance.	Actually, increasing the number of qubits without improving the quality of qubits can lead to worse performance (more noise).	Chapters 2&4
Quantum computers solve every kind of problem faster.	Quantum advantage is expected to apply only to specific problems where quantum algorithms outperform classical methods.	Chapter 3
Quantum computers solve problems exponentially faster.	Speedup varies based on the type of problem; improvements can be exponential in certain cases.	Chapter 3
Classical algorithms are irrelevant once quantum computing matures.	Classical algorithms continue to evolve, often narrowing the gap with quantum algorithms. They remain critical tools in computation.	Chapter 3
Quantum computing is ready for widespread use.	Technology is still in the early stages (NISQ era), with most applications remaining theoretical or experimental.	Chapter 4
My industry will not be affected.	Think again! Optimisation and machine learning—key strengths of quantum computing—are integral to most industries, making impacts inevitable.	Chapter 5
Quantum computers will be in our pockets one day.	Nobody knows the future, but quantum's potential for radical transformation makes it worth imagining how it could shape tomorrow's world.	Chapter 6
Quantum computers can break all encryption today.	While Shor's algorithm poses a threat to current encryption, quantum computers capable of executing it effectively are still years away. Preparation, however, must begin now.	Chapter 4&7
Quantum-proof cryptography is unbreakable.	There are no currently known ways to break quantum-proof cryptography, but it's impossible to guarantee its long-term invulnerability against future advances.	Chapter 7
Every company needs a quantum strategy now.	While every company should understand the possibilities and threats, a dedicated strategy is essential only for specific industries or use cases.	Chapter 8
I can't explore quantum computing because I don't know enough about it.	You don't need to be a physicist—starting with awareness-building, collaborations, and small experiments can unlock its potential for your business.	Chapter 9
Quantum computing is viable only for big businesses.	Quantum computing is very accessible via the cloud for all kinds of companies and even for interested individuals.	Chapter 9

Co-learning and sense-making

Beyond our initial data collection, we collaborated with companies from various fields in the FutureQ project[4], employing sense-making foresight methods to gain further insights. We identified potential opportunities and threats that quantum computing could accelerate in these fields through horizon scanning. We collaborated to build quantum computing technology scenarios, considering its development's uncertainties. The materials from both approaches facilitated further discussions with experts.

> **"This is just the beginning; the need to understand the opportunities and threats of quantum computing from the perspective of its beneficiaries through research and collective sense-making will only grow as development progresses."**

Maaria Nuutinen, VTT

Three distinct time horizons

Although we cannot precisely answer the "when" question, meaning when something will happen and become possible, we help the reader understand the timeframe by using the same three distinct time horizons throughout the book:

Short-term: Race to develop quantum computers that can solve real-life business problems.

Mid-term: Era of increasing business benefits - Tackling challenges that are impossible for classical computers[i] yet feasible with quantum computing.

Long-term: Era of broad commercial adoption - Imagine a future when technology challenges have been solved, and quantum computers and the software around them work seamlessly, enabling impossible things today.

Actively participating in the development of quantum computing is essential for identifying the right moments for action and investment. Understanding these three time horizons allows you to effectively manage this potentially disruptive technology and prepare for its consequences.

> **"With fast-evolving technology, we must work on shaping the future rather than forecasting. Technology – such as quantum computing – opens the doors. We need to start thinking about which is the right passageway, or are there many?**
>
> **For example, material science will be taking quantum leaps in terms of how fast you can enter the market, and taking an idea for commercial use will test the company's capability to shape the future."**

Jussi Hyvärinen, Metsä Group

i When quantum computing developers refer to classical computers and computing, they mean the traditional form of computers and computing that we use daily.

1/ Why should I care about quantum computing?

What if the next great disruption to your industry comes from a technology you barely understand?

Quantum computing is an extraordinarily complex technology, fundamentally different from anything we have seen before. Its principles and mechanics challenge conventional understanding, making it a field that requires deliberate effort to grasp. Yet, gaining even a basic understanding can open the door to exploring its transformative potential. By addressing problems that are too complex or computationally demanding for classical systems, quantum computing could unlock opportunities that redefine the boundaries of what is possible in business, science, and technology.

While quantum computing may seem like a future technology, its potential for disruption draws closer, making it essential for businesses to prepare for the transformative changes it could bring, from revolutionising material design and accelerating drug discovery to enhancing supply chain optimisation. The implications extend far beyond faster computation. Even marginal speed, accuracy, or energy efficiency improvements can provide a competitive edge, while entire discoveries could create unprecedented markets and opportunities.

Understanding quantum computing is not about becoming a technology expert. It is about recognising the possibilities it creates, preparing for the disruptions it may bring, and positioning your business to thrive in this emerging quantum era. To start this journey, ask yourself:

- ✓ **What if you could solve previously impossible problems?**
- ✓ **What if you could solve a complex problem 1000x faster?**
- ✓ **What if you could get better solutions?**
- ✓ **What if you could solve problems with 1000x less energy?**
- ✓ **What if your industry will be disrupted?**
- ✓ **What if you could create unimaginable solutions?**

This first chapter is optimistic, envisioning a future where major technical challenges have been solved, and quantum computing is transforming both business and society.

What if you could solve a previously impossible problem?

Quantum computers are fundamentally different from classical computers. Due to their unique nature, quantum computers have the potential to find efficient solutions to problems that are too complex for even the most powerful supercomputers. For example, the simulation of quantum systems offers an exponential advantage over classical simulations. Classical computers struggle to simulate the behaviour of molecules, atoms, or materials due to the exponential growth in complexity as the system size increases. Quantum computers, however, can naturally simulate these quantum systems, offering a pathway to breakthroughs in drug discovery, material science, and chemical engineering. This capability could enable researchers to discover new medicines or materials in a fraction of the time it currently takes. These practical innovations have the potential to reshape industries and spark entirely new markets, making quantum computing a key driver of future discovery and innovation.

What if you could solve a complex problem 1000x faster?

Beyond areas that promise extraordinary speedups, quantum computing holds potential in many other domains where more moderate improvements could deliver significant benefits. While these problems may not be impossible for classical computers, solving the problem faster could still have a transformative impact. Imagine a quantum computer solving in minutes a problem that takes a classical computer all day. Now consider the implications if your competitors had access to such technology while you did not. What would this mean for your business?

Even if the improvement in efficiency is not that radical, the impact on your business could be profound. If your competitor could, for example, optimise their supply chain or identify financial risks just a little bit faster than you, they would always be ahead of you when something surprising happens and seize opportunities before you can even react. This competitive advantage, granted by quantum computing, would put your business at a significant disadvantage unless you, too, are prepared to harness the power of this transformative technology. The breakthroughs in optimising supply chains and investment portfolios are just the tip of the iceberg of conceivable.

What if you could get better solutions?

While speed is often highlighted as quantum computing's primary advantage, its ability to deliver higher-quality solutions is just as critical. For instance, in optimisation problems, businesses often face vast possibilities, and classical methods typically settle for "good enough" solutions—referred to as local minimums—that may not be optimal. Quantum computing, however, has the potential to navigate these complex landscapes more effectively, uncovering superior solutions that even the best classical methods might miss. Even if it would take more time with the quantum computer, the improved quality of the solution could justify the extra time and effort.

What if you could solve problems with 1000x less energy?

Quantum computing may also offer significant benefits in terms of sustainability. It might surprise you, but quantum computers can be remarkably energy-efficient despite operating at temperatures close to absolute zero. In some tasks, the primary advantage of quantum computing could lie in its substantial energy savings, even if classical computers compete closely on other performance metrics.

Beyond operational efficiency, quantum computers also stand out in their design. Unlike supercomputers, which rely on thousands of chips, future quantum computers are expected to require far fewer components. This simpler architecture, though still evolving, has promising implications for sustainability. Reduced complexity could lead to lower resource consumption during manufacturing—using fewer raw materials, less water, and less energy while generating fewer emissions and less waste compared to the production of supercomputer components. Together, these factors position quantum computing as not only a technological breakthrough but also a potential contributor to greener, more sustainable solutions.

What if your industry will be disrupted?

Quantum computing might seem like tomorrow's technology, but the decisions you make today could determine whether your business thrives or becomes obsolete in a quantum future.

While specific industries are often highlighted in discussions about opportunities in quantum computing, no industry is safe from quantum computing's transformative impact. The ripple effects of quantum advancements are set to resonate across the entire business landscape.

Information processing is at the core of every industry—optimising supply chains, determining pricing strategies, or calculating risks. Quantum computing has the potential to revolutionise how industries manage and act upon this data, making the impossible possible in everything from operational planning to product development. Moreover, the convergence of quantum computing and AI is a potential game changer. Although there is much uncertainty in this area, these pairings promise to enhance the speed, accuracy, and capability of data analysis, predictive modelling, and decision-making processes across sectors. By optimising complex tasks central to business operations, quantum technology could unlock new levels of efficiency and innovation, creating competitive advantages for early adopters. From logistics to research and development, the operational shifts made possible by quantum computing will reshape the competitive landscape, making it essential for businesses to embrace disruption or be disrupted.

Unimaginable solutions

Beyond solving existing problems, the new era of computing may unveil opportunities we have not yet imagined. One of the paramount promises of quantum computing is its profound capability to simulate quantum systems. This ability is not merely about tackling the known; it is about venturing into realms of the unknown, exploring the quantum mysteries embedded in material science, chemistry, and even the universe's fundamental laws. It is akin to embarking on a voyage into uncharted waters, where each wave and ripple reveals new layers of understanding, and every discovery holds the potential for transformative breakthroughs.

The implications of such explorations are boundless. Simulating quantum systems can foster a deeper understanding of molecular structures and interactions, accelerating advancements in material science, chemistry, and pharmaceuticals. However, quantum computing's potential reaches far beyond these domains. All industries that rely on physical materials and production processes can potentially benefit from innovations with unprecedented properties.

Furthermore, these breakthroughs may not only drive efficiencies in existing industries but also redefine them—or even give rise to entirely new markets.

Finally, quantum computing is a potential tool to probe the enigmatic quantum phenomena that govern the cosmos, potentially unlocking new dimensions of knowledge. This new understanding could fuel the new waves of scientific and technological innovation, propelling humanity into realms we can scarcely imagine today.

2/ What is quantum computing?

Quantum computing is not a more powerful version of classical computing—it's a completely different way of thinking about computation.

Many people incorrectly believe that quantum computers are simply faster versions of current computers or that if a company does not utilise supercomputers, quantum computing will not be relevant to them. In reality, quantum computers are not simply about speed—they are about a completely different way of solving problems. While classical computers process information as ones and zeros, quantum computers use qubits that can exist in multiple states at once, unlocking solutions to complex challenges that classical computers cannot even approach.

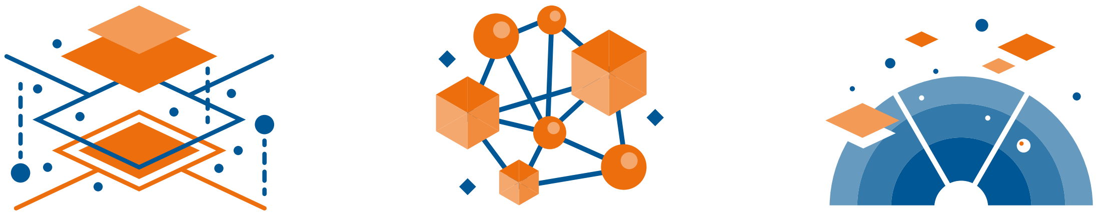
Quantum computing is not designed to replace traditional machines but to tackle problems that have been unsolvable until now. Instead, businesses will increasingly adopt hybrid approaches, leveraging the strengths of both classical and quantum systems to address diverse challenges. From optimisation to breakthroughs in science and technology, quantum computers open entirely new possibilities. From optimisation to breakthroughs in science and technology, quantum computers open entirely new possibilities. Even businesses that do not rely on supercomputers today will benefit from quantum's unique abilities as this technology transforms industries. Understanding quantum computing now means getting ahead of the curve on the next wave of innovation that will shape the future of business.

- ✓ **Quantum computers are not just faster—they are different**
- ✓ **Quantum computing is one form of quantum technologies**
- ✓ **Different paradigms of quantum computers are suitable for different uses**
- ✓ **Winning qubit technology is still unclear**
- ✓ **Both the number of qubits and their quality matters**

This chapter provides a high-level overview of the fundamentals of quantum computing, offering a foundational understanding of this transformative technology.

Three quantum technologies

Quantum technologies utilise the principles of quantum mechanics, a branch of physics investigating the strange and often counterintuitive behaviour of the smallest particles in the universe. Quantum technologies can be divided into three primary domains: computing, communication, and sensing (see Figure 1). Each of these domains leverages the behaviours of sub-atomic particles to transcend the limitations inherent in classical systems. Although this book focuses on quantum computing (QC), it should be noted that when delving deeper into the quantum realm, the interplay among these quantum technologies could lead to a holistic quantum ecosystem, opening avenues of innovation and problem-solving beyond our current comprehension.



QUANTUM COMPUTING

A technology for computation which leverages quantum mechanics to provide performance unattainable for classical computers (for some applications)

QUANTUM COMMUNICATIONS

Leverages quantum entanglement and teleportation to enable ultra secure communications channels

QUANTUM SENSING

Exploits the inherent sensitivity of quantum systems to external perturbations, providing measurement and detection capabilities with unparalleled precision

Figure 1. Three main areas of quantum technologies.

Exploring the quantum computing landscape

The communication around quantum computing can often seem confusing as there are many types of quantum computing systems and recurring claims of breakthroughs expected to transform the field. To make sense of these discussions, it is essential to distinguish between hype and genuine achievements. Gaining an understanding of the fundamental paradigms and different types of quantum computers (known as modalities) is invaluable, as each employs a unique approach to harnessing quantum principles.

Quantum computing paradigms

The paradigms represent the fundamentally different ways of quantum computing, each with its unique capabilities and challenges. Table 2 provides a concise overview of these various quantum computing paradigms. Understanding these paradigms is essential to grasp the broader landscape of quantum computing technologies and their respective stages of development. For example, quantum annealing is fundamentally different from universal quantum computers; it excels in solving a specific subset of optimisation problems that can be formulated in a specific way[5]. By exploring these paradigms, we gain a clearer perspective on both the potential and the hurdles on the road to fully realising the promise of quantum computing.

Table 2. Different paradigms of quantum computing: description and purpose.[6]

CLASSICAL COMPUTERS		ANALOG QUANTUM COMPUTERS		UNIVERSAL GATE-BASED QUANTUM COMPUTERS	
Quantum-inspired classical computing	**Quantum emulators**	**Quantum annealing computers**	**Quantum simulators**	**Noisy intermediate-scale quantum computing (NISQ)**	**Fault-tolerant quantum computing (FTQC)**
Borrowing ideas from quantum mechanics to design classical algorithms running on classical computers	Classical systems designed to mimic certain quantum behaviours. Hardware ranges from simple laptops to classical super computers	Specialised quantum computers tailored for particular types of problems	Quantum system designed to simulate specific quantum phenomena by mimicking the behaviour of more complex quantum systems.	Early-stage quantum computers with a limited number of qubits that are prone to errors, which limits their computational accuracy	The ultimate goal for quantum computing. These systems will be able to solve computational problems that are currently unsolvable
Used by businesses to take advantage of some benefits of quantum computing without waiting for quantum hardware to mature	These emulators help test and refine quantum algorithms but are limited by classical computational power and cannot fully replicate true quantum behaviour.	Ideal for optimisation, machine learning, and logistics challenges (for finding the global minimum of a function)	Used by scientists and industries like material science for very specific quantum behaviour simulation, but not suitable for general computation.	Useful for exploring quantum algorithms and developing applications, but not yet at the scale to solve most real-world business problems efficiently	Solving a wide range of problems significantly faster than classical computers.

Competing qubit technologies

The development of a universal quantum computer has sparked intense competition among various qubit technologies (modalities), each with its unique approach to harnessing quantum principles. Currently, superconducting qubits dominate media attention and investment. However, many less-known and more immature modalities could still become significant players in the race for dominant design. Table 3 compares the maturity levels of some of the most relevant approaches currently in development. Each competing qubit technology has advantages, challenges, and technical nuances, reflecting the multifaceted nature of quantum computing endeavours. The dominant design may be one of the existing options or something that has yet to be invented.

Table 3. Examples of qubit technologies.

Qubit technologies	Maturity	Physical qubits	Vendors	Strengths	Challenges
Super-conducting	Most mature, widely used in quantum computing research and industry	1121 (IBM Condor, 2023)	IBM, Rigetti, Amazon, Google, IQM	Relatively easy to scale (roadmaps up to 1M) High-speed quantum gates Significant funding and research progress	Requires cryogenic cooling to near absolute zero Prone to decoherence and noise Connectivity limit in 2D
Silicon-based	Emerging, potential to leverage existing semiconductor infrastructure	12 (Intel Tunnel Falls, 2023)	Intel, SemiCon	Leverages existing silicon manufacturing technologies Potential for high scalability	Very low qubit counts Challenging to achieve long coherence times Requires cryogenic temperatures
NV (Nitrogen-Vacancy) centers	Mature for sensing, emerging for quantum computing	5 (Quantum Brilliance)	Quantum Diamond Technologies, Element Six	Room-temperature operation Highly stable qubits Long coherence times	Scalability is challenging Primarily used for sensing applications rather than large-scale computing
Topological	Experimental, still in research phase, not yet commercially available	0	Microsoft	Theoretically highly resistant to errors Offers potential for fault-tolerant quantum computing	Experimental and unproven at scale No functioning large-scale system yet
Neutral (cold) atoms	Emerging, promising scalability, in experimental phase	1225 (Atom computing, 2023)	Pasqal, QuEra, Atom Computing	Highly scalable, many qubits can be packed into small spaces Long coherence times due to weak interaction with the environment	Requires complex cooling and precise laser control Still in early stages of development for large-scale commercial use
Trapped ions	Mature technology, used in various quantum research projects	56 (Quantinuum, 2024)	Quantinuum, IonQ, Alpine Quantum Technologies (AQT)	High-fidelity qubits Long coherence times Precision control of qubits	Slower gate operations compared to other modalities Scalability is a challenge due to complex ion trap setup
Photons	Emerging, in research phase with promising developments in quantum communication	215 modes GBS (Xanadu, 2023)	PsiQuantum, Quandela, Xanadu	Room temperature operations Minimal decoherence over long distances Particularly suited for quantum communication and networking applications	Noise from photon loss Two-photon interactions (required for gates) are difficult to implement Limiting scalability

From the number of qubits to their quality

Quantum computing has come a long way since its first demonstration nearly three decades ago. In recent years, the pace of development has accelerated significantly, fuelled by advancements in research and growing investment. While progress has been made on multiple fronts, much of the focus in marketing and public discussion has centred on hardware advancements, with a particular emphasis on the count of physical qubits - a simple yet misleading measure of a quantum computer's true capabilities.

By 2024, a shift in narrative appears to be underway. Leading companies are moving beyond the "qubit race" and emphasising a more nuanced competition involving a range of technical factors. The era of merely adding qubits has reached its limit; further progress now requires simultaneous advancements in hardware and software. To truly understand the state of quantum computing, the conversation must expand to include critical factors such as system stability, reliability, and scalability, which ultimately determine a quantum computer's real-world usefulness.

Beyond the number of qubits, the *quality* of qubits is equally, if not more, significant. This is measured by fidelity, which tells the probability of whether one gate operation on a qubit will succeed without error[ii]. As fidelity improves due to technological advances, it will be possible to perform more and more gate operations in sequence with a reasonable success rate, and the quantum computer will be able to solve increasingly complex problems. Currently, the fidelities of best computers hovers around 99,9%, allowing for *2,000–3,000* gate operations. According to some roadmaps[7], this figure could reach *10,000* gate operations by 2027. It is believed that with the suitable NISQ[iii] algorithm (currently unknown), it could be possible to gain an advantage with 10,000 gate operations in a specific problem[8].

Error correction is essential for improving quantum computer accuracy.

Error correction, enabled through software techniques, is a key approach to enhance the fidelity of quantum computers. By combining multiple physical qubits to create a single logical qubit (see infobox), error correction uses additional qubits to detect and correct errors in noisy systems. This will further accelerate the improvement in the fidelity of this logical qubit with the cost of using more physical qubits. When millions of sufficiently high-quality physical qubits exist, it will be possible to create hundreds or thousands of sufficiently high-quality logical qubits and, finally, run fault-tolerant quantum algorithms with a theoretically proven advantage over classical computing. Then, it is just up to the algorithm and the problem of how many error-corrected qubits are needed to gain an advantage.

ii The reverse of fidelity is an error rate, i.e. the probability that a quantum operation (like gate) produces an incorrect outcome. Mathematically fidelity = 100% - error rate

iii NISQ refers to Noisy Intermediate-Scale Quantum

Improving fidelity is an essential step toward enabling *fault-tolerant quantum computing*, which is discussed further in Chapter 4.

WHAT IS LOGICAL QUBIT?

A logical qubit is a stable unit of quantum information created by grouping multiple physical qubits to protect against errors. Physical qubits are prone to noise and mistakes, making them unreliable on their own. Logical qubits can detect and fix these errors through quantum error correction, enabling more reliable quantum computations.

It is important to note that logical qubits differ from mathematically perfect qubits, an ideal concept with no errors. In practice, logical qubits can still have some errors but are far more stable than physical qubits. Depending on the application, different quality standards are required for logical qubits:

- **High-precision tasks (e.g., cryptography or large-scale simulations) demand logical qubits with very low error rates and greater redundancy.**
- **Less sensitive tasks (e.g., certain types of optimisations) can tolerate higher error rates, requiring fewer physical qubits for error correction.**

Other layers of the quantum stack

While much of the discussion around quantum computing has focused on hardware advancements, attention is now shifting to the upper layers of the quantum stack. This transition reflects the growing recognition that the real-life usefulness of quantum computing requires advancements beyond just hardware.

The quantum stack elucidates the hierarchical structure from the foundational quantum physics, ascending through the layers of hardware, middleware, up to algorithms. On the top of the stack are quantum computing business applications, which is the focus of this book. Figure 2 illustrates the quantum stack and its components.

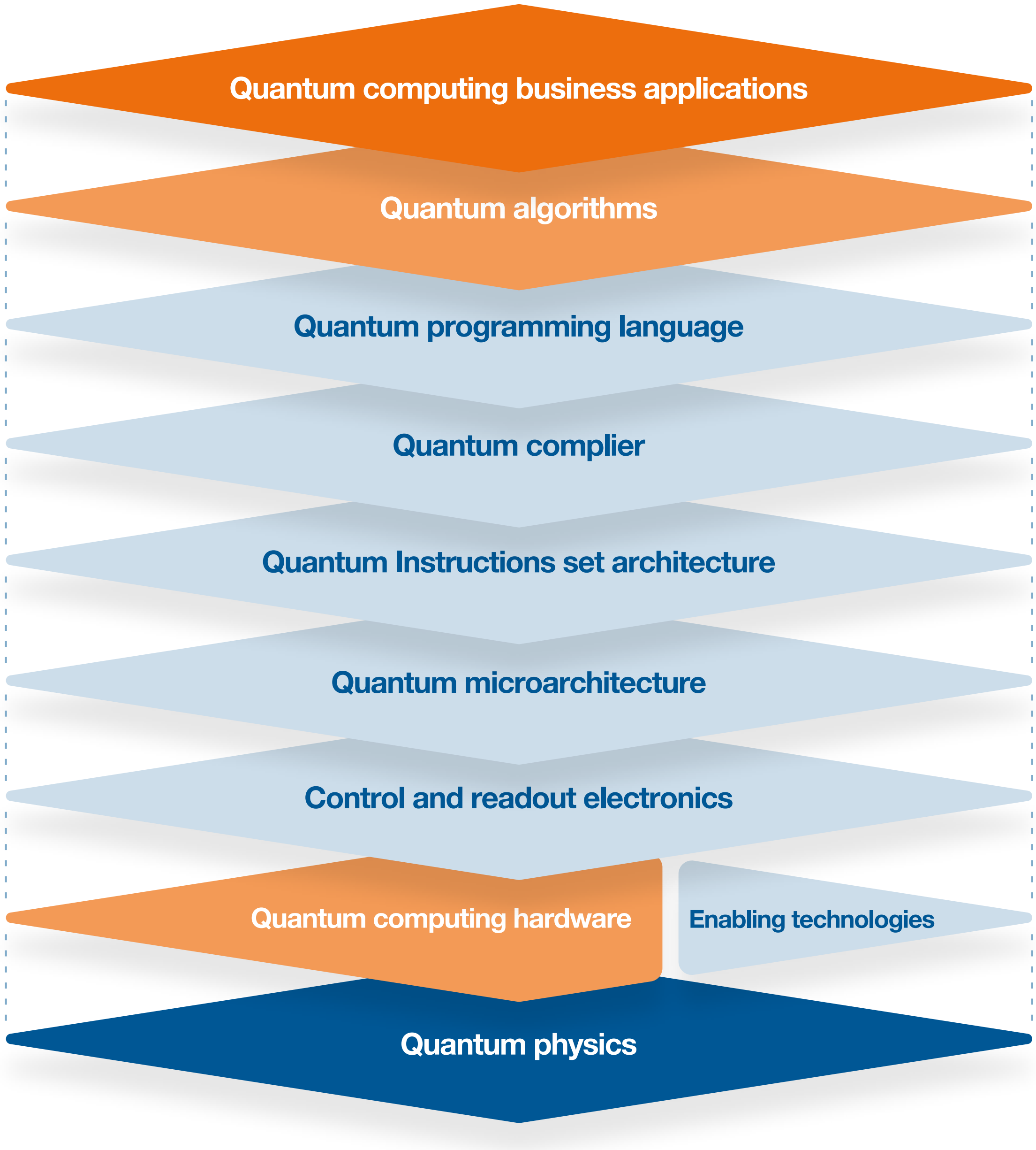


Figure 2. Quantum stack.[9]

As quantum hardware continues to evolve and the community garners a deeper understanding of quantum algorithms and their potential applications, the horizon of quantum computing continues to expand. It is a dynamic, evolving field that promises to unlock new dimensions of computational capability, yet requires a concerted effort across academia, industry, and policy domains to fully realise its transformative potential.[10]

Bridging the gap with hybrid quantum computing

Hybrid quantum computing is a pivotal development within quantum computing those bridges current capabilities and future potential. It is a collaborative approach where classical and quantum computers work together to solve computational problems. This method acknowledges that quantum computers are not designed to replace classical systems but to complement them, leveraging the strengths of both technologies.

In hybrid quantum computing, the classical computer handles tasks such as data preparation, optimisation of algorithms, and result interpretation. Meanwhile, the quantum processing unit (QPU) executes the quantum-specific computations. This collaboration enables the system to tackle complex problems more effectively. For instance, while the classical computer excels in handling large datasets and general-purpose tasks, the QPU focuses on specialised operations, such as quantum state exploration or complex optimisation.

This approach is particularly significant for today's Noisy Intermediate-Scale Quantum (NISQ) devices, which are limited in qubit count, coherence time, and fidelity. By offloading certain tasks to classical computers, hybrid quantum computing allows us to harness the unique capabilities of NISQ devices while minimising their weaknesses. Hybrid architectures also offer the flexibility to integrate different types of quantum computers and classical resources, tailoring solutions to specific problems.

Hybrid quantum computing provides several tangible benefits:

Improved performance: By combining classical and quantum resources, hybrid systems can accelerate the resolution of certain computational challenges, achieving results faster than classical methods alone.

Enhanced accuracy: Integrating quantum and classical computations enables hybrid algorithms to achieve higher accuracy in problem-solving, especially for optimisation and machine learning tasks.

Greater flexibility: Hybrid systems allow organisations to utilise the best combination of hardware and algorithms for their specific needs, paving the way for practical applications even during the NISQ era.

As quantum computing evolves, hybrid quantum computing will play a vital role in bridging the gap between the current state of quantum technology and its future potential. This enables businesses to realise tangible benefits in the near term while building a foundation of transformative breakthroughs in the years ahead.

3/ Which problems can quantum computing solve?

Quantum computing is a transformative technology that aims to solve problems intractable for classical computers. Quantum computers are well-suited for a limited set of problems, especially in the near term, due to the limitations of quantum hardware. They work best for problems with specific characteristics: high complexity, small to medium input sizes, and a (hidden) structure that quantum algorithms can exploit. Examples include the factorisation of large numbers (used in cryptography), boosting machine learning, solving complex optimisation challenges, and the simulation of quantum systems such as molecules or materials.

Quantum speedup is a key metric for evaluating the power of quantum computing compared to classical computing. Depending on the problem, quantum computers can offer polynomial, superpolynomial, or exponential speedups. The most promising quantum applications can leverage exponential speedup to solve real-world challenges more efficiently than classical methods can. However, it is essential to note that practical quantum advantage—where a quantum computer clearly outperforms a classical one in real-world applications—is still primarily a theoretical concept. As quantum hardware matures, we expect breakthroughs in cryptography, optimisation, and simulation of quantum systems - areas where classical computers are severely limited in their ability to manage the complexity or tackle quantum-specific challenges.

- ✓ **Focus on problems where classical systems struggle due to exponential complexity or quantum mechanical processes.**
- ✓ **Differences between polynomial, superpolynomial, and exponential speedups**
- ✓ **Practical advantage of quantum computer vs. theoretical speedup**

In this chapter, we focus on the present-day realities of quantum computing. While chapters 1, 5 and 6 explore technology's future promise and potential impact, we aim for a more grounded perspective here. We examine where quantum computing's potential is most viable today and the obstacles that must be overcome before fully realising that potential. This balanced approach should provide a clear-eyed view of the current landscape, highlighting both exciting possibilities and the critical challenges ahead.

Why are quantum computers powerful?

Quantum mechanics introduces principles that defy classical explanations, and these principles are what give quantum computers their unique power. Classical computers rely on binary processing, where bits are either 0 or 1, limiting their ability to handle certain types of complex problems. Quantum computers, on the other hand, operate on qubits that can include multiple states simultaneously, enabling them to explore a vast array of possible solutions at once. This ability to modify multiple computations in parallel makes them especially powerful for tasks like optimisation and cryptography.

Moreover, quantum computers excel by harnessing the intricate connections between qubits. These connections allow information to flow in ways that are impossible in classical systems, drastically speeding up problem-solving. In addition, quantum algorithms utilise special techniques to direct computations toward the correct outcomes more efficiently, giving them a significant edge over classical algorithms in tackling specific challenges, like simulating molecules or solving large-scale optimisations.

Despite their extraordinary capabilities, the true value of quantum computers—especially fault-tolerant ones—comes from how they outperform classical systems to solve real-world problems. When fully realised, a fault-tolerant quantum computer with the right specifications offers significant advantages in several key areas.

Key advantages of fault-tolerant quantum computers include:

Speed: Solve a computational task much faster than current methods.

Accuracy: Find a solution with higher accuracy than current methods.

Scalability: Solve a problem at a larger scale than is possible with current methods

THE FUNDAMENTALS OF QUANTUM COMPUTING

Superposition
A qubit is different from a classical bit, which can only be either 0 or 1. Instead, a qubit can exist in a state that is a combination of both, with varying probabilities. This property, called superposition, is what gives qubits their extraordinary computational power.

Entanglement
When qubits are entangled, the operation on one of these qubits instantly affects the state of another, even if they are far apart. In computing, entanglement offers a resource that is not available in classical computing. Many quantum algorithms use entanglement to perform multiple calculations simultaneously. Entanglement allows quantum computers to manipulate many qubits in a single operation instead of manipulating each qubit individually, as in classical computing.

Quantum Interference
Quantum interference occurs when the amplitudes and phases of different quantum states combine in ways that can either amplify or cancel out certain outcomes. Interference guides computations toward correct solutions by amplifying the likelihood of desired outcomes (reinforcing constructive computational paths) and suppressing incorrect ones. The possibility of utilising constructive and destructive interference may allow shorter computational paths.

Unitarity
Unitarity is a fundamental principle of quantum mechanics and the basis of the mathematical framework of quantum theory. A unitary operation is one that preserves the total probability of all possible outcomes, ensuring that the sum of probabilities remains 1. This is crucial because it means that information is not lost during the computation process.

Linearity
Quantum computers are naturally adept at performing linear operations (a special case of linearity called unitarity) because quantum mechanics is inherently linear. Linearity allows multiple versions of reality to exist simultaneously within the state vector. However, it implies that there is no interaction between versions and that there will never be the perception of more than one version. This is the key behind quantum parallelism.

Parallelism
Quantum parallelism allows a vast number of operations to be performed parallel, a key difference from classical information processing and computing. Classical parallelism increases proportionally with system size, while quantum parallelism increases exponentially. Quantum computing exploits parallelism, performing calculations in the superposition of states, yet in a very distinctive and unique way. Differently from classical (silicon- and electronics-based) computing systems, consisting of thousands of cores completing serial tasks, a quantum computing core is inherently an elementary parallel computing unit: calculations can be performed in parallel by unitary transformations acting on a superposition of quantum states.

Measurement
Computation on a quantum computer ends with a measurement, which selects one of the basis states based on the probabilities encoded in the quantum state. In a successful quantum algorithm, this process yields the correct result with high probability.

Which problems are suitable for quantum computers?

Understanding which problems quantum computing is useful is challenging, particularly for non-experts. However, certain common characteristics can help clarify the nature of these problems and make them easier to grasp.
In the long term, quantum computers are expected to excel in addressing complex computational challenges where classical computers struggle – or are outright incapable. They are particularly suited for problems that are inherently difficult or inefficient for classical computers to solve. That said, even within this category, there is uncertainty about which problems will truly demonstrate quantum advantage, as some may also pose challenges for quantum computers themselves.

Input data size limits near-term applications.

One major near-term limitation is the size of the input data. Quantum computers currently lack the scale needed to handle large datasets, so the problems they tackle must be relatively small to “fit” within the system’s capacity. Therefore, in the near term, quantum computers are most effective for “big compute” problems with small data—tasks that demand substantial computational power but do not involve massive datasets as input or output.

One reason for the exponential potential of quantum computing lies in its ability to exploit the structure of specific problems – something classical computers cannot effectively do. Unfortunately, this “need for structure” has essentially limited the biggest potential of quantum computing to certain specific areas of mathematics. This is the fundamental reason why the greatest successes of quantum algorithms research have been in cryptography. Finding such hidden structures in other problems of practical interest remains a significant open problem.

Theoretical accessibility refers to the suitability of a problem for quantum computing based on how it can be mathematically described, modelled, and reasoned about. There is potential for an advantage in problems with a clear mathematical structure that allows known quantum algorithms or subroutines (primitives) to be applied effectively. Ideally, the problem can be formulated to highlight patterns or structures that quantum computers can exploit, such as symmetries in data (see also infobox) or well-defined mathematical rules. Without these features, developing quantum algorithms or proving their potential superiority over classical approaches becomes challenging, limiting the problem’s feasibility for quantum computation.

HARNESSING SYMMETRY FOR QUANTUM EFFICIENCY

Symmetry plays a crucial role in making quantum computations more efficient. Many quantum systems, especially in fields like quantum chemistry, exhibit symmetries—such as translational, rotational, or reflection symmetry. These symmetries allow quantum systems to be described using fewer variables, significantly simplifying computations. For instance, a system with rotational symmetry only requires analysis of one unique orientation rather than every possible one, drastically reducing computational effort.

Quantum information theory takes advantage of these symmetries by transforming problems from a local, qubit-level description to a global, symmetry-based framework. This compact representation minimises storage and processing requirements, enabling quantum algorithms to perform more efficiently. Additionally, symmetry-aware quantum machine learning offers a promising avenue, combining quantum computing's strengths with the inherent symmetries in data to develop faster, more effective learning models. This makes symmetry a powerful tool for tackling complex challenges in quantum computing.

In summary, the following characteristics of the problem make it "fit" for quantum computing:

High computational complexity - Problems (not all, however) that scale exponentially on classical computers

Size of inputs – Input sizes are currently severely limited by the number of qubits available in quantum computers.

Problem structure - Problems with a well-defined, often repetitive or periodic, structure.

Theoretical accessibility - Problems that can be mathematically modelled and reasoned about.

So, if these are the desired characteristics of the problem, what are the actual problems that quantum computers can solve? Let's break this down with examples of applications where quantum computing is expected to offer the most outstanding value (see Table 4).

Table 4. Example applications for quantum computing.

Problem type	Goal	Why quantum computers excel	Example applications
Optimisation problems with exponential complexity	Finding the best solution for a problem where the computational resources required grow exponentially with the input size.	Quantum computers can process multiple states simultaneously	Supply chain optimisation, route planning
Optimisation under uncertainty	Optimising systems where data is incomplete or uncertain	Quantum computers can handle probabilistic and uncertain data effectively	Risk analysis, predictive modelling, traffic routing
Search problems	To locate a particular item or configuration that meets a predefined criterion in an unstructured or structured data set.	Grover's algorithm provides a quadratic speedup for unstructured search problems.	Search optimisation, data mining
Factorisation problems & cryptography	Tasks involving factorisation and discrete logarithms are the basis of many cryptographic systems.	Quantum algorithms like Shor's algorithm can factor large numbers exponentially faster	Breaking encryption (RSA)
Simulation of quantum systems	Problems that naturally involve quantum mechanical processes, such as simulating molecular structures, chemical reactions, or materials science.	The foundational challenge is that every quantum mechanical particle added to the simulation doubles the classical computing resources required, growing exponentially. As a result, quantum computers are uniquely suited to simulate quantum systems on a much larger scale than classical systems can manage.	Drug discovery, materials science, chemistry research
Machine learning	Training AI models on large datasets or optimising learning algorithms	Quantum algorithms can potentially accelerate training processes and handle large datasets	Quantum-enhanced machine learning, pattern recognition, data analytics
Solving linear systems	Finding solutions to systems of linear equations	Quantum algorithms like HHL (Harrow, Hassidim, Lloyd) can solve certain linear systems exponentially faster, but speedup comes with various caveats that limit its practical application	Physics simulations, engineering, financial modelling

Demystifying quantum advantage and speed

Quantum advantage[iv] refers to a situation where a quantum computer outperforms its classical counterpart. Traditionally, it has been defined as a situation where a quantum hardware-software combination solves a problem faster than the best-in-class classical solution. Such a speed advantage would render classical computing methods inferior for solving certain large-scale problems.

Quantum speedup refers to how much faster a quantum computer can solve a problem compared to best-in-class classical computers.

Whereas quantum advantage can be seen as more or less a yes/no question, the concept of quantum speedup is fundamental for understanding how *much* faster quantum computers are expected to be. Depending on the problem, quantum computers offer varying degrees of speedup over classical computers. These speedups fall into two main categories: polynomial speedup and exponential speedup. Both represent different levels of improvement in the number of steps quantum computers require to solve specific tasks compared to their classical counterparts.

Unlocking the impossible with exponential speedup

Algorithms that achieve exponential speedup, such as Shor's algorithm for factoring large numbers, are considered the crown jewels of quantum computing. This level of speedup enables quantum computers to tackle problems previously deemed impossible for classical systems.

For example[11], imagine a quantum computer solving a problem in time T, while a classical computer takes time 2^T (or any other exponentially growing function of T). This difference becomes incredibly large for even moderately sized inputs such as $T = 100$. A classical computer would require an astronomical 2^{100} time units – approximately:

1 267 600 000 000 000 000 000 000 000 000

This vast difference illustrates the impracticality of solving such problems with classical systems. However, implementing these exponential-speedup algorithms for practical, real-world applications remains a long-term goal, as current quantum computers lack the necessary scale and precision.

iv Also concepts of quantum supremacy and quantum utility are used with slightly different emphasis.

Practical gains from polynomial speedup?

Polynomial speedup refers to a situation where a quantum computer solves a problem in time T, while a classical computer does it in time T^2, T^k or other polynomial function of T. For instance, a quantum computer might complete a task in 1,000 steps, compared to $1{,}000^2 = 1{,}000{,}000$ steps on a classical computer. *Grover's algorithm* for unstructured search problems (finding a single target element out of N elements) is the most famous algorithm for this category. While less dramatic than exponential speedup, polynomial speedup has the potential for meaningful improvements, especially for certain business and scientific applications.

In addition to polynomial and exponential speedups, there is a *superpolynomial speedup* category, which falls between the two but has relatively few known algorithms. Furthermore, there is a category of *unknown speedup* that includes heuristic-based algorithms. These algorithms are particularly relevant for near-term quantum computers (NISQ devices) and are hoped to provide practical benefits even without formal speedup guarantees (see infobox on heuristic quantum algorithms on page 46).

Speedup in theory and practice

At first, the promise of speedup sounds amazing. However, discussion is almost always about *theoretical* speedup, which can differ significantly from *practical* speedup.

Theoretical speedup refers to idealised, predicted performance improvement of quantum algorithms under perfect conditions. Typically, the assessment also includes the worst cases that define the boundaries for the proof. These cases may never be encountered in the real world.

Practical speedup refers to actual performance improvement observed when running a quantum algorithm on a real-world quantum system.

Practical speedup accounts for the many real-world constraints of quantum computing, such as hardware limitations, noise, and error rates, which prevent us from achieving the full theoretical speedup—at least for the foreseeable future. It also acknowledges delays in data loading, such as the time needed to encode input data into a quantum state and the increased running time introduced by using error correction techniques. Consequently, the practical speedup is often much smaller than theoretical predictions or, for small-scale problems, non-existent.

> **Theoretical speedup highlights the promise of quantum computing, while practical speedup reflects the reality of its current limitations and opportunities.**

Another challenge in achieving quantum advantage (speedup) is that claims of advantage often spur developers to rethink classical algorithms. This has led to breakthroughs in classical computing, where problems once considered extremely difficult to solve have been tackled with much faster classical solutions[12], making the quantum advantage claim quickly outdated.

While classical hardware development follows a relatively predictable trajectory, the pace of innovation in classical algorithms can be much less predictable. These advancements often complicate direct comparisons between quantum and classical approaches, underscoring the evolving nature of this competitive landscape.

Quantum utility and other forms of advantage

Demonstrating quantum advantage in real-world applications (measured by quantum speedup) has proven to be extremely challenging. As a result, some companies have shifted the discussion to other topics or introduced new terms. IBM coined the term *Quantum utility*[13], which means that quantum computing provides reliable, accurate solutions to problems beyond brute force classical computing methods. Thus, their claim of achieving quantum utility means that quantum computers can now solve large-scale problems that were previously only accessible through problem-specific classical approximation methods. This is considered to be a significant milestone, making quantum computers a valuable tool for scientific research and exploration. It does not, however, mean that there would be speedup over all known classical methods.

The concept of quantum advantage has also evolved to include more nuanced interpretations that encompass additional dimensions worth exploring:

Qualitative advantage - Beyond speed, quantum computing can achieve qualitative advantages by delivering results superior in quality to those produced by classical systems. For instance, in machine learning, quantum systems might require less training data or produce more accurate prediction models. To qualify as a true quantum advantage, however, these qualitative results must be unattainable by classical algorithms, ensuring that the improvement is genuinely quantum in nature.

Energy Advantage - Another important dimension to consider is the potential energy efficiency of quantum computing. Quantum systems could significantly reduce energy consumption compared to classical systems—a benefit that becomes increasingly relevant as organisations prioritise sustainability and as global energy consumption on computing doubles every 3.4 months.

For example, some claims suggest that quantum computers could save energy by a factor of three orders of magnitude. In practical terms, this means that while a supercomputer might require around 10 MW of power to complete a task, a quantum computer with comparable computational capacity could accomplish the same task with just 10 kW. However, these claims have been challenged and remain speculative. Accurately predicting the future energy requirements of quantum computing is difficult, particularly because the nature of future quantum hardware is still unknown.[14]

It is essential to rigorously evaluate such claims on a case-by-case basis to ensure their validity. While the potential for energy savings is exciting, it requires careful scrutiny to separate genuine advantages from speculation.

In summary, the concept of quantum advantage—and its related ideas—continues to evolve, with new interpretations providing a more comprehensive view of the value quantum computing can offer, even without achieving outright speedups. While this broader perspective may add complexity, it better aligns quantum computing's progress with practical business and societal needs.

What are the most promising applications?

The most promising quantum applications are those that are expected to leverage the unique strengths of quantum computing to solve challenges beyond the reach of classical systems. In this section, we explore key application categories, offering insights into their potential without delving too deeply into the complexities of quantum algorithms—the "mysterious recipes" that make these applications possible.

Simulation of quantum systems

Quantum simulations specifically model quantum systems—such as molecules, atoms, or particles—where quantum mechanical properties are central. Quantum computers are particularly well-suited for these tasks because they can directly model quantum states using qubits and harness the principles of superposition, entanglement, and interference. This capability is crucial in quantum chemistry, materials science, and molecular physics, where quantum effects dominate and cannot be accurately represented by classical methods alone.

Quantum chemistry is fundamentally about understanding the quantum-level interactions between atoms and molecules. It involves calculating properties such as molecules' ground and excited states, reaction pathways, and energy levels. These calculations are critical in any application where precise molecular interactions and energy configurations are essential, including catalysis and chemical reactions. Quantum computers are used here to simulate these interactions at a fundamental level, and they can be applied broadly across many industries.

In materials science (quantum systems), quantum computing is applied to discover and design new materials with specific properties, such as improved strength, conductivity, or energy storage capabilities. Here, quantum computers simulate solid-state systems, molecular structures, and crystal lattices, aiming to optimise the arrangement of atoms to produce desired material properties. This has applications in industries like energy, electronics, and aerospace, where designing materials with unique properties can be transformative. Unlike quantum chemistry, which might focus on single molecules or reactions, materials science often involves simulating bulk properties and structures over larger scales.

Drug discovery is a specialised application of quantum chemistry focusing on biological molecules, such as proteins, enzymes, and drug compounds. In drug discovery, quantum computers help predict how drug molecules will interact with biological targets at an atomic level, which aids in understanding binding affinities, reactivity, and pharmacodynamics. This is particularly valuable for designing effective drugs more efficiently and reducing the trial-and-error involved in conventional drug design. While it utilises quantum chemistry principles, drug discovery has unique considerations like biological compatibility and toxicity, setting it apart from the broader study of chemical reactions.

Cryptography

Cryptography is one of the areas where quantum computing promises the most significant theoretical speedup, especially with algorithms like Shor's. However, labelling cryptography as the most promising application of quantum computing can be debated, as the primary focus here is on the threat quantum algorithms pose rather than the opportunities they present. Shor's algorithm, for instance, has the potential to break widely used cryptographic systems such as RSA, posing a serious challenge to the security of current encryption methods. The concern is that once sufficiently powerful quantum computers are developed, they could render many of today's cryptographic systems obsolete, risking the security of sensitive information worldwide.

As a result, much of the research in quantum cryptography is centred around developing quantum-resistant encryption methods—cryptographic systems that can withstand quantum attacks. Therefore, cryptography is not only a significant application of quantum computing but also a key driver behind efforts to establish new, more secure standards for future-proof encryption. (See more in Chapter 7)

Optimisation

Optimisation is often touted as one of the most promising applications for quantum computing—mainly due to its crucial role across industries and domains. However, quantum computers are not inherently superior to classical computers for all optimisation tasks. Their true potential lies in addressing specific types of optimisation problems, particularly those characterised by 1) limited data input but high computational intensity and 2) problems where approximate solutions hold significant value.

IS QUANTUM ANNEALING A LOW-HANGING FRUIT FOR OPTIMISATION?

Quantum annealing refers to a specific (analogue) approach of quantum computing that shows promise for solving particular optimisation problems. Optimisation is about finding the minimum value of a cost function, and quantum systems are naturally inclined to find minimum energy states. Programming an optimisation problem into a quantum system could, theoretically, reach an optimal solution by finding this lowest energy state.

Quantum annealing, like the system developed by D-Wave, leverages this approach and is designed explicitly for optimisation tasks. However, while it shows potential, it is still too early to say whether quantum annealing will achieve practical, large-scale advantages over classical methods in real-world applications.

Combinatorial optimisation is probably the most promising subclass of optimisation problems for quantum computers – particularly useful in finance and logistics. It is a type of optimisation that focuses on finding an optimal solution from a finite set of possible solutions, often by selecting or arranging discrete items in a particular way to meet a defined objective. These problems usually exhibit combinatorial explosion; as the problem size increases, the number of possible solutions grows exponentially, making it computationally intensive.

Notable examples include:

Travelling salesman problem (TSP): Find the shortest route to visit a set of cities exactly once and return to the starting town.

Knapsack problem: Maximise the value of items placed in a knapsack without exceeding its weight limit.

Job scheduling: Allocating tasks to resources (e.g. workers or machines) to minimise completion time or maximise efficiency.

The actual speedup achievable with quantum computers for combinatorial optimisation is complex and problem-specific. While quantum algorithms offer exciting potential, the performance boost depends heavily on factors like the chosen algorithm, the structure of the problem, and the limitations of current and future quantum hardware. Many quantum algorithms theoretically provide a polynomial speedup over classical counterparts. While this is a substantial improvement, doubts remain about their practical advantage (especially in the near term) due to the inherent slowness of quantum gates and the overhead of error correction.

Quantum search algorithms

Quantum search algorithms aim to speed up search tasks, where the goal is to find a specific item or solution within a large, unsorted dataset. Unlike classical search algorithms, which may require checking each entry one by one, quantum search leverages unique quantum properties to reduce the number of checks needed, leading to faster results for certain types of search problems.

The most famous quantum search algorithm, Grover's algorithm, demonstrates a quadratic speedup over classical approaches. While a classical algorithm might need to examine all items in a database to find the target, Grover's algorithm can locate it in roughly the square root of that number of steps. This advantage grows significantly with larger datasets, making quantum search valuable for applications where vast amounts of data need to be searched efficiently—such as in cryptography, optimisation, and data retrieval.

Despite its promise, the current impact of quantum search is still limited by the scale and error rates of today's quantum computers. Yet, as quantum hardware advances, search algorithms are expected to be among the first applications to realise practical speedups, especially in areas like data mining, cryptographic analysis, and pattern recognition, where even modest improvements in search efficiency could provide meaningful benefits.

QUANTUM WALKS: A STEP AHEAD IN EXPLORING COMPLEX NETWORKS

What are quantum walks?

Quantum walks are the quantum equivalent of classical random walks, where particles "move" through a graph or network. Unlike their classical counterparts, quantum walks leverage quantum principles like superposition and interference, allowing them to explore complex structures more efficiently.

Why do quantum walks matter?

Quantum walks excel at analysing graph structures—mathematical models of networks. They are particularly effective in identifying structural differences, such as comparing graphs, ranking nodes by importance, or searching for specific points (e.g., "marked vertices") within a network.

Applications in business and technology

Quantum walks have promising applications in industries where networks play a central role, including:
-Optimising communication networks: Identifying bottlenecks and improving data flow.
-Supply chain management: Ranking the importance of nodes (e.g., distribution centres).
-Social media analytics: Ranking influential users or detecting clusters of activity.
-Cybersecurity: Mapping vulnerabilities within network structures.

Quantum machine learning

Quantum machine learning (QML) combines the principles of quantum computing and machine learning to create algorithms that leverage the unique properties of quantum systems, such as superposition and entanglement. The goal is to perform machine learning tasks—like pattern recognition, data classification, and predictive modelling—more efficiently or accurately than classical algorithms.

In theory, QML could offer advantages in recognising patterns that classical machine learning algorithms might miss. This potential arises because quantum entanglement creates correlations among qubits that extend to relationships between data points, potentially revealing complex patterns. For instance, entangled qubits can process and relate multiple data points simultaneously, offering richer insights that may be especially valuable for complex data sets. While much of this potential remains theoretical, QML shows promising potential in two key areas:

Speed: Some QML algorithms may offer exponential speed advantages for tasks like training deep learning models or solving large-scale optimisation problems.

Quality: QML can enhance outcomes for pattern recognition and anomaly detection by leveraging quantum properties like entanglement.

The theory and applications of quantum machine learning are still evolving. The mechanisms that lead to successful applications in QML may differ significantly from those in classical machine learning, and there is much we have yet to understand. Although QML holds exciting potential, its practical effectiveness remains to be proven, especially given the current limitations of quantum hardware.

Current limitations and future potential

As we explore the potential of quantum computing, it is important to approach claimed breakthroughs with a healthy dose of scepticism. In their effort to simplify highly complex science, journalists can unintentionally miss crucial nuances, leading to overly optimistic or even misleading interpretations. For example, a recent claim by Chinese researchers suggested they had developed a quantum algorithm capable of breaking encryption. Some media outlets sensationalised this, but the reality was far less dramatic—they had decrypted only a 50-bit encryption, a far cry from the 1024- and 2048-bit encryption widely used today.

Despite such misunderstandings and marketing exaggerations, the promise of quantum computing remains profound. Algorithms offering exponential speedup are poised to become the “killer applications” of quantum computing. Fields such as drug discovery, cryptography, and optimisation hold tremendous potential, reshaping industries and societal functions. However, these groundbreaking algorithms depend on much more advanced quantum hardware than is currently available, keeping their practical advantages largely theoretical for now.

Even lower-speedup categories, such as heuristic and polynomial speedup algorithms, could deliver meaningful, practical benefits as quantum hardware improves and problem scales grow. However, unlocking this potential requires overcoming significant bottlenecks, such as high error rates, limited scalability, and integration challenges.

Finally, beyond the known applications, quantum computing may uncover entirely new opportunities in areas where classical computers fall short. Researchers are diligently exploring novel algorithms that could broaden the scope of quantum applications. As technology advances, so will our understanding of how to harness its unique capabilities to address some of the world's most complex challenges.

4/ When is quantum computing ready for use?

When considering the right time to adopt quantum technologies, it is essential to understand that quantum readiness is multifaceted. The first step is understanding the specific requirements of your application—some industries and problems may benefit from quantum sooner than others. However, beyond the specific needs of your application, it is essential to consider the broader readiness of quantum computing itself. This includes the maturity of the hardware, the availability of algorithms suited for practical use, the readiness of the talent to implement these solutions, the development of software tools and platforms, and the health of the ecosystem and supply chain supporting quantum innovation. Each component is vital in determining when quantum computing can truly be adopted on a scale.

Critical milestones and breakthroughs will indicate when quantum computing is ready for broader commercial use. A key measure of hardware readiness is not just the number of qubits but also their quality and stability. While systems with over a thousand physical qubits have already been introduced (e.g., by IBM and Atom Computing), these systems face significant challenges due to high error rates in computations. To unlock the most promising applications, advancements are needed not only in increasing the number of qubits but also in improving error rates and coherence times (how long qubits can maintain their state)—along with solving many related challenges on the way.

- ✓ **Multifaceted nature of readiness**
  - **hardware**
  - **software & algorithms**
  - **talent**
  - **ecosystems**
- ✓ **Signposts of readiness**

Determining when quantum computing is "ready" requires a comprehensive assessment of various factors. These include the maturity of the hardware, the availability of suitable algorithms, and the readiness of the talent pool. This chapter explores these factors and highlights key indicators that signal readiness for broader commercial adoption.

How can we measure readiness?

If you have been following the news about quantum computing, you almost certainly have noticed the race to set new records in a number of qubits[15]. Too often, this single measurement unit (number of physical qubits) has been regarded as a measure of the readiness of quantum computers, which provides a false hope of the actual usefulness of state-of-the-art computers. The number of physical qubits can be misleading because it does not indicate how many of those qubits are actually usable for addressing real-life problems. Adding more qubits can even worsen the situation by increasing noise. As a result, recently, the focus of many companies developing quantum systems has shifted more to improving the quality of qubits (moving up in Figure 3) than increasing the number of those (moving right).

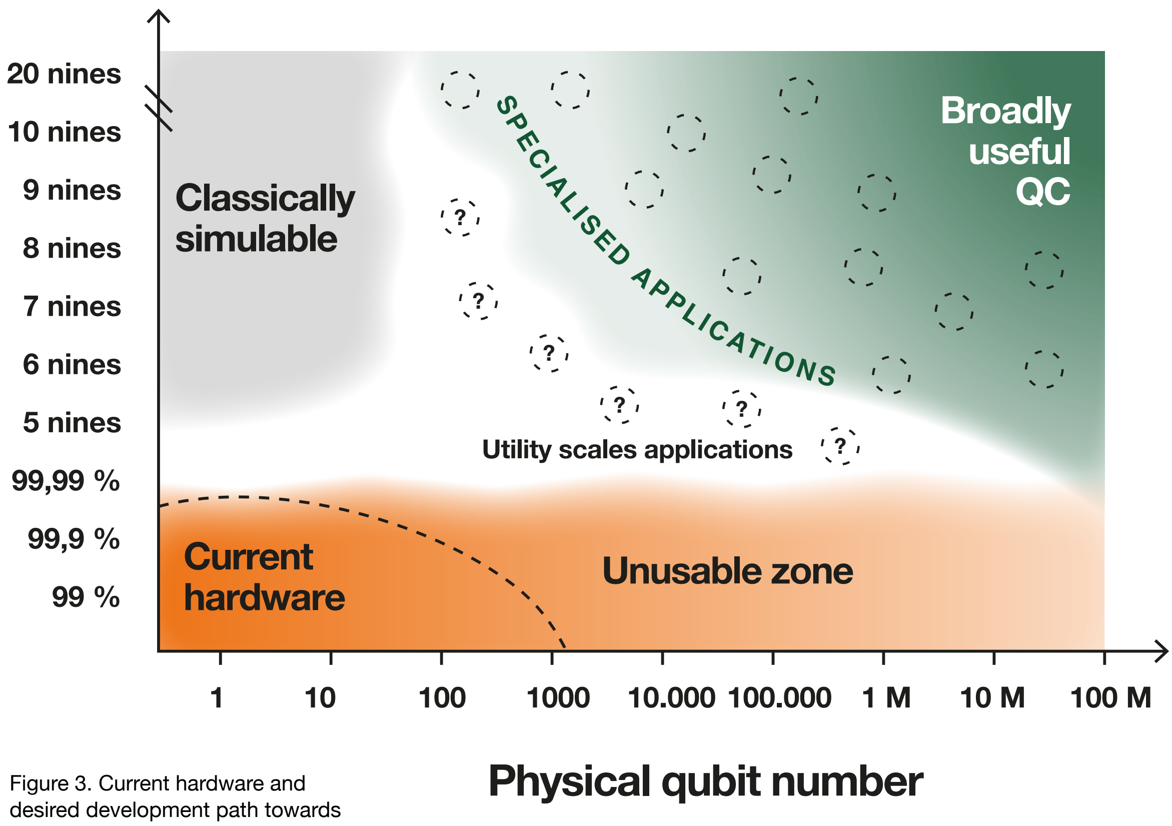


Figure 3. Current hardware and desired development path towards large-scale fault-tolerant quantum computing.[16]

Defining the “readiness” of quantum computing is also challenging since there are multiple dimensions other than hardware readiness that describe how much benefit can be achieved from quantum computing. Additional aspects of readiness should include, at least, software development, the availability and maturity of algorithms, and the preparedness of the workforce. In addition, businesses need to consider the readiness of the entire quantum ecosystem—from vendors to supply chains. Each area is critical in determining when quantum computing will be ready to make a significant impact.

High-level view of the evolution of quantum computing

As we near the end of 2024, quantum computing remains a controversial topic. In recent years, there has been a wave of optimism surrounding its potential. However, this has been met with pessimism, particularly from those grappling with the highly complex challenges hindering development. In this book, we aim to acknowledge both viewpoints, recognising that each perspective holds merit. Ultimately, the main difference lies in how much time will pass before significant breakthroughs are achieved.

Rather than make specific predictions about when certain milestones will be reached, given the wide range of guesses in the field, we instead offer a more flexible framework to understand the development phases ahead. This approach allows us to estimate the business impact expected in each phase of quantum computing’s evolution.

Be aware that even these eras are educated guesses, and breakthroughs in science and technology and ways of using technology may eventually take us to unforeseen paths. We can look at the advancement of classical computing to gain perspective on the challenge of predicting quantum computing’s development. Even with hindsight, it is difficult to pinpoint precisely when classical computers were considered “ready.” What we can identify, however, are the transitions between eras, key milestones, and breakthroughs that expanded the possibilities of what computers could achieve—many of which early pioneers never envisioned.

In the same way, the development of quantum computing should be understood as a gradual progression through various developmental phases, each with distinct capabilities and limitations. Every phase marks a significant step toward the ultimate goal: fault-tolerant, scalable quantum computers capable of solving complex, real-world problems far beyond the reach of classical systems (see Figure 4). By understanding these phases or “eras” of quantum computing development, we can better understand where technology stands today and is expected to lie ahead. Recognising that some phases’ boundaries are not sharply defined is essential. Transitions to the next might happen gradually, and there is often significant overlap between eras. However, just like with geological eras, we can identify some major events that could define the boundaries between quantum computing eras. The first major event could be the first NISQ algorithm that beats the best classical algorithms in a useful task.

> **"Identifying the first practical NISQ algorithms is one of the most critical challenges of our time. Every company leveraging computing power should explore which of their use cases could benefit from these early-stage algorithms."**
>
> Ville Kotovirta, QMill

There is a growing community that is searching for near-term solutions. If found, this could be a pivotal moment that accelerates the development of and investments in quantum computing. However, some experts remain sceptical about the usefulness of NISQ-era applications. They think a groundbreaking event will be when the first algorithm, which is theoretically proven to beat the best classical algorithm, can be successfully executed on a fault-tolerant quantum computer. This will start the fault-tolerant era and accelerate the applications and the market growth of quantum computing.

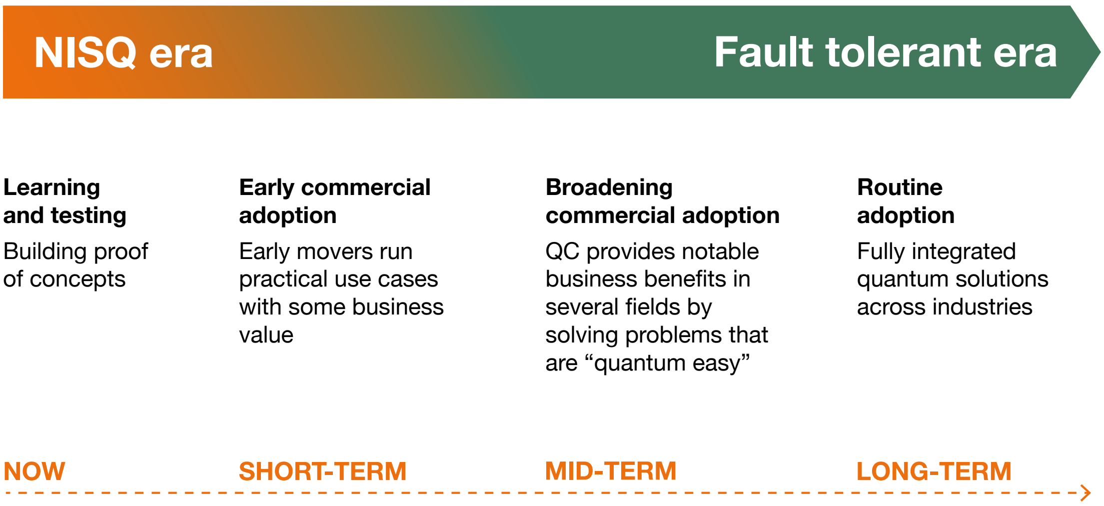


Figure 4. Eras of quantum computing development.

These eras provide a high-level roadmap for assessing when quantum computing will be ready for large-scale, practical use. They also offer businesses insights into how companies can strategically position themselves to benefit from its evolution. In the following chapter, we will explore these use cases in greater detail to help you better understand how quantum computing might impact your industry.

Quantum computing now

The current phase of quantum computing is often called the NISQ (Noisy Intermediate-Scale Quantum) era, based on the type of hardware we are limited to. NISQ designates the transition from purely research-based purposes to building proofs-of-concept with the companies to learn and identify the use cases that can be the most beneficial in the first phases of quantum breakthrough.

Focus and practicality now

Currently, the focus is on experimenting with small, niche problems, in which quantum computers are particularly good, to explore quantum computing's potential while working to overcome noise and scalability issues. Despite some premature claims, so far, there has not been proof that quantum computers would perform better than the best classical computers in any practical problem. Nevertheless, quantum computing systems are already used to solve specific problems (e.g. optimisation, small-scale quantum simulations, a specific type of machine learning), though without the speedup expected over classical methods. These use cases are limited to areas where noise and error rates are less critical. As a result, early applications are mainly experimentation, learning, and preparing for the future potential of technology.

Hardware (limitations) now

Hardware is limited in multiple ways, but the two most challenging limitations are:

- **Noise and errors**
- **Limited qubit number and connectivity**

In the current stage of quantum computer development, systems are vulnerable to environmental disturbance and the noise from the system itself, so they can only perform limited computations before noise disrupts results.

NISQ computers have a limited number of qubits, typically ranging from tens to a few hundred. This constrains the size and complexity of the problems they can tackle. Additionally, the connectivity between qubits can limit how effectively algorithms can be implemented.

Algorithms now

Although quantum computing holds immense promise, no quantum algorithms have yet been shown to consistently outperform classical ones in real-world settings. While certain algorithms, such as Shor's algorithm, have been theoretically proven to offer exponential speedups, their practical deployment depends on future, more advanced hardware. There is ongoing debate among researchers about whether there are already near-term algorithms that could provide benefits using NISQ hardware. If such algorithms exist, the question remains whether they can be effectively run on noisy quantum systems or if we must wait for fault-tolerant quantum computing.

Software tools now

The quantum software environment at this stage is designed for researchers and quantum specialists, with Software Development Kits (SDKs) like Qiskit (IBM) and Cirq (Google) providing low-level access to quantum hardware. Developers need a basic understanding of quantum mechanics to work with these tools, as they must build algorithms at the gate level. At this stage, high-level abstractions are minimal, meaning quantum software is accessible primarily to experts.

During this phase, simulators (running on classical computers) are crucial for testing quantum algorithms since access to quantum hardware is limited and noisy. Error mitigation tools are integrated into the SDKs, but true error correction is still beyond reach. Still, the overall focus is on developing proof-of-concept algorithms and exploring quantum computing's potential in highly specialised domains.

Talent now

One of the key challenges in the NISQ era is building a skilled quantum workforce. While academic institutions are increasing efforts to train quantum engineers and scientists, and early adopters have begun hiring quantum specialists, a significant talent gap remains. For businesses looking to experiment and learn, it is crucial to recruit specialists with expertise in quantum algorithms and software development or find someone to partner with. Additionally, it will be essential to upskill existing employees and managers to understand the unique aspects of how quantum computing operates.

Ecosystems and supply chains now

The current quantum ecosystem is highly fragmented, with multiple companies working on different approaches to quantum hardware (see different modalities in Chapter 2). While collaboration between academia, industry, and governments is increasing, the supply chains for quantum hardware and components still need to be developed. Building a robust supply chain will be crucial to scaling production and supporting broader commercialisation as quantum technologies advance.

Short-term future

In the coming years, we will likely see an increase in the number of qubits in NISQ systems, along with the gradual transition towards fault-tolerant computing (sometimes called early fault-tolerance). This transition means that quantum computers will experience fewer errors during computations, enhancing their computational capacity as more logical qubits become available for actual calculations. However, scalability will remain a major challenge during this phase, limiting quantum computers' applicability to large-scale problems.

Focus and practicality in short-term

Quantum computers will continue to face various limitations, so they will be used in tandem with classical systems in a hybrid computing approach. In this setup, quantum systems will tackle specific parts of a problem—particularly those with significant advantages—while classical computers will handle most tasks, as they are still better suited for most applications. This hybrid model will be key to introducing quantum computing into practical business environments.

This phase marks a shift from experimentation to real-world business applications. Quantum-classical hybrid systems will begin to demonstrate value in specific areas, where quantum computers will be used to solve sub-problems that play to their strengths. However, the limited scalability of quantum systems will confine their use to targeted, specialised applications.

Hardware (limitations) in short-term

As quantum hardware advances, we will likely see increased competition between several competing paradigms for quantum computing. Each of these paradigms has its strengths and weaknesses, and it is unlikely that a clear winner will emerge without a breakthrough in a specific qubit technology. Some systems may be categorised as advanced NISQ machines with more qubits but higher error rates. In comparison, others will prioritise reducing error rates (with fewer qubits) to achieve early fault-tolerant computing. Either way, these early systems will continue to face significant hardware limitations:

- **limited qubit scaling**
- **communication bottlenecks**
- **expensive and inaccessible hardware**

While the number of qubits is expected to increase, creating logical qubits will still require a large overhead of physical qubits, limiting the overall computational power. Most qubits will be devoted to error correction rather than computation. Furthermore, communication bottlenecks present another challenge. Loading data into quantum computers and reading the results back into classical systems can be time-consuming and introduce additional latency. In hybrid systems, this back-and-forth exchange offsets some of the computational gains offered by quantum speedups. Finally, early fault-tolerant systems are likely to be expensive and require highly specialised infrastructure, such as cryogenic cooling, making them inaccessible to many.

Algorithms in short-term

In the short term, we can expect progress in quantum algorithms across several areas, including:

- **heuristic algorithms**
- **new industry-specific algorithms**
- **quantum-inspired classical algorithms**

Many algorithms being explored in the near term, such as those used in quantum machine learning (QML) and quantum annealing, are heuristic (see infobox on the next page). To prove sceptics wrong, companies and researchers will need to experiment extensively to determine if these algorithms can outperform classical approaches.

The development of quantum algorithms tailored for industry-specific use cases (e.g., finance, healthcare, logistics) will be critical during this phase. These algorithms will need to show clear, quantifiable benefits over classical methods for businesses to justify investments in quantum computing. Currently, most algorithms are still experimental or theoretical, and more testing is needed before we can expect widespread industry adoption.

As quantum algorithms evolve, a parallel race exists in developing quantum-inspired classical algorithms. These classical algorithms attempt to mimic the structure of quantum algorithms, often improving classical performance in unexpected ways. This race between classical and quantum algorithms can be seen as positive for businesses, as the goal is ultimately to improve efficiency, regardless of the technology being used.

ARE HEURISTIC ALGORITHMS SECRET TO NEAR-TERM QUANTUM ADVANTAGE?

Heuristic quantum algorithms (e.g. VQE, QAOA, quantum annealing) are designed for quantum computers to provide approximate solutions rather than mathematically proven optimal results. These algorithms are useful for complex problems where an exact solution is impractical. While the terms “heuristic algorithm” and “NISQ algorithm” are not synonymous, they often go hand in hand in the current landscape of quantum computing.

Heuristic algorithms are often iterative, meaning they repeatedly refine a solution until it meets certain criteria or reaches a satisfactory level of performance. They do not guarantee finding the absolute best solution but aim for “good enough”, practical solutions within acceptable timeframes.

So far, no heuristic quantum algorithm has demonstrated a clear advantage over the best classical algorithms. Experts are divided on whether NISQ computers can achieve a quantum advantage or if more advanced hardware is necessary. Sceptics argue that the noise and limitations of NISQ systems may prevent these algorithms from outperforming classical methods. However, proponents highlight those heuristic algorithms, much like those used in classical AI, can still be valuable for specific problems, even without formal proof, by drawing on domain expertise and practical application.

Software tools in short-term

The development of software tools for quantum computing is expected to advance significantly in the coming years, driven by the growing demand for more accessible, powerful, and practical quantum computing solutions.

- **Improved developer toolkits and frameworks**
- **Quantum algorithm libraries**
- **Quantum-classic hybrid solutions**

The quantum software environment will become more sophisticated and accessible. SDKs (Software Development Kits) allow integration of hybrid workflows, where quantum computers handle specific parts of a problem that benefit from quantum speedups, while classical systems manage most tasks. Cross-platform SDKs are expected to enable developers to write code that can run on multiple quantum hardware platforms with minimal changes.

Higher-level libraries tailored to specific industries, such as finance or healthcare, will likely become available at this stage, making quantum computing more approachable for non-experts. No-code and low-code platforms may also appear, allowing users with little to no quantum expertise to experiment with quantum computing in their fields. Modular quantum functions for specific tasks, like optimisation or quantum chemistry, will become more common, reducing the need for deep quantum knowledge.

Talent in short-term

One of the primary challenges for businesses will be building a skilled workforce capable of developing, deploying, and maintaining early fault-tolerant quantum systems. This means training specialists in quantum hardware and software and integrating classical and quantum systems in hybrid architectures. The talent pipeline for quantum computing is still relatively small, so early adopter organisations must invest in quantum education programs and workforce development.

Ecosystems and supply chains in short-term

As quantum hardware becomes more mature, we will likely start seeing major tech corporations' acquisitions of the most promising quantum startups. This would lead to the emergence of larger quantum ecosystems consisting of hardware vendors, software developers, research institutions, and industry partnerships. These ecosystems will support the broader commercialisation of quantum technology and drive the creation of standardised quantum tools for business use.

Mid-term future

Focus and practicality in mid-term

This mid-term phase represents the broadening commercial adoption of quantum computing, where high-impact applications begin to solve complex problems previously considered unsolvable. Quantum computing will start to have a widespread impact, influencing numerous industries and global systems:

- **Simulating larger, more complex quantum systems**
- **Solving large-scale optimisation problems across industries**
- **Adopting quantum machine learning (e.g. pattern recognition and predictive modelling)**
- **Quantum-proof cryptography adopted as an industrial norm**

Hardware (limitations) in mid-term

The hardware of this era is defined by the acronym FTQC (Fault-Tolerant Quantum Computing). Although there is no clear definition of the milestones required to reach, the hardware in this era is generally expected to scale up to millions of physical qubits while maintaining very low error rates. There is also a need for drastically improving coherence times (how long qubits can keep their quantum state).

Even if these are reached, some limitations are likely to exist:

- **Resource demands (high overhead) for error correction**
- **Complex and expensive physical infrastructure**
- **Manufacturing and material defects**
- **Multiprocessor qubit communication**
- **Quantum memory, QRAM**

Although fault tolerance will be more advanced, maintaining logical qubits will still require a significant number of physical qubits. While systems can handle more qubits, scaling towards millions of logical qubits is expected to pose challenges due to the overhead. Furthermore, quantum computers, particularly those using superconducting qubits or trapped ions, are still expected to require complex infrastructure like cryogenic cooling systems and ultra-stable environments to operate. This infrastructure is expensive and difficult to maintain, limiting the accessibility and scalability of quantum computers. In addition, building quantum processors with millions of qubits will require highly precise manufacturing processes, and any defects in the materials or design could cause errors. Maintaining consistent quality in manufacturing at large scales will be difficult.

Ensuring fast, reliable communication between qubits in large quantum systems will likely remain a technical challenge. Quantum information must move efficiently between qubits in a processor and between multiple processors in a more extensive network, which could present bottlenecks. Finally, the practical implementation of quantum memory (QRAM) remains uncertain (see infobox on the next page), as building it at a useful scale presents significant technical challenges, including coherence maintenance, resource demands, and error correction.[17]

DO FUTURE QUANTUM COMPUTERS HAVE A MEMORY?

Quantum Random Access Memory (QRAM) is a theoretical concept, with no large-scale practical implementation yet. It aims to provide quantum computers with the ability to store and access data in superposition. Unlike classical RAM, which retrieves data from a single address at a time, QRAM could theoretically access multiple memory addresses simultaneously, greatly enhancing the efficiency of quantum algorithms when working with large datasets.

QRAM is particularly important for certain quantum algorithms, such as those used in machine learning and database searches, where parallel data access offers a major advantage. Many of these algorithms assume that your input for the algorithm comes from QRAM (or similar persistent quantum state), which is currently impossible as QRAM does not exist, and the quantum states collapse after measurement.

Algorithms in mid-term

In the mid-to-long term, quantum algorithms will continue to evolve. However, there are a few key areas of uncertainty.

It is unclear whether quantum computing will develop highly specialised algorithms tailored for particular problems or if we will see the emergence of *general-purpose algorithms* that can be widely applied across different industries. The competitiveness of polynomial and heuristic algorithms will also remain an open question. If the overhead caused by quantum operations remains high, well-optimised classical algorithms may still outperform quantum ones.

Software in mid-term

In the mid-term, quantum software is expected to mature significantly, offering user-friendly tools and platforms that make quantum computing more accessible to businesses. Quantum SDKs (Software Development Kits) will become highly abstracted, offering high-level quantum APIs (Quantum Application Programming Interface) that allow users to focus on solving business problems rather than understanding the technicalities of quantum hardware. Quantum computing platforms will likely offer domain-specific SDKs and tools that enable users to run quantum applications without writing any quantum code.

Quantum-as-a-service is likely to become the norm, with businesses leveraging quantum power for real-time decision-making, optimisation, and data analysis. Quantum resources will be dynamically allocated across cloud platforms, making quantum computing as ubiquitous and accessible as classical cloud computing is today.

Talent in mid-term

As quantum computing becomes more practical, the talent landscape will likely evolve. Ongoing debates exist about how much quantum-specific expertise future software developers will need. With trends like no-code and low-code development on the rise, future quantum computing platforms may not require every developer to have a deep knowledge of quantum mechanics. Instead, high-level development tools could make quantum computing more accessible to a broader range of professionals. Furthermore, cross-disciplinary collaboration will become increasingly important. Talent will need to span across quantum specialists, software engineers, and domain experts in industries like healthcare, finance, and logistics. Integrating quantum computing into existing workflows will be essential for practical adoption.

Ecosystem and supply chain in mid-term

Will we have a dominant design? Breakthroughs in different modalities can be defining factors in the race for dominant design (e.g. superconducting vs. neutral atom qubit technology). This may have surprising effects on winning ecosystems. If one actor has bet on the wrong horse, they may be forced out of the game. On the other hand, some players may rise above qubit technologies and become fully cross-platform players.

Long-term future and beyond

The ultimate goal of quantum computing is to reach the large-scale fault-tolerant phase, where machines can perform large-scale, error-corrected quantum computations without limitations caused by noise from the environment. When this level of technology is reached, it will open the door to discoveries, disrupt entire industries, and lay the groundwork for the future of computing (see Chapters 5 and 6).

Hardware, algorithms, and software development may be complicated to envision. For example, at the time of inventing classical computers, probably no one could see the real-life use cases in the 2020s. Additionally, uncertainty also arises from other factors, such as geopolitical shifts and the development of artificial intelligence. These factors could significantly influence the pace and direction of quantum computing development. Geopolitical competition might accelerate investments and breakthroughs in quantum technologies, while advancements in AI could help optimise quantum algorithms, discover new applications, or enhance quantum error correction techniques.

Conclusion – When will it be ready?

While quantum computing still needs time before it is ready for widespread business use, and significant challenges remain before it can meet its high expectations, the field is advancing rapidly. Both the public and private sectors are investing heavily, and recent breakthroughs have bolstered confidence that practical applications are on the horizon. Building an understanding of the signs of readiness and preparing now will be critical for those aiming to lead in the future of innovation.

5/ Which industries are ripe for quantum disruption?

In business management, it is crucial to shift focus towards the problem-solving capabilities of quantum computing rather than speculating on which industries will face disruption first.

Quantum computing has the potential to yield diverse benefits, with impacts varying across different sectors. For instance, optimisation challenges are relevant to logistics, manufacturing, and finance industries. In some areas, quantum computing might deliver modest efficiency improvements. In contrast, in others, it could enable transformative changes that inspire a new way of doing business, such as shifting from annual planning to real-time control.

Quantum computing also promises to revolutionise industries that rely on phenomena based on quantum mechanics, such as materials science and pharmaceuticals. These advancements could lead to discoveries and innovations that reshape entire fields. The competitive edge will likely belong to businesses that adopt quantum computing early, especially in computationally intensive fields like finance, where even a temporary quantum advantage could provide a significant advantage.

A more strategic approach is to explore the business opportunities and risks of quantum computing across three time horizons: short-term, medium-term, and long-term. In each phase, quantum computing will play different roles and hold varying significance across industries.

- ✓ **Optimisation opportunities**
- ✓ **Quantum mechanics-based breakthroughs**
- ✓ **Adopt three time horizons thinking to structure possibilities**

Foresighting quantum computing helps us prepare for the changes it may bring. In this chapter, we will examine its impact on both industry sectors and the wider society, using the same three time horizons explored earlier in the book to assess the development of quantum technology and quantum computing.

How can foresight unlock quantum opportunities?

Foresight offers a valuable perspective for examining the future business landscape, particularly in the context of complex and transformative technologies like quantum computing. By systematically exploring potential technology scenarios, identifying emerging industry trends, and analysing how these trends intersect with opportunities presented by quantum computing, we can gain valuable insights into the opportunities and challenges.

A networked foresight approach is precious in quantum computing, where uncertainty and complexity make it challenging to pinpoint business relevance. This approach, which harnesses the collective intelligence of diverse stakeholders, is embodied in the "future radars" we present (see Figure 5 and Figure 6). Compiled from research and collaborative sense-making with companies and other actors in the financial and pharmaceutical industries, these radars provide a dynamic framework for understanding the evolving quantum landscape.

The approach in these radars differs somewhat from the more common use of future radar for horizon scanning. Typically, foresight radars identify signals across a broad range of future technologies and trends, primarily relying on literature studies. However, in this instance, our focus has been on deeply exploring a single emerging technology – quantum computing – across multiple dimensions and with a high level of granularity. Quantum computing's novelty means existing information often centres on technical aspects while providing limited insight into the possible transformations and wider consequences within specific industries. This has necessitated a degree of imaginative thinking to identify signals relating to the future development trajectories of various sectors.

These radars are living documents, constantly evolving to reflect new insights and encourage ongoing dialogue. By sharing these, we hope to inspire your company to think creatively about the possibilities this technology might bring. They can serve as a foundation for developing your company's future-scanning capabilities and strategies, enabling you to identify emerging trends and potential disruptions. The true value lies not in isolated signals but in understanding the broader patterns of change these signals indicate.

Let's begin by examining the financial services sector and the potential impact of quantum computing on its development. We'll highlight some signals from the future radar to illustrate key trends. After finance, we'll take a similar look at the pharmaceutical industry, and finally, we'll touch upon other sectors, such as energy and manufacturing.

Financial services in three quantum time horizons

In financial services, quantum computing will offer a transformative advantage in the future by enabling robust optimisation and stochastic modelling capabilities. Unlike classical computing, quantum algorithms will be able to handle probabilistic calculations and evaluate multiple scenarios simultaneously. This is particularly valuable in finance, where statistical models and algorithms are often applied to predict asset prices, returns, and risk factors that evolve randomly over time. The more complex the calculations, the more quantum computing's strengths become apparent.

Quantum computing has the potential to speed up combinatorial optimisation, allowing financial models to consider a broader set of variables and yield global rather than local solutions. Though quantum simulations might play a lesser role in finance than in industries like pharmaceuticals or aeronautics, it is crucial to recognise the considerable potential of quantum technology to revolutionise market simulations and real-time optimisations. Furthermore, by integrating with machine learning, quantum computing may ultimately enhance predictive analytics and anomaly detection, improving decision-making in finance in ways that classical computing cannot achieve[18]. You can find more detailed information about the types of problems suitable for quantum computing on page 28.

The future radar is presented in Figure 5 highlights signals that illustrate the potential impact of quantum computing across various dimensions – societal, environmental, legal/security, and political/economic – in addition to potential use cases. It employs the same time horizons used throughout this book: short-term, mid-long-term, and very long-term. However, the precise placement of individual signals on the radar is less critical in this context. The goal is not to make specific predictions but to highlight various potential paths and encourage strategic thinking. It is important to note that technologies and applications will likely advance alongside improvements in quantum computers and algorithms. For example, while portfolio optimisation can be performed with quantum-inspired algorithms today, future quantum computers will enable us to perform this optimisation directly. As those computers advance, we can expect even greater precision, the ability to handle more variables, and operation closer to real-time. So, it is essential to note that the signals identified in this radar represent the outcome of a single foresight exercise and are based on current perspectives. The placement of signals on the radar, both in terms of time and dimension, depends on the specific development aspect that each signal aims to convey.

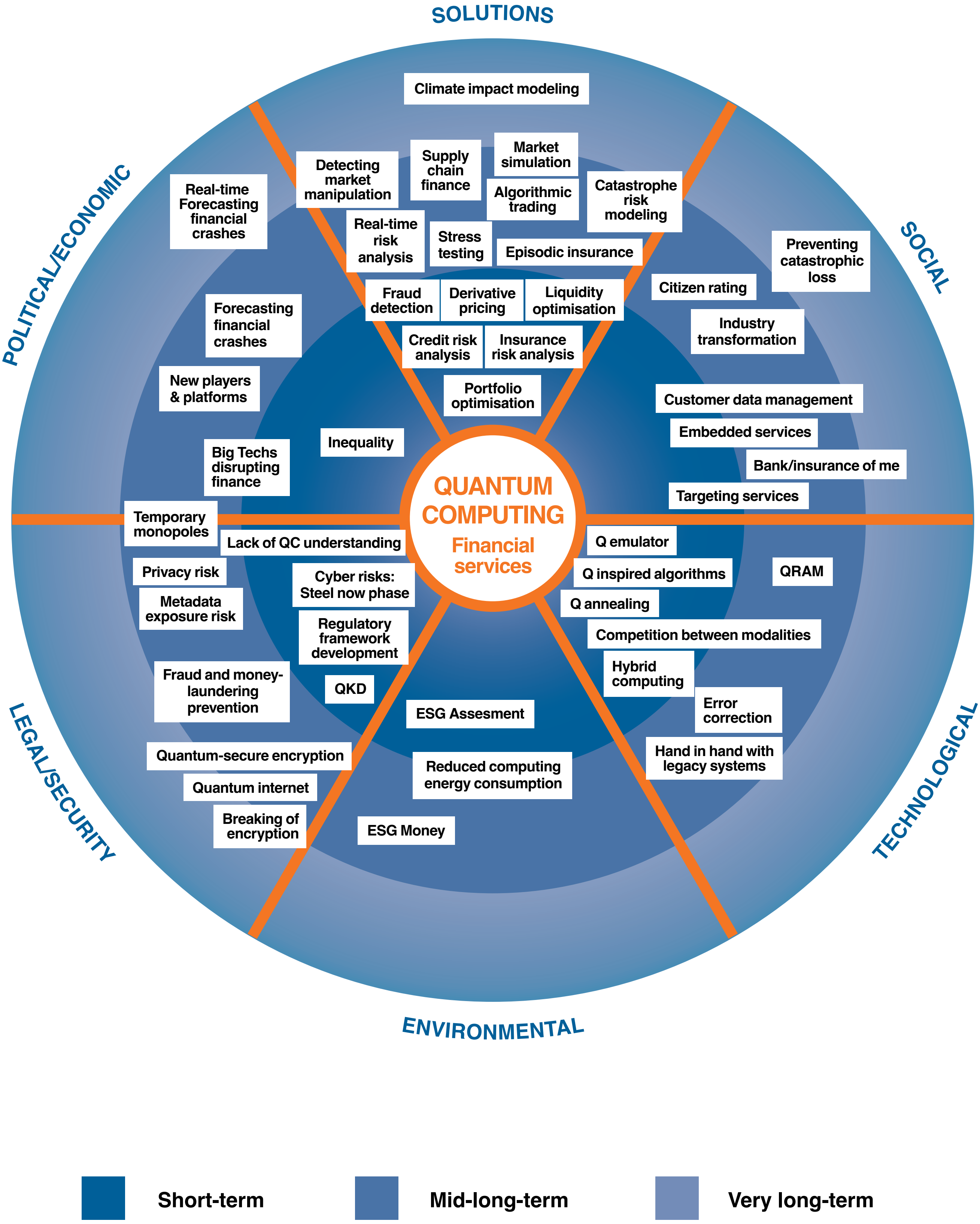


Figure 5. Example of a future radar showcasing the role of quantum computing in financial services.

Financial services now and in the short term

Within the financial services sector, several pioneering companies, particularly large banks, have already established dedicated quantum computing teams. These companies are actively now exploring use cases in areas such as carbon footprint assessment, service feature optimisation, credit risk analysis, portfolio optimisation and quantum machine learning opportunities[19]. The financial sector is precisely the kind of industry where even minor improvements in optimisation can lead to significant cost benefits due to the global scalability of its operations[20].

In the near term, quantum algorithms can potentially significantly enhance risk assessment in credit and insurance. These areas, often involving complex optimisation problems, are well-suited to leverage the computational advantages of quantum computers. For example, quantum algorithms could be used to more effectively model and predict credit defaults and assess the likelihood of insurance claims. Quantum-enhanced Monte Carlo simulations could offer significant improvements in these areas, enabling more accurate and efficient analysis of complex risk scenarios with fewer computational resources. Financial institutions could make more informed decisions regarding loan approvals and insurance pricing by improving risk models. This could lead to a more efficient allocation of capital, reduced risk exposure, and potentially more competitive products and services for customers.

Quantum algorithms are also being applied to ESG investing, potentially enabling more sophisticated analysis and optimisation of portfolios considering environmental, social, and governance factors. As quantum computers and algorithms advance, they can process larger datasets more efficiently, facilitating highly sophisticated ESG modelling and supporting investors in making informed and sustainable choices.

Moreover, quantum computing may accelerate the entry of BigTech companies into the financial services market. Many of today's BigTech giants are already active in the quantum computing field, and their expertise could give them a significant advantage in developing and deploying quantum-enhanced financial applications. This trend has the potential to disrupt the financial landscape significantly. For example, several BigTech companies already offer loans in addition to bank accounts, blurring the lines between technology and finance[21]. As many of these companies could leverage quantum computing to provide innovative and personalised financial products, the traditional boundaries of the financial services market could erode, leading to increased competition and potentially reshaping the industry.

Furthermore, financial institutions must be mindful of quantum computing's impact on cybersecurity. As they handle highly sensitive data and manage contracts that must remain tamper-proof, the "harvest now, decrypt later" threat, where encrypted data is recorded today for future decryption with quantum computers, is of particular concern. Financial institutions should proactively address this vulnerability to ensure the long-term security of their systems and customer data. A more detailed discussion of quantum computing risks can be found in Chapter 7.

Financial services in mid-long term

In the mid-long term, quantum computers may transcend the limitations of classical computing, tackling even problems previously deemed impossible. With a significant increase in the number of logical qubits, quantum algorithms may enable tackling complex optimisation problems at unprecedented scales, leading to solutions that were previously out of reach. In simulation, quantum computers could model increasingly complex phenomena, even enabling real-time simulations of dynamic environments. In the mid-term, the financial sector may also experience the emergence of quantum-boosted AI systems for large-scale data analysis, pattern recognition, and predictive modelling.

BANKING AND FINANCIAL INSTITUTIONS

Quantum computing has the potential to reshape the banking industry by enabling the handling of intricate datasets and elevating decision-making processes to new levels. It is highly probable that quantum algorithms will outperform classical methods in areas such as portfolio optimisation, price optimisation, forecasting, risk management, and arbitrage. This leads to faster and more accurate operations. It aligns with the rise of data-driven decision-making and automated systems. Real-time insights and predictive analytics may quickly become the standard.

Quantum technologies may also support the trend toward personalised financial services by enhancing customer profiling and credit assessments, aligning with the shift toward tailored financial solutions. Quantum computing could also accelerate changes in banking models by enabling more sophisticated financial products, favouring tech giants and non-traditional players. This would intensify competition and may push financial services toward platform-based models, where real-time, personalised financing is seamlessly embedded into everyday transactions, blurring the lines between banks and other service providers.

Supply chain finance helps streamline cash flow by ensuring suppliers are paid promptly while buyers manage payments over time[22]. Quantum computing could take this a step further by dramatically optimising how financial resources flow through complex supply chain networks. With its unparalleled data processing capabilities, quantum computing can track and analyse transactions in real-time, efficiently managing liquidity and allocating funds where they're most needed. As quantum technology evolves, it could become an invaluable tool for businesses, boosting resilience and responsiveness across their supply chains.

Additionally, quantum-driven economic scenario modelling could improve risk mitigation strategies, potentially helping financial systems to become more resilient in a volatile global economy.

> **"Fundamentally, finance is all about optimisation and trust."**
>
> Petri Liimatta, OP

INSURANCE

Quantum computing has the potential to reshape the insurance industry by enabling more precise risk assessment[23] and pricing optimisation, allowing insurers to offer more personalised and competitively priced policies. With the ability to process vast datasets and consider far more variables than classical methods, quantum technologies could enable faster, more accurate risk calculations, making it possible to adapt policies in real time to evolving risks. Additionally, quantum technologies may improve fraud detection, scenario modelling, and portfolio management for insurers' investment strategies.

Quantum-enhanced data analysis may also empower insurers to provide proactive, real-time risk mitigation advice to their customers, shifting their role from risk mitigators to partners in risk prevention. For example, the ability to model natural phenomena more accurately could help insurers advise clients on minimising potential damages from disasters.

The industry is considering whether early adopters of quantum computing will secure a more favourable risk pool, potentially leaving higher-risk clients to those who are slower to adopt. Furthermore, quantum-powered real-time risk assessment could accelerate the integration of insurance products directly into other services, blurring the lines between traditional insurers and digital service providers.

> **"Quantum computing in itself provides insurance companies with almost limitless and carbon-free computing power. Combined with artificial intelligence and the Internet of Things, the industry is undergoing a revolution comparable to when computers first entered the scene."**
>
> Heikki Lassila, LähiTapiola

REGULATORY FRAMEWORK DEVELOPMENT

With quantum computing reshaping financial services, regulatory frameworks must evolve to address both its benefits and risks. Beyond concerns about data security and privacy, quantum's speed and power introduce challenges related to transparency and compliance. Stricter reporting standards will likely be required to ensure quantum-powered tools, such as real-time risk assessments, operate within legal and ethical boundaries.

Quantum's data-processing capabilities may offer opportunities to improve market oversight, enabling regulators to detect systemic risks and potential financial crises earlier. This could lead to more proactive measures to stabilise markets before disruptions occur. Quantum-enhanced fraud detection could provide regulators and institutions with faster, more accurate tools to identify fraud by analysing complex datasets, reinforcing financial system integrity.

> **The growing importance of data as a critical resource raises vital questions about its ownership and reliability. To regulate a quantum-driven financial landscape effectively, we must first understand the evolving connections, dependencies, and shifts in business practices shaping the industry.**

Katja Taipale, Bank of Finland

Quantum technologies may also shift market competition, giving early adopters an edge. Regulators must monitor potential imbalances and broaden their oversight to include non-traditional players, such as tech companies leveraging quantum, to maintain a fair and competitive financial landscape.

Financial service in the long term

In the long term, quantum computing can potentially transform the financial services sector, influencing industry practices and delivering broader societal impacts. This technology could enable real-time forecasting of financial crashes[24] by analysing vast and complex market data with unprecedented speed and accuracy, offering the possibility of predicting and mitigating financial crises before they escalate. Such capabilities would contribute to a more stable and resilient financial system, safeguarding economies worldwide.

With enhanced abilities to model and predict risks, financial institutions could develop more effective risk management strategies, including creating innovative insurance products and optimising investment portfolios to withstand potential shocks. Quantum-powered climate models, for example, could allow insurers to assess and price climate-related risks more accurately and advise their clients on risk mitigation strategies, ultimately supporting a more sustainable and informed approach to managing climate impacts.

Real-time simulation models could also become the norm, powered by quantum computing's capacity to process and simulate market dynamics and risk factors in real-time. This advancement would enhance the precision of pricing, portfolio optimisation, and investment strategies, leading to a more dynamic and efficient market environment that benefits both investors and the broader economy.

However, integrating quantum technology presents challenges. RSA encryption, which underpins much of today's online security, could become vulnerable, prompting financial institutions to adopt quantum-resistant cryptography to protect sensitive data and maintain trust within the digital financial system. The development of a quantum internet could eventually enable secure communication in selected high-security applications.

Pharmaceuticals in three quantum time horizons

The pharmaceutical industry stands apart with its unique challenges and long development timelines. Bringing a new drug to market is a complex and costly endeavour, often requiring decades of research and billions of euros in investment. Most drug development projects fail, underscoring the intricate nature of biological systems and the difficulty of predicting the efficacy and safety of new therapies. However, these challenges make the pharmaceutical sector a prime candidate for quantum computing. At the heart of drug discovery lies the interaction of molecules governed by the laws of quantum mechanics. Quantum computers, with their inherent ability to simulate quantum phenomena, offer the potential to accelerate drug development, optimise clinical trials, and pave the way for more personalised medicine. This chapter examines how quantum computing could transform the pharmaceutical landscape, potentially leading to significant healthcare and human health advances.

One way to begin analysing the potential of quantum computing is to break down key processes within the industry and identify their associated challenges and development needs. Understanding the underlying mathematical problems within each process allows you to explore how quantum computing offers solutions. In the pharmaceutical industry, this approach can be particularly valuable. The following table 5 categorises pharmaceutical industry processes by the challenges associated with each stage, along with potential quantum computing use cases.

Table 5. Examples of pharmaceutical industry processes, key challenges, and potential quantum computing use cases.

	Need for	Potential quantum use cases
Drug discovery entailing the conceptualisation of the therapeutic into a molecule with known pharmacologic effects • Target identification • Target validation • Assay development • Screening	• Improved signal detection in large datasets • Overcome experimental limitations • Enhanced test reliability • Comprehensive analysis • Virtual screening of massive libraries	• Accelerate molecule finding • Enhancing CADD approaches • Generate deepfake data for ML learning data • Hypothesis finding by ML to structure relationships properly and predict the 3D structure of target proteins • Enhance hit generation and identification • Virtual screening • Disease understanding
Drug development steps taken to convert the molecule above into an approved and registered drug product • Optimisation • Preclinical studies • CMC (chemistry, manufacturing, controls)	• Significantly improved drug design • Enhance lead optimisation to improve R&D productivity • Algorithms that reflect human systems • Predicting clinical outcomes from preclinical results	• Optimisation of candidate properties • ADME (absorption, distribution, metabolism, excretion) prediction • Activity prediction • Toxicity prediction • Molecular-mechanics simulation • Molecular-dynamics simulation • Dosing optimisation • Solubility optimisation • Financial risk optimisation • Catalysis optimisation • New product formulation
Drug development – Clinical trials • Phase I • Phase II • Phase III	• Reduce failure rate (>90%) • Cost reduction • Algorithms that simulate drug-patient interaction • In vitro-in vivo correlation • Pharmacokinetic-pharmacodynamic prediction • Patient virtualisation	• Patient identification and stratifications • Patient pharmacogenetic modelling • Causality analysis for side effects • Trial-site selection optimisation • Imputing missing data in clinical trials/ real-world evidence
Approvement • Regulatory submission and review	• Reduce uncertainty • Minimise launch delays • Rapid analysis of clinical trials • Rapid analysis of various data sources	• Enhanced risk assessment • Predictive modelling for patient responses • QML for pattern identification and data analysis
Commercialisation • Post-marketing surveillance & clinical studies (Phase IV) • Market access – commercial & medical	• Treatment optimisation and cost-effectiveness from a societal perspective • Personalised medicine	• Patient understanding: analysis of real-world data and QML for personalised insights • Automatic drug recommendation • Tailored healthcare providers – patient engagement • Forecasting of market demand, regulatory changes, competitor actions, and market dynamics
Production	• Sustainability and cost-efficiency	• Calculation of reaction rates in API production • Optimisation of catalytic processes • Optimisation of material and waste flow in production facilities • Enhance new product formulations • Quality monitoring • Optimisation of temperature in production facilities • Predictive maintenance
Logistics & supply chain	• Sustainability and cost-efficiency	• Route optimisation • Network optimisation • Dynamic inventory optimisation • Dynamic warehouse optimisation • Procurement optimisation
Life cycle management	• LCM by repurposing/ reformulation	• Identifying and validating potential new targets • Optimising formulation • Predicting clinical outcomes

As with finance, we have also gathered signals for three time horizons on the future radar for the pharmaceutical industry (see Figure 6). The radar includes social, legal/security, political/economic, and environmental perspectives specific to the pharmaceutical industry and elements relevant to other sectors, such as general product development, logistics, and market analysis.

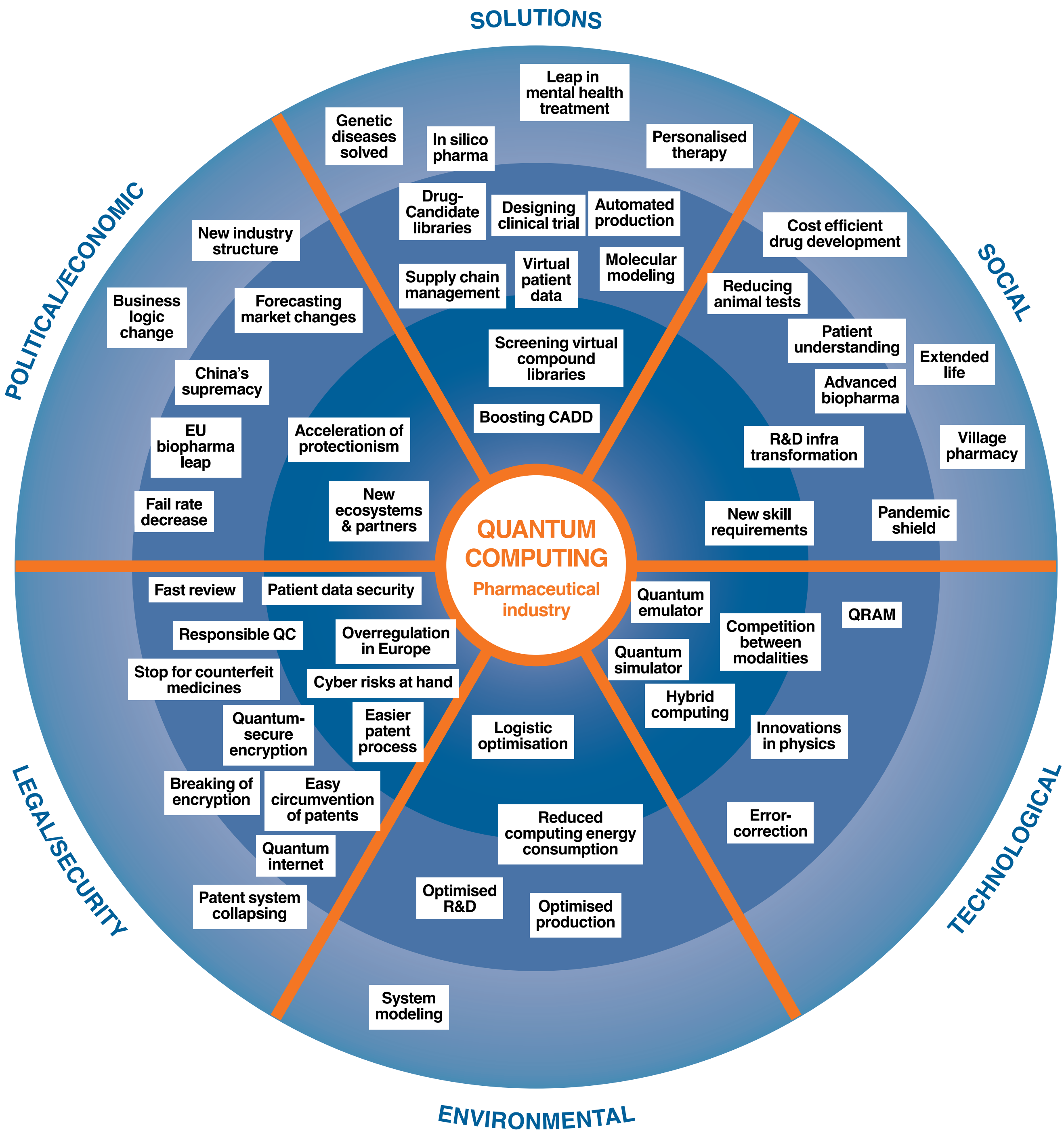


Figure 6. Example of a future radar showcasing the role of quantum computing in the pharmaceutical industry.

Pharmaceuticals now and in the short term

The pharmaceutical industry is where large R&D-intensive companies are already making significant progress in identifying potential use cases, testing quantum algorithms, and building partnerships and ecosystems to drive innovation[25]. Several startups are also actively developing algorithms specifically for the noisy quantum era[26]. In the drug development process, the initial applications may not necessarily be molecular modelling but screening virtual compound libraries. Quantum computing is expected to enhance computer-aided drug design (CADD) by predicting molecular properties with high accuracy in the future. Currently, CADD is limited to small to medium-sized drug candidates and is sequential mainly due to the capabilities of existing computers. AI and quantum-inspired CADD are already paving the way towards the future of automated drug development in this early stage.

Moreover, drug development and production involve numerous optimisation problems where early-stage quantum and quantum-inspired algorithms can be applied, such as designing clinical trials and optimising logistics. As quantum computing advances, pharmaceutical companies build new networks and capabilities to leverage this technology effectively. To prepare for the business benefits these advancements may bring, many pharmaceutical companies are establishing collaborative learning ecosystems that involve both internal teams and external partners.

Pharmaceuticals industry in mid-term

DRUG DEVELOPMENT

Quantum computing is poised to be crucial in supporting silico drug development, where simulations and modelling replace traditional lab experiments. Quantum algorithms will enable more accurate simulations of molecular interactions, allowing researchers to identify drug candidates faster and with greater precision. This advancement could significantly accelerate the drug discovery process, reduce costs, and unlock new possibilities for treatments that were previously too complex to explore.

In addition to drug discovery, quantum technologies will likely improve clinical trial design and optimisation. Quantum algorithms could analyse large patient datasets to identify optimal trial participants, reduce the time needed for trials, and increase the likelihood of success. The technology may also support the rise of personalised medicine by allowing for more precise matching of treatments to individual genetic profiles, leading to more effective therapies with fewer side effects.

A particularly promising application of quantum computing is in biopharma, where drug development often involves large, complex biological molecules. Quantum technologies excel at handling the intricate interactions between these larger molecules, offering the potential for breakthroughs in areas like protein folding and biologics. This capability could help biopharma's quest to develop targeted therapies for chronic and rare diseases. Additionally, quantum-powered simulations could reduce the reliance on animal testing by improving early-stage testing accuracy.

EFFICIENT AND SUSTAINABLE PHARMA

Beyond drug development, quantum computing may drive efficiency in pharmaceutical production by optimising manufacturing processes. Quantum algorithms will enhance automation in production lines, reducing waste and increasing resource efficiency. Quantum computing may also transform logistics and supply chain management in the pharma sector. By enabling real-time tracking and predictive logistics, quantum technologies could help streamline operations, ensuring that medicines are delivered more quickly and reliably, even across global supply chains.

Additionally, fraud detection may improve with quantum-enhanced security measures, safeguarding against counterfeit drugs—a growing concern in the industry. With better tracking and authentication systems, quantum technologies could help ensure that only genuine products reach patients.

PHARMACEUTICALS AS R&D INTENSIVE INDUSTRY

Quantum computing's ability to accelerate drug discovery may shift the balance of the patent system. Pharmaceutical companies rely heavily on patents to protect original drugs and generate profits. However, as quantum computing and AI can make processing vast amounts of data easier, the competitive advantage of patents could weaken.

Quantum's impact on patents may also shift where drug development occurs. For instance, China is rapidly increasing its investments in quantum computing and AI, leveraging its regulatory framework on data usage to advance personalised medicine and drug discovery. China is already a major player in manufacturing active pharmaceutical ingredients (APIs), the components of medications that produce therapeutic effects. With the adoption of quantum technologies, China could further strengthen its position in the pharmaceutical value chain by accelerating drug development and reducing time-to-market.[27]

Quantum-enabled healthcare in long term

As quantum computing advances, we are approaching a point where it can fulfil its transformative potential. This opens exciting possibilities in medicine and life sciences, allowing us to address previously unsolvable challenges. Quantum computing could transform healthcare by tackling complex issues such as decoding genetic diseases and advancing our understanding of mental health. With vast amounts of data becoming more accessible, quantum computing could drive personalised therapies on a large scale, tailoring treatments to individual patients with unprecedented precision.

> **"Currently, it takes approximately 10-12 years to develop a single molecule into a treatment for the patients. The path is very risky, and the project might end at any point. Quantum computing presents a promising opportunity to accelerate this process, allowing faster, more cost-effective development of new treatments and developing new treatments faster. Especially the early phases in development may change if the quantum computing increases the probability to take the right molecules forward. At best, it means decreasing development costs and faster access to new treatments."**

Nadia Tamminen, Pharma Industry Finland

Quantum computing might also significantly reduce the failure rate of drug development. Currently, over 90% of new drug candidates fail, often during expensive late-stage trials. By enabling more accurate simulations of molecular interactions, quantum computing could predict toxicity and efficacy earlier in the process, reducing risks and allowing more companies to participate in drug development.

Furthermore, quantum computing has the potential to significantly enhance the process of in silico drug development by shifting a significant portion of the discovery process into virtual simulations. By rapidly modelling molecular behaviours, quantum computing could speed up drug testing, predicting safety and efficacy without requiring extensive laboratory experiments. This transition to digital labs would necessitate significant investments in IT infrastructure, capabilities building, data management, and cybersecurity.

Quantum simulations could also optimise pharmaceutical production, reducing waste and improving efficiency in manufacturing. Ultimately, quantum computing might help people stay healthier by enabling faster treatments and more precise therapies, potentially easing the burden on healthcare systems and reducing societal healthcare costs.

Catalysing future transitions

Earlier, we explored how strategic foresight reveals opportunities for quantum computing in various industries, focusing on financial services and pharmaceuticals. We noted trends such as the rise of Big Tech and embedded services in finance and the role of quantum computing in personalised medicine.

We can extend the approach to identifying transitions beyond individual industries. By focusing on broader trends, we can explore how quantum computing might accelerate progress toward sustainable development as a whole or delve into specific areas such as the energy transition or the rise of electrification.

In this section, we highlight a selection of these compelling themes, examining how quantum computing can catalyse their development and reshape the future.

Energy transition

The energy sector has been at the forefront of exploring quantum computing applications, driven by the need to address the complex challenges of transitioning to a more sustainable and resilient energy system. Major companies are exploring quantum algorithms to optimise power generation, storage, grid management, and complex energy management tasks. They are also investigating customer-facing applications such as demand forecasting and smart charging. At this stage, the primary motivations for collaborating with research partners on quantum computing topics are the expected improvements in efficiency and innovation.

As technology matures, quantum computing is set to transform how we generate, distribute, and consume energy. Looking further ahead, quantum computing can potentially drive breakthroughs in clean energy innovation and sustainable material design. By enabling a deeper understanding of complex chemical reactions, quantum simulations could unlock new technologies such as advanced solar cells, more efficient biofuels, and even fusion energy. At the same time, quantum-enabled material science could lead to lighter and more durable components for renewable energy infrastructure, from wind turbines to solar panels, making clean energy solutions both more efficient and cost-effective.

Circular economy in manufacturing

The circular economy presents a compelling opportunity for quantum computing to catalyse transformative change in manufacturing. While these possibilities remain largely exploratory, the potential is clear: quantum technologies could enable the industry to reimagine production systems with sustainability and resource efficiency at their core.

Creating new materials designed for recyclability or biodegradability is an area where quantum computing could significantly impact. By leveraging its ability to simulate materials at the atomic level, quantum technology could accelerate the discovery of sustainable alternatives that are easier to recycle or decompose, supporting circular design principles from the outset. Quantum simulations could also help model complex chemical processes, enabling more efficient separation of materials or their conversion into reusable forms.

Quantum algorithms also hold the potential for optimising resource use and minimising waste in production processes. Manufacturers could significantly reduce costs and environmental impact by finding more efficient ways to use raw materials while aligning their operations with circular economy objectives. Similarly, quantum-enabled insights could improve the modelling and optimisation of product lifecycles, leading to designs that prioritise durability, reparability, and end-of-life recyclability.

Efficient logistics and resource distribution are critical for achieving circularity at scale. Quantum computing's optimisation capabilities could transform how materials and products are transported and redistributed in circular supply chains, creating more resilient systems that minimise waste and energy consumption. Additionally, traceability is essential to circular systems, ensuring materials and products can be tracked throughout their lifecycle. Quantum cryptography could offer a secure and reliable way to maintain transparency in circular supply chains, building trust and efficiency in the flow of resources.

Energy efficiency is another crucial factor. Many recycling and material processing techniques today are energy-intensive. Quantum simulations could uncover new, less energy-demanding methods for handling and processing materials, making circular practices more economically viable and environmentally sustainable.

6/ How can quantum computing create a brighter future?

Quantum computing has the potential to unlock solutions to some of humanity's most pressing problems, reshaping industries, economies, and even the future of our planet.

Throughout history, scientists have discovered amazing new technologies, such as electricity, computing and the internet, which initially seem to lack real-world applications. The extremely limited views that people had about potential applications for these technologies may seem amusing with the benefit of hindsight. Today, we know that electricity powers our homes, industries, and communication systems. At the same time, modern computing and the internet are 'carried in our pockets' and have transformed nearly every aspect of life. Now, as we stand on the brink of another technological revolution—quantum computing—we are similarly constrained by our ability to imagine a future that looks significantly different from today.

Quantum computers harness the principles of quantum mechanics to perform calculations in ways we are only beginning to comprehend. Just as electricity was once viewed as a scientific curiosity, quantum computing's early applications may seem very limited — especially if we view them through the lens of current technological boundaries.

This chapter aims to broaden that perspective and encourage us to look further into the future, where quantum computing could enable transformative advancements across industries. In this envisioned future, quantum computing holds the promise of improving our lives by addressing humanity's most pressing challenges, such as climate change, while unlocking some of the universe's deepest mysteries.

- **Benefits across industries**
- **Solving the most pressing problems of humankind**
- **It helps to understand the universe**

In this chapter, we will highlight these longer-term opportunities that quantum computing may offer once the related technological challenges are resolved.

Solving complex challenges across industries

Quantum computing has the potential to drive transformational changes across a wide range of industries, not by offering short-term fixes but by addressing complex, large-scale challenges in the long term.

Optimisation at a global scale

One of quantum computing's most impactful benefits will be its ability to optimise large, interconnected systems that span industries and geographies. From global supply chains to urban traffic management and energy grids, large-scale quantum computers might be able to process countless variables in real-time, helping to make these systems more efficient and resilient. Whether it is adjusting logistics during a global crisis or managing fluctuating energy demands in real-time, quantum computing promises to revolutionise how we manage and optimise resources.

Accelerating innovation

Quantum computing's ability to simulate highly complex processes could drive innovation across numerous sectors, from manufacturing to healthcare and energy. The discovery of materials with enhanced properties—such as increased strength, flexibility, or conductivity—could revolutionise industries like automotive and aerospace. By providing unparalleled insights into the molecular and atomic levels, quantum simulations can accelerate the development of new technologies and materials, advancing innovation at an unprecedented pace.

Enhancing data processing and AI

As quantum-enhanced AI and machine learning gradually become feasible, industries that rely heavily on data—such as finance, healthcare, and retail—could experience faster and more accurate insights. In the future, quantum computing may enable businesses to process vast datasets in previously unthinkable ways, potentially leading to improvements in predictive modelling, customer behaviour analysis, and real-time decision-making. This capability could transform how companies respond to market changes, tailor their offerings, and strategise for the future.

Improving sustainability

One of the key areas where quantum computing is likely to have an impact across industries is sustainability. The technology could enable more efficient energy use, better waste management, and the design of low-carbon technologies. From optimising energy grids to discovering new, more efficient energy storage solutions, quantum computing could be crucial in reducing industries' environmental footprints and driving the shift towards greener technologies.

Tackling global challenges

Beyond its impact across industries, quantum computing has the potential to address some of the most pressing global challenges that humanity faces today. By offering new methods to solve complex, interconnected problems, quantum technology could pave the way for improved healthcare, a sustainable environment, and global security—all of which are essential for the future of our planet.

Advancing healthcare

Quantum computing's ability to process and simulate biological systems at a quantum level could bring unprecedented advancements in healthcare. One of its most transformative contributions may be in drug discovery. Quantum computers could simulate molecular interactions with unparalleled accuracy, allowing researchers to model how potential drugs interact with the human body at the atomic level. This has the potential to drastically speed up the discovery of new treatments and vaccines, reducing the time and cost associated with bringing life-saving medications to market.

Moreover, quantum computing could enable personalised medicine by analysing massive datasets of genetic and environmental factors. This could allow healthcare professionals to tailor treatments to individual patients, improving outcomes and reducing side effects. The ability to model complex biological systems in real-time could also enhance disease prediction and prevention, allowing for earlier interventions and more precise diagnoses.

Tackling climate change

The fight against climate change is one of the most significant challenges of our time, and quantum computing offers new tools that could help address it. One area where quantum computing can have a considerable impact is climate modelling. Today's climate models, while advanced, are limited by the processing power of classical computers. Quantum computers could take climate simulations to the next level, enabling more accurate predictions of how ecosystems will respond to rising temperatures, melting ice caps, and changing weather patterns. This, in turn, would allow policymakers to create more effective strategies for climate mitigation and adaptation.

In addition, quantum computing could play a key role in developing clean energy technologies. Quantum simulations can help researchers design more efficient solar cells, batteries, and energy storage systems, making renewable energy more viable globally. Furthermore, quantum algorithms could optimise energy consumption across industries, reducing carbon footprints and contributing to a more sustainable future.

Ensuring global security

The need for enhanced cybersecurity grows as the world becomes more digitally connected. Quantum computing presents both a challenge and an opportunity in this space. On the one hand, quantum computers could potentially break foundational encryption methods, such as RSA and ECC, which secure today's data—posing a significant threat to global security.

However, the quantum threat is also driving innovation in the field of cryptography. In response, researchers are developing quantum-safe encryption algorithms designed to withstand attacks from quantum computers. While these algorithms are classical in nature, they are inspired by the capabilities of quantum computing. They will be critical for securing communications, financial transactions, and sensitive government data in a post-quantum world.

Additionally, quantum computing could improve global security by enhancing risk analysis and predictive modelling for large-scale events such as pandemics, natural disasters, and geopolitical conflicts. By processing vast amounts of data in real-time, quantum computers could help governments and organisations anticipate and respond to emerging threats more effectively.

Advancing sustainable agriculture

Another global challenge that quantum computing can address is ensuring food security and promoting sustainable agricultural practices. Quantum simulations may model complex agricultural systems, allowing researchers to develop crops more resilient to droughts, pests, and disease. Additionally, quantum algorithms could optimise water usage and resource distribution in agriculture, leading to more sustainable farming practices that produce higher yields with less environmental impact.

From unseen challenges to unimaginable solutions

Quantum computing is not just about solving today's problems; it is about preparing for the future. As with all breakthrough technologies, its full potential may take time to be visible. However, just as we could not have predicted the transformative effects of electricity or the internet in their early stages, we must recognise that quantum computing will likely unlock possibilities we cannot yet fully comprehend.

Preparing for the unknown

Quantum computing can potentially solve problems we do not yet know exist. As the world continues to evolve, new challenges will arise—whether in technology, science, or society. Quantum systems will provide the tools needed to address these unforeseen obstacles by offering solutions beyond classical computers' capabilities.

For instance, as industries become more digitally interconnected, new layers of complexity and risk will emerge. Quantum computing's ability to process vast, complex systems may enable us to model and manage these risks in ways we have not yet imagined. This applies not only to data-driven fields like cybersecurity and AI but also to social systems, where quantum computers could model economic dynamics, global supply chains, or even urban infrastructure with greater accuracy, providing predictive insights into future disruptions.

Moreover, quantum computing may help shape a brighter, more resilient, and data-driven future. It could enable real-time, multi-variable analysis of global systems such as energy distribution, urban planning, and global healthcare. Instead of reacting to crises, we may be able to predict trends, optimise resources, and develop solutions before problems arise. This would allow governments, businesses, and societies to build resilience and respond more effectively to unforeseen challenges.

Enabling unimaginable discoveries

In addition to addressing challenges, we can foresee that quantum computing will likely lead to discoveries in areas we have not yet considered. In the same way that the internet gave rise to entirely new industries, quantum computing may spawn applications and breakthroughs that reshape the future of science and technology.

For example, quantum computers could help unravel some of the most mysterious phenomena in science. Whether it is understanding the true nature of dark matter, unlocking the secrets of quantum gravity, or developing new approaches to fusion energy, quantum computing could enable new fields of exploration that push the boundaries of human knowledge. This ability to model the universe at a quantum level might lead to a deeper understanding of fundamental physics, which could, in turn, transform how we understand the world around us.

7/ How can we navigate the quantum computing risks?

While the full potential of quantum computing may still be years away, the threat it poses to current encryption standards is undeniable. The risk is heightened by the potential for sensitive information to be stolen and decrypted in the future when quantum computers can break current encryption methods. This potential impact on data security is a cause for concern and underscores the need for organisations to assess their current vulnerabilities and begin planning for a post-quantum world.

Any organisation that wants to protect its financial data, intellectual property, or other sensitive information, particularly sensitive personal information like health records, must act immediately. This is especially critical for businesses that operate critical infrastructure such as power grids, telecommunications networks, transportation systems, and financial institutions.

The threat affects data that will still be classified ten years from now, underscoring the need for immediate action. Identifying and transitioning critical systems to quantum-safe encryption will be complex and time-consuming. To minimise this risk, the industry must transition to quantum-safe encryption, prioritise sensitive data, adopt quantum-resistant technologies, and enhance collaboration with governments and regulatory bodies.

Quantum computing presents not only challenges to data security but also has significant implications for society and geopolitics. As countries enter a 'quantum arms race,' disparities in resources and capabilities threaten to increase global inequalities. Additionally, the swift advancement of quantum technologies raises ethical and societal issues, including effects on privacy, data ownership, and surveillance. It is essential to understand these risks to prepare for and mitigate the potential downsides of advancements in quantum technology.

- ✓ **Sensitive data is at risk**
- ✓ **Immediate action is needed to transition to quantum-safe solutions**
- ✓ **Collaboration is critical to navigating this challenge**

This chapter shifts the focus from the opportunities presented by quantum computing, as discussed in previous chapters, to the risks and threats it may introduce. As quantum technologies develop, they could create new vulnerabilities in data security, critical infrastructure, and global stability. By understanding risks and threats early, we can take proactive measures to mitigate them effectively.

Quantum computing as a security threat

While quantum computing offers transformative opportunities, it also presents significant risks, particularly in the realm of cybersecurity. These risks could impact individual privacy, disrupt critical infrastructure, and threaten national security, necessitating immediate and coordinated action.

Threats to data confidentiality and privacy

Quantum computing has the potential to profoundly threaten data confidentiality and privacy by rendering current encryption algorithms obsolete. Quantum computers running Shor's algorithm could eventually compromise highly sensitive information, such as financial transactions, medical records, and government communications. This vulnerability is exacerbated by scenarios like "harvest now, decrypt later," where attackers steal encrypted data now and plan to decrypt it once quantum technology matures (see infobox).

The most urgent threat concerns long-term sensitive data, such as government secrets or critical national infrastructure information. Such breaches could significantly erode public trust in digital systems, undermining the reliability of essential services and threatening the stability of the digital economy. These risks highlight the urgency of transitioning to quantum-resistant cryptographic solutions to ensure secure data.

RISK OF DATA HARVESTING FOR FUTURE DECRYPTION

"Harvest now, decrypt later" refers to a cyberattack where encrypted data is stolen today with the intent to decrypt it later when quantum computers become powerful enough to break current encryption methods.

- **Harvesting phase:** Attackers steal encrypted data from laptops, servers, or during transit across networks. The attacker stores stolen data until advancement in quantum computing enables decryption.
- **Decrypting phase:** Quantum computers are used to break the encryption, compromising sensitive data.

This tactic poses a significant threat to data that retains its value over time. Think of it as a ticking time bomb for your sensitive information. The potential consequences of such attacks are significant. If confidential information is decrypted, it could lead to serious privacy breaches, putting individual and corporate data at risk. Exploiting vulnerabilities in authentication systems could disrupt business operations, resulting in financial and reputational damage. Attackers could also steal valuable intellectual property or R&D insights, leading to a significant loss of competitive advantage. In addition, digitally signed contracts could be manipulated, resulting in the forgery of legal records, while long-term ransomware campaigns could further compromise organisational stability.

Disruption of critical infrastructure and services

Quantum computing could also disrupt the operation of critical infrastructure and essential services if adversaries break the encryption protecting classified communications and control systems. Power grids, financial systems, and communication networks are all at risk. Attacks on these systems could lead to widespread economic disruption and compromise a nation's sovereignty. For law enforcement and intelligence agencies, encryption is crucial for secure communication, intelligence gathering, and data storage. If encryption becomes breakable, their ability to protect national interests and conduct covert operations is compromised. This could affect public safety and national defence capabilities.

How can we build a quantum-safe future?

Building a secure quantum future requires addressing these challenges through two complementary approaches: Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). PQC focuses on developing new cryptographic algorithms resistant to both classical and quantum attacks, while QKD leverages the principles of quantum mechanics to establish secure communication channels. Together, they form the backbone of a quantum-safe digital landscape.

THE DECRYPTION OF RSA - WHY DO YOU NEED TO ACT NOW?

Some quantum applications, such as using Shor's algorithm to break a 2048-bit RSA key, require extremely high-performance hardware. Estimates suggest this could necessitate millions or even tens of millions of physical qubits. However, the exact number remains uncertain, as advances in error correction could significantly reduce this requirement. Given this uncertainty, predicting when quantum computers will be capable of breaking RSA encryption is extremely difficult, with expert opinions ranging widely—between 5 to 40 years.

Regardless of when the threat materializes, acting now is critical. Transitioning to quantum-safe encryption algorithms is a complex and time-consuming process, estimated to take 3 to 12 years, depending on the industry. Additionally, you must account for how long your data needs to remain confidential. Delaying action increases the risk of your sensitive data being vulnerable once quantum decryption becomes feasible.

Post-quantum cryptography and standardisation

PQC refers to new cryptographic algorithms that are believed to be secure against attacks from classical and quantum computers. Although algorithms are already available, they are not yet widely used. Standards are vital in this transition to ensure wide-scale adoption. Standards ensure that different systems using these new algorithms can seamlessly work together, providing a unified defence against quantum attacks. They also guarantee that the algorithms used have been rigorously tested and are genuinely secure. Furthermore, standards simplify the transition to quantum-safe cryptography by offering clear guidelines and best practices, making the process more efficient and cost-effective.

The National Institute of Standards and Technology (NIST) is a critical player in this effort, leading the way in standardising quantum-resistant algorithms. In 2024, NIST released the first three standardised algorithms for quantum-safe encryption, marking a significant milestone in this transition. Governments worldwide recognise the importance of this issue and are implementing regulations and initiatives to promote the adoption of quantum-safe solutions.

Exploring the quantum key distribution

While PQC is essential for a quantum-safe future, it may not be enough. New methods for breaking even the most robust PQC algorithms could emerge as quantum computing evolves. This necessitates a multi-pronged approach to exploring alternative solutions like Quantum Key Distribution (QKD). It leverages quantum mechanics principles to distribute encryption keys securely between two parties. This makes it virtually impossible for eavesdroppers to intercept the keys without detection, ensuring secure communication even in the face of quantum attacks.

QKD is a fundamental building block for the *quantum internet*, a future network that uses quantum phenomena to achieve unprecedented security and capabilities. By enabling highly secure communication that is resistant to attacks - even from powerful quantum computers – QKD could become a critical part of tomorrow's communication infrastructure. These systems can be integrated with classical communication infrastructure, such as fibre optic cables. This compatibility could facilitate a gradual transition to a hybrid quantum-classical internet, where QKD secures the most sensitive communications.

Collaboration for a quantum-safe future

The transition to a quantum-safe world is a complex and long-term undertaking requiring significant resources, technical expertise, and global coordination. Collaboration among governments, industries and research institutions is critical to overcoming these challenges and ensuring the security of the digital landscape. Ultimately, standards and advancements in technologies like QKD are the foundation upon which we can build a quantum-safe world, enabling a safe, interoperable, and innovative digital landscape in this new era of technology.

The risk posed by quantum computing has prompted the U.S. to take early action, starting with President Biden's signing of the Quantum Computing Cybersecurity Preparedness Act in 2022[28], leading to a phased migration plan to quantum-safe cryptography. In contrast, the European Union has been slower, recently issuing a recommendation in April 2024 to coordinate its transition to post-quantum cryptography[29]. Although still in the recommendation stage, stronger regulations may follow, and businesses should be prepared for more stringent EU guidelines shortly.

Societal and geopolitical implications

The rapid advancement of quantum computing has sparked a global "quantum arms race," with nations vying for dominance in this transformative technology. This competition carries significant societal and geopolitical implications. The first countries to achieve advanced quantum capabilities could gain a significant geopolitical advantage, potentially leading to shifts in the balance of power and dominance in areas like cybersecurity, economic influence, and technological innovation. However, this race also risks exacerbating existing global inequalities. Wealthier nations and organisations are better positioned to invest in quantum technologies and transition to quantum-safe security, potentially leaving less developed countries and smaller organisations vulnerable. Protectionist policies restricting access to quantum technologies or intellectual property could further hinder international cooperation and exacerbate these inequalities.

Public perception of quantum computing will play a crucial role in its development. Fear and misunderstanding could hinder progress and delay the potential benefits that quantum computing could bring to society. Therefore, it is essential to increase public awareness of the positive impacts of quantum computing while addressing potential concerns. At the same time, the rapid advancement of quantum technologies raises critical ethical questions surrounding privacy, data ownership, and increased surveillance capabilities. Without a well-developed ethical framework, there is a risk that quantum technologies could be misused.

The need for urgent action and collaboration

By working together, we can promote responsible innovation and ensure that quantum technology serves the betterment of humanity. Mitigating risks requires urgent and international collaborative action across multiple fronts:

- **Adopt quantum-safe cryptography**
- **Build awareness and expertise**
- **Foster international cooperation**

Investing in quantum-safe cryptography is crucial, with a focus on developing, standardising, and deploying new algorithms that are resistant to quantum attacks. Governments and organisations must adopt cryptographic agility, ensuring their systems can be easily updated as new cryptographic solutions emerge.

Awareness and expertise are also critical components of preparedness[30]. Policymakers, business leaders, and the public must understand the importance of quantum-safe security. Building a skilled workforce capable of developing and implementing quantum technologies will be essential to addressing these challenges.

Quantum threats are global challenges requiring collaborative initiatives in research, standardisation, and information sharing. International coordination will help protect digital infrastructure and ensure that the benefits of quantum technology are shared widely rather than concentrated in a few regions.
In conclusion, while the societal and national security implications of quantum computing are daunting, proactive measures can mitigate these risks. Societies can safeguard their digital infrastructure by developing and deploying quantum-resistant solutions, investing in skills and awareness, and fostering international collaboration. This will pave the way for a secure and resilient future in the quantum era, allowing societies to harness quantum's full potential without compromising core values such as privacy, fairness, and global cooperation.

> **"Quantum computing also produces societal risks, but these are already being considered, and attempts are being made to mitigate them in advance, so the situation is not hopeless."**
>
> Jasmin Jutila, August Associates

8/ What is the best quantum strategy for my business?

As businesses navigate the constantly changing landscape of technological advancements, quantum computing emerges as a significant frontier. With many emerging technologies competing for attention, it is essential to assess whether quantum computing aligns with your business goals and why having a quantum strategy might be worthwhile. Even if the immediate relevance of quantum computing is not entirely clear, exploring its potential now and considering the role of quantum computing within your business can provide valuable insights into future applications and opportunities.

For most companies, a dedicated quantum strategy is not essential at this stage. Instead, prioritising *continuous learning and experimentation* is key. It is essential that threats and opportunities of quantum computing are understood at the executive level, integrated into the broader business strategy, and regularly monitored within the organisation's technology radar. The best plan for your business cannot be defined externally only based on the expected disruptive impact of quantum computing on your industry and your role in it. Your plan depends also on available R&D resources, technology adoption culture, and renewal capabilities.

Above all, your quantum strategy should reflect your ambition and risk tolerance. Integrating quantum computing opportunities into your business will involve several stages and strategic decisions as the technology advances. It is essential to plan for different time spans and remain flexible, including the possibility that quantum computing may not meet all the expectations set for it. However, you will ultimately enhance your readiness to capitalise on new technologies by exploring what quantum computing could offer and making informed decisions based on a strategic analysis of its developments.

- ✓ **Be curious about quantum computing**
- ✓ **Explore early**
- ✓ **Tailor your strategy**
- ✓ **Be adaptable**
- ✓ **Enhance your future readiness**

This chapter discusses the essential considerations for creating a quantum strategy that aligns with your specific starting point and objectives. It provides a framework for evaluating the potential role of quantum computing in your business.

How do you evaluate quantum computing's significance for your business?

As with all emerging technologies, the journey towards adopting quantum computing follows a path shaped by its perceived usefulness and ease of use. However, quantum computing's early stage of development presents a unique challenge: it has yet to deliver clear business benefits, and its full potential will take time to materialise. Moreover, the ways quantum computing will be used in industries are not fully known and can vary significantly.

Despite these uncertainties, the first step is to place quantum computing on your technology radar. Awareness of the technology and its possibilities will allow your business to assess its potential and understand when to engage in relevant experiments. When shaping your quantum strategy, you should evaluate the potential benefits, reflect on possible applications, and consider alternative starting points for exploration.

Evaluating the potential benefits and internal readiness

To evaluate quantum computing's potential for your business, begin by exploring relevant applications and use cases already identified in existing literature, such as optimisation, machine learning, or simulations. Reflect on how these align with your business's current priorities and long-term strategies for innovations.

Next, consider your company's approach to innovation and technology adoption. Are you a pioneer willing to experiment with emerging technologies, or do you prefer to follow proven trends? Evaluate your organisation's ambition, risk tolerance, available resources, R&D intensity, and culture of experimentation. These factors will shape how aggressively you should pursue quantum computing opportunities. For some businesses, cautious exploration may be prudent, while for others, early adoption could provide a significant competitive edge and foster innovative thinking.

External factors in assessing industry context

Quantum computing's relevance will also depend on your industry and competitive position. For industries like finance, logistics, or pharmaceuticals, quantum applications could offer substantial advantages, such as a notable cost reduction in logistics or breakthroughs in drug discovery. Reflect on whether quantum computing can address critical challenges in your industry or provide new opportunities to differentiate your offerings. Businesses in stagnant or highly competitive industries may find that quantum technologies open doors to fundamentally reshape industry dynamics.

> **“Is your company in a position where a vastly superior solution could enable you to disrupt your own industry or enter a new one?”**

Topias Uotila, Unitary Zero Space

Focus on long-term readiness

Adopting quantum computing is a long-term endeavour, especially for businesses whose core systems—such as supply chain management, financial operations, or data analysis—are deeply embedded and require substantial effort to adapt to new technologies. For these organisations, readiness will depend on gradual integration and continuous learning as the technology advances. Recognising this, companies should build flexibility into their strategies to adapt to the evolving quantum landscape.

Tailoring your approach to quantum computing means balancing ambition with caution and aligning exploration with your organisation’s capabilities and goals. By evaluating potential benefits, understanding your industry’s dynamics, and starting with accessible entry points, you can position your business to seize quantum opportunities as they arise.

What strategy suits your business?

The journey into quantum computing offers businesses various roles to choose from, ranging from trailblazing innovators and early adopters to cautious observers and those opting to wait and see. Understanding your role in this evolving ecosystem is critical to aligning quantum opportunities with your strategic goals. Your brand image, risk appetite, and the resources available for experimenting with quantum technology are critical factors in making a strategic decision. The risks and opportunities differ depending on when you get involved in quantum computing and what your role is in the development.

There are several strategies companies can adopt, each suited to different risk profiles, innovation capabilities, and business goals. Given that quantum computing is still in its early stages with many uncertainties, whatever you choose, make sure that your strategy remains flexible and adaptable to potential changes. In addition, adopting a phased strategy is generally advisable, starting with small-scale experiments (proof-of-concept projects) and scaling up as the technology matures. By doing so, you can identify potential partners and better understand how quantum computing development connects to other technologies that support your business. Let’s explore four broad strategies:

Do nothing – strategy

If quantum computing appears irrelevant to your business or its potential benefits seem unappealing, adopting a 'Do nothing' strategy may be appropriate. This approach works well for industries like traditional construction, where quantum computing is not expected to disrupt the market in the near or mid-term. Companies with limited R&D resources, slow technology adoption cycles, tight financial constraints, and business models that do not prioritise innovation may also find this strategy suitable. However, even if your industry is not an early adopter, you should remain aware of decryption risks and potential long-term implications (see Chapters 6 and 7).

Should your perception of quantum computing change in the future, the opportunity to be an innovator might have passed, but late adoption could still be an option. This strategy can also be suitable if there's scepticism about the potential benefits of quantum computing. However, even *Sceptics* have a valuable role in the development community by asking tough questions that could help move progress forward.

> **"Quantum is not for everyone. Not yet."**
>
> Aparna Prabhakar, Schneider Electric[31]

Monitor and explore – strategy

For businesses interested in quantum computing but not yet ready to make significant investments, the 'monitor and explore' strategy offers a balanced approach. This strategy involves regularly monitoring quantum computing developments, participating in relevant discussions or initiatives (e.g., Business Finland events and research projects), and periodically evaluating the benefits of engaging in small-scale experiments or partnerships.
This approach suits a wide range of businesses. It is particularly beneficial for industries likely to be transformed by quantum computing but where heavy investments in emerging technologies are currently impractical. For companies under pressure to innovate due to environmental or financial challenges, this strategy allows you to test the waters without overcommitting resources.

This strategy allows exploring quantum computing's potential through small, focused learning experiments, which helps your team and decision-makers adopt a long-term perspective. It also allows you to stay informed, ensuring you're ready to act when the technology matures.

Pilot and adopt – strategy

This strategy positions your company as an *Early adopter*, actively exploring the potential of quantum computing and its applications. By running pilot projects or proof-of-concept experiments, you gain valuable insights into how quantum computing could enhance your operations and contribute to your long-term goals.

This strategy is ideal for companies with a strong culture of innovation and research, especially those looking to become or remain thought leaders in adopting new technologies. It is also a good fit for industries where even a modest quantum advantage could translate to significant benefits—such as financial risk assessment and logistics optimisation —are prime candidates for this approach. These opportunities may be too important to miss.

By adopting this strategy, your business can remain at the forefront of quantum technology, positioning itself as a leader in this rapidly evolving field and preparing for future breakthroughs.

Lead the frontier – strategy

This strategy is for companies aiming to establish themselves as *Pioneers* in quantum computing. It requires substantial investments in R&D, fostering partnerships with academic institutions, and creating an innovation ecosystem to accelerate quantum advancements. Given the complexity of quantum computing, achieving practical business benefits requires collaboration across multiple stakeholders, including industry leaders, startups, and government bodies.

Pioneering companies go beyond early adoption by committing more resources to quantum technology than their competitors. This approach enables the development of a tailored quantum ecosystem, addressing industry-specific challenges and positioning the organisation as a key beneficiary of quantum breakthroughs. By investing early and significantly, you can shape the quantum landscape to align with your sector's unique needs.

Strategic partnerships play a critical role in this approach. Collaborating with government initiatives, quantum startups, and established technology providers can fast-track the development of viable quantum solutions while mitigating risks. These alliances also help secure a place at the forefront of innovation, ensuring your business benefits directly from emerging opportunities.

Adopting this strategy not only establishes your business as a leader in the quantum revolution but also provides a unique opportunity to influence the trajectory of quantum development. By taking an active role in shaping this transformative technology, you position your organisation to define its future rather than simply reacting to it.

Maintaining a flexible, forward-looking approach

Whether your business chooses to do nothing, monitor and explore, pilot and adopt or lead the frontier, each approach has its merits. The key is to adopt a flexible strategy that evolves alongside quantum technology, ensuring your organisation is prepared for the opportunities and challenges that lie ahead. Table 6 summarises each strategy and role, including who might benefit from each approach and potential applications to consider.

Table 6. Strategies and roles.

Strategy	Role	Description	Suitable For	Examples of activities
A) Do nothing	Non-adopter or Sceptic	Minimal engagement with quantum computing. Monitor risks and advancements from a distance.	Traditional industries with low-tech focus, limited R&D, or financial constraints.	Occasionally review advancements and industry-specific risks.
B) Monitor and explore	Cautious observer	Stay informed about quantum advancements by participating in discussions, attending events, and conducting low risk experiments to explore potential applications.	Those wanting to explore QC without full commitment and/or those who lack capabilities or resources for more active experimentation.	Monitor, conduct learning experiments, prepare for threats
C) Pilot and adopt	Early adopter	Actively investigate quantum computing's potential through pilot projects and proof-of-concept experiments. Build internal capabilities and assess strategic advantages.	Research-intensive industries (e.g., material science, chemistry), and sectors where QC is expected to provide significant advantages.	Engage with QC ecosystems. Lead or participate in projects with proof-of-concepts. Prepare roadmap
D) Lead the frontier	Pioneer	Commit to significant investments in quantum R&D, forming ecosystems with academic institutions, startups, and government bodies to drive innovation.	Large organisations with robust R&D budgets, strong innovation cultures, and the ambition to lead technological disruption.	Large-scale innovation ecosystems or dedicated quantum labs.

Quantum computing is an emerging technology with the potential to transform businesses. While we are still waiting for practical business benefits to realise, early exploration of quantum computing can provide valuable insights and better prepare your business for future opportunities. Regardless of the strategy you choose, maintaining a long-term perspective is crucial. The field of quantum computing is evolving rapidly, and the ability to adapt your approach as the technology develops will be vital for staying competitive.

Key takeaways

- **Quantum computing is a transformative technology that businesses should consider, even if its immediate relevance for them is not clear.**
- **Early exploration can provide valuable insights and prepare your business for future opportunities.**
- **The best quantum strategy depends on your company's R&D resources, innovation culture, industry, and risk tolerance.**
- **Strategic flexibility is vital - be ready to adapt as quantum computing develops.**
- **Exploring quantum computing now improves your ability to leverage new technologies in the future.**

> **"Very soon, if not already, we will be at a stage where quantum computing should be taken into account in all companies' long-term strategic scenario planning, but this, of course, requires a basic understanding of the subject also on the part of senior management."**

Jasmin Jutila, August Associates

9/ How can my company get started?

Quantum computing is emerging as a transformative technology with the potential to redefine industries. Raising awareness about quantum computing and making well-informed strategic decisions throughout the organisation is crucial to starting your quantum journey. Building a foundational understanding of quantum computing within teams—particularly in IT, R&D, and leadership—can demystify the technology and spark innovative thinking. Simple initiatives like knowledge-sharing sessions and pilot projects help align your organisation with quantum advancements.

Since no single organisation can master all aspects of quantum technology, partnerships with academic institutions, startups, and innovation hubs are essential. Collaborating within regional quantum networks and consortia accelerates learning and embeds your company in the growing quantum ecosystem. Starting small with proof-of-concept projects or quantum-inspired methods allows you to explore practical applications without requiring more advanced quantum hardware, providing valuable insights and preparing your teams for future breakthroughs.

For research-intensive organisations, investing in dedicated quantum teams or collaborating with academic institutions can help uncover tailored solutions. Pioneering companies demonstrate how early investments in quantum research drive innovation and establish leadership positions in their fields. Regardless of your current level of quantum expertise, recognising its transformative potential and fostering a flexible, long-term strategy ensures your organisation remains competitive in this rapidly evolving landscape.

- ✓ **Awareness and understanding**
- ✓ **External partnerships and networks**
- ✓ **Pilot projects**

This chapter provides practical examples and best practices to guide your company's first steps in exploring quantum computing and its potential applications, tailored to your specific needs and chosen strategy.

Spark curiosity and build understanding

Quantum computing is a unique technology that offers immense opportunities and presents specific business challenges. It is not solely the realm of physicists and computer scientists; a diverse group of individuals from various organisational functions and levels must be involved to harness its potential fully. Successfully navigating this journey requires fostering curiosity and building a foundational understanding across the organisation.

As quantum computing has the potential to change areas in a company, such as research and development, logistics, production planning, and financial analysis, it is crucial to engage different functions and areas of expertise. This collaboration will help identify both disruptive and efficiency-enhancing opportunities that quantum technology can provide.

This phase demands a strategic perspective, in-depth insights into current business processes, and a thorough understanding of quantum computing. From a practical standpoint, IT teams, for instance, should consider how "data readiness"—having clean, structured data—will be essential for future quantum applications. Early team awareness and engagement will establish a shared understanding of quantum's potential impact, enabling the organisation to make informed decisions when opportunities emerge. This requires a clear vision from leadership, guiding the organisation's exploration of quantum technologies and fostering a culture of innovation.

Quantum computing is a team sport

Collaboration across departments and functions is essential for understanding and harnessing the potential of quantum computing. Quantum computing fundamentally differs from classical computing, so fostering a shared understanding and learning together is an effective way to move forward. While only some need to understand the complexities of quantum computing, teams must gain insight into the projected timeline for quantum development and business and industry.

As noted earlier, misconceptions and unrealistic expectations about quantum computing are common. This collective learning approach helps inform team members and manage expectations, ensuring they engage with quantum opportunities based on realistic, well-rounded insights.

CASE: RAISING AWARENESS BY CO-LEARNING

At LähiTapiola, quantum awareness has been built by raising the observations of the FutureQ research project on the intranet blog. Raisa Peltoniemi says, "I have looked at the possible effects of quantum computing in general and how it could be utilised in projects already underway. Although quantum computing is still a developing technology, its potential should be considered now. I have also noticed that awareness of the value of data is increasing and understanding of the importance of data quality is deepening."

Shared sense-making is an essential way to understand the possibilities of quantum computing in the insurance industry. The potential of quantum computing in risk management, data analysis and optimisation of insurance processes has been highlighted. In addition, improving the accuracy of various scenarios and simulations can improve the prediction of losses and pricing accuracy in the future. Raisa Peltoniemi states: "I believe that the insurance industry will develop internally and externally with quantum computing and will offer its customers individual insurance products and services based on data in the future."

Building awareness in your organisation

To effectively build awareness of quantum computing within your organisation, consider the following practical approaches tailored to your chosen quantum strategy's specific needs and goals. Showcasing pilot projects through internal presentations demonstrates how emerging technologies can support business unit goals and provides concrete examples of quantum computing in action.

In addition to practical demonstrations, fostering a learning culture around quantum computing can be achieved through various initiatives. Appoint someone to share quantum insights on the company blog or through other internal communication channels to disseminate knowledge across teams.

Providing accessible learning resources is also crucial. Curate articles, videos[32], and online courses[33] that explain quantum computing in simple terms, making it easier for employees at all levels to understand the technology. Informal "Lunch-and-Learn" sessions can also be effective. These casual gatherings allow teams to learn about quantum concepts through relatable analogies and real-world examples, fostering engagement and understanding. By actively promoting knowledge sharing and providing learning opportunities, you can build the capabilities and nurture the talent needed to thrive in the quantum era.

Establishing external networks

External networks are as crucial as internal teams in the quantum journey. No single organisation can master all aspects of quantum technology, especially given its early stage of development. Collaboration with academic institutions, large companies, and startups is essential for accessing the latest innovations and expertise.

No dominant quantum design has yet to emerge, and various modalities (ways to build qubits) are competing, each with its ecosystem. Global players like IBM offer quantum computing through cloud services and innovation hubs, while some large companies and governments are investing in their own quantum computers. Meanwhile, distinct quantum ecosystems have formed around specific technologies and regional interests. These hubs facilitate peer learning within industries—such as pharmaceuticals—as well as regional quantum networks or groups of organisations exploring shared quantum interests.

For example, hubs like Finland's InstituteQ[34] and the Netherlands' Quantum Delta initiative[35] encourage collaboration among companies. Similarly, regional quantum umbrella organisations, like the European Quantum Industry Consortium (QuIC), aim to accelerate the commercialisation of quantum technology through partnerships that bring together research, adopters and technology providers. Open innovation initiatives and hackathons can also be valuable ways to explore new ideas and connect with potential collaborators.

CASE: BOOSTING QUANTUM COMPUTING ECOSYSTEM

Business Finland's quantum computing campaign is a prime example of how external networks can accelerate progress in quantum technologies. Events and workshops allow businesses to learn about quantum computing and connect with experts and peers. Additionally, companies can engage in hands-on experimentation by joining research consortia or initiating their own projects, supported by funding and collaboration opportunities.

Your preferred partners will depend on your chosen quantum strategy and existing resources. Consider talent availability now and in the future when deciding which capabilities to build internally versus accessing through your network. Remember that a diverse range of skills is needed, not just quantum algorithm developers. The European Quantum Flagship has developed a framework to assess different skill levels for various roles[36].

Gain practical experience

Starting small is essential for gaining practical experience with quantum computing[37]. Proof-of-concept projects allow organisations to explore specific use cases while learning the fundamentals of quantum computing. Since we are still in the early stages—unable to consistently outperform the best classical system—you can broaden your selection criteria beyond the most critical processes. For companies that lack internal quantum expertise, partnering with consultants, technology providers or research organisations can be helpful for pilot project design and implementation.

CASE: EXPLORING QUANTUM POTENTIAL IN CREDIT SCORING

OP Financial Group has been actively exploring the potential of quantum computing, recently investigating its application in credit risk management. In collaboration with universities, OP Lab examined whether quantum annealing could enhance feature selection in credit scoring models. The aim was to identify the most predictive variables from a large dataset to improve the accuracy of credit scoring. While current hardware limitations constrained the capacity of the quantum system, this research[38] highlighted the potential of quantum methods in finance. OP's proactive approach highlights financial institutions' experiments with quantum technology, setting the stage for future advancements.

Focusing on learning and experimentation often leads to valuable insights, even without directly applying quantum algorithms. For instance, many early projects that began by experimenting with quantum algorithms eventually discovered new quantum-inspired algorithms[39], which can be implemented effectively on classical computers. The concept of "dequantisation" is important for understanding the connection between quantum-inspired solutions and true quantum algorithms. Dequantisation aims to:

1. identify conditions under which quantum algorithms offer genuine speed-ups over classical approaches,

2. develop more effective quantum algorithms by understanding their foundational principles and

3. potentially create new classical algorithms by translating insights from quantum algorithms into a classical framework.

Initial experiments in quantum computing might benefit from exploring less obvious applications; an approach organisation may wish to consider sparking interest and build awareness. Such projects can help engage more individuals in identifying viable use cases and create a foundational understanding that equips leadership to make informed investment decisions for further exploration. For example, a pharmaceutical company focused on marketing in its pilot project, demonstrating quantum technology's broader potential[40]. Similarly, the Alliander Research Centre in the Netherlands chose a power grid optimisation project that was easily understood across the organisation, fostering engagement beyond technical teams[41].

From problem to quantum solution

To start experimenting quickly, pre-built quantum algorithm libraries and cloud-based quantum computing platforms[42] reduce the entry barriers, enabling companies to start small and learn progressively. However, quantum algorithms differ fundamentally from classical ones, and adapting business problems to quantum systems often requires specialised expertise. Most companies will need a partner who understands how to translate their problem into a quantum-suitable format.

The steps outlined below provide an overview of how companies can systematically explore quantum solutions, from identifying suitable use cases to implementing the final solution:

- Identify promising business problems
- Break down problems into manageable components and set clear goals
- Design a workflow that separates classical tasks from quantum tasks
- Develop a tailored quantum algorithm
- Evaluate algorithm speed and scalability advantage
- Evaluate quantum algorithms using quantum simulators or hardware
- Integrate the quantum and classical components into a cohesive solution and assess its impact

Research-based understanding and solutions

Many organisations adopt research-driven strategies as their entry point into the quantum field, particularly those with significant research resources.

One common strategy is to hire PhD students to investigate quantum topics that align with the company's objectives. This often involves partnerships enabling companies to incorporate quantum research findings, participate in academic conferences, and develop connections within the hardware and software ecosystems. In Sweden, the Wallenberg Centre for Quantum Technology (WACQT) facilitates collaborations between companies and PhD researchers, allowing exploration of industry-specific applications such as quantum noise radar for defence and quantum chemistry for drug discovery[43].

CASE: QUANTUM COMPUTING FOR ENERGY TRANSITION[44]

EDF (Electricité de France), an integrated energy company with a strong focus on R&D, has been proactively exploring quantum computing since 2018. With a dedicated team of 20 researchers and over 20 academic papers published, EDF combines a research-first approach with forward-looking considerations, such as integrating quantum technologies into future data centres. Their work addresses classical computing limitations in critical areas like material ageing under radiation and solving partial differential equations essential for infrastructure integrity.

EDF's early adoption of quantum computing has positioned the company to navigate fundamental algorithmic disruptions. They focus on mastering new algorithms tailored to energy management and materials research, emphasising open science and fostering innovation. Educating stakeholders about the realities of quantum progress and its potential impact is central to their strategy.

> **"The key thing was to build a skill set."**
> Stéphane Tanguy, EDF Lab

Collaboration is at the heart of EDF's approach. EDF's approach includes active participation in a dynamic ecosystem, working with partners like Pasqal, Eviden, Quandela, and IBM alongside academic institutions like Sorbonne University. As a QuaTERA (Quantum Technologies Energy Result Accelerator) member, EDF leverages high-performance computing (HPC) and quantum computing to advance sustainable energy solutions, demonstrating its commitment to driving both innovation and practical impact[45].

Another approach is to establish dedicated quantum teams. For example, Deutsche Bahn has a quantum team that explores quantum applications and cybersecurity implications[46]. Similarly, financial institutions like Erste Bank, Intesa Sanpaolo, and J.P. Morgan have formed quantum teams to investigate relevant use cases, ranging from optimisation algorithms to risk assessment tools[47]. Among the crucial aims of all these efforts, including establishing a dedicated quantum computing research group, is to build capability for when quantum computing delivers significant practical benefits.

Building a future-proof organisation

Regardless of your chosen quantum computing strategy, recognising this emerging technology as a potential future opportunity or risk is crucial. Understanding quantum computing's fundamentals is essential, even if it does not immediately influence your roadmap, given its potential to transform businesses. Recognising quantum computing and initiating internal discussions about its implications can spark valuable future-oriented thinking within your organisation, preparing you for transformative shifts before they happen.

Extending these sense-making discussions and experiments beyond your company's boundaries positions you as part of a broader ecosystem and network. Engaging with external partners—such as universities, research consortia, or industry groups—enables you to share expertise and harness collective strengths, which are vital for unlocking quantum computing's full potential.

While this book has primarily highlighted opportunities, Chapter 7 addressed risks that cannot be ignored. Even if your primary motivation for exploring quantum technologies is risk assessment, we strongly encourage you also to consider the potential benefits. As illustrated in the future radars in Chapter 5, the same trends can appear as risks for some and opportunities for others—particularly for early adopters who are prepared to act. By proactively engaging with quantum computing, your organisation can safeguard its future and lead in shaping the next wave of transformative innovation.

Endnotes

1 Recent reports, e.g. McKinsey, 2021 & 2024; Deloitte, 2024; Capgemini Research Institute, 2022; & Yole, 2024.

2 Using quantum computing as an example, researchers (Hilkamo et al., 2021) demonstrate through inductive analysis how consultants act as active intermediaries and create nascent market

3 e.g. IBM's quantum utility (IBM Quantum Research Blog, 2023), Pasqal's business utility (Pasqal Blog, 2024), and Google's quantum supremacy (Arute et al., 2019)

4 The book is based on the FutureQ research project, "Towards shaping the future sustainable markets of quantum computing: Needs, barriers, drivers, and beliefs of beneficiaries."

5 D-Wave What is Quantum Annealing? - YouTube

6 adapted from Ezratty (2024, p. 261).

7 IBM Technology roadmaps

8 X Prize Guidelines, 2024

9 Bandic et al., 2022

10 For a comprehensive overview of the development of quantum technology, Olivier Ezratty maintains a yearly updated online resource

11 Kothari, 2020

12 Ewin Tang, a computer scientist and PhD student, developed a classical alternative to a QML algorithm that was believed to offer exponential speedup, proving it could be done with classical methods (Davis, 2023)

13 IBM Research Blog, 2023

14 Chen, 2023

15 e.g. a record of +1000. 24.10.2023. (Wilkins, 2023)

16 Adapted from Ezratty, 2024

17 Phalak et al., 2023

18 Reports with use cases in the financial services sector, e.g. Deloitte, 2024 and IBM Institute for Business Value, 2019, and scientific papers discussing these, e.g. Orús et al., 2019b and Egger et al., 2020

19 review of potential quantum machine learning applications Doosti et al., 2024

20 e.g. Herman et al., 2023 summarise financial applications of quantum computing

21 International Monetary Fund, 2022

22 more about supply chain finance, e.g. Griffin and Sampat, 2021

23 about insurance risk assessment, e.g. Bramblet, 2022

24 Research relating to forecasting financial crashes, e.g. Orús et al., 2019a

25 For instance, at the Q2B Paris 2024 event, speakers from AstraZeneca, Merck, and Amgen highlighted the importance of building ecosystems, collaborating with startups, and developing expertise, including through targeted recruitment. Several pharmaceutical companies have also partnered with quantum hardware firms, including Bayer and Google, Boehringer Ingelheim and Google, as well as Moderna and IBM. One notable initiative in the field is the Novo Nordisk Foundation's long-term Quantum Computing Programme.

26 e.g. Finnish Algorithmiq is a research-based start-up developing algorithms for life sciences and chemistry (Rajah, 2023), French Qubit Pharmaceuticals in collaboration with Pasqal has developed a hybrid approach for protein hydration (Pasqal Blog, 2023), and Danish Kvantify accelerates hit identification while advancing quantum readiness (Kvantify, 2024)

27 China leads the pharmaceutical sector R&D, accounting for 33% of global patent filings (Pharmaceutical Technology, 2024) and producing 44% of the world's APIs (active pharmaceutical ingredients) (Statista, 2023). China invests twice as much in quantum technologies as all EU countries combined and holds around half of global quantum technology patents, including in quantum computing (Statista, 2023)

28 H.R.7535, 2022

29 European Commission, 2024

30 More about quantum cybersecurity e.g. WEF, 2023; Mosca & Piani, 2023; NIST Post-quantum cryptography

31 Prabhakar, 2024

32 YouTube provides a wealth of material on quantum computing, including CERN Lectures. A practical introduction to quantum computing

33 University of Jyväskylä provides the course The ABCs of Quantum Computing, and other online courses you can find from MOOC platforms such as Coursera, EDX, and FutureLearn, MIT is one of the few to offer courses targeted at business leaders

34 The Finnish Quantum Institute – InstituteQ

35 The Netherlands' quantum ecosystem – Quantum Delta NL

36 Quantum Flagship, 2024

37 A variety of online resources offer introductions to quantum programming e.g. Pennylane Codebook, IBM's Qiskit, Google's Cirq, and Quantum Algorithm Zoo.

38 Liimatta et al., 2024

39 e.g. BosonQ Psi, 2024

40 Fachot & Cimino, 2024

41 Nas, 2024

42 Quantum computing cloud services include IBM Quantum, Amazon Braket, and Microsoft Azure Quantum. European machines are accessible via providers such as IQM, IBM, and OVHcloud.

43 Wallenberg Center for Quantum Technology - WACQT

44 Case is based on Tanguy's (2024) presentation and Dargan's (2024) article

45 Swayne, 2022

46 Rieck, 2024

47 Erste Bank has an 8-person QuanTeam (Fratini, 2024), and Intesa Sanpaolo has its own Quantum Competence Center (Corbelletto, 2024), both exploring banking use cases and utilising real data to assess when quantum computing will deliver business value.

Acknowledgements

The insights in this book come from the FutureQ project, “Towards shaping the future sustainable markets of quantum computing: Needs, barriers, drivers, and beliefs of beneficiaries.” Together with participating companies and experts, we used foresight methods to explore the future evolution and influence of quantum computing.

We thank Business Finland for funding this project and allowing us to investigate this transformative field. Special thanks go to FutureQ project steering group: Outi Keski-Äijö (Business Finland), Mika Niskanen (Business Finland), Katja Taipalus (Bank of Finland), Jussi Hyvärinen (Metsä Group), Jasmin Jutila (August Associates), Heikki Lassila (LähiTapiola), Nadia Tamminen (Pharma Industry Finland), Topias Uotila (Unitary Zero Space), Petri Liimatta (OP), and Katri Valkokari (VTT) for their collaboration and expertise.

We appreciate all participants in the foresight workshops, especially those from the pharmaceutical, financial services, and manufacturing sectors and companies developing quantum computing applications. Their insights greatly enriched our understanding. We also thank the individuals we interviewed for their reflections on quantum computing and its future impact.

We acknowledge the key contributions of our VTT colleagues: Jutta Suksi, who brought essential regulatory expertise to the horizon scanning phase, and Katri Valkokari, whose support throughout all stages of the writing process and insightful comments helped refine the manuscript to address the target audience better. Additionally, we extend our gratitude to Topias Uotila and Petri Liimatta for their instrumental roles in achieving the project’s outcomes and for providing valuable feedback during the manuscript phase.

We also appreciate the Business Finland Quantum Programme and Finnish Quantum Flagship participants for their insights, especially those who provided feedback on the draft guidebook: Valter Uotila (University of Helsinki), Jorma Kilpi (VTT), Mikael Johansson (CSC), Jukka K. Nurminen (University of Helsinki), and Matti Palomäki (VTT).

We also wish to thank the researchers at TNO Vector, particularly Julian Rabbie, Amber Geurts, and Hugo Gelevert, as well as other actors within the Dutch quantum ecosystem. We are also grateful to everyone we have spoken with at international conferences and events about quantum computing's future possibilities. These discussions have deepened our understanding of the field's current landscape and future opportunities.

Finally, we extend special thanks to our VTT colleagues who, at various stages of the project, helped us understand the future potential of quantum computing. Their expertise and insights have been invaluable: Pekka Pursula, Pauli Komonen, Matthias Deschryvere, Kalle Kantola, Johanna Anteroinen, and Piia Konstari.

Thank you all for your support, contributions, and trust as we explore the future possibilities and challenges of quantum computing. This work exemplifies the power of collaboration and shared curiosity.

References and literature

Aaronson, S. (2024). Quantum computing: Between hope and hype.

Aaronson, S. (2008). The limits of quantum computers. Scientific American. March. pp. 62–69.

Abbas, A., Ambainis, A., Augustino, B., Bärtschi, A., Buhrman, H., Coffrin, C., Cortiana, G., Dunjko, V., Egger, D. J., Elmegreen, B. G., Franco, N., Fratini, F., Fuller, B., Gacon, J., Gonciulea, C., Gribling, S., Gupta, S., Hadfield, S., Heese, R., . . . Zoufal, C. (2023). Challenges and Opportunities in Quantum Optimization. ArXiv.

Abbot, J. (2022). Future-proofed. The journey toward quantum-safe security. Vanguard report.

Accenture. (2017). Think beyond ones and zeros. Quantum computing. Now.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., . . . Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510.

Auer, R., Dupont, A., Gambacorta, L., Suk Park, J., Takahashi, K., & Valko, A. (2024). Quantum computing and the financial system: opportunities and risks. BIS Papers 149.

Ball, H., Biercuk, M. J., & Hush, M. R. (2021). Quantum firmware and the quantum computing stack? Physics Today. 74(3), 28–34.

Bandic, M., Feld, S., & Almudever, C. G. (2022) Full-stack quantum computing systems in the NISQ era: algorithm-driven and hardware aware compilation techniques

Bauer, B., Bravyi, S., Motta, M., & Chan, G. K. (2020). Quantum algorithms for quantum chemistry and quantum materials science. *ArXiv*.

BCC Research. (2023). Quantum computing: Technologies and global markets to 2028.

BCG. (2024). The Long-term forecast for quantum computing still looks bright.

BCG. (2023). Quantum computing is becoming business ready.

Berger, C., Di Paolo, A., Forrest, T., Hadfield, S., Sawaya, N., Stęchły, M., & Thibault, K. (2021). Quantum technologies for climate change: Preliminary assessment. ArXiv.

Blunt, N.S., Camps, J., Crawford, O., Izsák, R., Leontica, S., Mirani, A., Moylett, A.E., Scivier, S.A., Sunderhauf, C., Schopf, P., & Taylor, J.M. (2022). Perspective on the current state-of-the-art of quantum computing for drug discovery applications. Journal of Chemical Theory and Computation, 18(12), 7001-7023.

BosonQ Psi. (2024). Quantum-inspired evolutionary algorithms: Revolutionizing optimization in engineering.

Bramlet, J. (2022). What quantum computing means for insurance. Accenture Insurance Blog.

Brandas, C., Cosmin, E., Didraga, O., & Albu, A. (2024). Enhancing the Financial Sector with Quantum Computing: A Comprehensive Review of Current and Future Applications. In: Ciurea, C., Pocatilu, P., Filip, F.G. (eds) Proceedings of 22nd International Conference on Informatics in Economy (IE 2023). 367. Springer, Singapore.

Capgemini Research Institute. (2022). Quantum technologies: How to prepare you organization for a quantum advantage now.

CEA. (2024). Quantum 2042. Prospective study on the impacts of quantum computing in 2042.

Chan, G. K. (2024). Quantum chemistry, classical heuristics, and quantum advantage. *ArXiv*.

Chen, S. (2023). Are quantum computers really energy efficient? Nature Computational Science, 3, 457–460.

Childs, A. M., Maslov, D., Nam, Y., Ross, N. J., & Su, Y. (2018). Toward the first quantum simulation with quantum speedup. Proceedings of the National Academy of Sciences, 115(38), 9456-9461.

Choi, C. Q. (2021). Quantum computing makes inroads towards pharma. Pharma giants and computing titans increasingly partnering on quantum computing. IEEE Spectrum.

Choi, S., Moses, W. S., & Thompson, N. (2023). The quantum tortoise and the classical hare: A simple framework for understanding which problems quantum computing will accelerate (and which it will not). *ArXiv*.

Cooper, P., Ernst, P., Kiewell, D., & Pinner, D. (2022). Quantum computing just might save the planet. McKinsey Digital.

Corbelletto, D. (2024). The Intesa Sanpaolo journey towards quantum. Presentation at Q2B 2024. Paris. 8.3.2024.

Daley, A. J., Bloch, I., Kokail, C., Flannigan, S., Pearson, N., Troyer, M., & Zoller, P. (2022). Practical quantum advantage in quantum simulation. Nature, 607(7920), 667-676.

Dalzell, A. M., McArdle, S., Berta, M., Bienias, P., Chen, C., Gilyén, A., Hann, C. T., Kastoryano, M. J., Khabiboulline, E. T., Kubica, A., Salton, G., Wang, S., & Brandão, F. G. (2023). Quantum algorithms: A survey of applications and end-to-end complexities. ArXiv.

Dargan, J. (2024) EDF CTO Stéphane Tanguy discusses quantum computing for energy transition. Quantum Insider.

Davis, R. (2023). How Ewin Tang's dequantized algorithms are helping quantum algorithm researchers. Qiskit.

De Wolf, R. (2017). The potential impact of quantum computers on society. Ethics and Information Technology, 19, 271-276.

Deloitte. (2024). Financial services industry market research: Market analysis of quantum computing use cases.

Doga, H., Sahin, M.E., Bettencourt-Silva, J., Pham, A., Kim, E., Andress, A., Saxena, S., Bose, A., Parida, L., Robertus, J.L., & Kawaguchi, H., 2024. Towards quantum computing for clinical trial design and optimization: A perspective on new opportunities and challenges. arXiv

Doosti, M., Wallden, P., Hamill, C.B., Hankache, R., Brown, O.T., & Heunen, C. (2024). A brief review of quantum machine learning for financial services. arXiv

Egger, D.J., Gambella, C., Marecek, J., McFaddin, S., Mevissen, M., Raymond, R., Simonetto, A., Woerner, S. and Yndurain, E. (2020). Quantum computing for finance: State-of-the-art and future prospects. IEEE Transactions on Quantum Engineering, 1, 1-24.

European Commission. (2024). Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

Evers, M., Heid, A., & Ostojic, I. (2021). Pharma's digital RX: Quantum computing in drug research and development. McKinsey.

Ezratty, O. (2024). Understanding quantum technologies. 7th ed.

Fachot, E., & Cimino, X. (2024). Quantum annealing and quantum-inspired solutions for resource allocation within the pharma industry. Presentation at Q2B 2024. Paris. 8.3.2024.

Ferrie, C. (2024). What you shouldn't know about quantum computers. *ArXiv*.

Flöther, F.F., (2023). The state of quantum computing applications in health and medicine. Research Directions: Quantum Technologies. 1(10), 1–10

Fratini, F. (2024). Erste Group Bank quantum prototypes. Presentation at Q2B 2024. Paris. 8.3.2024.

Google. Quantum AI.

Google AI. Our focused and responsible approach to quantum computing.

Graps, A. (2024). The Many faces of hybrid classical – quantum computing – Part 1. GQI Quantum Computing Report.

Griffin, P. & Sampat, R. (2021). Quantum computing for supply chain finance. 2021 IEEE International Conference on Services Computing (SCC), Chicago, IL, USA, 456-459.

Gunashekar, S., d'Angelo, C., Flanagan, I., Motsi-Omoijiade, D., Virdee, M., Feijao, C., & Porter, S. (2022). Using quantum computers and simulators in the life sciences: Current trends and future prospects. RAND Corporation.

Heidari, N., Olgiati, S., Meloni, D., Pirovano, F., Noorani, A., Slevin, M. and Azamfirei, L., 2021. A quantum-enhanced precision medicine application to support data-driven clinical decisions for the personalized treatment of advanced knee osteoarthritis: development and preliminary validation of precisionKNEE_QNN. medRxiv, pp.2021-12.

Herman, D., Googin, C., Liu, X., Sun, Y., Galda, A., Safro, I., Pistoia, M. & Alexeev, Y. (2023). Quantum computing for finance. Nature Reviews Physics, *5*(8), 450-465.

Hilkamo, O., Barbe, A. S., Granqvist, N., & Geurts, A. (2021). Temporal work by consultants in nascent market categories: constructing a market for knowledge in quantum computing. Technology Analysis & Strategic Management, 33(11), 1303–1316.)

H.R.7535. (2022). Quantum Computing Cybersecurity Preparedness Act, 117th Cong.

IBM. Qiskit.

IBM Institute for Business Value. (2023). The quantum decade. A playbook for achieving awareness, readiness, and advantage. 4th ed.

IBM Institute for Business Value. (2019). Exploring quantum computing use cases for financial services. Expert Insight.

IBM News. (2023). Moderna and IBM to explore quantum computing and generative AI for mRNA science.

IBM Technology Roadmaps. (2024). Quantum roadmap.

IBM Quantum Research Blog. (2023). What is quantum utility?

International monetary fund. (2022). BigTech in financial services: Regulatory approaches and architecture. Fintech Notes.

Koen Groenland. 2024. Introduction to quantum computing for business.

Kothari, R. (2020). Quantum speedups for unstructured problems: Solving two twenty-year-old problems. Microsoft Research Blog.

Kvantify. 2024. Kvantify launches first product to revolutionize drug discovery.

Langione, M., Bobier, J-F., Meier, C., Hasenfuss, S., & Schilze, U. (2019). Will quantum computing transform biopharma R&D? BCG.

Leijnse, K. (2024). Photocatalysis for water splitting. Quantum Application Lab.

Liimatta, P., Taipale, P., Halunen, K., Heinosaari, T., Mikkonen, T., & Stirbu, V. (2024). Research Versus Practice in Quantum Software Engineering: Experiences from Credit Scoring Use Case. In IEEE Software, 41 (6), 9–16). IEEE.

Liu, H., Low, G. H., Steiger, D. S., Häner, T., Reiher, M., & Troyer, M. (2022). Prospects of quantum computing for molecular sciences. Materials Theory, 6(1), 1-17.

Maheshwari, D., Garcia-Zapirain, D. & Sierra-Sosa, D. (2022). Quantum machine learning applications in the biomedical domain: A systematic review. IEEE Access, 10, 80463-80484

Matsuura, A., Johri, S. & Hogaboam, J. (2019). A systems perspective of quantum computing. Physics Today, 72(3), 40-46.

Mazzola, G. (2024). Quantum computing for chemistry and physics applications from a Monte Carlo perspective. The Journal of Chemical Physics, 160(1).

McKinsey. (2024). Quantum technology monitor.

McKinsey. (2021). Quantum computing: An emerging ecosystem and industry cases.

Meige, A., Eagar, R, & Arribart, H. (2023). Quantum summer or winter? Arthur D. Little. Brue Shift report.

Meige, A., Könnecke, L., & Eagar, R. (2022). Unleashing the business potential of quantum computing. Arthur D. Little. Brue Shift report.

Montanaro, A. (2016). Quantum algorithms: An overview. Npj Quantum Information, 2(1), 1-8.

Mosca, M., & Piani, M. (2023). Quantum threat timeline report 2023. GRI.

Nas, D. Societal impact of quantum technologies. Keynote at QuTech – Quantum computing for industry and public sector. Delft.17.10.2024.

National Academies of Sciences, Engineering, and Medicine. (2019). Quantum computing: Progress and prospects. Washington, DC: The National Academies Press.

Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press.

NIST. (2024). NIST releases first 3 finalized post-quantum encryption standards.

Nuutinen, M., Apilo, T. & Wallin, A. (2023). Turning emerging technology towards innovations in ecosystems - quantum computing case. Proceedings of 24th CINet Conference 17th-19th September 2023. Continuous Innovation Network (CINet).

Orús, R., Mugel, S. & Lizaso, E. (2019a). Forecasting financial crashes with quantum computing. Physical Review A, 99(6), p.060301.

Orús, R., Mugel, S., & Lizaso, E. (2019b). Quantum computing for finance: Overview and prospects. Reviews in Physics, 4, 100028.

Pakin, S., & Coles, P. (2019). The problem with quantum computers. Scientific American.

Pasqal Blog. (2024). Pasqal announces new roadmap focused on business utility and scaling beyond 1,000 qubits towards fault tolerance era.

Pasqal Blog. (2023) Quantum algorithm can help drug discovery.

Peral-García, D., Cruz-Benito, J. and García-Peñalvo, F.J. (2024). Systematic literature review: Quantum machine learning and its applications. Computer Science Review, 51,100619.

Phalak, K., Chatterjee, A., & Ghosh, S. (2023). Quantum random access memory for dummies. *ArXiv*.

Pharmaceutical Technology. (2024). Q3 2024 update: patent activity in the pharmaceutical industry.

Potter, K. & Stilinski, D. (2024). Quantum Machine Learning: Exploring the Potential of Quantum Computing for AI Applications.

Prabhakar, A. (2024). Getting ready for Quantum in AI-first world – the role of different ecosystem players. Keynote speech at Quantum.Tech USA 2024, Washington. 24.4.2024.

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum 2, 79.

Puhakainen, P. (2023). 7 steps to quantum secure cryptography – the transition must start now. VTT Blog.

Quantum Computing Report. (2024). NISQ Versus FTQC in the 2025 – 2029 Timeframe. GQI.

Quantum Delta. (2023). Exploratory quantum technology assessment. Centre for Quantum and Society.

Quantum Flagship. 2024. European Competence Framework for Quantum Technologies. v.2.5.

Quera. (2023). Understanding fault-tolerant quantum computing.

Rajah, P. (2023). Seven observations about how Algorithmiq is bringing quantum algorithms to life. Quantum Life Science Blog.

Rieck, M. (2024). An update on Deutsche Bahn's quantum security strategies. Presentation at Quantum Tech 2024 USA. Washington.

Ruane, J., McAfee, A., & Oliver, W. D. (2022). Quantum Computing for Business Leaders. Will the reality live up to the hype? Harward Business Review.

Santagati, R., Babbush, R., Degroote, M., González, L., Kyoseva, E., Moll, N., Oppel, M., Parrish, R. M., Rubin, N. C., Streif, M., Tautermann, C. S., Weiss, H., & Wiebe, N. (2024). Drug design on quantum computers. Nature Physics, 20(4), 549-557.

Schetakis, N., Aghamalyan, D., Boguslavsky, M., Rees, A., Rakotomalala, M. and Griffin, P.R. (2024). Quantum machine learning for credit scoring. Mathematics, 12(9), p.1391.

Scholten, T. L., Williams, C. J., Moody, D., Mosca, M., Hurley, W., Zeng, W. J., Troyer, M., & Gambetta, J. M. (2024). Assessing the benefits and risks of quantum computers. ArXiv.

Soller, H. Hijazi, H., Gschwendtner, M., & Taibah, R. (2024). Enabling the next frontier of quantum computing. McKinsey Digital.

Swayne, M. (2022). EDF, Exaion Inc., PASQAL and the Quantum Innovation Zone bring high-performance computing and quantum technologies to the forefront of energy solutions. Quantum Insider.

Tanguy, S. (2024). Quantum computing for the electric grid. Key learning from a quantum early adopter. Keynote presentation at Q2B Paris 2024.

Taylor, P. (2023). Bayer taps Google's quantum power for drug discovery. Pharmaphorum.

TNO. (2023). The PQC migration handbook. Guidelines for migrating to post-quantum cryptography.

Troyer, M., Benjamin, E. V., & Gevorkian, A. (2024). Quantum for good and the societal impact of quantum computing. ArXiv.

Ukpabi, D., Karjaluoto, H., Bötticher, A., Nikiforova, A., Petrescu, D., Schindler, P., Valtenbergs, V., & Lehmann, L. (2023). Framework for understanding quantum computing use cases from a multidisciplinary perspective and future research directions. Futures, 154, 103277.

von Burg, V., Low, G.H., Häner, T., Steiger, D.S., Reiher, M., Roetteler, M. & Troyer, M. (2021). Quantum computing enhanced computational catalysis. Physical Review Research, 3(3), p.033055.

WEF. (2023). Quantum readiness toolkit: Building a quantum-secure economy.

Wilkins, A. (2023). Record-breaking quantum computer has more than 1000 qubits. New Scientist.

X Prize Guidelines. (2024). Quantum for Real World Impact.

Yole. (2024). Market and technology trends: Quantum technologies 2024

Writers

Dr. **Arto Wallin**, Senior Scientist at VTT, specialises in corporate foresight and guiding companies in leveraging emerging technologies for renewal. With a focus on quantum computing, he helps businesses navigate its complexities to prepare for transformative opportunities and disruptions in the evolving business landscape.

Dr. **Tiina Apilo** is a Senior Scientist at VTT, with expertise in corporate foresight, innovation ecosystems, and leveraging emerging technologies to create business opportunities. She is particularly interested in understanding how quantum computing could transform business environments across industries and exploring the broader societal impacts it may hold for the future.

Olli Nurmi is a Principal Scientist in Quantum Algorithms and software team with expertise in quantum computing applications. He is interested in industrial relevant applications of machine learning, computational chemistry and optimisation using both classical and quantum computing resources.

Dr. **Maaria Nuutinen** is a psychologist and Senior Principal Scientist at VTT. She has robust expertise in human-centred design, innovation practices, corporate foresight, social sustainability, and business transformation. Dr. Nuutinen is particularly enthusiastic about helping companies incorporate quantum computing into their long-term strategies.

Dr. **Ville Kotovirta** led the Quantum Algorithms and Software team at VTT while contributing to this book. Currently, he is the Co-Founder and CTO at QMill. He focuses on early-stage quantum algorithms, bridging the gap between emerging quantum technologies and practical applications.

10/ When is the best time to start?

The answer is to
start now.

Wallin, A., Apilo, T., Nurmi, O., Nuutinen, M., & Kotovirta, V. (2024).
Quantum computing: Practical guide to navigating the future. VTT
ISBN: 978-951-38-8839-8
DOI: 10.32040/2024.978-951-38-8839-8

Get in touch with us:
name.surname@vtt.fi