Citi GPS

QUANTUM COMPUTING

Moving Quickly From Theory to Reality

Citi GPS: Global Perspectives & Solutions

July 2023

Authors

Tahmid Quddus Islam
Analytical Insights Team
Citi Global Insights

+44-20-7986-3503 |
tahmid.quddus.islam@citi.com

Robert Garlick
Head of Innovation, Technology, and the Future of Work
Citi Global Insights

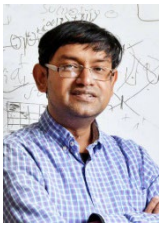
+44-20-7986-3547 |
robert.j.garlick@citi.com

Wenyan Fei
Analytical Insights Team
Citi Global Insights

+44-20-7986-3543 |
wenyan.fei@citi.com

Professor Deeph Chana
Chair of the NATO Advisory Group on Emerging and Disruptive Technologies

Dr. Stefano Gogioso
Computer Scientist & Researcher in Quantum Computing
Oxford University



Professor Sougato Bose
Physicist and Researcher in Quantum Computation
University College London

Sean Kornish
Chair
Citi Cryptography Security Center of Excellence

sean.kornish@citi.com

David W. Edelman
Co-chair
Citi Cryptography Security Center of Excellence

david.w.edelman@citi.com

Anuj Gangahar
Analytical Insights Team
Citi Global Insights

anuj.gangahar@citi.com

Helen H. Krause, CFA
Head of Data Science Insights
Citi Global Data Insights

+44-20-7986-8653 |
helen.krause@citi.com

Yehuda Dayan
Data Scientist
Citi Global Insights

+44-20-7986-5502 |
yehuda.dayan@citi.com

Devon Stone
Data Scientist
Citi Global Insights

+44-20-7986-8691 |
devon.stone@citi.com

Ronit Ghose, CFA
Head of Future of Finance
Citi Global Insights

ronit.ghose@citi.com

Kaiwan Master
Future of Finance Analyst
Citi Global Insights

kaiwan.hoshang.master@citi.com

Atif Malik
Semiconductor Cap Equipment & Specialty Semiconductor Analyst
Citi Research

+1-415-951-1892 |
atif.malik@citi.com

Ronald Josey
U.S. Internet Analyst
Citi Research

+1-212-816-4545 |
ronald.josey@citi.com

Carol Gibson
Analytical Insights Team
Citi Global Insights

+44-20-7986-4137 |
carol.gibson@citi.com

QUANTUM COMPUTING

Moving Quickly From Theory to Reality

Kathleen Boyle, CFA
Managing Editor, Citi GPS

Technology advances seem to be dominating the headlines. There are new ways to search the web using artificial intelligence and machine learning, alternate payment systems using blockchain and digital currency, and innovative ways to socialize gaming, and shop using the metaverse. In most cases, the advances have been facilitated by increasing computing speeds that enable faster calculations as well as better connectivity, but all are based on existing computing technology.

But that is all about to change. The next phase of computing — quantum computing — is getting close to moving from being theoretical to practical, and we are quickly coming to a point where quantum computers will be able to perform tasks faster, more efficiently, and cheaper than classical computers. Quantum computing breaks away from traditional classical computing using quantum mechanics as a base. If you made it through physics class in high school or college, you might remember that quantum mechanics as a daunting concept associated with geniuses like Albert Einstein, Niels Bohr and Max Planck. But you don't have to be a rocket scientist to start thinking about how quantum computing can revolutionize industry and society. And given the speed that quantum computing is progressing, we believe now is the time to for nation-states, corporates, and market participants to start getting ready for its arrival.

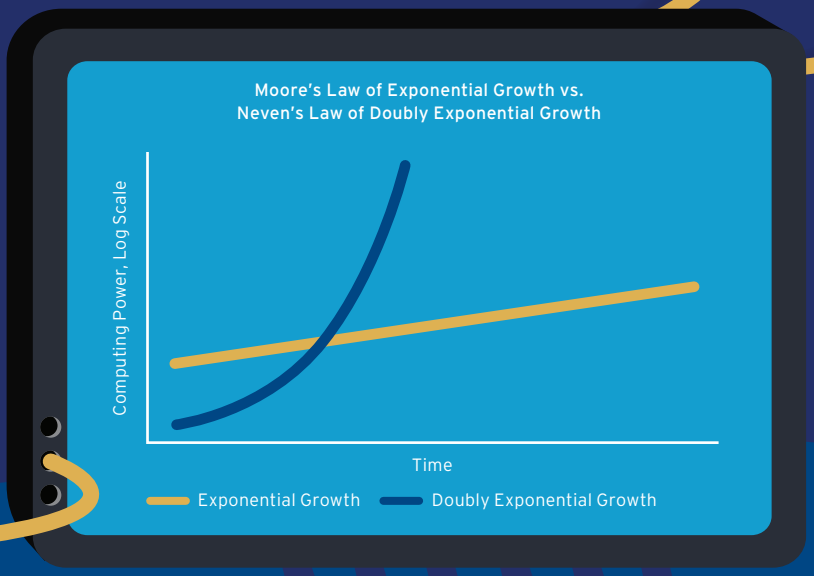
In the report that follows, we look at what quantum computing is and what its advantages are compared with classical computing in terms of optimization, machine learning, simulation, and cryptography. We then apply those advantages to specific industries to highlight areas where quantum computing can materially advance processes from logistics and drug discovery to portfolio optimization and cybersecurity.

Most importantly, we set out steps that nation-states and corporates can begin implementing in preparation for the arrival of quantum computing. Setting up appropriate funding to encourage research and development is important on a national scale, as is ensuring education and training to avoid a talent skills gap. Corporates need to improve their awareness of how quantum computing will affect their industry, create impact assessments, and contextualize opportunities.

THE QUANTUM COMPUTING OPPORTUNITY

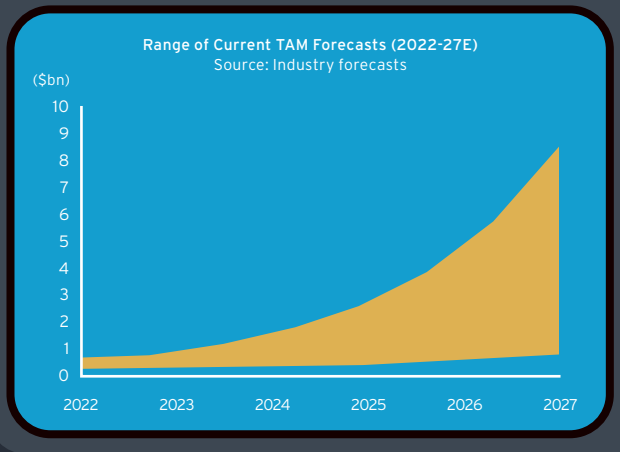
WHY QUANTUM COMPUTING IS A BIG DEAL

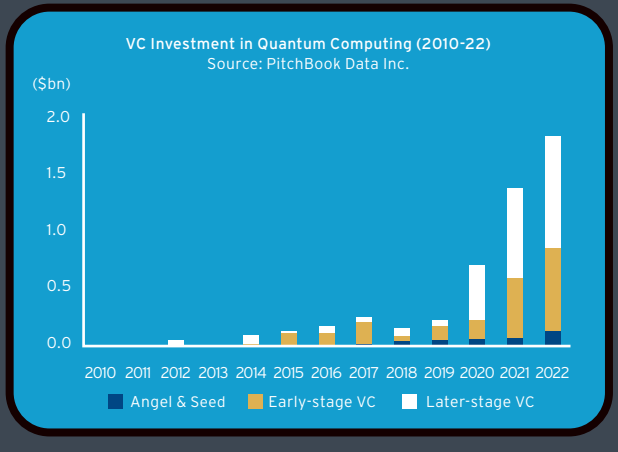
Computing is at an inflection point. After five decades of increasing computational power by Moore's Law (i.e., doubling the number of transistors per chip every 2 years), the growth rate of classical computing is reaching its physical limit. At the same time, the capabilities of quantum computers (QCs) are advancing at a "doubly exponential" rate – in line with Neven's Law – and are close to generating commercial value.

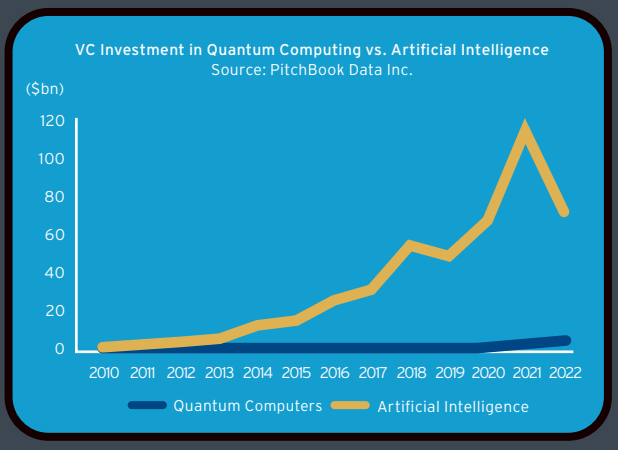


HOW BIG COULD QUANTUM COMPUTING BECOME?

Total addressable market (TAM) estimates for quantum computing vary widely – ranging in 2027 from $700 million to $8.6 billion. Venture capital investment in the QC space has been strong but still pales in comparison to investment in artificial intelligence (AI).







HOW WILL QUANTUM COMPUTING DISRUPT INDUSTRY?

Quantum computers will likely solve practical problems faster, cheaper, or more efficiently, than classical computers in four broad areas – optimization, machine learning, simulations, and cryptography. Three of these attributes offer significant upside for numerous industries, including Manufacturing & Logistics, Artificial Intelligence, Healthcare, Energy & Climate, and Finance. However, with cryptography, QCs pose a potential threat to existing cryptographic standards that underpin computer systems and cryptocurrencies.

MANUFACTURING AND LOGISTICS

- Transition to Industry 5.0
- Advanced materials discovery
- Enhanced digital twin processes
- Logistics optimization

ARTIFICIAL INTELLIGENCE

- Enhanced natural language processing
- Artificial neural networking

ENERGY AND CLIMATE

- Improved crude refinery processes
- Economically viable green hydrogen
- Accelerated battery technology development
- Ammonia synthetization
- New catalysts for carbon capture

FINANCE

- More personalized services
- Enhanced portfolio optimization
- Improved risk management/ fraud detection

HEALTHCARE

- Expedited drug discovery and delivery
- Improved diagnoses
- Tailored treatments
- Better insurance risk assessment/fraud detection

PREPARING FOR QUANTUM

Due to the exponential scaling power of quantum computers, by the time they offer a practical advantage to business, the gap between early adopters and those using only classical computing will widen at an increasingly accelerated pace. Now is the time to prepare for the transition to capitalize on opportunities and safeguard against risk. To take advantage of the opportunity...

GOVERNMENTS SHOULD:

- Establish a holistic quantum policy
- Invest in quantum infrastructure
- Upskill workforce
- Develop international strategic initiatives
- Consider future ethical concerns

CORPORATES SHOULD:

- Build quantum awareness
- Develop preparedness
- Position yourself for quantum advantage through investigation and technology investment
- Understand and develop an enterprise approach to cryptography modernization and agility

Contents

Executive Summary

"Never mind AI (artificial intelligence) — quantum computing is the next big thing," said Martha Lane Fox, president of the British Chambers of Commerce, in June 2023.[1] While this is up for debate as we marvel at the innovation taking place currently in AI, quantum computing may become the defining technology of the 2020s. We believe quantum computing will radically change the way things are done and commercial advantages to business will arrive sooner than many expect. Both nation-states and corporates need to prepare. We hope this report helps raise awareness and preparation as we move into an era of quantum computing.

State of the Quantum Computing Industry

Moore's Law, the observation that transistor density in integrated circuits tends to double every 18-24 months, has driven huge progression in computing but is slowing down. The next leap for computing is quantum. Rather than the linear scaling capabilities of our current computers (otherwise known as "classical computers"), quantum computers (QCs), by their nature, scale exponentially.

Many believe we have already passed the point of "quantum supremacy," the point at which we can perform tasks with QCs beyond the capabilities of classical computers. The next major milestone in the development of QCs is that of "commercial quantum advantage" — i.e., the phase where QCs can solve practical problems faster, more cheaply, or more efficiently than classical computers — and is something most companies feel will come around the middle to the end of this decade. While progress announced by IBM in June 2023 has increased optimism, commercial quantum advantage will materialize at different times in different use cases — and in distinctly granular ways.[2] After the point of commercial quantum advantage, we will have leapt into what many will consider the next stage of computing.

QCs process information by harnessing the principles of quantum mechanics — the laws that govern the behavior of atoms and photons. The basic building block of a QC is a quantum bit or "qubit." Qubits can simulate their classical counterparts — occupying a state of either 0 or 1 — but can also be in a combination of both states at the same time through the quantum mechanical property of "superposition." Furthermore, due to the process of quantum entanglement, every additional qubit doubles the number of potential states a QC can be in. In 2019, the Director of Google's Quantum Artificial Intelligence Lab, Hartmut Neven, noted at a conference that QCs were gaining computational power relative to classical ones at a "doubly exponential" rate. His observation was eventually dubbed "Neven's Law." He went on to describe the rate of progress as "It looks like nothing is happening, nothing is happening, and then whoops, suddenly you're in a different world." If so, this would follow the recent inflection point in AI, but we note a hybrid approach to computing is inevitable, where QCs are used in tandem with classical computers.

QCs are highly specialized in nature and currently commercial quantum advantage is expected in four specific areas:

1. **Optimization:** QCs are likely to improve on the ability to find the most efficient answer to a problem with numerous potential solutions.

[1] Martha Lane Fox, "I've Seen the Future and It Could Be Great for Britain," *The Times*, June 18, 2023.
[2] Davide Castelvecchi, "IBM Quantum Computer Passes Calculation Milestone," *Nature*, June 14, 2023.

2. **Machine Learning:** QCs may accelerate existing workloads or unlock entirely novel methods outright, impacting and further enhancing the development of artificial intelligence.

3. **Simulation:** QCs are expected to have an exponential speed-up over classical computers when it comes to the simulation of molecules and other quantum systems.

4. **Cryptography:** QCs will be able to significantly weaken — or in some cases, break — certain cryptographic standards.

Comparing different QCs is difficult given the existence of numerous qubit technologies (e.g., superconducting, trapped ion, photonic, etc.), and widely varying qubit quality depending on model and company.

Industry Use Cases and Risks

Manufacturing and logistics are widely considered to be among the main early beneficiaries of quantum computing. In contrast to the limitations of classical computers, QCs are expected to enable the comprehensive modeling of sophisticated molecules, dramatically benefiting material discovery in the manufacturing industry. QCs are expected to enhance the ability of digital twins (virtual simulations of products or system lifecycles that can be updated from real-time data) to monitor and automate production processes, as well as dramatically lower costs. QCs are also expected to improve operational capabilities in industries that require the consideration of a high number of complex variables such as logistics systems (e.g., supply chains, airlines, or traffic flows).

Training large-scale AI models is becoming increasingly difficult and costly for classical computers. Two promising areas where QCs are expected to help drive AI even further forward are Natural Language Processing and Artificial Neural Networks.

QCs could offer a big leap forward for drug discovery and medical services. This is because drug molecules are quantum mechanical systems themselves, meaning that QCs are inherently more suitable to simulate them than classical computers. QCs are expected to enable better Computer-Assisted Drug Discovery (CADD) tools and thus reduce current high failure rates, R&D costs, and long development cycles. For example, QCs could help model 3D protein-folding structures in drug discovery or help predict the interaction of a drug candidate with multiple biological targets to provide clues into toxicity, pharmacokinetics, and multi-target action. In addition, QCs are expected to better analyze the increasing amount of data in the healthcare industry, leading to improved personalization and precision interventions; earlier, more accurate, and faster diagnoses; and ultimately, more lives saved.

Supporting climate agendas, QCs may help simulate the complicated chemistry of prototype battery designs and accelerate the R&D process, supporting the transition to renewable energy. By boosting efficiency and reducing emissions, QCs could help discover new catalysts for oil refining; Carbon, Capture, Utilization, and Storage (CCUS); or ammonia manufacturing. In addition, QCs' potential ability to simulate the Earth's climate more dynamically may enable the more accurate prediction of natural disasters.

In finance, QCs are expected to improve targeting and prediction, portfolio optimization, risk management, and fraud detection. The use of QCs is expected to improve the performance of Monte Carlo-based options pricing, portfolio optimization, and dynamic arbitrage.

It is thought that QCs could help overcome the limitations of existing analytical models to sift through large amounts of behavioral data, enabling financial institutions to offer more personalized products and services to customers in real time. Quantum-optimized loan portfolios focused on collateral could also allow financial institutions to improve their offerings, possibly lowering interest rates and freeing up capital.

Cybersecurity risks from QCs need significant attention. Shor's algorithm theorized that a large fault-tolerant QC could break the asymmetric (public-key) encryption used to secure most of the internet in a fraction of the time required by classical computers. It has been estimated that a QC capable of breaking today's RSA encryption would need around 100,000 times more qubits than today's best machines, as well as 1/100th of the error rate. Grover's algorithm would similarly need a large fault-tolerant QC but would provide a quadratic speed-up in terms of attacking symmetric encryption standards like the Advanced Encryption Standard (AES). However, the idea of "Harvest Now, Decrypt Later (HNDL)," whereby bad actors may harvest the encrypted data now with the intent of utilizing a QC to decrypt it in the future, means the threat is in the present. This quantum threat is akin to the Y2K problem at the turn of the millennium (which had an estimated cost of $200 billion to $850 billion), although the quantum threat is less well-defined, in that we do not know when it is going to happen, and countries are unlikely to be fully transparent about their progress on QC.

The cryptography underpinning Bitcoin and cryptocurrencies in general is also at risk of being broken. Furthermore, with the increasing investment in Metaverse and Web3 projects that are intended to build a more decentralized web using distributed ledger technologies (DLTs), breaking the underlying cryptography could enable nefarious actors to break claim ownership over digital assets on DLTs. To reduce this threat and improve security, the cryptocurrency community should agree on and deploy a quantum-resistant signature scheme.

How Nation-States, Corporates, and Market Participants Can Prepare

Countries are uniquely positioned to prepare for quantum computing due to their ability to facilitate the long-term funding necessary for the sector to grow to scale. Governments that engage with industry early are more likely to set themselves up with a strong foundation in developing quantum computing technologies — the UK National Quantum Technologies Programme is a good example of this. Countries that do not invest risk falling behind in a future quantum computing arms race, similar to that of AI. However, government funding is only useful if it yields results — we used the number of papers published and patents filed in the space as proxies of how successfully countries have been investing in QCs so far.

There is currently a talent shortage of quantum computing experts, and as competition to deliver larger-scale QCs heats up, the talent shortage risks becoming a significant barrier to the growth of the industry. This is in part because the quantum computing industry is not yet mature enough that most individuals cannot do without at least a basic understanding of quantum mechanics. Consequently, progress in the space until now has been predominantly achieved by PhD-level scientists with advanced knowledge from disciplines including quantum mechanics, computer science, and electronic engineering. However, to bridge this gap, professional development courses and internship programs are emerging. As products mature, more commercial and industrial skills will be needed, such as engineering and project management. One additional concern for governments is that the talent pool in the quantum computing field is global in nature, potentially creating national security concerns.

Supply chains for QCs could also be of strategic importance to nation-states. The quantum computing supply chain is as global as that of semiconductors but even more highly specialized and complex, with different types of QCs using completely different qubit technologies. It is too early to say if there will even be a winning qubit technology that achieves adoption across the world (in the same way that the silicon chip became predominant in the manufacturing of classical computers), or to predict the impact this may have on a still-developing quantum computing supply chain. Qubits are susceptible to noise, which comes in the form of ambient thermal energy. Thus, quantum computing technologies, such as superconducting qubits, need to be supercooled to extremely low temperatures to prevent decoherence. This need for QCs to be protected from environmental factors is one of the reasons that, for many, the cloud will be the main method of access.

Similar to AI, QCs have the potential to reshape our world by enabling breakthroughs in medicine, material science, finance, and other industries, while also posing equally great risks if used improperly. For example, breakthroughs in medicine design also bring potential breakthroughs in the design of chemical weapons. Shortly after the 2019 National Defense Authorization Act (NDAA) authorized the Department of Defense (DoD) to create a Quantum Information Science (QIS) research, development, and deployment program, Congress added a mandate for ethical considerations in the NDAA, requiring the DoD to develop a plan for the "development of ethical guidelines for the use of quantum information science technologies."

Corporates should also prepare for the era of commercial quantum advantage, through actions including improving quantum computing awareness within the company, creating impact assessments at the C-suite and board level, examining collaboration and partnerships, and contextualizing opportunities. Total addressable market (TAM) forecasts vary both in terms of their starting number (spanning from $370 million to $1.1 billion in 2022) and their growth rate (25% to 50%), resulting in significantly diverging forecasts over time. The use of QCs will mostly be a cloud-based service in the near- and medium-term, accelerating adoption. On the other hand, barriers include the complexity of integration with existing technology stacks and the upskilling of employees.

The encryption methods that both protect both stored data and establish secure networks are at risk. Protective steps are needed today, as adversaries may already be harvesting data. The National Institute of Standards and Technology (NIST) released the third-round result for their Post-Quantum Cryptography (PQC) standard competition in 2022 and is expected to finalize and publish their standards by 2024. Public key encryption algorithms will need to be replaced in every platform that uses them. Given the scale of the challenge and the opportunity, we suggest the time to act is now.

There has been a significant rise in the amount invested by venture capitalists (VCs) since the claims of quantum supremacy in 2019 that brought quantum computing to the attention of the public. Eighty percent of VC investment in quantum computing has occurred since the start of 2020. Despite the market turmoil in 2022, quantum computing received more VC investment than ever, with $1.8 billion of investment, equating to around a third of all VC investment to date. That the most active investors in companies have included government agencies is not surprising given the importance of digital economies.

Purpose of this Report

This report assumes the reader has no prior knowledge of quantum computing and is targeted at those hoping to get a better understanding of the burgeoning industry. It is split into three separate chapters, each with their own purpose.

1. Acts as a "Quantum Computing 101" and explains why now is the time to take notice.

2. Provides an overview of industries that quantum computing is likely to disrupt (both negatively and positively) and the kinds of use cases it may have in those industries.

3. Helps nation-states, corporates, and market participants understand the quantum computing landscape in order to prepare them for computing's next leap.

With special thanks to the experts below who kindly shared their insights in conversations with us:

- **Dr. Alan Baratz**, CEO, D-Wave
- **Professor Sougato Bose**, Physicist and Researcher in Quantum Computation, University College London
- **Alex Challans**, CEO, The Quantum Insider
- **Professor Deeph Chana**, Chair, NATO Advisory Group on Emerging and Disruptive Technologies
- **Peter Chapman**, CEO, IonQ
- **Mark Danchak**, Partner, General Innovation Capital
- **Nick Farina**, CEO, EeroQ
- **Dr. Dario Gil**, Senior Vice President and Director of Research, IBM Quantum
- **Dr. Stefano Gogioso**, Computer Scientist and Researcher in Quantum Computation, Oxford University
- **Rob Hays**, CEO, Atom Computing
- **Rajeeb Hazra**, CEO, Quantinuum
- **Jack Hidary**, CEO, SandboxAQ
- **William Hurley**, CEO, Strangeworks
- **Matt Johnson**, CEO, QC Ware
- **Roger McKinlay**, Head of the Quantum Technologies Challenge, UK Research and Innovation
- **Celia Merzbacher,** Executive Director, U.S. Quantum Economic Development Consortium (QED-C)
- **David Moehring**, General Partner, Cambium Capital
- **Dr. Michele Mosca**, CEO and Co-Founder, evolutionQ
- **Dr. Christopher Savoie**, CEO, Zapata Computing
- **Professor Simone Severini**, Director of Quantum Computing, Amazon Web Services (AWS)
- **Professor David J. Wineland**, Nobel Laureate and Philip H. Knight Distinguished Research Chair in Physics, University of Oregon
- **Stuart Woods**, Chief Operating Officer, Quantum Exponential
- **Dr. Anthony J. Yu**, Vice President of Silicon Photonics Product Management, GlobalFoundries

Quantum Computing 101

Introduction

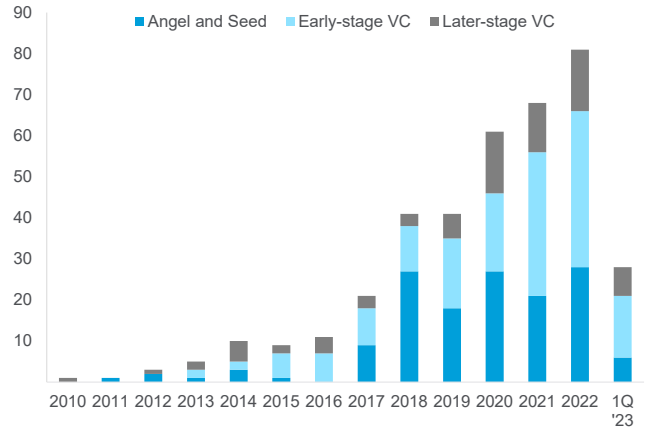
Quantum computing is coming. It will radically change the way we do things. It may even alter our very understanding of the world around us and beyond. Its power and potential are difficult to overstate. As such, we need to be prepared.

Each of the last three decades has had its own computing revolution — the personal desktop revolution in the 1990s, the mobile revolution of the 2000s, and the cloud computing revolution of the 2010s. While each gradually changed how we interacted with computers, none have made us fundamentally rethink what it means to actually "compute."

Quantum computing may do exactly that.

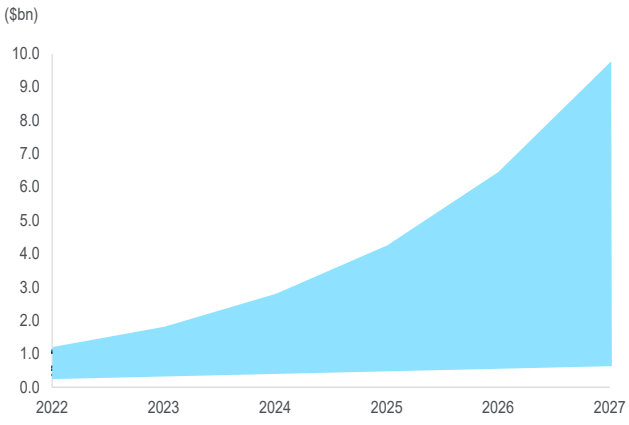
Our analysis of third-party total addressable market (TAM) forecasts for quantum computing range between $700 million and $8.6 billion by 2027, with a compound annual growth rate (CAGR) of up to 50%. By some estimates, the global Quantum Computing as a Service (QCaaS) market could reach $26 billion by 2030, representing an approximate 80% CAGR from 2021.[3] A deep dive into investment flows shows us that over the past few years, the quantum computing market has received significant investment from venture capital (VC) investors, making it one of the most densely invested technologies when compared to over 100 other areas of innovation. In 2022, nearly $1.8 billion was invested into quantum computing companies by VCs in the private markets (Figure 1).

Figure 1. Venture Capital Invested From 2010 through 1Q 2023



Source: PitchBook Data Inc., Citi GPS

Figure 2. Range of Current TAM Forecasts (2022-27E)



Source: Citi GPS, Multiple TAM Forecasts

Inflection Point

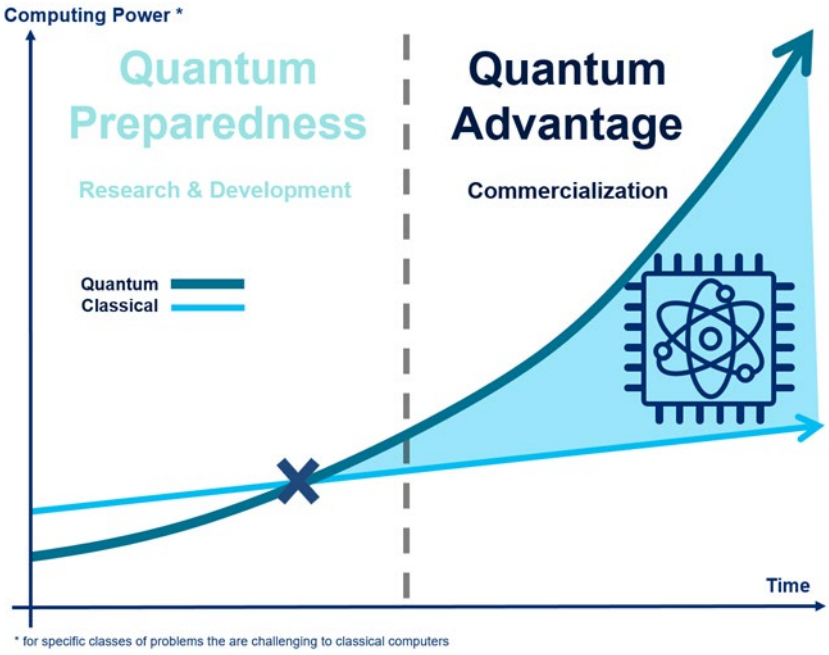
Computing is at an inflection point. After decades of consistent increases, the growth rate of computing power is reaching its physical limit. At the same time, quantum computers are edging closer to generating commercial value. This presents both a potential opportunity for early adopters and a potential risk for others. In a number of industries, even a small advantage in computational power could be business critical.

[3] The Quantum Insider, "Quantum Computing as a Service Market to Hit $26 Billion by End of Decade," August 12, 2021.

Why Quantum Computing May Be the Defining Technology of the 2020s

Since access to quantum computing on the cloud was launched in 2016 by IBM, a number of competitors have begun to offer Quantum Computing as a Service (QCaaS). The demand for such services is increasing rapidly, with 74% of large global enterprises having some form of plan to adopt quantum computing, according to a survey by Zapata Computing.[4] This reflects the fact that 48% of executives believe quantum computing will play an important role in their organization as early as 2025.[5]

Figure 3. Anticipated Quantum vs. Classical Computing Power Over Time



Source: Citi GPS

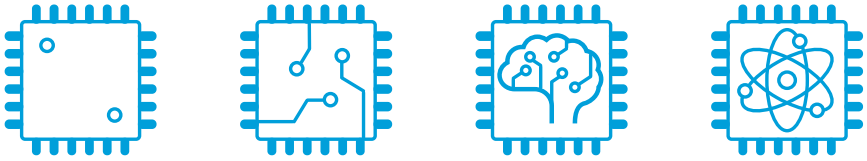
The advancement in semiconductor circuit fabrication over time — or the doubling of transistors per chip every 1.5 to 2 years — is dubbed Moore's Law. According to some observers, its tenets have been under threat for the past decade and the rate of progress in the current non-quantum computing (otherwise known as "classical computing") paradigm is expected to tail off in the coming years.

[4] Zapata Computing, *The Second Annual Report on Enterprise Quantum Computing Adoption*, January 11, 2023.
[5] EY, *How Can You Prepare Now for the Quantum Computing Future?*, June 2022.

The capabilities of quantum computers, on the other hand, are advancing and doing so at an increasing rate. Many believe we have passed the point of quantum supremacy following Google's claim of achieving this milestone in 2019, as well as further such claims since then by researchers in China and at Canadian firm Xanadu.[6] Quantum supremacy, coined by John Preskill in 2012, defines the point at which we can perform tasks with quantum computers beyond the capabilities of classical computers.[7] Something that is often misunderstood about these claims is that these are benchmarking tasks rather than commercially useful ones. In other words, the tasks were specifically chosen for the sole purpose of demonstrating the quantum computer's computational superiority. They otherwise do not have any functional use and are more akin to the quantum computer executing a randomly chosen sequence of instructions.[8]

The next major milestone in the development of quantum computing is that of commercial quantum advantage. This term describes when quantum computers will be able to offer practical advantages in solving a *valuable problem*, whether that is by solving it faster, cheaper, or more efficiently than any available classical solution.[9] One of the biggest technical challenges in solving the more complex real-world problems to reach this point, is the high levels of noise current quantum processors have. In 2023 however, IBM used error-mitigation techniques to compensate for their noise problem and solve a simplified model of a material — an experiment that IBM claims suggests that quantum computers could have useful real-world applications within two years. Regardless of any specific timeframe, this experiment is being considered by many as a key proof-of-principle that quantum computers could soon provide commercial quantum advantage in the near term.[10] Also, for simplicity going forward, the term "quantum advantage" will be used in this report to refer to commercial quantum advantage.

Figure 4. Generations of Computing



Source: Citi GPS

[6] Elizabeth Gibney, "Hello Quantum World! Google Publishes Landmark Quantum Supremacy Claim," *Nature*, October 23, 2019; Matthew Sparkes, "Quantum Supremacy Has Been Achieved by a More Complex Quantum Computer," *New Scientist*, September 21, 2021; Lars S. Madsen et al., "Quantum Computational Advantage with a Programmable Photonic Processor," *Nature*, Vol. 606, June 2022.
[7] Edwin Penault et al., "On 'Quantum Supremacy'," IBM, October 21, 2019; John Preskill, Quantum Computing and The Entanglement Frontier, California Institute of Technology Institute for Quantum Information and Matter, November 13, 2012.
[8] John Preskill, "Why I Called It 'Quantum Supremacy'," Quanta Magazine, October 2, 2019.
[9] W. J. Zeng, "Clarifying Quantum Supremacy: Better Terms for Milestones in Quantum Computation," Medium, January 31, 2019.
[10] Davide Castelvecchi, "IBM Quantum Computer Passes Calculation Milestone," *Nature*, June 14, 2023.

With the increasing pace that the capabilities of quantum computers are growing at, the shift to quantum advantage is likely to be sudden. At the same time, due to the inherently specialist nature of quantum computers, the step change to quantum advantage should come at different times for different industries and use cases. Furthermore, quantum computers are also not likely to be a replacement for our current classical computing infrastructure, but rather an invaluable addition to it. After the point of quantum advantage, we'll have leapt into what many will consider the next era of computing.

Understanding Quantum Computers

The Basics

A quantum computer is a machine that uses the quantum states of matter such as atoms or superconducting circuits to perform calculations. They are inherently probabilistic machines — quantum computers output a sample of a probability distribution. In contrast, the classical computers we know and use today are deterministic machines, meaning that they operate using binary computation of only 1s and 0s and provide an exact answer.

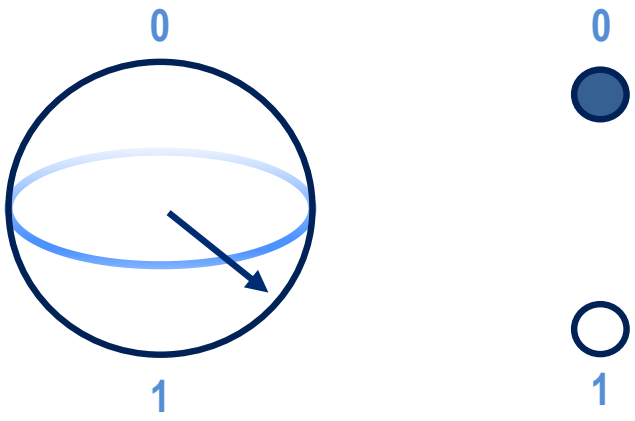
The probabilistic nature of quantum computers makes them incredibly powerful when it comes to solving some types of problems. As they grow in capability, they are expected to improve our computational abilities and solve problems that would otherwise be impossible to address on our current classical computers. We look into this further in our “Areas Quantum Advantage Could Occur” section below.

However, that same probabilistic nature of quantum computers means they are only good at certain tasks and not likely to replace classical computers in the medium term. Instead, they will augment the current computational infrastructure.

How They Work

Quantum computers process information by harnessing the principles of quantum mechanics — the laws that govern the behavior of atoms and photons. By isolating these particles and finding ways to manipulate them, scientists can create the basic building block of a quantum computer — typically a two-state quantum bit or “qubit.” Qubits can simulate their classical counterparts — occupying a state of either 0 or 1 — but can also be in any combination of both states at the same time through the quantum mechanical property of “superposition.” Qubits are often represented by a “Bloch sphere,” as shown on the left side of Figure 5.

Figure 5. Diagrammatic Representation of a Quantum Bit (Qubit) vs. a Classical Bit



Source: Citi GPS

Superposition is the ability of a qubit to represent both 0 and 1 simultaneously. Imagine that a qubit is a coin spinning on a tabletop. As it spins it can be considered a probability function, with a chance of being heads or tails when it stops spinning. It will continue to be a probability function of possible results until it falls or is stopped, and the result is measured.

Another quantum mechanical property known as “entanglement” occurs when two quantum systems interact in such a way that their states cannot be described independently. This unique quantum behavior binds the destiny of a set of different particles so that what happens to one will affect the others. Entanglement, which was once described by Albert Einstein as “spooky action at a distance” (and was the basis for the 2022 Nobel Prize in Physics), seemingly makes it possible to manipulate both states of the qubits simultaneously. So, instead of performing a set of calculations one after another, a quantum computer could perform them all at the same time.

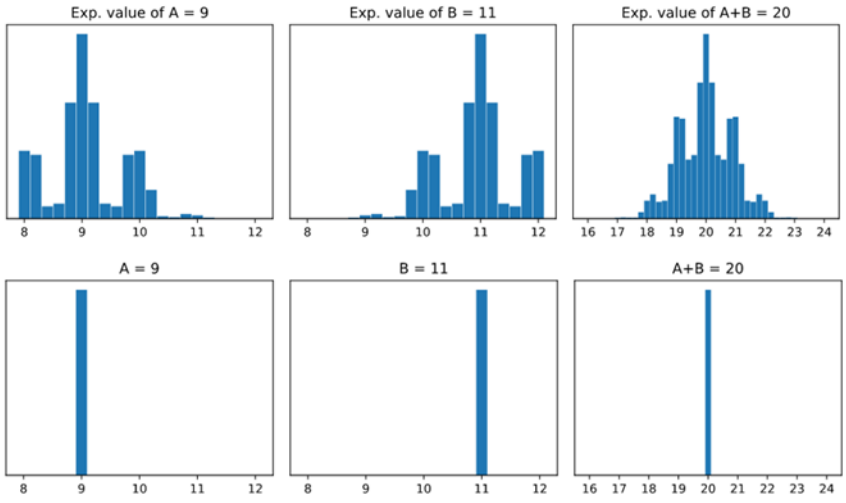
To perform calculations, a quantum computer must be able to put qubits into a state of superposition and manipulate the superpositions. The length of time that a system can maintain this state is called the “coherence” time. Just as the spinning coin from the above example will eventually stop due to friction, qubits are susceptible to noise — something that raises its own challenges.

Although spinning coins is a useful analogy for conceptualizing quantum mechanical concepts, the real science is far more complex. For instance, there are numerous models for building a quantum computer, something we also provide a high-level description of in the “The State of the Quantum Computing Market” section below.

A Highly Simplified Example

One very simplistic way of attempting to conceptualize how a quantum computer processes information is to use the example of probability distributions being added together. The deterministic nature of a classical computer means that when asking it to add two numbers, say 9 + 11, it will output the exact same answer each time — 20. In contrast, a quantum computer works with probability distributions, so it would input two probability distributions centered at 9 and 11 and output a probability distribution centered at 20, meaning that while the quantum computer would tell you 9 + 11 = 20 the vast majority of the time, it may also tell you it’s equal to 18 or 22 on other occasions. To obtain the correct result with more certainty, the quantum algorithms can be run multiple times, generating a probability distribution.

Figure 6. Probabilistic vs. Deterministic Computing



Source: Citi GPS

That said, probability distributions added together is an incredibly simplified illustration of how quantum computers operate. Quantum computers are orders of magnitude more complex than this, and a complete explanation requires an understanding of trigonometry, differential equations, and numerous areas of mathematics beyond the scope of this report.

Nobel laureate and famed physicist Richard Feynman is often quoted as saying that "If you think you understand quantum mechanics, you don't understand quantum mechanics."[11] And while there is some truth to this statement, in that quantum mechanics is probably as divorced from our lived reality as a field of science can be, it risks potentially painting quantum physics (and hence, quantum computing) as a mystical, esoteric, and incomprehensible subject. If one is able to put one's knowledge of the classical world and lived reality aside and evaluate quantum computation purely using mathematics, the topic is considerably more approachable.

[11] *New Scientist*, "Quantum Mechanics," accessed March 6, 2023.

The Rapid Development of Quantum Computers

Many people ask why there needs to be a discussion about quantum computing when the point of quantum advantage has yet to be reached. The answer is because the era of quantum advantage is likely to arrive relatively suddenly. Why? In short, because quantum computers have exponential scaling power.

This, alongside the fact that quantum advantage, by definition, comes after quantum supremacy, means that by the time that quantum computers can offer a practical advantage to businesses in solving valuable problems, they will be widening the gap to their classical counterparts at pace.

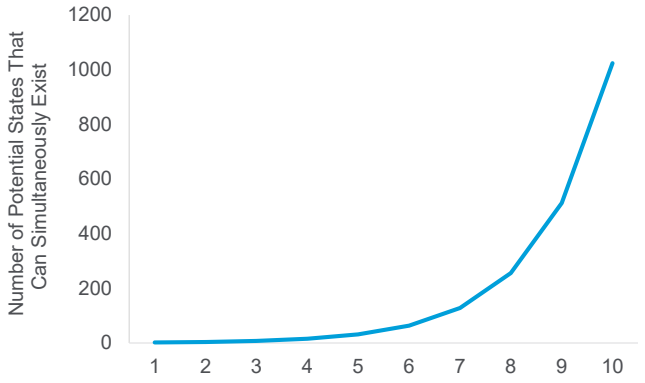
One of the consequences of quantum mechanics is that by just adding one additional qubit to a quantum computer, you can double the total number of potential states the quantum computer can be in at the same time. Given that the number of states a quantum computer can occupy at any one time is often considered proportional to the computational capabilities of that machine, we can see how quantum computing may very easily overtake classical computing. As Figure 7 and Figure 8 show, the exponential nature of quantum computers means that, as they grow in size, they can very quickly have more potential states that can simultaneously exist than there are atoms in the observable universe![12]

Figure 7. Exponential Scaling of Qubits

Number of Qubits (n)	Number of Potential States That Can Simultaneously Exist (2^n)
n=1	$(2^1) = 2$
n=2	$(2^2) = 4$
n=3	$(2^3) = 8$
n=4	$(2^4) = 16$
n=5	$(2^5) = 32$
…	…
n=100	$(2^{100}) = 1{,}267{,}650{,}600{,}228{,}229{,}401{,}496{,}703{,}205{,}376$

Source: Citi GPS

Figure 8. Visualization of Exponential Scaling of Qubits



Source: Citi GPS

In other words, to match the rate of progress seen in classical computing for some applications (i.e., the doubling of classical computing power observed in Moore's Law), the number of qubits in a quantum computer would only, in theory, need to increase by one every two years. However, we are seeing considerably faster progress.

Google's observations suggest that the rate of progress in the industry could be described as doubly exponential growth. As Scientific American reported, in December 2018, Google was able to replicate calculations run on their best quantum computer using a normal classical laptop.[13]

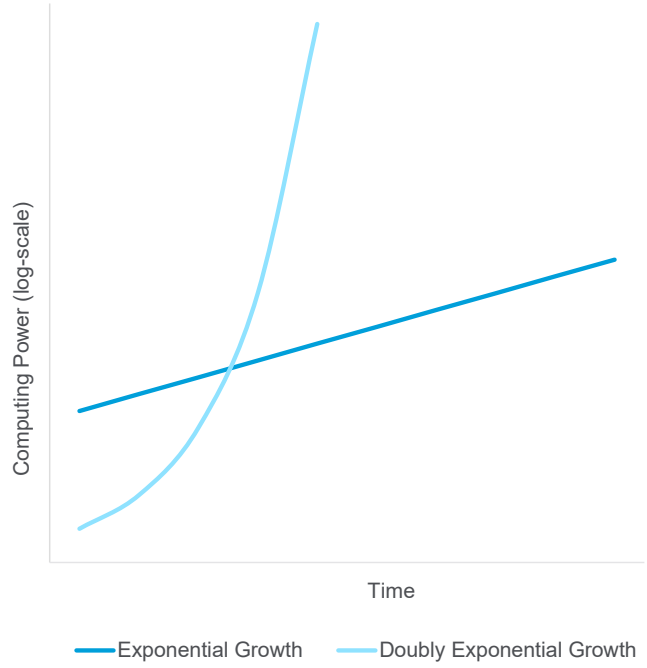
[12] By some estimates, the number of atoms in the observable universe is around 10^{78} to 10^{82}

[13] Kevin Hartnett, "A New 'Law' Suggests Quantum Supremacy Could Happen This Year," *Quanta Magazine*, June 21, 2019.

By January 2019, however, they had managed to improve their quantum computer to the point that a powerful classical desktop computer was needed to replicate the results. This rate of progress continued to the point that by February 2019, to replicate the results of their then-most advanced quantum computer, Google had to instead use their incredibly powerful server network.

This rate of doubly exponential improvement is referred to as “Neven’s Law” after Hartmut Neven, Director of the Quantum Artificial Intelligence Lab at Google. Neven’s Law, like Moore’s Law, is an empirical law — one that has come about from observation. Hence, whether Neven’s Law will hold true in the long term remains unclear. It depends a lot on the progress of the industry and whether it is fundamentally possible to keep control of qubits as we build larger quantum computers. It can be neither proven nor ruled out.

Figure 9. Neven's Law of Doubly Exponential Growth vs. Moore's Law of Exponential Growth



Source: Citi GPS

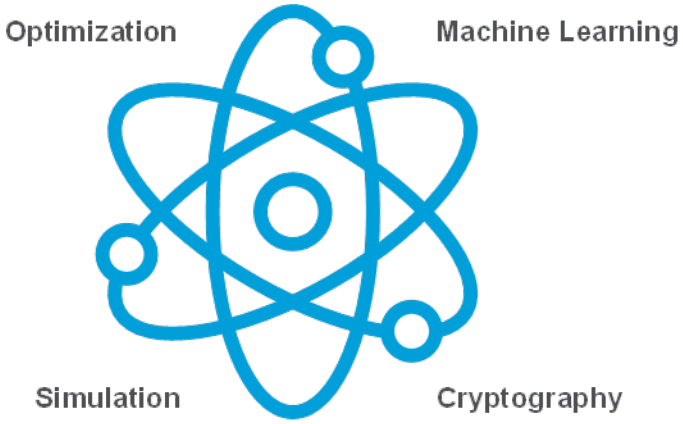
What this means is that given the rate at which quantum computing technologies are maturing over time, the increase in computing power is exponentially increasing even when plotted on a logarithmic graph (Figure 9). Neven explained that with quantum computers’ doubly exponential growth, “it looks like nothing is happening, nothing is happening, and then whoops, suddenly you’re in a different world.”

We can see from the figure above how quantum computers following such a path of progress could easily catch up to and overtake classical computers, despite the latter’s multi-decade head start.

Areas Quantum Advantage Could Occur

There are four broad areas where quantum computers can provide an advantage. We dive deeper into how these for areas will impact different industries and discuss practical use cases later in the report.

Figure 10. Areas of Anticipated Quantum Advantage



Source: Citi GPS

- In **optimization**, quantum computers are likely to outperform their classical counterparts when solving such problems. This will lend itself to any use case where there is an efficient answer to a problem with a high number of potential solutions, including portfolio optimization and route planning.
- For **machine learning**, quantum computers may accelerate existing workloads or unlock entirely novel methods outright. This is likely to have an impact on the likes of fraud detection and the development of artificial intelligence.
- Regarding the **simulation** of molecules and other quantum systems, quantum computers are expected to have an exponential speed-up over classical computers. As legendary physicist Richard Feynman put it, "Nature isn't classical…if you want to make a simulation of nature, you'd better make it quantum mechanical."[14] Quantum simulation is one of the areas of greatest potential for this technology due to the number of areas that rely on the simulation of chemical reactions.[15] This includes the likes of fertilizer production, battery technology, drug development, and the manufacturing of advanced materials.
- In **cryptography**, quantum computers of sufficient size and operating efficiency pose a threat to existing cryptographic standards, which is in fact what really launched the widespread interest in quantum information and computing. Fortunately, there are efforts by the National Institute of Standards and Technology (NIST) and the cryptographic community to introduce new quantum-resistant protocols. The challenge will lie in ensuring their broad adoption across the globe.

[14] Andreas Trabesinger, "Quantum Simulation," Nature Physics, Vol. 8, No. 263, April 2012.
[15] John Preskill, "Quantum Computing in the NISQ Era and Beyond," Institute for Quantum Information and Matter and Walter Burke Institute for Theoretical Physics, California Institute of Technology, July 30, 2018.

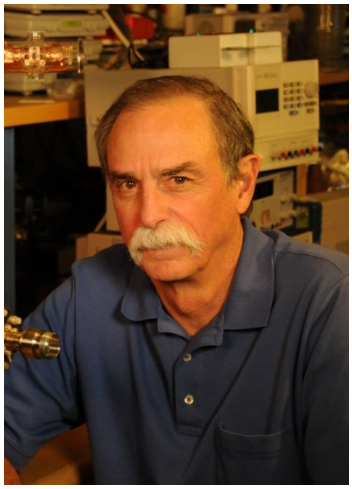
While the above-mentioned areas will affect a broad range of industries, it is important to note that quantum computers, given their highly specialized nature, will only impact discrete areas within each industry at first. In other words, quantum advantage will reveal itself over time far more granularly than at an overall industry level. It will probably first occur in very specific use cases, such as modeling a particular type of protein or running a particular type of machine learning algorithm better than a classical computer. In part due to the granular nature of quantum advantage, a hybrid approach to computing looks inevitable.

Regarding which of the four areas of quantum advantage will appear first, this question is still open to debate — most companies and experts we spoke to tended to have relatively strong convictions in their chosen area of quantum advantage. What we can say is that due to the need for error correction and the large number of qubits required to break today's cryptography standards, quantum advantage in cryptography looks likely to be the last.

Regardless of where commercial quantum advantage is first observed, when it occurs, quantum computing may very well be the future of computing in that area.

We spoke to Professor David J. Wineland, who won the 2012 Nobel Prize in Physics for his "ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems" and is currently a Philip H. Knight Distinguished Research Chair in Physics at the University of Oregon, to get his insights on the future of quantum computing.

Expert Interview with Nobel Laureate, Professor David J. Wineland, at the University of Oregon



Professor David J. Wineland
Nobel Laureate and Philip H. Knight Distinguished Research Chair in Physics, University of Oregon

Q: You won the Nobel Prize for your work in manipulating quantum systems — something that many consider a milestone in the development of quantum computing. What initially attracted you to the field and to what extent was quantum computing on your mind?

Prof. Wineland: Like many others, my interest in quantum computing really started back in 1995 after Peter Shor published his now-famous factoring algorithm. At first, I think that got a lot of people interested in the idea of a quantum computer because of its potential impact on cybersecurity. Not surprisingly, government agencies also became very interested in this and there was a sudden influx of support for investigating quantum computing. As you point out, however, my 2012 Nobel Prize wasn't technically for quantum computing, but rather for developing experimental methods that enabled the measuring and manipulation of individual quantum systems (although, of course, this is inherently important to quantum computing). As such, I can't say building some kind of large universal quantum computer was something I'd thought of day-to-day during my research. Rather, back then, and as is still the case, my work and that of the group I was involved with, was focused on demonstrating the simple primitives of quantum computing as well as quantum "gedanken," or thought, experiments that were posed by Einstein and his colleagues in the early days of quantum mechanics. So rather than aiming to build a quantum computer, we hoped to make useful contributions to the general problem in the long run, such as through the development of better quantum gates.

What I find particularly interesting about the study of quantum systems is that, even now 100 years on, we are still addressing questions that the founding fathers of quantum physics asked themselves, such as the postulated Einstein–Podolsky–Rosen (EPR) type experiments. An example of an EPR experiment is that when you entangle two atoms and then separate them by a large distance, their entangled state implies that measuring the first atom results in an effectively instantaneous impact on the second atom such that its measured state is correlated in a precise way to the measured state of the first atom. And the amazing part is that the measured state of the first atom is completely random, but the correlations between the measured states of the two atoms are preserved and occur instantaneously. These instantaneous correlations have now been unambiguously demonstrated with the quantum states of photons. At first glance, it appears as if these two quantum entangled atoms are communicating faster than the speed of light and thus violate a law of physics — that information cannot travel faster than the speed of light. But because the measurement outcome of the first atom is random, no information can be transferred. However, we do know that these correlations are being transferred faster than the speed of light and I just find that fascinating, and I don't think anyone has a satisfactory answer as to why this occurs.

In fact, Einstein himself is often quoted as describing this as "spooky at a distance," and it very much is. I think the fact that we're still trying to find an answer as to why nature works in this way a century later is very interesting to me.

Q: What do you think of the prospects of building a "universal" quantum computer?

Prof. Wineland: With respect to the idea of building a large-scale fault-tolerant quantum computer (often referred to as a "universal" quantum computer), especially one which would have the capacity to factor cryptographically significant numbers that underpin much of cybersecurity, I think we're a long way off yet. We are still in what is sometimes referred to as the Noisy Intermediate Scale Quantum (NISQ) computing era, where quantum computers are characterized by noisy gates and lack the error-correction needed to run complicated algorithms. To move into the era of Fault-Tolerant Quantum Computing (FTQC), in which we can truly consider having a universal quantum computer, we will need machines with significantly more qubits than even the most advanced quantum computers have today, and the necessary error-correction needed for these complicated quantum algorithms.

That's not to say it won't happen though. Even as far back as the mid-90s, I wouldn't say there was anyone suggesting building such a universal quantum computer one day was impossible — it was just that our technology back then was not good enough for the precise manipulation of atoms or superconducting qubits — and in fact, we still haven't mastered control of these. The current challenges involved in creating a universal quantum computer are still difficult, but I'm optimistic in the long run. As to when this may happen, however, I couldn't really say. Quantum computing has been a technology that's often been oversold, so I would caution against over-optimistic forecasts. Back in 1995, when I was at the National Institute of Standards and Technology (NIST) and we'd learned of Peter Shor's algorithm, many of us thought that we'd have made much more progress by now almost 30 years later. However, I do find it difficult to believe we won't eventually be able to create a universal quantum computer.

Q: As well as the risk to cryptography, we identified three other areas of potential "quantum advantage": optimization, machine learning, and molecular simulation. What are your thoughts on quantum computing being practically useful in these areas in the nearer term?

Prof. Wineland: There are definitely a lot of scientists out there looking at various uses for quantum computers beyond just creating a large factoring machine. One particular area of quantum advantage that could have a significant impact on society is that of molecular simulation.

All molecules at the smallest of scales are inherently quantum mechanical, and these characteristics are something that quantum computers are anticipated to be far better at modeling than our current classical computers. As Richard Feynman is often referred to as putting it: "in order to understand quantum systems, you need a quantum computer." In the nearer term, it is very plausible that if quantum computers continue to develop at their current rate, one of the areas they could potentially be of great value would be the simulation of molecules that may be useful in drug therapy. Rather than having to synthesize a new drug in a lab, scientists may be able to simulate the action of a new molecule on a quantum computer to verify or nullify its usefulness.

A lot of people feel that, well before quantum computers are able to factorize cryptographically significant numbers (i.e., the extremely large numbers that are used in internet encryption), the first real application of quantum computers will be in one or more of the areas mentioned or for applications that haven't yet been considered. I also think there are a lot of areas in quantum information theory that are very interesting, and some that are already aiding classical computing.

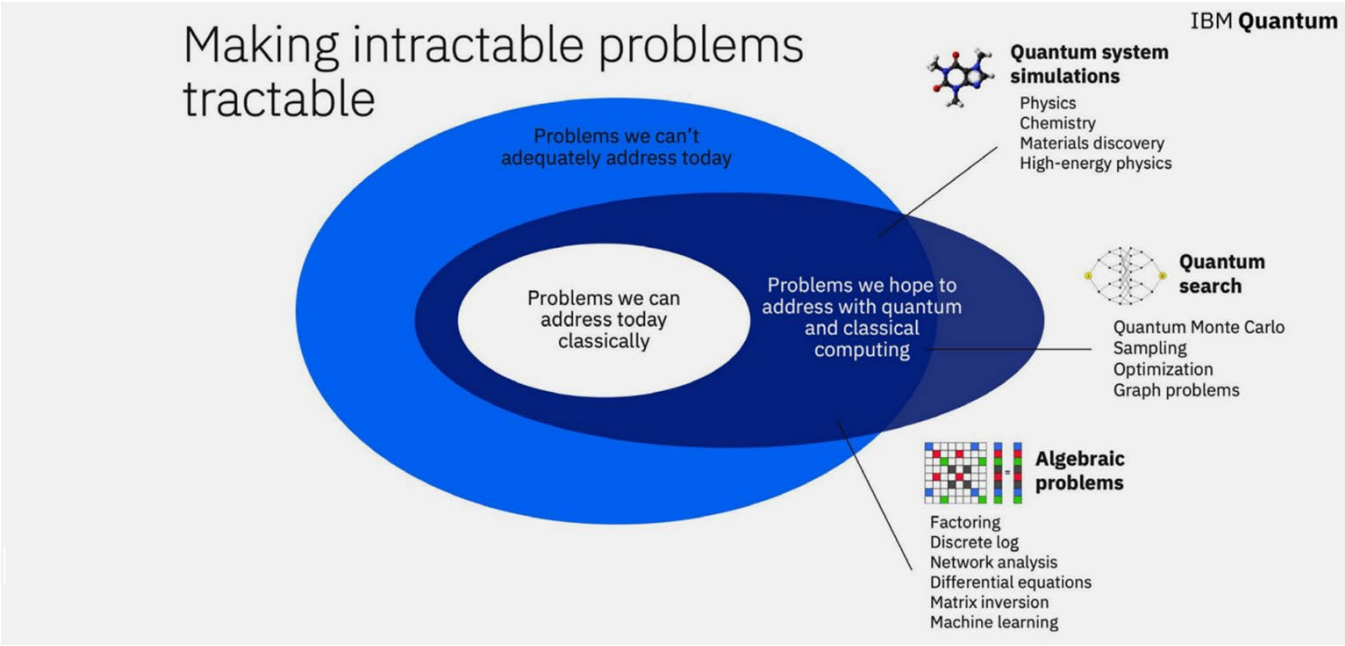
A Hybrid Approach to Computing Is Inevitable

After the point of quantum advantage, we anticipate a combination of classical and quantum computing is highly likely for the foreseeable future.

Quantum Complexity Theory

Quantum complexity theory is a sub-field of computational complexity theory that looks to determine the "hardness," or difficulty, of certain computational problems. Hardness is defined as the allocation of resources needed by computational models to solve certain problems. In other words, it is asking how the difficulty of a problem increases as the size of the problem set increases. Unsurprisingly, the ways different types of problems overlap are quite complex. Figure 11 illustrates this in a simplified graphical form:

Figure 11. Example of How Problems Can Be Categorized by Their Quantum Complexity



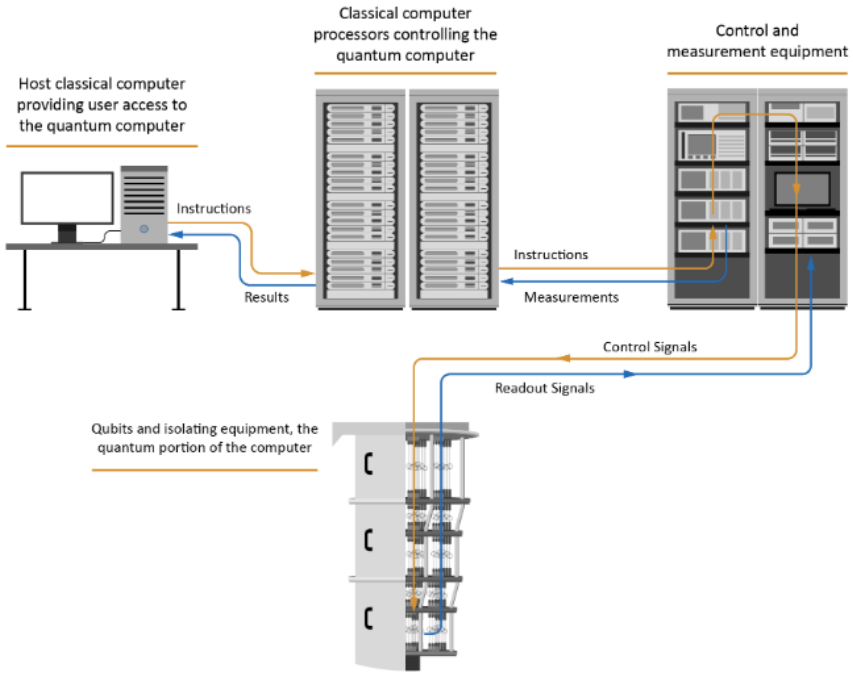
Source: IBM Quantum, IBM Corporation

Quantum computers and their classical counterparts excel at different types of problems. Based on current assessments, there will always be areas of computing where quantum computers do not provide a material speed advantage over classical computers. Thus, as illustrated in Figure 11 above, the vast majority of applications of quantum computing that offer a competitive advantage in a given industry, are likely to occur in the dark blue area. If only part of an overall problem is solved faster by a quantum computer, then it makes sense to only allocate that specific piece to a quantum computer.

The Practicalities: Error-Correction and Hybrid Algorithms

Another reason to believe we will always need classical computers is more practical. The error-correction that quantum computers will need to grow in scale requires classical computer co-processors. This means that even if in a quantum-enabled future, we reach a point at which quantum computers are far superior at calculations to classical computers (and perhaps are even one of the main sources of computing in the cloud), quantum computers will always need classical computers surrounding them in order to operate. Figure 12 is an illustration of how such a setup may work.

Figure 12. How Quantum Computers and Classical Computers Will Work in Parallel



Source: Citi GPS

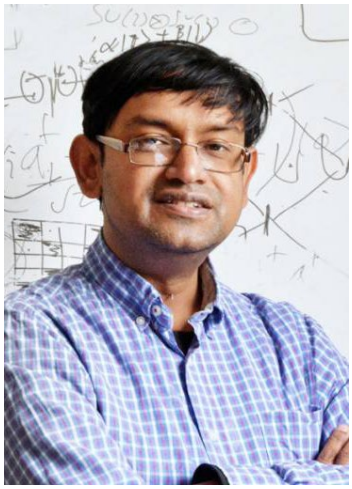
Many algorithms intended to run on quantum computers are, in fact, hybrid quantum-classical algorithms that will always require a classical computer by design. Algorithms such as the Variational Quantum Eigensolver (VQE) and the Quantum Approximate Optimization Algorithm (QAOA) use the quantum computer to explore the space of possible solutions and classical machine learning to optimize search parameters.

A potential way of thinking about quantum computing's future path is to compare a quantum processor to a classical graphics processor. Analogous to how a Graphical Processing Unit (GPU) is often a key addition to a high-end personal computer, providing a significant speed-up on the specialist tasks that the standard Central Processing Unit (CPU) cannot handle as efficiently, a Quantum Processing Unit (QPU) may likely be a key addition to the commercial High Performance Computing (HPC) sector.

We spoke to Professor Sougato Bose, a leading physicist and researcher in quantum computation at University College London (UCL), whose work featured in *New Scientist* magazine, to get his insights on how technology may be used.[16]

[16] Thomas Lewton, "The Quantum Experiment That Could Prove Reality Doesn't Exist," *New Scientist*, November 3, 2021.

Expert Interview with Physicist, Professor Sougato Bose, at University College London



Professor Sougato Bose
Physicist and Researcher in Quantum Computation, University College London

Q: How likely is a quantum-classical hybrid approach to computing?

Prof. Bose: It is almost certain that a hybrid approach to computing will have to be pursued. Classical computers and processors are robust and operate under minimally demanding circumstances (you use your laptop and mobile phone anywhere). Quantum computers require exceptional protection from the environment and will require dedicated centers. Thus, we will access these only for special problems or as subroutines of various problems, with the rest of the computation taking place on classical computers. This is why there are many current algorithms that are hybrid by construction. Additionally, to control and error-correct quantum computers, we require classical computers.

Q: What impact do you think quantum computers could have in our understanding of the universe?

Prof. Bose: It is our current understanding that the universe is made from interacting quantum components — so it is a giant quantum computer in a certain sense, albeit not the fully controllable and programmable one we are building in the laboratories for usage. So far, humans have tried to comprehend the universe using simplified assumptions and approximate solutions, and the great deal that has been achieved has been based on the ingenuity of our approximations. Simulations allow us to go beyond these solvable pen-and-paper limits, but classical computers are not ideally suited to this task as the components of the universe are quantum, and typically, you are required to apply exponentially large matrices to exponentially large vectors.

Thus, quantum computers will enable us to probe the "complexity" frontier in our understanding of the universe — for example, phases of matter with complicated patterns of quantum entanglement. This may, in turn, help us in understanding phenomena such as high temperature superconductivity or even the emergence of space and time. On a different front, quantum computers, or at least elements developed for quantum computing, could be incorporated in sensor devices, and help with higher-precision sensing of various fundamental particles and forces, which will, again, deepen our understanding.

Q: What do you think that about the current level of quantum education in terms of the potential workforce in the industry?

Prof. Bose: I think the current level is below what will soon be required by society. At universities, quantum mechanics itself is typically taught, at least in the form needed for quantum computation, to undergraduates taking physics as a major, only in the last or third year. It has not spread out to the curriculum of other disciplines, as well as to earlier levels of physics curriculum in terms of the very fundamentals such as qubits and gates. I think this will be a change that will be necessary to have a larger volume of educated workforce in this area — so, we should introduce quantum mechanics in the form of quantum computation earlier, as well as use quantum computation as the example to learn quantum mechanics.

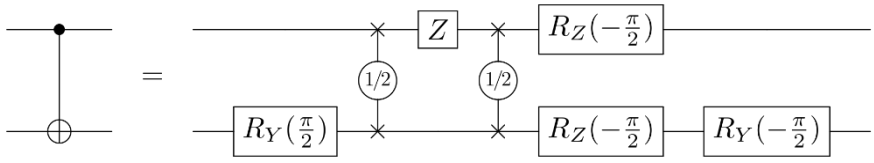
The State of the Quantum Computing Market

Quantum computers are often mistakenly thought of as being just a homogenous architecture, in the same way that all classical computers rely on silicon transistors. However, in quantum computing, two different fundamental architectures are being explored.

Types of Quantum Computers: Gate-Based vs. Quantum Annealing

The most widely explored model for building a quantum computer is that of a gate-based quantum computer. As the name suggests, this model involves the usage of a set of universal gate operators to execute circuits that outline the desired calculation. This model is applicable to numerous general-purpose use cases, as it can run various types of algorithms efficiently. This is one of the reasons that most of the hardware development in the quantum computing industry is currently being done on gate-based quantum computers. As such, most of the algorithmic research being done today focuses on being applied to this type of machine.

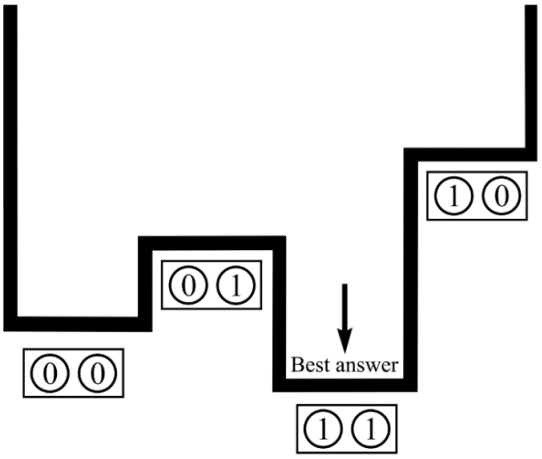
Figure 13. Example of Quantum Logic Gates



Source: Wikimedia Commons, licensed under the Creative Commons Attribution-Share Alike 4.0 International license

A second model — a quantum annealer — is a device specialized in solving optimization problems. It works by harnessing a process called annealing to find the lowest energy state of a system corresponding to the most optimal solution to a specific problem. For this reason, it is particularly good at solving quadratic unconstrained binary optimization (QUBO) problems.

Figure 14. Visualization of the Quantum Annealing Process



Source: D-Wave Systems Inc.

Different Qubit Technologies

Today, numerous methods of building physical qubits for gate-based quantum computers are being explored. This is in part because the quantum physics a quantum computer attempts to exploit can be seen in various mediums of matter and energy. So, different teams around the world have chosen different physical starting points to build a quantum system into a quantum computer.

Examples of qubit technologies include:

- Trapped Ions
- Superconducting
- Photonic
- Neutral Atoms
- Quantum Dots
- Nitrogen Vacancy Centers

Where We Are Today

Decades of R&D and billions of dollars have gotten the quantum computing industry to where it is today, and it is only now we are beginning to see the fruits of that labor.

Physical quantum computers (QCs) exist today and have anywhere up to 433 physical qubits. Despite the qubits being physically very small, the overall amount of space QCs need is typically anywhere from around the size of a cupboard to a small room, due to all the apparatuses needed to control the physical qubits. Far more important is the actual number of physical qubits and high error rates of these early machines — something that led quantum physicist John Preskill to dub this era of hardware Noisy Intermediate-Scale Quantum (NISQ).

As John Preskill put it, when he described the NISQ era, he was "imagining quantum computers with noisy gates unprotected by quantum error-correction."[17] The term "noisy" refers to the imperfect control scientists currently have over qubits, resulting in the noise introduced into quantum systems that results in QCs being error-prone today. The term "intermediate scale" references the size of current quantum computers as measured by their qubit count, expected to range from 50 to a few hundred physical qubits in the near term.

Currently, NISQ-era QCs are measured in terms of the number of physical qubits, as opposed to the number of logical qubits. Logical qubits can be described as multiple physical qubits that are operated in such a way that they are guaranteed to retain their information without errors. The most prominent technique is to create a circuit of physical qubits that output a single error-corrected result. However, this technique and other error-correction techniques only work if certain qubit error rates are low enough to begin with. The proposed ratio of physical to logical qubits varies, but with current designs, it can be anywhere from around the order of 1,000:1 to 10,000:1.

[17] John Preskill, "Quantum Computing in the NISQ Era and Beyond," Institute for Quantum Information and Matter and Walter Burke Institute for Theoretical Physics, California Institute of Technology, PDF, July 30, 2018.

Notably, the qubit count is by itself not necessarily the best way to compare quantum computers; the quality of those qubits is just as important. Simply put, a QC with 50 high quality (i.e., low-noise) qubits may very well perform calculations far better than a QC with 5,000 low quality (i.e., high-noise) qubits. In addition to differences in qubit quality, the variation in underlying qubit technologies makes direct comparisons between different QCs very difficult. Factors such as clock speed, operational speed, and connectivity between qubits also have a significant impact. To truly determine how advanced and useful a QC is, additional metrics beyond the scope of this report, such as the error rates and the connectivity of qubits, need to be considered. However, even all these metrics do not tell the full story.

IBM's recent proof-in-principle of quantum advantage — where they solved a simplified (unrealistic) model of a material — was in fact undertaken on their older 127-qubit quantum processor from 2021. For this experiment, they described running calculations involving all 127 qubits and "up to 60 processing steps — more than any other reported quantum-computing experiment."[18] They then used an error-mitigation technique where they measured the noise in each of their qubits and extrapolated back to what these measurements would have looked like in the absence of noise. Ultimately, in doing so, IBM showed just how important employing the right techniques and algorithms are, regardless of the qubit count of the QC.

However, to provide some context on the state of the quantum computing market, the table in Figure 15 highlights the qubit counts of QCs from different companies based on publicly available information. As it stands, IBM is currently leading the qubit race with their 433-qubit QC announced in 2022. Pasqal then follows with their 324-qubit QC.

Figure 15. Qubit Counts for Some Quantum Computing Companies (as of June 2023)

Qubit Technology	Company	No. of Qubits
Superconducting	IBM	433
Cold Atom	Pasqal	324
Cold Atom	QuEra	256
Photonic	Xanadu	216
Superconducting	Rigetti	84
Superconducting	Google	72
Trapped Ion	IonQ	32
Trapped Ion	Quantinuum	32

Source: Company Reports, Citi GPS

While it is impossible to precisely predict the roadmap to our quantum future, we have investigated the plans of some of the top players in the sector. For instance, Google intends to have a 1 million physical qubit QC before the end of the decade. However, to scale the qubit count of individual QCs to this level, it is expected by some to result in QCs occupying increasing amounts of floor space.[19] While this potentially presents its own challenges, it is not unlike the early era of classical computers, which have advanced and shrunk in size immeasurably in the decades that followed. This challenge is unlikely to hinder the use of QCs, as we expect the vast majority of end-users are likely to use the same technology used to access their classical computers today — the cloud. We discuss this further in the "Collaboration and the Cloud" section.

[18] Davide Castelvecchi, "IBM Quantum Computer Passes Calculation Milestone," Nature, June 14, 2023.

[19] Simon Benjamin, "Separating Quantum Hype From Quantum Reality," *Financial Times*, September 2, 2022

Figure 16 shows, in no particular order, the current publicly-available qubit roadmaps of various companies — something regularly subject to change. It is also important to note that many companies choose not to disclose their qubit roadmaps for strategic reasons. The below table was put together from publicly available information to, again, provide some context to the market. Regardless of these qubit roadmaps, we found that most companies feel they will be able to provide quantum advantage to businesses sometime this decade.

Figure 16. Qubit Roadmaps for Some Quantum Computing Companies (as of August 2022)

Company	Qubit Tech	2023	2024	2025	2026	2027	2028	2029	2030
ColdQuanta	Cold Atom		1,000+						
Google	Superconducting							1mn+	
IBM	Superconducting	1,121	1,386+	4,158+			10K-100K		
Pasqal	Cold Atom		1,000+						
Rigetti	Superconducting	84	336	1,000+			4,000+		

Source: Company Reports, The Quantum Insider, The Verge, Citi GPS

The list above is also by no means exhaustive. For instance, one estimate by the Quantum Computing Report identified over 106 organizations working on 135 projects in the quantum computing space.[20] In addition, in conversations with corporates, nearly all companies developing a QC have opted to solely pursue a gate-based structural model, with the exception of companies like D-Wave, which are pursuing the development of both gate-based and quantum annealing QCs. As quantum annealers are very different from gate-based QCs, they are not included in the tables above.

The Challenges We Face

One pressing question in the field is whether NISQ machines are capable of achieving quantum advantage (which we describe earlier as the point at which QCs can offer practical advantages in solving a valuable problem, whether that is by enabling faster, cheaper, or more efficient solutions than classical computers). There is notable debate surrounding this topic, but most companies we spoke to feel NISQ machines have the potential to achieve quantum advantage in one or more of the areas identified earlier. One of the goals of the NISQ era is to either prove or disprove this conclusively and this effort will require the right combination of hardware development and algorithm design, as well as an application to the right problem.[21]

In terms of hardware design, there are still many challenges that lay ahead for developing better QCs in the NISQ era. The primary challenge is qubit quality — manufacturers can create many qubits; however, controlling them all at once is a problem. Another key challenge is the size of QCs (i.e., the number of qubits that make them up) — current QCs do not have enough qubits of a high enough quality.

High levels of noise pose yet another key challenge for QCs. For QCs to perform calculations, they must be able to maintain their qubits in a superposition of states for a reasonable amount of time, known as the "coherence" time. Similar to how a spinning coin is subject to friction, qubits are susceptible to noise, which can come in the form of ambient thermal energy or electromagnetic interference, for example. This ultimately leads to "decoherence," which is when the calculations become unreliable as the noise introduces errors and faults into the system.

[20] Quantum Computing Report, "Homepage," accessed March 6, 2023.
[21] Kishor Bharti et al., "Noisy Intermediate-Scale Quantum (NISQ) Algorithms," Reviews *of Modern Physics*, Vol. 94, No. 1, February 2022

The process of error-correction attempts to mitigate or outright eliminate noise-induced errors in a quantum circuit through the introduction of additional error-correcting qubits to the system. Mitigating the impact of noise in quantum systems and extending coherence times are some of the leading challenges in working towards entering a future era of Fault-Tolerant Quantum Computing (FTQC) machines.

The fault-tolerant era is generally considered to be one in which QCs have the necessary quantum error-correction built in to prevent the quantum errors (or "faults") inherent to qubits from cascading through quantum circuits.[22] Like classical error-correction, quantum error-correction involves the allocation of redundant qubits to undertake the role of correcting errors in other qubits — whether this is due to the imperfect control we have over them or to environmental interactions. The idea behind using error-correction is that there will be a point at which the fundamental accuracy of individual qubits is high enough that the error-correction is correcting more errors than are being created.[23]

While we are potentially years away from FTQC machines, most agree that reaching this stage is required for QCs to reach their full potential and unlock all the areas of quantum advantage. This is because many quantum algorithms today, including those that pose a threat to cryptography, require the implementation of error-correction.

We spoke to Dr. Dario Gil, who is the Senior Vice President and Director of Research at IBM Quantum, one of the most advanced players in the quantum computing market, about his opinion on the state of the industry today.

[22] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press, 2010).
[23] Alexandru Paler and Simon J. Devitt, "An Introduction to Fault-Tolerant Quantum Computing," downloaded from arXiv, PDF, August 15, 2015.

Expert Interview with Dr. Dario Gil, Senior Vice President and Director of Research at IBM Quantum

Dr. Dario Gil
Senior Vice President and Director of Research, IBM Quantum

Q: Where is the quantum industry today?

Dr. Gil: Quantum computing is no longer a futuristic concept. We believe we are entering the Quantum Decade — an era when enterprises will begin to see quantum computing's business value. The unprecedented advances in quantum hardware, software development and services validate the technology's momentum, creating an ecosystem that paves the way and prepares the market for the adoption of this revolutionary technology.

The groundwork for this adoption is being laid by a global ecosystem of more than 400,000 users tapping into the cloud to experiment on IBM's more than 25 quantum systems. These users include individuals exploring the technology, to the developers, scientists, engineers, and domain experts at the more than 200 Fortune 500s, government labs, academic institutions, and startups that make up the IBM Quantum Network.

Our quantum roadmap, first made public in 2020, outlines how the entire stack of quantum technology, from processor advancement to software modules and services, will support the industry's progress. Last year, we debuted the 127-qubit IBM Quantum Eagle chip, our first with more than 100 qubits, and previewed IBM Quantum System Two. To simulate Eagle, you would need a classical computer with more classical bits than the number of atoms contained in all of humanity's 7.9 billion people on Earth. System Two, with its capacity to scale beyond 1,000-qubit processors, will move us closer to a true quantum data center.

In November 2022, we released the 433-qubit IBM Quantum Osprey, the largest quantum processor to date, three times larger than the Eagle processor. Like Eagle, Osprey includes multi-level wiring to provide flexibility for signal routing and device layout, integrated filtering to reduce noise and improve stability, plus our new high-density control signal delivery with flex wiring to provide a 70% increase in wire density and a 5x reduction in price-per-line. We debuted our third-generation control system, controlling 400 qubits in a single rack at an even lower price point than the previous generations. And we made strides in our other performance metrics — quality and speed — with a 4x improvement of quantum volume from 128 to 512 and a 10x improvement in Circuit Layer Operations Per Second (CLOPS) from 1,400 to 15,000 — beating our goal of 10,000 CLOPS.

We also showcased the IBM Quantum System Two, a newly designed "quantum-centric supercomputer," that is going to be the path for how we go from the noisy, small-scale quantum devices of today to the thousands and eventually million-plus qubit systems of the future. See here for more on IBM Quantum System Two.

Working with our partners, working groups, opensource and researcher programs, we've seen over 1,700 papers published using IBM Quantum and Qiskit technology in areas including chemistry, finance, and machine learning. For example, our partners in finance are exploring how quantum computers could help solve risk analysis, and options pricing problems. Quantum could also help cut through the complexity of today's trading environments. Using combinatorial optimization, quantum could help investment managers improve portfolio diversification, and rebalance portfolio investments to more-precisely respond to market conditions and investor goals.

Q: What are the remaining hurdles to achieving quantum advantage?

Dr. Gil: Quantum computers are not a replacement for classical ones. But we know that certain problems exist that classical computers will never solve. This is why we need to reach Quantum Advantage: when quantum computers are either cheaper, faster, or more accurate than classical computers at the same practical task. To deliver on the promise of Quantum Advantage, we're committed to improving three critical quantum system attributes: scale, quality, and speed.

We are rapidly scaling the number of qubits in our systems, as evidenced by the launch of Osprey, and our plans to deploy a processor with more than 1,000 qubits in 2023, when we believe it will be possible to explore applications with a Quantum Advantage. Beyond 2023, we are preparing modular, interconnected systems — quantum datacenters — for processors with millions of qubits as exhibited by our design for IBM Quantum System Two.

The quality, or how accurately a quantum computer's qubits process information, is also doubling every year. This is obviously a critical element to the interpretation of the results from quantum computing experiments. But quantum computing must also be able to complete this useful, practical work in a reasonable amount of time.

We are committed to improving these three attributes, in parallel, with the goal of finding practical quantum computing use cases.

Q: Where will quantum computing be by the end of the decade?

Dr. Gil: Innovation alone can't unlock the full potential of quantum computing. At IBM, we see the continued, rapid growth of a global ecosystem — from individual students, scientists, developers, and engineers, to organizations and institutions — being the key to making the leap into the second half of the decade that explores and develops applications in new materials, drug discovery, supply chain and macroeconomic optimization, and more. And it will all be done over the cloud on multiple, interconnected systems with millions of qubits, and frictionless, open developer tools.

The end of the Quantum Decade will look nothing like the beginning. We'll be working with quantum processors with thousands of qubits; we'll have a whole workforce with years of experience in quantum, and enterprises will have seen the payoff of quantum. Any technology leader who isn't actively building quantum into their plans risks being left behind.

Industry Impact

As we discussed previously, quantum computing is expected to surpass the capabilities of its classical counterpart in four main areas: optimization, machine learning, simulation, and cryptography. With these anticipated areas of quantum advantage, quantum computers are likely to bring disruptive changes to many industries.

A survey conducted by the National Quantum Computing Centre (NQCC) and EY in the UK investigated the views of senior corporate executives on the ability of quantum computing to disrupt their sectors. The NQCC found that, in the UK, almost all (97%) of the 501 executives surveyed expected quantum computing to disrupt their sectors to a moderate or high extent. Furthermore, nearly half (48%) of the respondents reported thinking quantum computing will play an important role in their organizations by as early as 2025. To address this, most respondents said that their firms will be taking concrete steps within the next one to two years to prepare.[24]

It is important to be aware of the practical opportunities and risks quantum computing poses to each industry. As such, in this chapter, we look at some quantum computing use cases in a few select industries including:

- Manufacturing and Logistics
- Artificial Intelligence
- Healthcare
- Energy and Climate
- Finance
- Cybersecurity
- Cryptocurrency

[24] EY, 81% of UK Business Leaders Expect Industry Disruption From Quantum Computing By 2030, According To EY Study," June 15, 2022.

Manufacturing and Logistics

The Fourth Industrial Revolution (Industry 4.0) Is Already Here

Manufacturing and logistics are widely considered to be among the main early beneficiaries of quantum computing. The entire supply chain has already entered a new era, Industry 4.0, where an intelligent network of machines and processes is adopted for industrial productions with the help of sensor, computing, and communication technologies.[25] We have seen an increasing adoption of cyber-physical systems (CPS), the industrial Internet-of-Things (IIoT), cloud computing, robotics, and artificial intelligence (AI) in smart factories.

Consequently, the datasets these systems are built upon are expanding rapidly in both size and complexity, bringing about challenges to the processing power of our current classical computers.[26] Quantum computing may offer solutions to these challenges and potentially open the door to a further transition from Industry 4.0 to an even more interconnected Industry 5.0.

Material Discovery

New materials are regularly discovered in the pursuit of producing better quality goods that are lighter, stronger, or cheaper. However, despite all our current industrial manufacturing processes, nature still produces numerous superior materials. For instance, the teeth of limpets, a type of aquatic snail, can be 13 times as strong as ordinary steel and are produced at limpets' body temperature, rather than the extremely high temperatures and pressures required by many industrial production processes.[27] Unfortunately, today's classical computers struggle to model even moderately sized molecules (with the accuracy needed to know how to recreate them), let alone large-molecule mineral-protein composites like limpet teeth.

One day, quantum computing may bridge this gap and enable the comprehensive modeling of sophisticated molecules, dramatically benefitting material discovery. Once quantum computing's anticipated advantages in molecular simulation become mature enough, manufacturing within various sectors, including automotive, airline, electronics, and military, could benefit from:[28]

- Materials with both lighter weight and higher strength.
- Batteries with higher efficiency and more durable storage capacity.[29]
- Catalysts with higher efficiency in fueling various industrial production processes.

---

[25] Thomas Philbeck and Nicholas Davis, "The Fourth Industrial Revolution," *Journal of International Affairs*, Vol. 72, No. 1, Fall 2018.
[26] David Reinsel, John Gantz, and John Rydning, *Data Age 2025: The Digitization of the World: From Edge to Core*, IDC (sponsored by Seagate), November 2018.
[27] John H. Lienhard, "Engines of Our Ingenuity No. 2996: Tensile Strength & Limpet Teeth," University of Houston, accessed April 5, 2023.
[28] Rhys Blakely, "Ministry of Defence to Develop Quantum Computer for Use on Battlefields," *The Times of London*, June 9, 2022; Masoud Mohseni et al., "Commercialize Quantum Technologies in Five Years," *Nature*, Vol. 543, No. 171-174, March 2017.
[29] Jeannette Garcia, "IBM and Daimler Use Quantum Computer to Develop Next-Gen Batteries," IBM, January 8, 2020.

Production Processes

As production processes become more digitalized in the era of Industry 4.0, quantum computing could in many ways help enable better and more efficient decision making.

One such area is that of "digital twins," or virtual simulations of products or system lifecycles that can be updated with real-time data. Although the use of digital twins has already proven to be an efficient tool for component testing and production processes, quantum digital twins could enhance production controls by enabling the visualization of real-time information on product quality in an intuitive form, while dramatically lowering simulation costs.[30] Quantum digital twins could also offer significant performance gains in testing simulations, enabling them to find the most optimal strategies in the shortest time.[31]

Other areas in which quantum computing shows promising potential to increase efficiency include:[32]

- Predicting customer requirements and demands based on complex data-driven simulations.
- Optimizing production targets in real time.
- Managing Automated Guided Vehicle (AGV) and Autonomous Intelligent Vehicle (AIV) fleets in factories.

Supply Chains

Global supply chains are sometimes not as agile as we expect them to be. World events ranging from the Suez Canal blockage to the COVID-19 pandemic have shown how susceptible our supply chain and logistics systems are to sudden changes in consumer and business demand, raw material availability, and shipping and distribution channels.

Most logistics systems are essentially optimization problems. When these optimization problems are applied to the real world, we find that actual situations become exponentially more complex for every extra variable involved. For example, introducing additional vehicles, routes, or drivers in a logistics system.[33] Moreover, as we head further into Industry 4.0, supply chains have become more digitalized and interconnected.

---

[30] C.K. Lo, C.H. Chen, and Ray Y. Zhong, "A Review of Digital Twin in Product Design and Development," *Advanced Engineering Informatics*, Vol. 48, No. 101297, April 2021; Javier Villalba-Diez et al., "Integration of Quantum Simulation on a CNC Machine for In-Process Control Visualization," *Sensors*, Vol. 21, No. 15, July 2021.

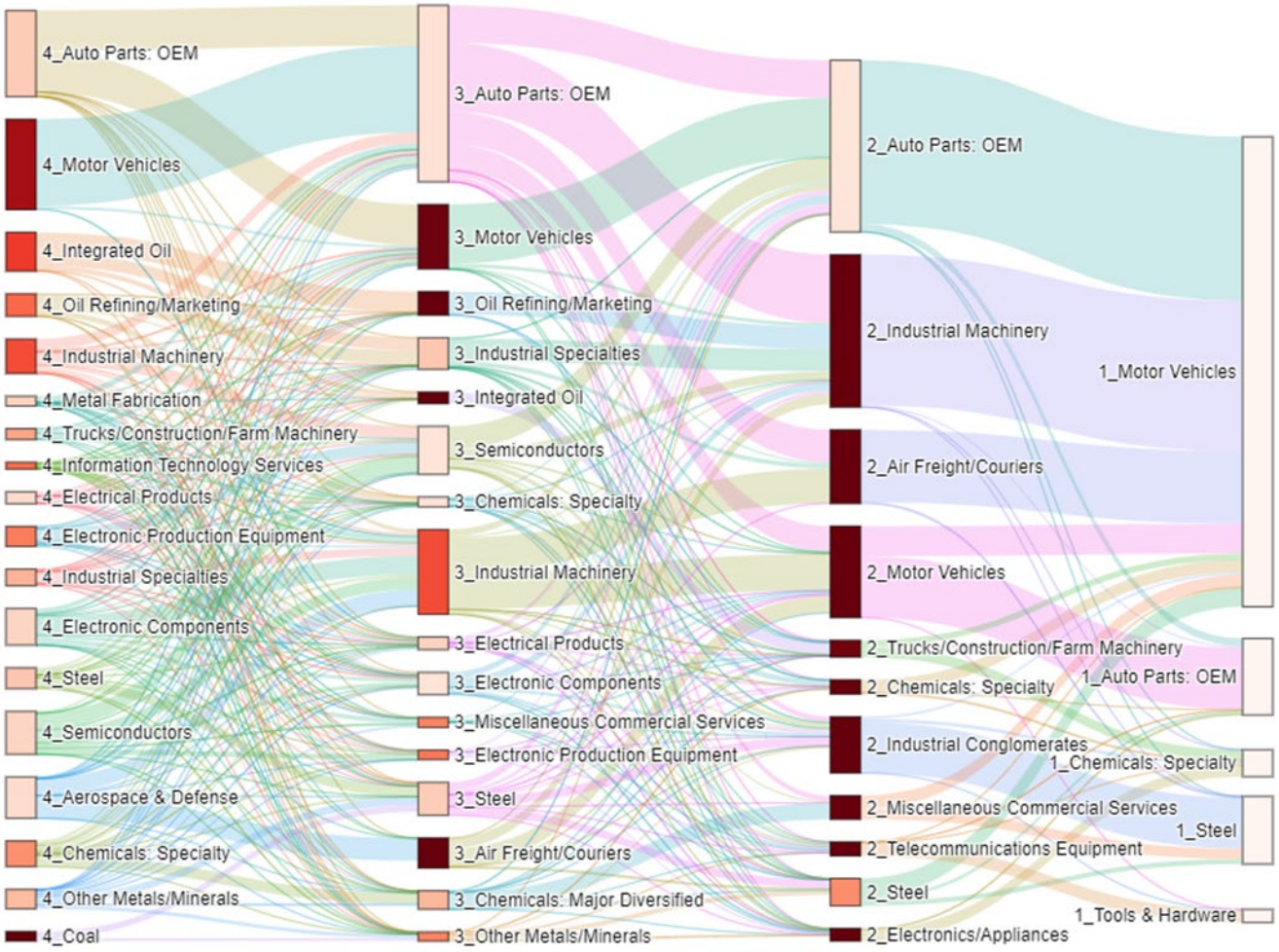
[31] Samir Khan et al., "On the Requirements of Digital Twin-Driven Autonomous Maintenance," *Annual Reviews in Control*, Vol. 50, No. 13-28, August 2020.

[32] Tim van Erp and Bartłomiej Gładysz, "Quantum Technologies in Manufacturing Systems: Perspectives for Application and Sustainable Development," Procedia CIRP, Vol. 101, No. 1120-1125, 2022.

[33] Robert Liscouski, "How Quantum Computing Will Power the Future of Logistics," SupplyChainBrain, August 8, 2021.

Increasing data visibility has driven supply chains to shift from a relatively static model (with infrequent data updates) to a more flexible model continuously updated by real-time market supply and demand data. (See our Citi GPS report *Global Supply Chains: The Complicated Road Back to "Normal"* for more details.) Fundamentally, modern supply chains are immensely complex, as shown in Figure 17 below.

Figure 17. Supply Chain Dependency Analysis — Industrials



Source: Bloomberg, Citi Global Data Insights, Citi GPS

There are a number of promising applications of quantum computing in logistics, such as traffic optimization to ease road congestion in real time. Quantum-optimized supply chains could even bring environmental benefits, as transportation accounts for 27% of all greenhouse gas emissions.[34]

We spoke to Dr. Alan Baratz, CEO of D-Wave, a quantum computing company building both quantum annealing and gate-based quantum computers, about the impact quantum computing may have on the manufacturing and logistics industry.

[34] United States Environmental Protection Agency, "Carbon Pollution from Transportation," accessed April 5, 2023.

Expert Interview with Dr. Alan Baratz, CEO of D-Wave

Dr. Alan Baratz
CEO, D-Wave

Q: Why do you feel that quantum computing has potential in manufacturing and logistics?

Dr. Baratz: Quantum computing is a technology that today is already demonstrating business value for manufacturing and logistics, specifically around the many complex optimization problems native in these industries. Quantum computing uses quantum mechanical effects to solve hard problems more quickly, more efficiently, or in some instances, for the first time. This means that quantum computing's primary value is in revenue generation and/or cost savings. With the dynamism of Industry 4.0, leaders in manufacturing and logistics are looking for innovative new ways to harness technology to deliver upon those benefits. And these leaders are beginning to see the impact of quantum computing and quantum hybrid (which combines both classical and quantum) today. Whether in autonomous vehicles used in factory floor automation, paint shop scheduling, or bin packing, quantum computing has far-reaching impact.

Q: Could you elaborate on some of the optimization problems that D-Wave is looking at applying quantum computing to?

Dr. Baratz: D-Wave's annealing quantum computers are designed specifically for optimization. And recent research suggests that because of the pre-processing overhead of gate-model quantum computers, annealing quantum computers will always be the best option for complex optimization problems. There are other use cases in material and drug discovery and manufacturing that will require gate-model quantum computers. This is why we announced last year that we are the only company building both annealing and gate-model quantum computers. Think about the value to manufacturing: longer-term, new metamaterials will be designed with gate-model systems, while today and tomorrow factory automation improvements, product customization, and optimized supply chains will deliver both existing and new products to market more efficiently using quantum annealing.

Q: What do you see as the biggest barrier facing quantum adoption in manufacturing and logistics?

Dr. Baratz: The biggest barrier, until recently, was the size of the systems. At D-Wave, we've not only commercialized a 5000+ qubit system, but we've also brought quantum hybrid computing to market. By using quantum and classical approaches, business can now run problems up to 1 million variables. This unlocks an entirely new set of potential use cases in manufacturing and logistics.

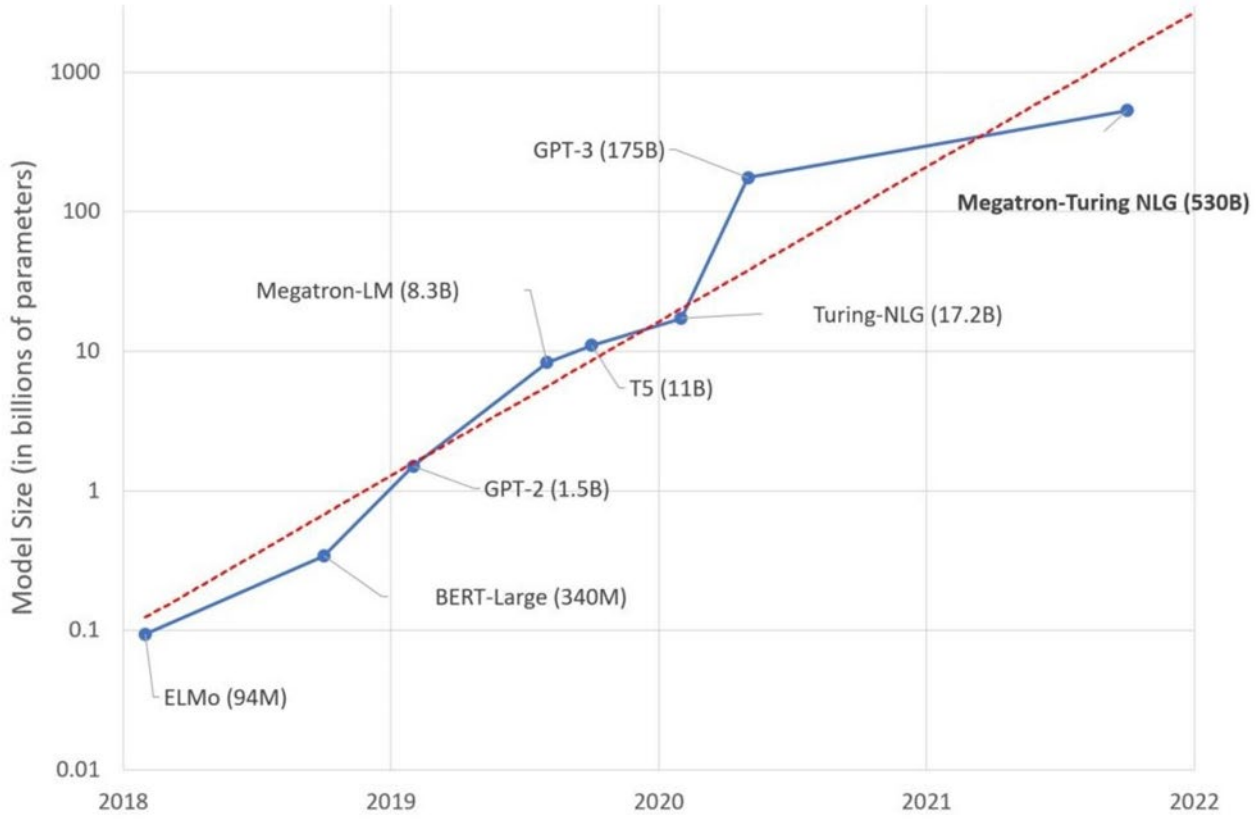
Artificial Intelligence

AI Has Become Ubiquitous, but Is Still a Half-Finished Technology

Artificial intelligence (AI) has been adopted in a variety of sectors to deliver solutions and improve efficiency, but it is still a half-finished technology. The ultimate form of AI, artificial general intelligence, should in principle be able to learn anything.[35] The capabilities of AI, however, are largely restricted by the computing power currently available. With the lowest-priced GPU cloud on the market, it would take 355 years and an electricity bill of around $4.6 million to train GPT-3 (an AI-based language model) to produce human-like text.[36] With Moore's Law under pressure in recent years, training larger language models will likely become an even more difficult task for classical computers.

We investigate how quantum computing will potentially be able to enhance AI capabilities through two examples: natural language processing and artificial neural networking.

Figure 18. Exponential Growth of the Number of Parameters in NLP Models



Source: Microsoft Research

[35] Peter Voss, *Essentials of General Intelligence: The Direct Path to Artificial General Intelligence* (Berlin: Springer, 2007), 131-157.
[36] Chuan Li, "OpenAI's GPT-3 Language Model: A Technical Overview," Lambda Labs, June 3, 2020.

Natural Language Processing

To achieve artificial general intelligence, machines must be able to understand and respond to humans. However, equipping them with advanced linguistic systems is difficult, as human language is filled with ambiguities and irregularities like homophones, sarcasm, idioms, and metaphors.[37] Natural language processing provides a way to overcome this challenge through machine learning. It enables computer systems to translate text, provide more relevant research results, and even talk to us. Most people have probably already interacted with natural language processing applications like Amazon's Alexa, Apple's Siri, Google's voice input search, or ChatGPT on Microsoft's Bing platform.

Impressive as state-of-the-art natural language processing systems like ChatGPT-3 and ChatGPT-4 are, we are still far from achieving artificial general intelligence. Natural language processing algorithms can only understand individual words, and the meanings of sentences and paragraphs have to be inferred through some kind of "black box."

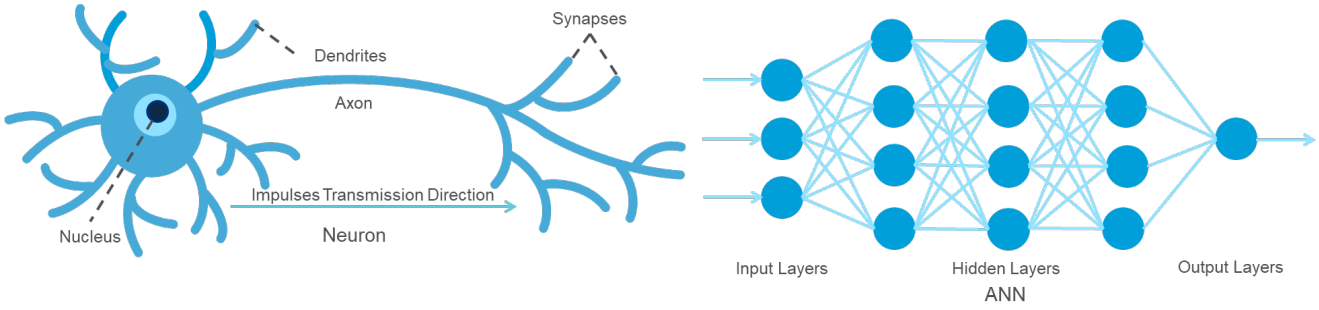
According to Bob Coecke, Chief Scientist at Quantinuum, AI could become "meaning-aware" for the first time through quantum computing. This means that instead of the risk of having everything taking place inside a black box, the flows of meanings in quantum natural language processing are more clearly exposed and understood. This is a completely novel approach that leverages the probabilistic nature of quantum computing to better resemble how human language works.[38]

At present, quantum natural language processing research is still largely at the stage of exploring and establishing theoretical foundations, and it will likely take several years before it becomes ready for wide adoption.

Artificial Neural Networks

Enabling AI to recognize patterns like images and correlations is another challenge to achieving artificial general intelligence. One of the best-performing machine learning models for this is the artificial neural network, an algorithmic mimicry of the biological neural network in our brains.

Figure 19. Layers of Biological Neurons (Left) and Layers of Artificial Neurons (Right)



Source: Citi GPS

[37] IBM, "What Is Natural Language Processing (NLP)?," accessed April 5, 2023.
[38] Bob Coecke et al., *Foundations for Near-Term Quantum Natural Language Processing*, Cambridge Quantum Computing Ltd. and Oxford University Department of Computer Science, December 8, 2020.

Demand for more human-like AI is driving up the size of training data sets. IDC predicts that worldwide data will grow from 33 ZB (ZettaBytes) in 2018 to 175 ZB by 2025.[39] Eventually, even supercomputers are likely to be overwhelmed with the amount of data generated.[40] It has been proposed that fault-tolerant quantum computers will in theory be capable of solving certain machine learning problems, such as those solved by artificial neural networks, faster than classical computers.[41]

We spoke to Rob Hays, CEO at Atom Computing, who explained:

"It's been 10 years since the first paper was published on using GPUs for 'ImageNet Classification with Deep Convolutional Neural Networks.' While that wasn't the first time a GPU was used in machine learning, the combination of highly-parallel GPU hardware + neural network software architecture + a compelling use case in image recognition marked an inflection point in the growth of AI. Quantum computers have the potential to offer a similar inflection point in AI computing performance. Working in conjunction with classical CPU + GPU systems, the inherent nature of quantum computing systems will allow AI applications to take in more complex environmental factors to simulate chemical and sub-atomic physical systems with a speed and cost that isn't practical today. This will unlock layers of complexity and natural world simulations that aren't possible or practical today. Expanding the physical world accuracy of AI will enable applications for improved materials development, medical applications, complex system optimization, and others."

Similar to quantum natural language processing, quantum neural networking is still in its infancy. Many proposals and ideas have been forwarded regarding the optimal structure and training of a quantum neural network to best utilize a quantum computer's potential.[42] As we continue to scale on the hardware side, quantum neural networking is likely to become more relevant.

We spoke to Jack Hidary, CEO of SandboxAQ, an enterprise SaaS company looking at the convergence of AI and quantum technologies, about the impact quantum computing may have on AI.

---

[39] David Reinsel, John Gantz, and John Rydning, *Data Age 2025: The Evolution of Data to Life-Critical: Don't Focus on Big Data, Focus on the Data That's Big*, IDC (sponsored by Seagate), April 2017.

[40] Avinash Chalumuri, Raghavendra Kune, and B.S. Manoj, "Training an Artificial Neural Network Using Qubits as Artificial Neurons," *Procedia Computer Science*, Vol. 171, No. 568-575, 2020.

[41] Jacob Biamonte et al., "Quantum Machine Learning," downloaded from arXiv, PDF, May 10, 2018; Srinivasan Arunachalam and Ronald de Wolf, "A Survey of Quantum Learning Theory," downloaded from arXiv, PDF, July 28, 2017.

[42] Stefano Mangini et al., "Quantum Computing Models for Artificial Neural Networks," downloaded from arXiv, PDF, May 20, 2021; Bob Ricks and Dan Ventura, "Training a Quantum Neural Network," Brigham Young University Department of Computer Science, accessed April 5, 2023.

Expert Interview with Jack Hidary, CEO of SandboxAQ

Jack Hidary
CEO, SandboxAQ

Q: Why do you feel that quantum computing has potential in artificial intelligence?

Jack: Quantum and AI are synergistic technologies. AI is at its best when we can train it on large amounts of data, but when we look at a novel drug candidate, for example, there is no big data. In these cases, we build up a new data set using the quantum equations governing atomic interactions and then apply AI to that new data to optimize for the best molecular structure to hit that condition.

Q: Could you elaborate on some challenges within artificial intelligence that SandboxAQ is looking at applying quantum computing to?

Jack: One area where AI and quantum approaches are having great success is in drug discovery – developing treatments for conditions such as brain cancer or Alzheimer's disease, two conditions which have stymied researchers for decades.

When you develop a novel drug, there is little data available, so AI by itself is not as effective. With large-scale quantum simulation, we can examine the interactions between chemical compounds and human receptors at the molecular level millions of times in silico, and optimize the chemical structure using AI. This greatly accelerates drug development, lowers R&D costs and reduces risk as the drug candidate enters clinical trials.

Q: What do you see as the biggest barrier facing quantum adoption in artificial intelligence?

Jack: More and more powerful GPUs are driving the advances we see in AI today. Chips from Nvidia, Alphabet and other companies are giving us unprecedented ability to build larger and larger AI models. However, as the chip industry faces increased challenges in developing chips with even higher density of transistors due to quantum limits, quantum computing will enter the picture. We foresee hybridized classical-quantum computing as a way forward in creating more capable AI models. The field of Quantum Machine Learning (QML) is at an early phase, but picking up momentum. As quantum computers scale further and we can implement error correction on qubits, we will see QML become a powerful tool in the AI toolchest.

Healthcare

A Potential Big Leap Forward

For the healthcare industry — long beset by inefficiencies and bottlenecks — quantum computing could offer a big leap forward. The reason: with their anticipated advantages in optimization, machine learning, and molecular simulation, quantum computers are expected to provide the computational toolkit required to solve some of healthcare's most entrenched problems. As discussed below, this has the potential to bring changes to the twin pillars of healthcare: drug discovery and medical services.

Drug Discovery

Drug research and development are essentially chemistry problems characterized by high failure rates, high R&D costs, and long development cycles. As the next generation of computing, quantum computing could become the main driver for new drug discovery. This is because drug molecules are quantum mechanical systems themselves, meaning that quantum computers are inherently more suitable to predict and simulate them than classical computers. More specifically, quantum computing may help:[43]

- Model three-dimensional (3D) protein-folding structures in structure-based drug discovery.
- Assess the synthesizability of a drug candidate more effectively in *de novo* discovery.
- Predict the interaction of a drug candidate with multiple biological targets to provide clues into toxicity, pharmacokinetics, and multitarget action.

These improvements could enable more effective and flexible computer-assisted drug discovery tools, and thus reduce failure rates and costs. In the long run, quantum computers may be able to expand current drug candidate libraries to include macromolecules with complex 3D folding structures like proteins rather than just small molecules. With direct hypothesis testing that helps better understand the relationships between overall molecule structures and their specific medical properties, quantum computers could possibly bring a paradigm-shifting change in drug R&D — ultimately, introducing a new era of simulation-based drug discovery.

Medical Services

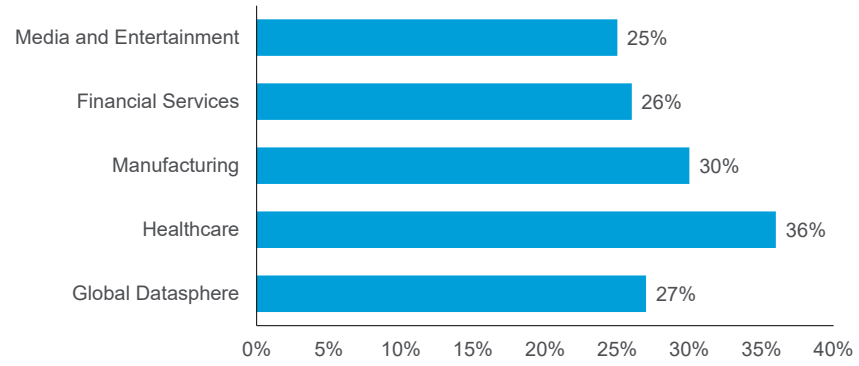
The amount of data collected by companies that provide medical services is exploding. Healthcare data is expected to grow at a compound annual growth rate (CAGR) of 36% through to 2025.[44] The rapid increase in data volume is a result of advancements in medical imaging and the increasing availability of real-time data from continuous health monitoring.

---

[43] Yuan Cao, Jacquiline Romero, and Alan Aspuru-Guzik, "Potential of Quantum Computing for Drug Discovery," *IBM Journal of Research and Development*, Vol. 62, No. 6, November 2018.

[44] David Reinsel, John Gantz, and John Rydning, *Data Age 2025: The Digitization of the World: From Edge to Core*, IDC (sponsored by Seagate), November 2018; Jessica Kent, "Big Data to See Explosive Growth, Challenging Healthcare Organizations," Health IT Analytics, December 3, 2018.

Figure 20. 2018-25 Data Growth CAGR Across Various Industries



Source: IDC

On the one hand, big data is a powerful tool if properly used. On the other hand, such an explosion of data also raises tough challenges for current data management systems. One recent report estimated that 99% of the data we generate is not analyzed, and of the 1% that is, this is mostly done in a discrete and shallow manner.[45]

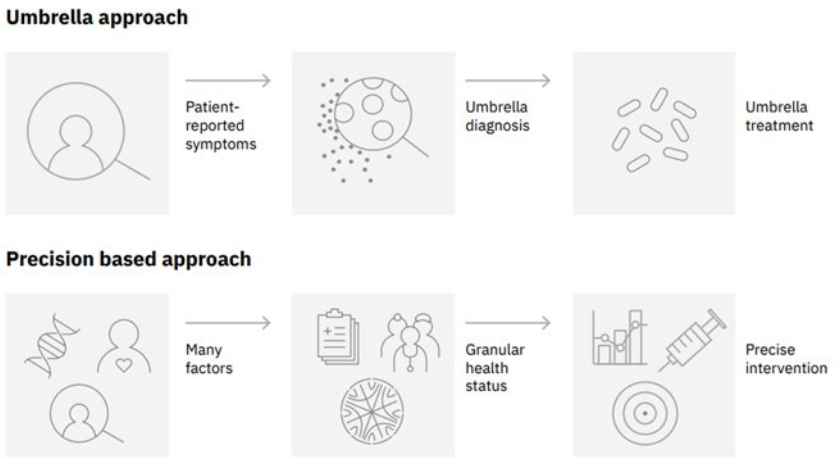
Quantum computing could help address this challenge and lead to:

- **Better Diagnoses:** Care providers may be able to make earlier, more accurate, and faster diagnoses — ultimately saving lives.[46] With improved data processing capabilities, care providers may be able to continuously monitor more physical indicators for our health and raise the alarm much earlier when something goes wrong. This could enable preventative analysis to become more predictive, helping providers determine in advance which procedure should be performed at what time.[47] Furthermore, quantum computers may even bring diagnostic procedures down to a cellular level, and for example, be used to detect cancer cells more accurately.[48]

[45] Nicolaus Henke, Ari Libarikian, and Bill Wiseman, "Straight Talk About Big Data," *McKinsey Quarterly*, October 28, 2016.
[46] Rishabha Malviya and Sonali Sundram, "Exploring Potential of Quantum Computing in Creating Smart Healthcare," *The Open Biology Journal*, Vol. 9, No. 56-57, September 2021.
[47] Devansh Mehta, "Quantum Computing Will Completely Change the Healthcare Infrastructure to New Level and Help Transform the Healthcare From Preventive To Predictive Healthcare: A Future Perspective," *Journal of Bio Innovation*, Vol. 9, No. 6, November 2020.
[48] Nilima Mishra et al., "Cancer Detection Using Quantum Neural Networks: A Demonstration on a Quantum Computer," downloaded from arXiv, PDF, November 1, 2019.

- **Tailored Treatment:** In the future, quantum computers could potentially enable a better and more detailed understanding of personal illness and deliver precision medicine that accounts for the patient's age, race, gender, and genetic makeup, among other factors.[49] This would be an improvement over the current umbrella approach, whereby diagnosis and treatment are based heavily on patient-reported symptoms. As such, the current approach fails to provide personalized medical actions at the individual level.[50] This is important because current medical care itself only contributes 10%-20% towards final patient outcomes today, while health-related behaviors, socioeconomic factors, and environmental aspects account for the rest.[51]

Figure 21. Umbrella Diagnosis vs. Precision-Based Diagnosis



Source: IBM

- **Enhanced Insurance Risk Assessments and Fraud Detection:** Quantum computers are expected to enable more granular modeling for insurance premium calculations, significantly improving the accuracy of individual health plan pricing, as well as likely reducing premiums.[52] In addition, the anticipated superior machine learning capacity of quantum computers is expected to help spot fraudulent medical claims and abnormal behavior accurately, lowering premiums further.[53]

We spoke to Peter Chapman, CEO of IonQ, which builds quantum computers based on trapped ion qubit technology, about the impact quantum computing may have on the healthcare industry.

[49] Rishabha Malviya and Sonali Sundram, "Exploring Potential of Quantum Computing in Creating Smart Healthcare," *The Open Biology Journal*, Vol. 9, No. 56-57, September 2021.
[50] IBM, *Exploring Quantum Computing Use Cases for Healthcare*, June 2020.
[51] Carlyn M. Hood et al. "Relationships Between Determinant Factors and Health Outcomes," *American Journal of Preventive Health Medicine*, Vol. 50, No. 2, February 2016.
[52] IBM, *Exploring Quantum Computing Use Cases for Healthcare*, June 2020.
[53] Ibid.

Expert Interview with Peter Chapman, CEO of IonQ

Peter Chapman
CEO, IonQ

Q: Why do you feel that quantum computing has potential in healthcare?

Peter: Quantum computers were originally envisioned to help solve hard chemistry problems — and there are few harder than understanding the human body and its many systems. As quantum computers become more accessible and more powerful, healthcare providers start to envision tackling increasingly ambitious problems from a genuine understanding of our bodies' biochemistry.

Whether it's simulating complex compounds for a new drug, identifying more effective therapies, or gaining an overall better understanding of how one treatment impacts another, quantum computers offer the greatest potential of upending the status quo and delivering more personalized, effective care to patients around the world.

Q: Could you elaborate on some challenges within healthcare that IonQ is looking at applying quantum computing to?

Peter: On average, it takes several years and billions of dollars to take a new drug from the lab to the marketplace, with years of R&D effort required before a candidate molecule even makes it into clinical trials. Quantum computing has the potential to expedite the entire process by simulating chemical reactions via software instead of in the lab.

In drug development, for example, scientists must first identify molecules with a set of desired properties, such as the ability to bind with specific proteins. While much of this work is already computer-assisted, extensive lab work is still required to fully understand candidate molecules, with many cycles of synthesis and testing required to find a suitable candidate. Quantum computers could quickly screen billions of molecules to identify suitable candidates for clinical trials, skipping the process of identifying what works or doesn't work earlier on, improving the cost and speed of development, increasing the likelihood of success, and improving the most important thing of all: patient outcomes.

Energy and Climate

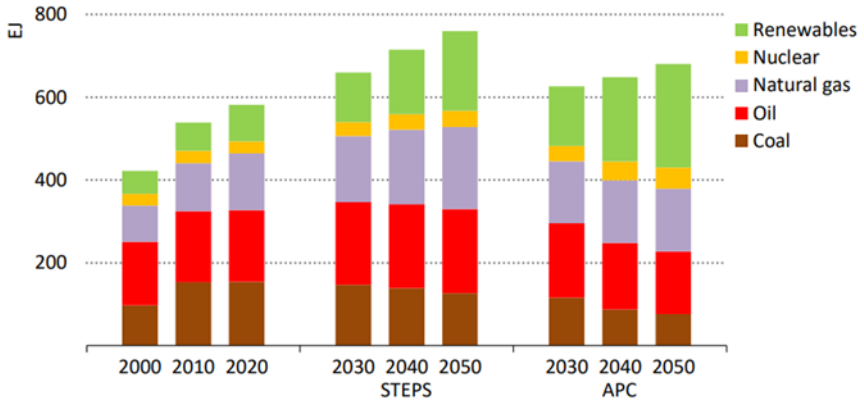
The Ability to Reduce Carbon Emissions

The energy and climate sectors are well poised to take advantage of quantum computing's future capabilities, especially in the areas of molecular simulation and optimization. One recent report claims that quantum-based climate technologies could help us avoid 7 gigatons of carbon emissions every year by 2035. This equates to around 20% of global carbon emissions today, and thus could contribute a great deal to achieving net-zero targets.[54]

Energy

Although the world has seen increased adoption of renewable energy, fossil fuels are still the primary source of the world's energy use, contributing to over 60% of global energy generation for the past decade.[55]

Figure 22. Global Energy Generation by Scenario



Source IEA (2021) Net Zero by 2050: A Roadmap for the Global Energy Sector. All Rights Reserved.

In the future, quantum computing could benefit various energy sectors in different ways, including:

- **Oil:** Improving identification of potential crude oil reservoirs by simulating the interactions of crude oil, water, and gas molecules with the surface of rocks.
- **Green Hydrogen:** Developing new catalysts for water electrolysis, which could make green hydrogen economically viable and encourage wider adoption. One report estimated that quantum computing has the potential to bring down the cost of green hydrogen by 60% (from $3/kg-$6.5/kg to $1.2/kg-$2.6/kg).[56]

[54] Peter Cooper, Philipp Ernst, Dieter Kiewell, and Dickon Pinner, "Quantum Computing Just Might Save the Planet," McKinsey, May 19, 2022.
[55] International Energy Agency (IEA), *World Energy Outlook*, November 2019.
[56] Peter Cooper, Philipp Ernst, Dieter Kiewell, and Dickon Pinner, "Quantum Computing Just Might Save the Planet," McKinsey, May 19, 2022; Tom DiChristopher, "Experts Explain Why Green Hydrogen Costs Have Fallen and Will Keep Falling," S&P Global, March 5, 2021.

-

- **Energy Storage:** Simulating the complicated chemistry of prototype battery designs and accelerating the development process. Durable and efficient battery technology is essential to the large-scale adoption of renewables, as most sources of renewable energy cannot continuously generate electricity. However, battery technology is only incrementally improving nowadays, with an approximate 5% improvement in efficiency every year.[57]

Agriculture

Nearly all fertilizers that help feed us today are made from ammonia, and about 50% of the world's food production relies on these fertilizers.[58] However, the most commonly utilized ammonia production process today, the Haber-Bosch process, dates back to the 1910s and requires stringent conditions, including very high pressures and temperatures. The ability to produce ammonia in a more efficient and environmentally friendly way could result in both cheaper and less energy-intensive fertilizers.

As quantum computers' anticipated ability to simulate the quantum properties of molecules increases, it may eventually become possible to identify and produce the enzyme that catalyzes ammonia synthetization at a large scale.[59] Thus far, scientists have been unable to reproduce this enzyme, as the chemical composition of soil is particularly complicated, and the current computational power of classical computers is insufficient to run the simulations needed to determine the enzyme.

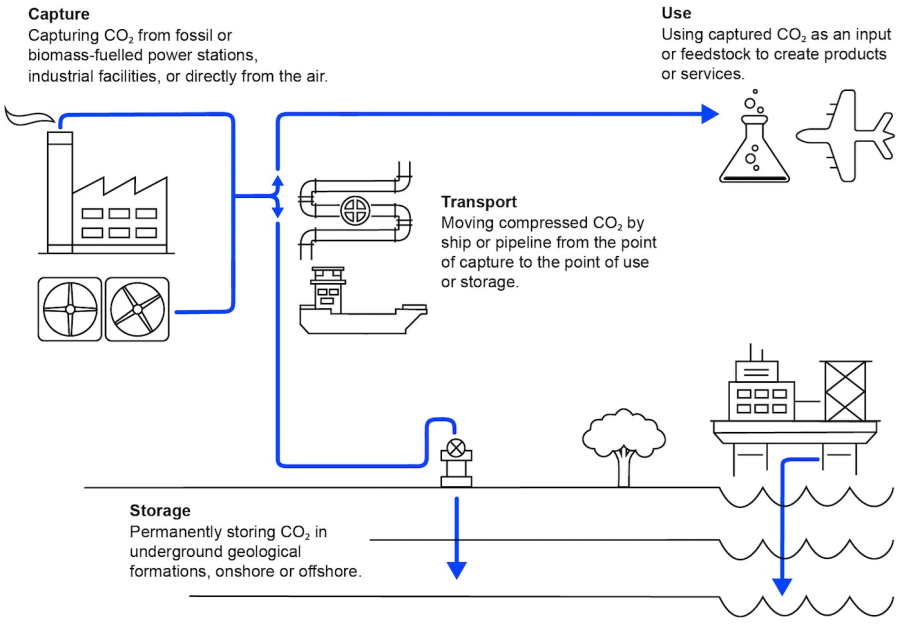
Climate Change

Quantum computers could also have an impact in carbon capture, utilization, and storage (CCUS), which, according to the International Energy Authority (IEA), is expected to make up 50% of heavy industry's emission reductions by 2050.[60]

---

[57] Scott K. Johnson, "Eternally Five Years Away? No, Batteries Are Improving Under Your Nose," *Ars Technica*, May 24, 2021.
[58] Leigh Krietsch Boerner, "Industrial Ammonia Production Emits More CO2 Than Any Other Chemical-Making Reaction. Chemists Want to Change That," *Chemical & Engineering News*, June 15, 2019.
[59] Sebastian Jeon, "Feeding the World with Die Rolls: Potential Applications of Quantum Computing," *Dartmouth Undergraduate Journal of Science*, Vol. 20, No. 1, 2017.
[60] Amy Flower, "How Quantum Computing Can Help Tackle Climate Change," Riverlane, November 4, 2021.

Figure 23. The CCUS Value Chain



Source: IEA (2020) CCUS in Clean Energy Transitions. All Rights Reserved.

Today, most CO_2 reduction processes are quite expensive, in part due to the involvement of precious metals. In the best-case scenario, one gram of a metal catalyst could capture 100 grams of carbon-dioxide emissions.[61] This means that a 1% reduction in global emission would require 3.63 million metric tons of this metal catalyst.[62] Quantum computers could potentially leverage their advantage in simulation to help discover new catalysts for carbon capture to absorb carbon directly out of the air more efficiently. The captured CO_2 could then be used in the production of synthetic hydrocarbons, polymers, and building materials.[63] Such work is already taking place — for example, in 2020, one energy company already announced that it would be working with the company now known as Quantinuum to improve materials for CO_2 capture.

The simulation capabilities of quantum computing could also help us better understand the Earth's climate system and ultimately allow us to react to natural disasters more efficiently and accurately.[64] For example, by combining quantum and classical computing, Rigetti claims to have developed an effective way to produce high-quality synthetic weather radar data.[65]

We spoke to Rajeeb Hazra, CEO of Quantinuum, about the impact quantum computing may have on the energy and climate sectors.

[61] Katie Lamb, "Carbon Capture and Conversion Must Not Rely on Rare Metals," *Phys.org*, January 29, 2019.
[62] Ibid; IEA, "Global CO2 Emissions Rebounded to Their Highest Level in History in 2021," March 8, 2022.
[63] Alcimed, "CCUS technology: CO2 As a Resource or a Waste?," March 12, 2020.
[64] Manmeet Singh et al, "Quantum Artificial Intelligence for the Science of Climate Change," downloaded from arXiv, PDF, accessed April 6, 2023.
[65] Rigetti, Rigetti Enhances Predictive Weather Modeling with Quantum Machine Learning," December 1, 2021.

Rajeeb Hazra
CEO, Quantinuum

Expert Interview with Rajeeb Hazra, CEO of Quantinuum

Q: Why do you feel that quantum computing has potential in the energy and climate sectors?

Rajeeb: Quantum computing is a profoundly new and different technology, drawing on the laws of quantum mechanics to tackle certain computational tasks that would otherwise be intractable. The kinds of problems that quantum computing shows promise in tackling include modelling complex molecular or material systems, or optimizing industrial processes.

Q: Could you elaborate on some challenges within energy and climate that Quantinuum is looking at applying quantum computing to?

Rajeeb: There are many examples within energy and climate change where quantum computing appears to offer novel and extremely relevant solutions, for example, in areas such as low- or no-carbon energy production, in manufacturing, supply chain optimization and distribution, or researching scalable methods that could help to reverse historic atmospheric emissions. Quantum computing offers a path to the rapid and cost-effective development of new complex materials, which in turn may have many uses for energy production and climate change mitigation. Examples include the development of highly efficient photo-voltaic cells, or the discovery of highly efficient chemical processes to enhance the efficiency and performance of hydrogen fuel cells for electric vehicles (work we continue to do with major industrial players in automotive and aerospace).

Q: What do you see as the biggest barrier facing quantum adoption in the energy industry?

Rajeeb: Quantum computing is a complex and rapidly advancing technology. This presents two related challenges, hardware development, and identifying suitable use cases that could be amenable to a quantum speed-up. As we approach the period where quantum computing hardware offers a meaningful advantage over classical computers, large corporations will increasingly seek to work with full stack companies like Quantinuum to accelerate their quantum know-how, build out their quantum workflows, and position themselves to benefit from the first developments that offer a quantum advantage.

Q: Is quantum computing going to be good for improving battery technology?

Rajeeb: The evidence is very positive in this field. Quantinuum has collaborated with the DLR – the German national aeronautics and space research center – on a broad project to investigate the use of quantum algorithms to model battery cells. The project specifically looked at using Quantinuum's quantum algorithms for solving partial differential equations to render a simulation of a lithium-ion battery cell, a central use-case in this field. We have also supported global enterprise partners to explore today's quantum devices for simulating chemical reactions within both batteries and hydrogen fuel cells with our state-of-the-art quantum chemistry platform, InQuanto™.

Finance

Tackling Probabilities in a Data-Heavy Environment

Several financial services activities, from securities pricing to portfolio optimization, require the ability to assess a range of potential outcomes. For this, banks rely on algorithms and models to calculate statistical probabilities. However, today's data-heavy environment has led to the need for ever-more powerful computers to calculate probabilities accurately. Therefore, the opportunity for quantum computing and its potential performance gap with classical computing methods keeps growing.

Quantum computing is still an emerging technology, and its use cases in finance have been an active area of experimental research and development. While several use cases are still in the proof-of-concept stage, we are seeing the emergence of a few practical applications. We believe quantum computing in finance could open up a range of compliance improvements, efficiencies, and new market opportunities. We list below some of the promising future applications.

Targeting and Prediction

Quantum computing could help overcome the limitations of existing analytical models to sift through large amounts of behavioral data. This may enable financial institutions to offer more personalized products and services to the right customers in real-time, resulting in greater revenue opportunities.

Quantum computers could also prove superior in finding patterns, performing classifications, and making predictions that are often not possible today due to complex and siloed data structures. Banks with large client databases could particularly benefit from the use of improved searching algorithms.

Using quantum computers to optimize loan portfolios focusing on collateral could also allow financial institutions to improve their offerings, possibly lowering interest rates and freeing up capital. For instance, banks may be able to offer more targeted products and services to their customers based on purchasing trends, preferences, and demographics. This could also help banks selectively tap into the underbanked small and medium-sized enterprise (SME) market.

Portfolio Optimization

An important aspect of the financial industry relates to the pricing of financial instruments and estimating their risk. Regulators also require banks to perform various stress tests in order to hold adequate capital depending on their risk-weighted assets. Analytical models may often be too simplistic to capture the complex dependencies between different elements, which may otherwise require extensive computational power.

Quantum machine learning is expected to help enhance robo-advisory capabilities and trading algorithms. It could also optimize collateral management across exchanges and currencies, facilitate dynamic arbitrage (for example, in cross-currency debt or cryptocurrency markets), and enable combinatorial and convex portfolio optimization methods.

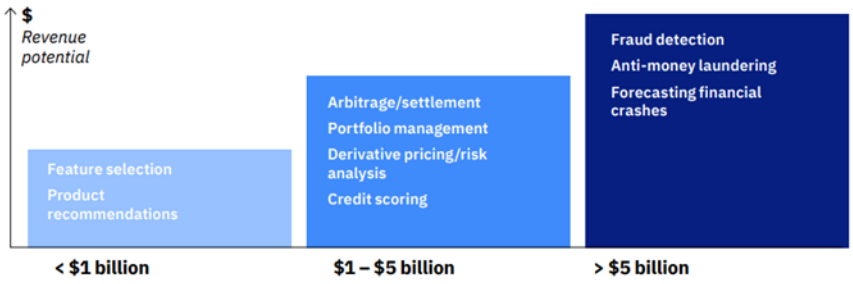
Improving computation speed in certain tasks could also reduce complexity in traditional environments, including settlement processes, associated capital requirements, systemic risk, and operational costs. Quantum computing could help optimize trade settlement from once-a-day cycles to more frequent intraday cycles. Many banks are exploring the use of quantum computing for trading strategies, portfolio optimization, asset pricing, and risk analysis.

Risk Management and Fraud Detection

Risk management plays a central role in the financial sector and includes aspects such as credit risk, liquidity risk, and market risk, which are often estimated using models. Quantum computers are expected to help build models incorporating a large number of variables to create comprehensive risk profiles and facilitate better decision making, as well as providing a significant increase in speed over established classical algorithms.

The use of quantum computing is expected to improve the performance of Monte Carlo-based options pricing and valuation methods. Similarly, it will likely be able to help in the modeling of complex financial market trading activities (e.g., valuation adjustment models for derivatives) wherein different scenarios are applied to a portfolio of financial instruments to calculate its value at a time in the future.

Figure 24. Potential Benefit to Financial Services Activity from Quantum Computing



Source: IBM

That said, quantum computers may also pose risks to the finance industry. Financial institutions are privy to sensitive customer data, which is often encrypted using techniques that even a modern supercomputer would be unable to decrypt (or "break") without an extremely long processing time — often in the order of thousands or millions of years. As we discuss further in the "Cybersecurity" section, calculations show that a sufficiently advanced quantum computer could break today's encryption standards in just a few hours, thus posing a risk to the global financial ecosystem.

Furthermore, as today's cryptography standards are a key building block to the blockchain and other distributed ledge technologies, quantum computers also pose a risk to the cryptocurrency ecosystem and the elements of the financial industry being built on top of it — which we discuss in the "Cryptocurrency" section.

We spoke to Matt Johnson, CEO of QC Ware, which provides professional services and enterprise software for quantum computers, about the potential impact quantum computing may have on the finance industry.

Matt Johnson
CEO, QC Ware

Expert Interview with Matt Johnson, CEO of QC Ware

Q: Could you elaborate on some challenges within finance that QC Ware is looking to apply quantum computing to?

Matt: Intra-day derivative pricing and performance analysis for complex portfolios is something that we believe will be a highly sought-after solution once adequate hardware becomes available. Currently, these pricing calculations happen overnight and take a few hours to complete. The results are provided to the traders to inform their decisions during the trading day, but the information can get stale very quickly, especially on days with significant market volatility. Being able to provide traders with a process that can price a very complex portfolio in minutes rather than hours will be a significant game-changer in the finance sector, and that is what QC Ware is currently working on.

Q: Do institutions need to hire their own teams of quantum algorithm experts in order to integrate quantum computing into their existing finance infrastructure?

Matt: Industry leaders will have to hire their own experts to maintain an in-house point of view on developments and to be able to validate what software and hardware vendors are proposing. We believe that 80% of quantum computing solutions that will be utilized in the market will come in the form of pre-packaged, off-the-shelf applications. However, we also believe that industry leaders will always look to innovate in-house and build unique and custom approaches that provide specific advantages.

Q: What do you see as the biggest barrier facing quantum adoption in finance?

Matt: The barrier is the same as for any other software solution. It needs to provide clear value, it must be easily accessible, and it should be integrated with existing technology and processes.

Q: Is quantum computing going to be good for high-frequency trading?

Matt: It is very hard to see something like this happening within the next 20 years. Our best guess is that in order to be able to beat classical solutions in high-frequency trading, the quantum computing ecosystem would need to develop a purely quantum pipeline starting with the input data that would have to live in some quantum state, the communication pipelines, the computation of the recommended trade, and its execution.

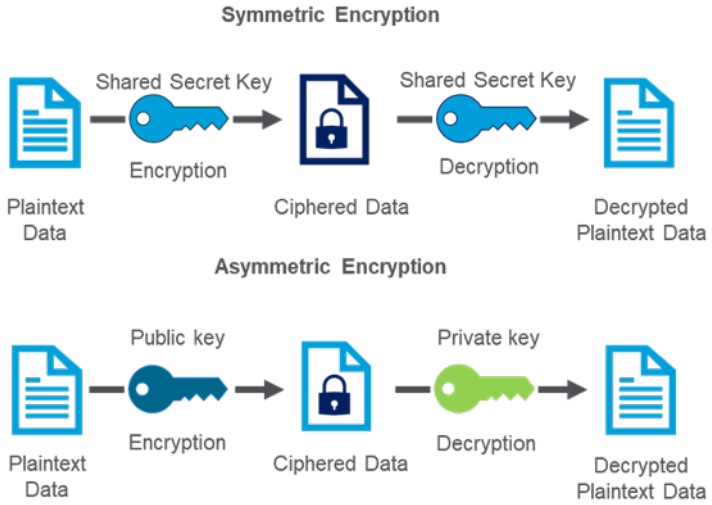
Cybersecurity

Opportunities rarely come without risks. One serious risk posed by quantum computing is to data privacy and cybersecurity. The power of quantum computing could be misused for breaking encryption, which is at the heart of all forms of electronic communication and data storage across the world today. This includes digital authentication, public key infrastructure (PKI), and mobile chat systems.

How Data Is Currently Protected

There are mainly two types of data encryption methods used today. One is symmetric-key encryption, where the sender and receiver have identical (symmetric) digital keys to encrypt and decrypt data. The other is public-key (asymmetric) encryption, where a publicly available key encrypts messages for a recipient who has a carefully guarded private key for decryption.

Figure 25. Symmetric vs. Asymmetric Encryption

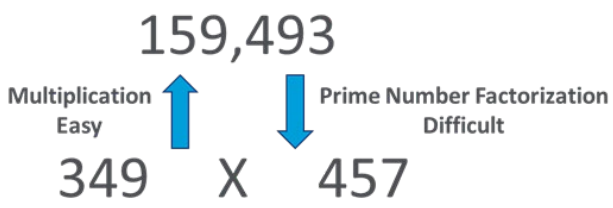


Source: Citi GPS

The main difference is that symmetric encryption requires the use of shared secret keys; otherwise, it is faster and believed to be more secure. Public key encryption, on the other hand, has the advantage of only requiring an authentic copy of publicly available keys (i.e., keys that need not be kept secret), and it provides a means for establishing symmetric keys for the more efficient symmetric encryption algorithms. However, public key encryption is generally believed to be more susceptible to cryptanalysis (the process of identifying and exploiting weaknesses in cryptographic algorithms without knowing the secret key). This is because it requires additional mathematical structure compared to symmetric key encryption algorithms.

RSA encryption is one of the most widely used public-key cryptographic standards. It is constructed in a way that is easy to decrypt using one's private key, but otherwise extremely difficult for anyone else. RSA encryption relies on the fact that, while a classical computer can easily multiply large prime numbers together, the reverse process of factoring (determining which large prime numbers multiply together to get to the final number) is extremely difficult. This is because while there exists a highly efficient algorithm for multiplying large numbers (the long multiplication method we all learn in school), there is currently no known efficient algorithm that can run on a classical computer to reverse this process.

Figure 26. Factorization vs. Multiplication



Source: Citi GPS

While a smartphone or laptop can easily multiply large prime numbers, even a classical supercomputer is unable to reverse such a calculation without an extremely long processing time — often in the order of thousands or millions of years, depending on the length of the number. Leveraging this impracticality for classical computers to factor large numbers, current public-key encryption has become uncrackable by using very long key pairs — such as 2048-bit keys, which equate to 617-digit decimal numbers.

The Threat to Encryption Standards

This foundation to asymmetric encryption was shaken by Shor's algorithm, proposed by Professor Peter Shor in 1994.[66] Shor's algorithm theorized that a large fault-tolerant quantum computer could find the prime factors of large numbers in a fraction of the time required by classical computers. While the nuances of the actual algorithm are far beyond the scope of this report, the broader point is that Shor's algorithm could provide a means to any hostile actor with a large enough quantum computer to start with a public key of an RSA public-key cryptosystem and reverse-engineer the associated private key, leaving asymmetric encryption techniques like RSA vulnerable to quantum attack.[67]

This is because encryption like RSA relies on the principle that the difficulty of factoring large numbers scales exponentially for classical computers, whereas a successful implementation of Shor's algorithm changes this to scale in a polynomial fashion, as Figure 27 shows. In fact, it has been calculated that sufficiently advanced quantum computers could decrypt even 4096-bit key pairs in just a few hours using Shor's algorithm. The effect of this would be to potentially render communications as insecure as if they were not encrypted at all.

Figure 27. Quantum Computing's Potential for Significant Speed-up Over Classical Computers

Type of Scaling	Time to Solve Problem				
Classical algorithm with exponential runtime	10 secs	2 mins	330 years	3,300 years	Age of the universe
Quantum algorithm with polynomial runtime	1 min	2 mins	10 mins	11 mins	~24 mins

Source: IBM

[66] Peter Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134, November 1994.
[67] Dorothy E. Denning, "Is Quantum Computing a Cybersecurity Threat?," *American Scientist*, March 2019.

As for symmetric encryption: While it is not impacted by Shor's algorithm, it is affected by Grover's algorithm. Grover's algorithm is a quantum computing algorithm proposed by Lov Grover in 1996 that makes it far simpler to search through unstructured data sets. Within the context of cybersecurity, it has been found that a large fault-tolerant quantum computer running Grover's algorithm could provide a quadratic speed-up in attacking symmetric encryption standards like Advanced Encryption Standard (AES).[68] Consequently, to resist such attacks and maintain the same level of security strength in the quantum era, it would be necessary to double key sizes. For AES, this means using 256-bit keys instead of today's 128-bit keys.[69]

Quantum computers currently have too little computing power and are too error-prone to crack today's strong codes. For context, one estimate by experts suggests a quantum computer would need at least 70 million physical qubits to crack 2048-bit RSA encryption.[70] Considering IBM's 433-qubit Osprey is the largest quantum computer we know about today, this would, on the face of it, suggest it could be a long time before we reach that point. In addition to needing almost 100,000 times more qubits than today's largest quantum computers, any fault-tolerant quantum computers that could be considered useful in cracking today's encryption standards would also need an error rate that is 1/100th of what today's best quantum computers can reach.[71] However, other factors mean that we may not be as far away from the day when the quantum threat materializes as many think.

This is because things are moving faster in this area than is generally understood, and technologies are developing in various directions. Not only are we seeing quantum computers with more qubits every year, but new algorithms are reducing the computing power and error-correction rates needed for quantum computers to crack current day encryption by orders of magnitude. For instance, Google and the KTH Royal Institute of Technology in Sweden claimed in 2019 that they found a more efficient algorithm for quantum computers to break encryption standards. Using their new algorithm, in theory, even a 20 million-qubit computer could break 2048-bit encryption in a mere 8 hours.[72]

To gauge how far away this quantum threat is, the Global Risk Institute interviewed 40 of the world's leading experts, asking when they thought quantum computers would be able to break the 2048-bit RSA encryption used today within 24 hours. A small share (2.5%) of the experts interviewed indicated there was a 50% or more likelihood of this occurring in the next 5 years. However, this rose to 22.5% and 55% when asked about the same likelihood of this occurring in the next 10 or 15 years, respectively. In fact, the vast majority (92.5%) of the experts estimated there was a 50% or more likelihood of quantum computers being able to break 2048-bit RSA encryption in the next 20 years.[73]

---

[68] Sandeep Rao et al., "The AES-256 Cryptosystem Resists Quantum Attacks," *International Journal of Advanced Computer Research*, Vol. 8, No. 3, April 2017.
[69] Ibid.
[70] QuantumXChange, "What Is The Impact Of Quantum Computing On Cybersecurity?," accessed March 7, 2023.
[71] Emily Grumbling and Mark Horowitz, *Quantum Computing: Progress and Prospects* (Washington, DC: The National Academies Press, 2019).
[72] *MIT Technology Review*, "How A Quantum Computer Could Break 2048-Bit RSA Encryption In 8 Hours," May 30, 2019.
[73] Dr. Michele Mosca and Dr. Marco Piani, Quantum Threat Timeline Report 2022, Global Risk Institute, December 2022.

It is important to note that such a stringent timeframe of 24 hours to break encryption inherently provides a very conservative estimate as to when the quantum computers would pose a threat. The quantum threat to cybersecurity is still very real, even if, rather than the 24 hours posed in the question above, quantum computers are able to break such modern encryption techniques in several days, weeks, or even months.

The Scope of the Problem

If these encryption methods are broken, nearly all encrypted communications and data could be transparent to hostile actors with access to a quantum computer. It is not difficult to imagine the scope of potential consequences if a nefarious group were to access and steal confidential information from governments, such as state secrets.[74] Similarly, the interconnected devices that make up Industry 4.0 are also at high risk from quantum attacks. With commercial machinery becoming increasingly interconnected under IoT systems, quantum cybercriminals could in theory attack and gain control over physical assets.

The risk that quantum computers pose to data security may be even more pressing than one would think: Hostile actors may be able to start harvesting encrypted data now, with the intent of utilizing a quantum computer to decrypt it in the future — known as a "Harvest Now, Decrypt Later" (HNDL) attack. This is a particularly important issue for companies and institutions that manage highly sensitive data, such as pharmaceutical companies, large banks, governments, and intelligence agencies. In practice, the use of HNDL attacks means a large amount of stolen data may be currently residing in databases, ready to be decrypted and exposed in the coming years.

Ultimately, what this means is that the post-quantum security threat exists in the present, not the future. Financial institutions and nearly every industry that deals with sensitive data need to review their security strategies and take appropriate steps, including creating multiple data classifications, each with their own encryption algorithm and encryption key, to protect against the quantum threat.

Post-Quantum Cryptography

As well as the risk to national security, breaches of current cryptographic systems by quantum computers could carry potentially significant consequences for civilian communications and the confidentiality of corporate information. Consequently, there are many endeavors by both governments and private companies to develop a quantum-resistant form of cryptography — commonly referred to as Post-Quantum Cryptography (PQC).

A quantum-resistant form of cryptography is a cryptographic problem that is intractable (i.e., very difficult) for both classical and quantum computers to solve. Fortunately, such cryptographic problems are not difficult to define, and can be retrospectively implemented into classical hardware. However, on the other hand, the actual commercial transition process to PQC will likely be quite challenging, as this will require the mass adoption of a completely new standard. Organizations around the world have been trying to determine what this transition might look like in order to recommend best practices.

[74] Bitdefender, "How Quantum Computing Will Impact Cybersecurity," March 13, 2021.

The U.S. National Institute of Standards and Technology (NIST) published the first public encryption standard, DES, in 1977.[75] Having since developed a full portfolio of classical encryption standards, NIST began the search for appropriate PQC standards in 2016 when it called for proposals.[76] Eighty-two initial submissions were received from 25 countries in 2017, with 69 making it to the second-round selection stage. After several more selection rounds, NIST recently announced the four final candidates for PQC algorithms: One (CRYSTALS-Kyber algorithm) is for general encryption, while the other three (CRYSTALS-Dilithium, FALCON, SPHINCS+) are specifically for digital signatures.[77] According to the NIST's latest timeline, draft standards are currently planned for release by 2024.[78]

The U.S. government, specifically the National Security Agency (NSA), recently notified all its National Security Systems (NSS) owners, operators, and vendors of the future quantum-resistant algorithm requirements. The press release explicitly stated that one of the reasons now was the time to plan, prepare, and budget for the transition to quantum-resistant algorithms was because of foreign pursuits in quantum computing. Rob Joyce, Director of NSA Cybersecurity, explained, "This transition to quantum-resistant technology in our most critical systems will require collaboration between government, National Security System owners and operators, and industry."[79]

Many cryptography practitioners expect all governments and institutions that interact with them (which includes a huge number of corporations) will be mandated to adopt the new standards. However, the migration process to a new PQC standard is not something that could typically be done overnight — in the case of governments, this process could take 5-10 years to complete, while for large companies, the transition will probably take multiple years as well. At the same time, it is important to note that PQC standards have not yet been fully established. As the Director of NSA Cybersecurity said, "We want people to take note of these requirements to plan and budget for the expected transition, but we don't want to get ahead of the standards process."[80]

Figure 28. NIST PQC Standard Timeline

Year	Milestone
2016	Criteria and requirements for PQC standard released and call for proposals
2017	1st round candidates announced
2018	1st PQC Standardization Conference
2019	2nd round candidates announced and 2nd PQC Standardization Conference
2020	3rd round candidates announced
2021	3rd PQC Standardization Conference
2022	4th round candidates announced and 4th PQC Standardization Conference
2022/2024	Draft standards available

Source: NIST, Citi GPS

[75] National Institute of Standards and Technology (NIST), "Data Encryption Standard," PDF, January 15, 1977.
[76] NIST, "Computer Security Resource Center," accessed March 7, 2023.
[77] NIST, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," July 5, 2022.
[78] NIST, "Post-Quantum Cryptography: Workshops and Timeline," last updated July 17, 2023.
[79] NSA, "NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems," September 7, 2022.
[80] Ibid.

In the interim period, until the finalized PQC standards are published and adopted, institutions are susceptible to the HNDL attacks we described above. One report explained that the use of longer encryption key lengths, such as migrating from 1024-bit RSA encryption to 2048-bit RSA encryption, could provide an additional 1-3 years of protection against the threat posed by early prototypes of error-corrected quantum computers.[81] Furthermore, some experts we spoke to explained that a number of companies are already moving to 2048-bit as their standard.

Notably, it is important to be aware that the adoption of the PQC standards does not necessarily provide 100% protection against quantum computers. This is because, as with any standard, there is always a chance that a new revolutionary algorithm could be created to decrypt it, especially as large quantum computers become available for codebreakers to experiment with. Hence, the notion of cryptographic agility is key to an institution's ability to address the future threat of quantum computers. For instance, one form of cryptography that was considered "quantum-safe" was recently hacked by a 10-year-old PC.[82]

We discuss this further in our "How to Prepare: For the Quantum Threat" section of this report, where we look closer at the problem and provide some high-level guidelines for corporates wishing to better understand the threat quantum computers pose to the security of their data. Regardless, the quantum threat to cybersecurity could take significant time and cost to address, similar to the Y2K problem.

Lessons from The Y2K Problem

The threat quantum computing poses to cybersecurity is in many ways akin to the Y2K problem at the turn of the millennium, when computers were incapable of processing dates containing "00" after "99" due to some initial program design to save memory. It is estimated that the U.S. alone spent around $100 billion in preparation for the problem, with around $9 billion provided directly from federal government.[83] Globally, various estimates have been provided for Y2K-readiness spending, from $200 billion to $850 billion.[84] IDC even launched a specific project, Project Magellan, back in 1999, with the sole purpose of studying the impact of the Y2K bug — it estimated a $320 billion bill spend over seven years, with a peak spending of $101 billion in 1999.[85]

The cost was not the only significant aspect of the Y2K problem. The scope of the impact was also very significant — there were over 100 million computers in the U.S. in 1999, and all of them were potentially at risk.[86] This is all the more stark when we consider that the Y2K problem occurred over two decades ago, when the internet only had 248 million users, compared to the over 5 billion users it has today.[87] Furthermore, $1 in 1999 would have an equivalent purchasing power of $1.81 today as a result of inflation.[88]

---

[81] McKinsey, "When—and How—to Prepare for Post-Quantum Cryptography," May 4, 2022.
[82] Charles Q. Choi, "'Quantum-Safe' Crypto Hacked by 10-Year-Old PC," IEE Spectrum, August 19, 2022.
[83] Farhad Manjoo, "Was Y2K a Waste?," *Slate*, November 11, 2009.
[84] IT Web, "Y2K Cost Beyond Reckoning, Global Coordinator Says," January 4, 2000.
[85] Jack Schofield, "Money We Spent," *The Guardian*, January 4, 2000.
[86] Infoplease, "U.S. Households With Computers and Internet Use, 1984–2014," updated June 26, 2019.
[87] Internet World Stats, "Internet Growth Statistics," accessed March 7, 2023.
[88] In 2013 Dollars, "CPI Inflation Calculator," accessed March 7, 2023.

The CEO of SandboxAQ, a SaaS provider combining AI and quantum technology to deliver solutions, pointed out in a recent quantum technologies conference that over 20 billion devices are currently exposed to the decryption risk from quantum computers (250 times more than the number for Y2K), and all of these will all need to migrate to a PQC standard to make them resistant to quantum attacks.[89]

Unlike the Y2K problem, however, the quantum threat to cybersecurity is less well-defined, in that we don't know when it will be realized. Estimating a precise date is made all the more complicated given that players are unlikely to disclose how close they are to making a quantum computer capable of breaking current encryption standards. Nonetheless, the ways that countries and corporations successfully managed their Y2K problems may provide a blueprint for how they can address the threat quantum computing poses to encryption. Irrespective of any such exact date, due to the threat of the "Harvest Now, Decrypt Later" attacks described earlier, the potential risk to data security could be happening right now.

We spoke to Dr. Michele Mosca, CEO and Co-Founder of evolutionQ, which provides quantum-safe cybersecurity products and services, about when this quantum threat to cybersecurity could occur and what organizations can do now.

[89] Lionel Sujay Vailshery, "Internet of Things (IoT) and Non-IoT Active Device Connections Worldwide from 2010 to 2025," Statista, September 6, 2022; David Joseph et al., "Transitioning Organizations to Post-Quantum Cryptography," *Nature*, Vol 605, May 11, 2022.

Expert Interview with Dr. Michele Mosca, CEO and Co-Founder of evolutionQ

Dr. Michele Mosca
CEO and Co-Founder, evolutionQ

Q: When are we likely to see the "quantum threat" materialize?

Dr. Mosca: By the time we know for certain, it's too late to respond. It's a matter of aligning your risk appetite or tolerance to the likelihood of the threat in five years or in 10 years, and so on. And for very critical systems where the risk tolerance is low, the latest Global Risk Institute report indicates that even the five-year timeline is already a concern.

Q: What can organizations start doing now to prepare for the quantum threat?

Dr. Mosca: Organizations must position themselves to manage this new threat using technology lifecycle management and not crisis management. The journey to a quantum-safe posture for your organization can be broken up into six phases: preparation, discovery, risk assessment, risk mitigation, migration, and validation. evolutionQ pioneered the "Quantum Risk Assessment" which brings organizations through the first three stages toward quantum-readiness, and positions them to prioritize their activities for the last three stages. There are great tools, both open-source and proprietary, to support the migration to quantum-safe cryptography, including our Quantum Delivery Network product.

Q: What realistic role does Quantum Key Distribution (QKD) play in protecting against quantum attacks? What can we do now?

Dr. Mosca: Post-quantum algorithms are a critical first line of defense for our digital systems. However, there is a non-negligible chance that they will be broken. So, for long-lived information and for critical systems where the risk of cryptanalysis is too high to just accept, it is imperative to have an additional layer of defense. QKD is a remarkable solution for the key establishment problem, which is not susceptible to unexpected mathematical attacks. It is already commercially available, and it's a technology that "ages well" — as quantum technology continues to advance, it becomes easier and easier to overcome QKD's current limitations.

evolutionQ pioneered the Quantum Delivery Network through its BasejumpQDN software product, a very simple and elegant solution for integrating QKD-generated keys into enterprise systems in a way that is scalable and vendor-independent. Specifically, BasejumpQDN provides organizations with a framework to transition from a low-cost testbed for simulated QKD to managing a complex multi-node network of QKD. BasejumpQDN enables QKD to be deployed in a cost-effective manner by expanding the number of nodes that can leverage QKD.

Cryptocurrency

Cryptography is the key underlying technology to the blockchain and contributes its name to the eponymous cryptocurrency. There are of course numerous types of cryptocurrencies. However, we will use Bitcoin as a proxy to discuss the potential effects of quantum computing on the industry more broadly. To be clear, we are not saying the introduction of quantum computing means Bitcoin or other cryptocurrencies will be hacked. But we are pointing out the increased risk to the cryptography of Bitcoin and other cryptocurrencies without the right technology protocols put in place.

Bitcoin's Cryptography

The Bitcoin network is secured by computers all around the world, referred to as miners, that use SHA-256, a 256-bit cryptographic hash function whose name stands for Secure Hash Algorithm-256. All Bitcoin transactions must be "confirmed" by the network of miners before they are added to the blockchain, an immutable ledger of all historical transactions including current ownership rights.

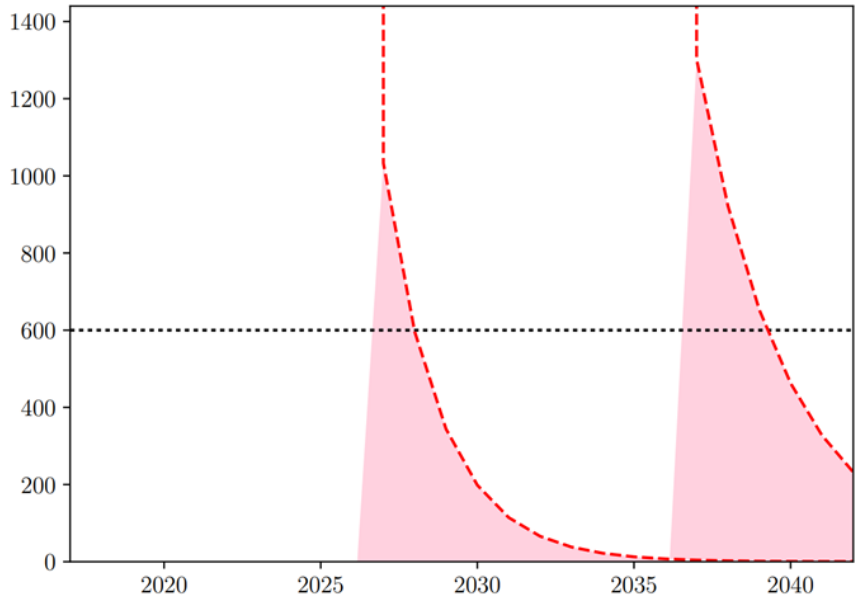
Bitcoin, for example, uses a different type of cryptography than the RSA encryption that protects most of the internet. Transactions in the Bitcoin network are digitally signed using the Elliptic Curve Digital Signature Algorithm (ECDSA), which is based on Elliptic Curve Cryptography (ECC) that relies on the principle that it would be intractable for a computer to deduce the private key from the public key.[90] Fundamentally, breaking this cryptographic primitive would mean that securely transferring ownership of one's Bitcoin would no longer be possible.

Classical computers are not able to break RSA encryption. However, both RSA and ECC can be broken by a quantum computer capable of running Shor's algorithm. Interestingly, it has been suggested that a quantum computer may be able to crack ECC in less steps than RSA.[91] Ultimately, using Shor's algorithm, it would be possible to calculate a private key and steal someone's Bitcoin.

With various alternative architectures for quantum computers all competing against one another, we can only very roughly estimate when quantum computers might become able to break Bitcoin's cryptographic signature scheme. Taking the 10-minute (or 600-second) transaction time as a cut-off, the Centre for Quantum Technologies at the University of Singapore estimated that that this could occur anytime ranging from the late 2020s to the late 2030s.[92]

[90] Pascal Urien, "Innovative Countermeasures to Defeat Cyber Attacks Against Blockchain Wallets: A Crypto Terminal Use Case," downloaded from arXiv, PDF, March 30, 2023;Certicom Research, "Certicom ECC Challenge," PDF, last updated November 10, 2009.
[91] John Proos and Christof Zalka, "Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves," downloaded from arXiv, PDF, February 1, 2008.
[92] Divesh Aggarwal et al., "Quantum Attacks on Bitcoin, and How to Protect Against Them," downloaded from arXiv, PDF, October 28, 2017.

Figure 29. Time to Break Signature Scheme for a Quantum Computer



The plot shows two estimates of the time in seconds required for a quantum computer to break the signature scheme (red curves) as a function of time. It also gives more and less optimistic estimates (red striped lines).
Source: Divesh Aggarwal et al. (2017)

Cryptocurrency Mining

As well as Shor's famed algorithm, there is another important quantum computing algorithm that could create challenges for a large subset of cryptocurrencies — specifically, those that reach consensus through Proof of Work (PoW). PoW is the original consensus mechanism for cryptocurrencies and debuted in Bitcoin, which still uses this methodology. PoW operates on the principle that transactions must be "confirmed" by the network of miners before they are added to the blockchain.

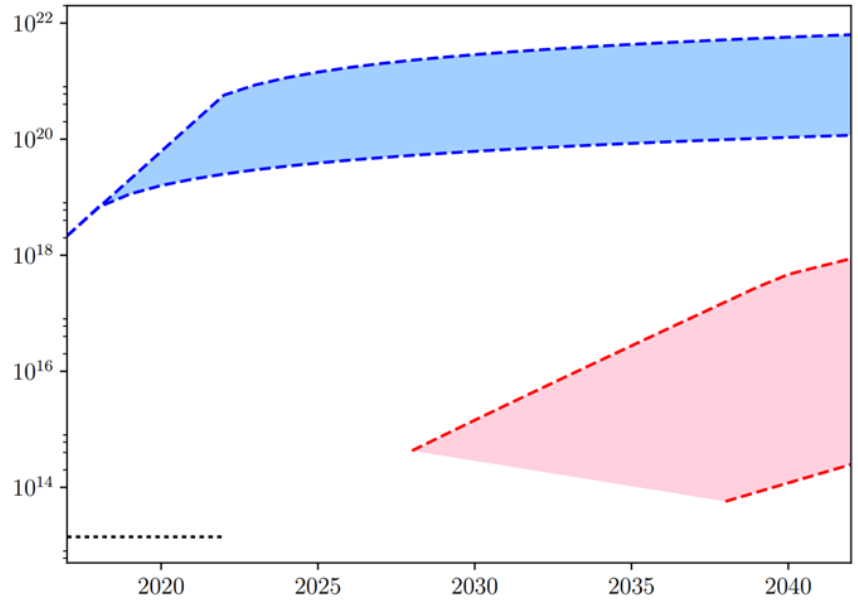
Grover's algorithm is a quantum computing algorithm that makes it far simpler to search through unstructured data sets. Researchers have found that when applied to the principle of mining cryptocurrencies, Grover's algorithm allows for a quadratic speed-up of finding the solution to a block and thus of winning that block in the blockchain, resulting in an increase in the hash rate of whomever is using the algorithm.[93]

Henceforth, in a post-quantum world, a Quantum-Equipped Actor (QEA) could gain an unfair advantage by mining blocks faster using Grover's algorithm. As the blockchain is an immutable ledger of all historical transactions including current ownership rights, one possibility is that a QEA could use this more efficient mining technique to undertake a 51% attack. This is where a single person or group of persons gains control of over 50% of a blockchain's hashing power, by secretly creating their own chain in a PoW cryptocurrency until they have gotten into the lead, and then publish their blocks to cause a reorganization of the public ledger.This threat will apply to all cryptocurrencies that use PoW, but as Bitcoin is understandably the most academically researched, we will examine what quantum computing could mean for its PoW consensus.

[93] Iain Stewart et al., "Committing to Quantum Resistance: A Slow Defence for Bitcoin Against a Fast Quantum Computing Attack," *Royal Society Open Science*, Vol. 5, No. 180410, May 22, 2018.

The same paper from the University of Singapore compared the hash rate of the total Bitcoin network to that of what a single quantum computer may be able to produce (Figure 30). It suggested that prior to 2028 (in the more optimistic estimate), there would not be any quantum computer with sufficiently many qubits to implement Grover's algorithm.

Figure 30. Hash Rate of Total Bitcoin Network vs. Single Quantum Computer



The plot shows two estimates of the hashing power (in hashes per second) of the Bitcoin network (blue striped curves) vs. a single quantum computer (red striped curves) as a function of time. It also gives more and less optimistic estimates and uncertainty regions (blue and orange areas). For comparison, the black dotted line shows the hash rate of a single classical ASIC miner. The graph is plotted on a logarithmic y-axis, meaning that the disparity between a quantum computer's hash rate and that of the total Bitcoin network is likely to be several orders of magnitude apart for many years to come.

Source: Divesh Aggarwal et al. (2017)

It is important to note that a quantum computer requires a highly specialized and precisely controlled environment making it unlikely to be generally available for use in crypto mining. Also, given the competitiveness of crypto mining, by the time quantum computers become reliable enough to be used for mining, they are likely to be adopted by the majority of miners and hence establish a network equilibrium. This is something we have seen throughout the history of crypto mining — a gradual hardware transition from humble laptop CPUs to more-specialized but widely available and general-purpose gaming GPUs, and eventually to the current highly specialized and purpose-built ASICs that dominate crypto mining today.

The Broader Cryptocurrency Ecosystem

While we have focused on Bitcoin as an example, as of 2023, there are nearly 9,000 cryptocurrencies, according to Statista.[94] However, it would not just be each cryptocurrency itself that would be at risk from a quantum attack, but everything built on top of it.

[94] Raynor de Best, "Number of Cryptocurrencies Worldwide from 2013 to February 2023," Statista, March 8, 2023.

A study conducted in 2021, when the total market cap of cryptocurrencies was a little under $2 trillion, stated that a quantum attack on crypto could result in a 99.2% collapse of value. Interestingly, while the immediate loss to cryptocurrency holders in this scenario was estimated at around $1.9 trillion, the indirect losses to the economy were projected to be a further $1.5 trillion.[95] We anticipate these potential indirect losses to the economy (relative to the immediate loss to cryptocurrency holders) could grow significantly due to everything now being built on top of the existing blockchain infrastructure, such as Decentralized Finance (DeFi).

However, DeFi is likely just the start. With the mainstream adoption of "layer 2" solutions that build on the underlying "layer 1" cryptocurrencies, as well as the increasing usage of decentralized apps (or dApps) built on cryptocurrency platforms, the value at risk could grow much higher. Take, for instance, the recent adoption of non-fungible tokens (NFTs), which are now finding uses well beyond just the art world — from music streaming to property ownership.[96] With the increasing investment in Metaverse and Web3 projects that are intended to build a more decentralized web using distributed ledger technologies (DLTs), breaking the underlying cryptography would enable a QEA to claim ownership over any digital assets on said DLTs, regardless of what specific DLT architecture is used.

Potential Courses of Action

As discussed in the "Cybersecurity" section, considerable thought is being put into Post-Quantum Cryptography (PQC). It is likely that in the near future, long before a sufficiently powerful QEA can exist, the Bitcoin community could agree on and deploy a quantum-resistant signature scheme.

Such a change is unlikely to be controversial at the time and rather could be seen as a part of necessary improvements in security protocols, which have been a part of the natural progress and development of the industry since its inception. There is the chance, however, of disagreement between various stakeholders about how to implement changes to an existing blockchain. Neven's Law shows us just how fast improvements in quantum computers can occur (apparently almost overnight, in fact). In the event of such a threat, necessitating agreement between various decentralized stakeholders could increase the time it takes to adopt a quantum-resistant form of cryptography.

Furthermore, several organizations are actively investigating quantum resistance in cryptocurrencies in general, with many marketing themselves as developing a quantum-resistant ledger in general or offering a post-quantum solution to Bitcoin. However, at the point when quantum computers are powerful enough to be able to break the cryptography of cryptocurrencies, they will likely be equally able to break the encryption associated with more pressing matters, such as most of the internet (including one's banking details).

[95] Arthur Herman, "Will Quantum Computers Burst the Bitcoin Boom?," *Forbes*, November 9, 2021.
[96] Citi GPS, *Money, Tokens, and Games: Blockchain's Next Billion Users and Trillions in Value*, March 2023.

With many countries “going dark” about their developments in quantum computing, it may very well be blockchains run by countries that are first to pivot to quantum resistance. For instance, central bank digital currencies (CBDCs), which many countries are still exploring or planning to roll out, have fundamental advantages in pivoting to quantum resistance. First, they are run by the central banks of countries, which means they may be privy to knowledge from their respective governments, earlier than industry players, about when quantum computers begin to pose a threat to cryptocurrencies. Second, their centralization makes them less constrained by the time it takes to necessitate agreement between stakeholders.

Understanding the Landscape and How to Prepare

The use cases of quantum computing will grow over time, and it will impact stakeholders in completely different ways during these stages. We recognize that the industry impact of quantum computing may be almost as broad as the impact of computing, and different types of stakeholders will thus need different information and guidance. For this reason, we have divided this chapter into the three broad stakeholder categories as follows:

1. Nation-States
2. Corporates
3. Market Participants

Within each of these stakeholder categories, we have evaluated the quantum computing landscape and identified topics that we feel each type of stakeholder should be aware of, as well as included a section on “How to Prepare.”

In our “Nation-States” section, we discuss:

- Government investment and how to measure the utility of such investment.
- Why the quantum computing education levels in the workforce matter.
- How quantum computing supply chains differ from those of classical computing.
- Ethical questions around the use of quantum computing.

In our “Corporates” section, we discuss:

- The total addressable market (TAM) forecasts for quantum computing.
- What value creation could look like within the quantum computing space.
- Why collaboration and the cloud are key to corporate adoption.

In our “Market Participants” section, we discuss:

- The quantum venture capital trends in terms of the capital raised and deal activity.
- How the company and funding environment looks in terms of regional divides and the most active market participants.

Nation-States

Overview

Countries are uniquely positioned to prepare for the rise of quantum computing as an emerging technology. This is due to their ability to bring together experts from otherwise distinct fields, as well as provide the long-term funding necessary for the sector to grow to scale.

Each nation-state will have its own approach that takes into account both the state of play of its current industries and its long-term strategic goals. Hence, in this section, we focus on the areas that would be conducive to a national landscape in which a nation-state could best capitalize on quantum computing.

The four broad categories we identified in our literature review are as follows:

- Government investment
- Workforce education
- Supply chains
- Ethics

We then tie together conclusions from our literature review in the section "How to Prepare: A Holistic Quantum Computing Policy."

Government Investment

All new technologies have an initial stage of development that requires considerable investment before any commercial benefits can be achieved. This is particularly true of quantum computers given the long development timeframes involved. Also, unlike their classical counterparts, quantum computers offer no guarantees that such investment will provide any return in the near term.

The Precedent for Nascent Technologies

While quantum computers are now moving out of laboratories and into commercial applications, they are still in their infancy in terms of commercial development. Private investors in quantum technology are likely to be motivated by potential advances in short-term commercial applications. This makes it even more important that nation-states provide long-term funding, particularly for the early development activities that are necessary to keep the quantum computing industry competitive.[97] This is because government funding is necessary to reach the stage where quantum computers become practically useful for businesses, at which point private investment should, in theory, sustain their development.

Government support is also not without precedent. We often think of the technologies that we take for granted today as simply being the by-product of competition between technology giants, but in many instances, they would not have had the opportunity to flourish without initial government support.

[97] U.S. Government Accountability Office, "Considerations for Maintaining U.S. Competitiveness in Quantum Computing, Synthetic Biology, and Other Potentially Transformational Research Areas," September 26, 2018.

For example, the internet would not have existed without the ARPANET network built in the 1960s by the U.S. Defense Advanced Research Projects Agency (DARPA) — in fact, it was the first network to transmit data in discrete chunks and created the building blocks for the development of the Transmission Control Protocol/Internet Protocol (TCP/IP) specification we still use today.[98] Our current global position system (GPS) can trace its origins to a constellation of just five DARPA satellites, called "Transit," used to locate U.S. Navy ships. Similarly, the speech translation that forms the backbone of modern-day digital assistants was developed with DARPA funding. Another example is European countries' support of the development of second-generation wireless networks based on Global System for Mobile Communications (GSM) technology. More recently, one of the leading providers of 5G technologies reportedly accessed $75 billion in different forms of state support from the Chinese government.[99]

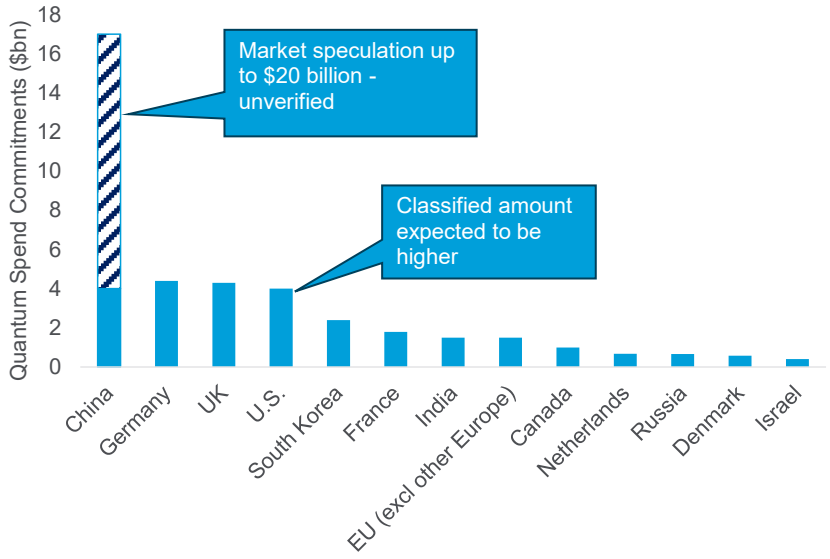
One of the key reasons that classical computing scaled in performance at the rate it did over the past 60 to 70 years is that the products and services ecosystem that used the latest classical computing technology grew at the same time. This allowed the classical computing industry to, at the earlier stages, generate exponentially more revenue and reinvest those profits into the research and development (R&D) needed to build the next generation of classical computers. As the National Academies of Sciences, Engineering, and Medicine points out in its report into the progress and prospects of quantum computing, in order for a Moore's-Law-type continuous exponential growth in quantum computing to occur, there must be exponential growth in investment, and there must be a similar cycle for quantum computers as there was for classical computers — where smaller, cheaper, or more easily accessible machines are commercially successful enough to grow investment in the overall area.[100] Absent of this dynamic, funding the development of each country's quantum computing ecosystem will become the responsibility of their governments.

The Public Investment Landscape

Numerous countries have already begun implementing national strategies for quantum technologies (which include quantum computing, communications, and sensing). As shown in Figure 31 below, the variations in announced government funding for quantum technology appear particularly stark. For instance, China appears to have declared four times more funding than its nearest competitor. Notably, The Quantum Insider, which compiled this data, have noted that the funding estimate for China is based on a limited number of sources and subject to significant dispute. At the same time, they also note that this number is unlikely to be below $4 billion.

[98] Duncan Graham Rowe, "Fifty Years of DARPA: Hits, Misses, and Ones to Watch," *New Scientist*, May 15, 2008.
[99] Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019.
[100] Emily Grumbling and Mark Horowitz, *Quantum Computing: Progress and Prospects* (Washington, DC: The National Academies Press, 2019).

Figure 31. Overview of National Quantum Technology Initiatives Globally in 2023



Note: Represents "total commitments" and does not reflect current annual spend.
Source: The Quantum Insider

It is also important to note that these announced funding numbers are also over different timescales. The above table shows both backward-looking numbers of amounts already invested and forward-looking numbers of current intentions to spend in the area. For example, it has been estimated that since 2014, the UK and U.S. governments have on average been spending £100 million ($124 million) and $500 million a year, respectively, on their quantum technology programs.[101] Of course, such estimates are likely to be incomplete because they will always exclude the classified spending of departments such as the Ministry of Defence (MoD) in the UK or Department of Defense (DoD) in the U.S. One of the risks of insufficient funding by governments is the potential of losing talent in quantum computing to other countries, discussed further below.

On the other hand, governments that engage with industry early will set themselves up with a strong foundation in developing quantum computing technologies. In fact, this is exactly what the UK government has been doing with its National Quantum Technologies Programme (NQTP), which is made up of the eight partner organizations listed below.

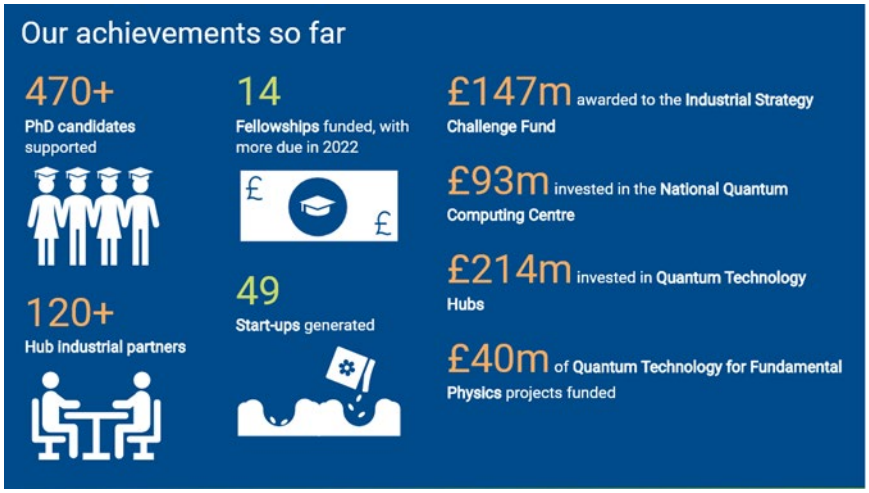
[101] Currency conversions are as of April 17, 2023; Karina Robinson, "Companies Cannot Afford to Be Left Behind in the Quantum Revolution," *Financial Times*, July 12, 2022. For more details see U.S. National Science & Technology Council, "National Quantum Initiative Supplement to the President's FY 2023 Budget," PDF, January 2023.

Figure 32. Partner Organizations that Make up the UK NQTP

Source: Used with permission from EPSRC on behalf of the National Quantum Technologies Programme

Fundamentally, the NQTP describes its purpose as supporting ideas, innovation, and investment to secure UK advantage and opportunities in the globally competitive new quantum era.[102] We reached out to the NQTP, and they explained that "The NQTP was established in 2014 and represents £1 billion of public and private investment. It is designed to bring together academia, industry, and government to accelerate the translation of quantum technologies into the UK marketplace and open up opportunities for British businesses to unlock new capabilities that can make a real difference to our everyday lives."

Figure 33. Achievements of the UK NQTP



Source: Used with permission from EPSRC on behalf of the National Quantum Technologies Programme

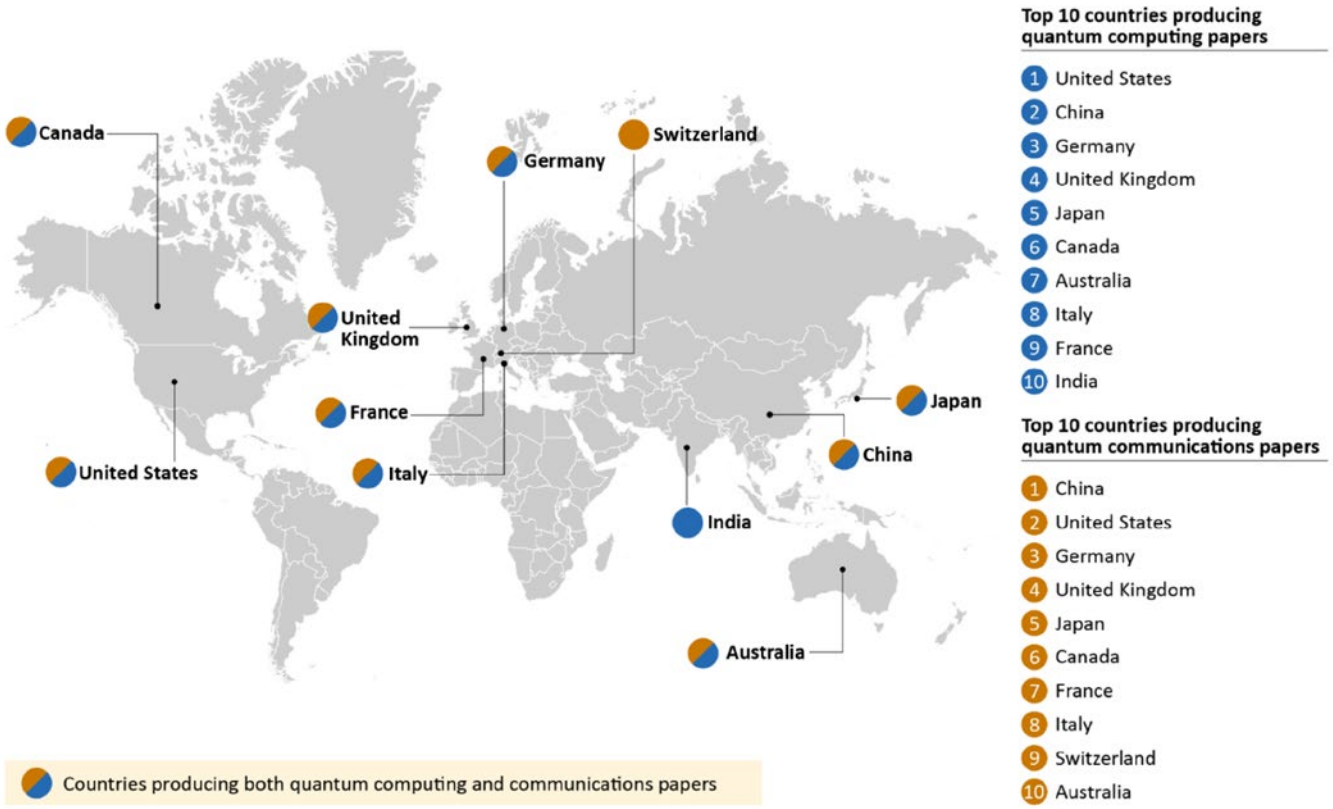
As well as supporting investment into research, innovation, skills, and technology, the program also provides UK companies with important grant funding to help them identify and develop uses and applications for quantum technologies. Figure 33 shows some of the UK NQTP's achievements so far. More recently, the UK government announced a National Quantum Strategy that is expected to more than double its investment into quantum technologies, investing £2.5 billion over the next 10 years. However, government funding is only useful if it yields results — something we discuss next.

[102] UK National Quantum Technologies Programme, "Transforming the World with Quantum Technology," accessed April 10, 2023.

Papers Published

Given the uncertainty of the direction of quantum computing technology and the sheer variety of different approaches to it (even just in qubit technology, as we touched on earlier in this report), it is difficult to compare different countries' levels of success objectively. One area we looked at as a potential early proxy of the success of investment was the publication of research papers. While of course research output will not necessarily correlate with successful government investment, especially since much government funding is targeted towards industrial commercialization, it does help in understanding the overall quantum computing landscape.

Figure 34. Map of Top 10 Countries Producing Quantum Computing and Quantum Communication Papers



Source: U.S. Government Accountability Office

The U.S. Government Accountability Office (GAO) analyzed the trends in countries producing research papers on quantum computing and quantum communications over a 20-year period from 1996 to 2016. Their findings clearly showed that most countries producing research in quantum computing also do so in quantum communications. Furthermore, the results show that the Top 10 countries (as measured by the number of research papers produced) in each of these fields are broadly similar. As expected, there also seems to be a moderately strong correlation between the amount of funding a country puts into quantum computing and the number of research papers it produces.

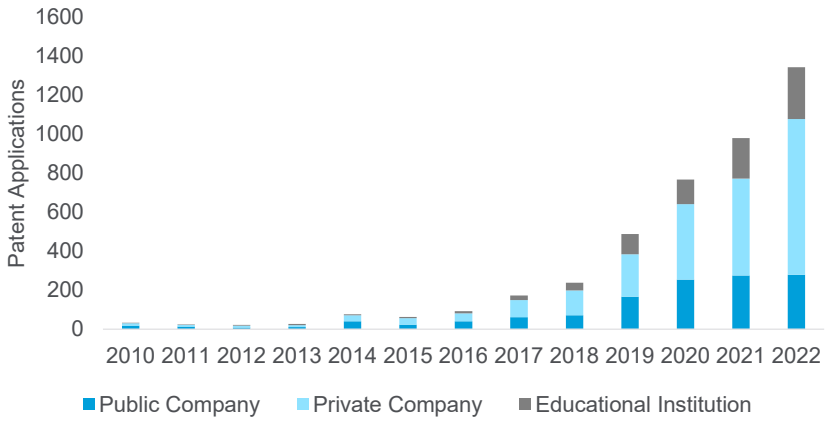
Patent Applications

Another proxy of the success of government investment, is its ability to generate intellectual property (IP) in the space, as measured by the number and quality of patents it has filed. The patent application landscape provides a unique insight into what is often the first stage of the commercialization lifecycle for any emerging technology — near the point of new idea generation, and often before the stage of receiving significant investment.

The ease with which different quantum technologies can be patented is incredibly nuanced. Consequently, we looked solely at the quantum computing sector, to allow for easier comparisons between countries. Leveraging the expertise of our in-house data experts, Citi Global Data Insights (CGDI), we analyzed data provided by QuantIP.

We found that there has been a substantial increase in global patent applications in recent years, from just over 30 at the start of the last decade to an average of over 1,000 in the past two years. This has been mostly driven by a sustained growth in the space since the middle of the last decade, with a 55% compound annual growth rate (CAGR) from 2015 to 2022. This was around the time when the idea of the commercialization of quantum computing was gathering momentum internationally.

Figure 35. Patent Applications Related to Quantum Computing (2010-22)



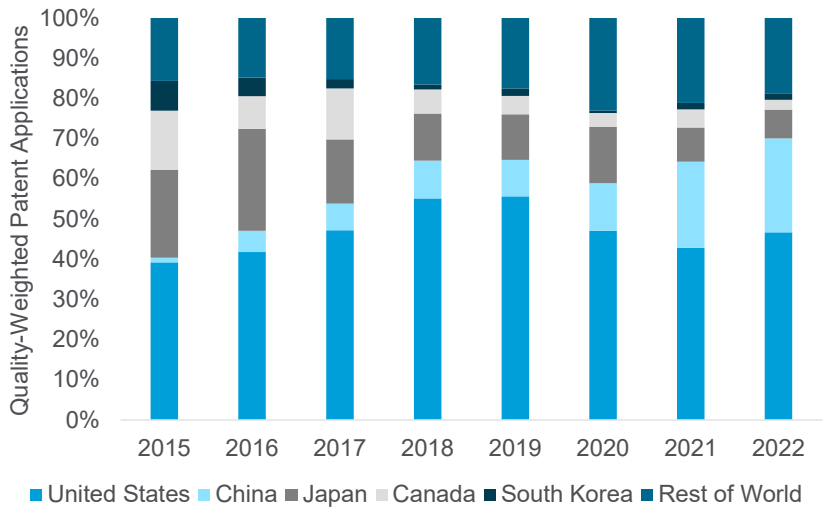
Source: Citi Global Data Insights, QuantIP

It was also not too long before various significant developments occurred in the field, including claims of quantum supremacy. While it is not possible to draw direct links to any specific developments, we feel that a healthy global patent environment is critical to the successful commercialization of the technology. This is as it provides a means for inventors to protect their ideas, ultimately giving them confidence to invest in further research and development, and likely be more willing to share those ideas with companies and governments.

Our analysis separated the different types of entities applying for these patents: public companies, private companies, and educational institutions. We found that while the number of patent applications from public companies grew 15x during this period, patent applications from private companies grew 60x (and now make up around 65% of all patent applications globally). This has most likely been facilitated by the increasing levels of private investment into the space — something we investigate further in our “Market Participants” section below.

In terms of the global distribution of patent applications by countries, it is of course important to take into account how the quality of patents varies from one country to another. For this reason, the CGDI team allocated patent quality weightings to each country based on their assessment of patent filing robustness, market potential, and citation potential. We then analyzed the global quality-weighted patent applications by country for the period 2015-20. Our analysis found that the U.S. dominated new idea generation, accounting for almost half (48%) of patent applications, followed by Japan (17%), Canada (8%), China (7%), South Korea (3%), and the rest of the world (17%).

Figure 36. Patent Applications Related to Quantum Computing by Country

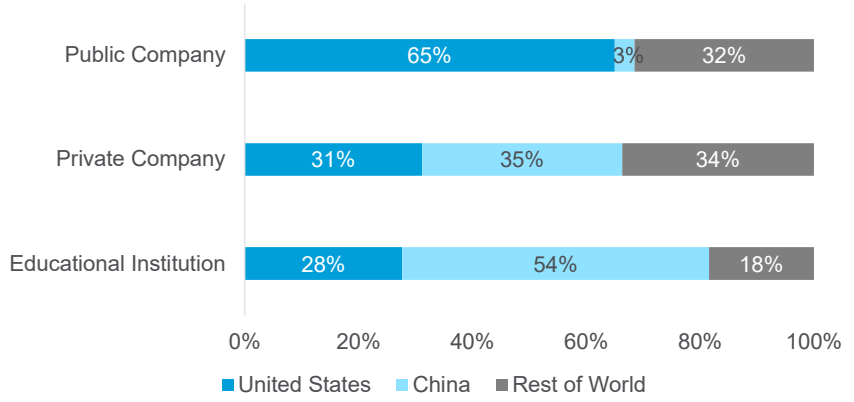


Source: Citi Global Insights, QuantIP

What is most striking to see from the figure above is the pace of change in recent years for certain countries. According to QuantIP, China's share of global quality-weighted patent applications grew from the aforementioned 7% to an average of 22% for the period 2021-22. This is even more impressive when considering that the CGDI's analysis attributed a quality-weighting to United States patents of 1.5x to that of China for this period. During 2021-22, the U.S. still led globally at 45%, with China in second place (22%), followed by Japan (8%), Canada (3%), South Korea (2%) and the rest of the world (20%).

Given the global dominance of the U.S. and China in patent applications over the past two years, we further investigated the distribution of patent applications by type of entity. In 2021-22, the U.S. accounted for 65% of all the quantum computing patent applications by public companies — most likely a reflection of the historical strength and size of U.S. public markets. The proportion of patent applications by private companies was generally split fairly equally between the U.S., China, and the rest of the world. Interestingly, however, China accounted for 54% of patent applications by educational institutions globally during this period. It is possible that this could be an early sign of the high levels of government investment committed to the space, or potentially a reflection of the traditional close links between government and academia in the country.

Figure 37. Patent Applications Related to Quantum Computing by Type of Entity (2021-22)



Source: Citi Global Data Insights, QuantIP

Ultimately, for both the U.S. and China, it seems there is notable strategic significance being placed in new idea generation and securing intellectual property in quantum computing.

Challenges for Government Investment

As with any nascent technology, high levels of government investment do not guarantee success, even if that country is able to successfully publish academic papers or apply for patents. Quantum computing is a very specific technology that requires specialist knowledge. Hence, one of the key questions facing nation-states regarding building their own quantum computing ecosystems is not just how much funding they can provide, but whether there exists a sufficient enterprise base to absorb it.

The UK, for instance, has a spin-off culture whereby academic departments with expertise in the quantum computing field set up their own enterprises. It is dynamics such as these that will play a key role in encouraging investment from the industry in the long run, and as discussed earlier, are necessary for the long-term development of the quantum computing industry beyond its incubation period. However, in order for technology development to continue in the meantime (before quantum computers offer a commercial advantage to businesses), governments must face the challenge of ensuring businesses have confidence in the technology's commercial potential.

We spoke to Roger McKinlay, Head of the Quantum Technologies Challenge for UK Research and Innovation (UKRI), about some of the difficulties governments face today when investing in quantum computing.

Expert Interview with Roger McKinlay, Head of the Quantum Technologies Challenge for UK Research and Innovation

Roger McKinlay
Head of the Quantum Technologies Challenge, UK Research and Innovation

Q: Given the high levels of private investment in quantum, why should governments continue to invest?

Roger: Governments need to act as co-investors, their investments being the vehicle by which they engage with industry and have influence over how the technology develops. It is not just about risk. It is now clear that private investors are prepared to take the risk. The issue is more about strategic co-investment — the public and private investment communities working together.

Q: What determines the level of funding that can be absorbed in a particular country?

Roger: There are many factors. Fundamentally, the growth of the sector will depend on the creation of new companies (spinouts or start-ups) and the rate at which existing companies see quantum technologies as being part of their future business. It does not all have to be "pulled" by end-use. Individual businesses just need a "customer" who may or may not be at the end of the supply chain. Some countries may excel at a component level, and others in quantum computing applications.

Q: Where does the international dimension come in?

Roger: There are two angles on this. Firstly, unless states want to grow their own start-to-finish supply chains, international trade will be essential. As with any expensive technology, companies will need access to global markets to make the case for the investment in developing new products and services. Secondly, the capabilities quantum technologies bring will be considered "sovereign" by many states. The issues will be what to "own," where to "partner," and what to "acquire." We will see groups of "trusted traders" form.

Q: To what extent will the availability of skills determine the growth of the sector?

Roger: In general, companies are good at competing for the talent they need to make their businesses work. They will recruit, train, and develop people as necessary. They will compete with other companies, not just for business but for the skills to deliver it. Governments can help by removing restrictions and by making sure that this skills and talent market really can function as a market. In the long term, the national education system needs to be able to deliver people who are capable of acquiring the necessary skills if the growth is to be sustained. STEM subjects will be key. At the moment, we tend to look at public investment as a measure of how seriously countries view quantum. In the longer run, the skills issue will dominate how and where the industry scales up.

Workforce Education

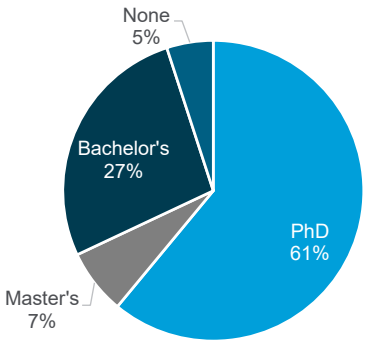
As with any emerging technology, in order for a nation-state to leverage its benefits effectively, it needs not only to invest in it financially, but invest in educating its workforce to ensure there is a sufficient supply of talent to drive further technological advancements. The challenge with quantum computing is that there have been so many significant developments in recent years, and the industry has grown so fast, that the supply of talent is becoming a bottleneck. Many believe this talent bottleneck risks becoming a significant barrier to the industry's growth in the long run.

Understanding the Talent Shortage

Working in quantum computing is quite different to other industries — for instance, many in the field have come directly from academia, making the talent pipeline quite different than in established disciplines like data science or cybersecurity. This is because the quantum computing industry is not yet mature enough that most individuals cannot do without at least a basic understanding of quantum mechanics. There is a close link between quantum hardware and software, which are more intricately connected than their classical counterparts. Consequently, experts need to have a sufficient understanding of the underlying physics that give rise to a qubit's special properties in order to be able to design quantum hardware and quantum software accordingly.

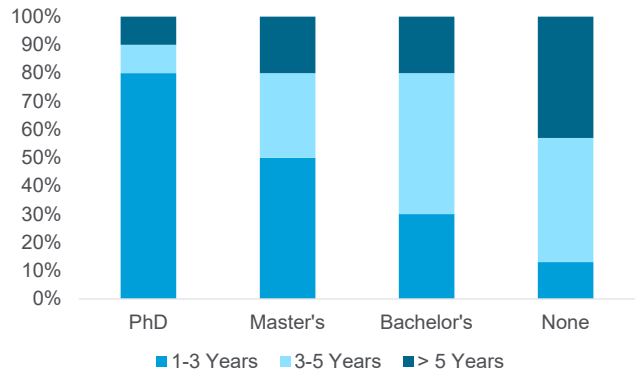
What this means is that, up until now, progress in the quantum computing sector has been mostly achieved by PhD-level scientists. This is something that continues to be reflected in today's job's market.[103] One recent study analyzed job posts on all quantum technologies (i.e., computing, communications, and sensing), of which 42% were focused in the quantum computing sector specifically. Investigating over 750 vacancies globally, researchers found that on average 61% were being advertised as requiring a PhD — although with some global regional variations with U.S./Canada (at 52%) and Europe/Other (at 67%).

Figure 38. Degree Requirements of Jobs in Quantum Technologies



Source: Kaur and Venegas-Gomez (2022)

Figure 39. Professional Experience Requirements of Jobs in Quantum Technologies



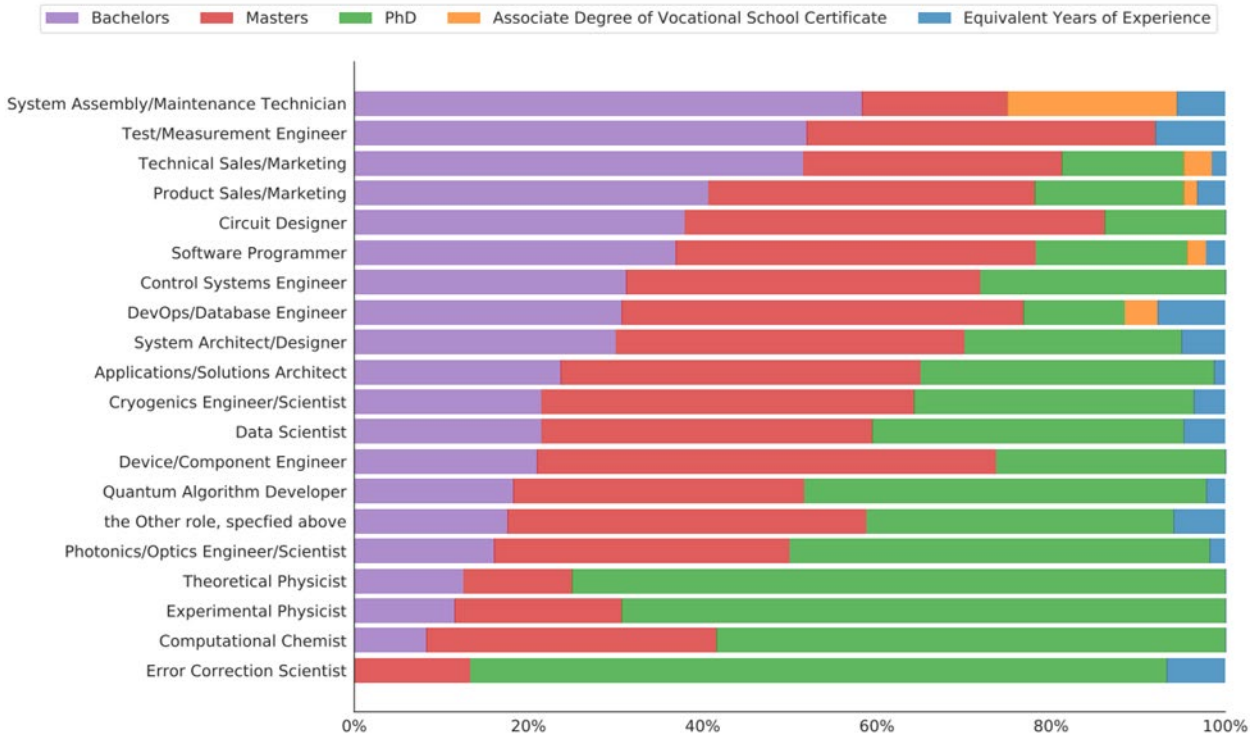
Source: Kaur and Venegas-Gomez (2022)

[103] Maninder Kaur and Araceli Venegas-Gomez, "Defining the Quantum Workforce Landscape: A Review of Global Quantum Education Initiatives," *Optical Engineering*, Vol. 61, No. 8, May 19, 2022.

The study also highlighted how significant holding a PhD was in terms of mitigating the additional years of industry experience required to fill roles. While only 20% of roles that required a PhD asked for more than 3 years of experience, this increased drastically to 50% and 70% for those only holding up to a Master's or Bachelor's degree, respectively — something that is likely due to the research skills and industry-specific knowledge gained through doing a relevant PhD. While a small 5% of the overall quantum-related roles did not advertise any form of higher education, almost 90% of these roles asked for more than the above mentioned 3 years of experience.

However, this requirement for a PhD is not universally distributed across all types of jobs in the industry. While, of course, some roles such as a theoretical or experimental physicist, would necessitate such a background, as Figure 40 below shows, there a number of other roles, such as maintenance technicians, measurement engineers or circuit designers, that typically only require a Bachelor's or Master's degree.

Figure 40. Distribution of Degree Requirements for Different Jobs in Quantum Technologies



Source: Hughes et al. (2021) [104]

[104] Ciaran Hughes et al., "Assessing the Needs of the Quantum Industry," downloaded from arXiv, PDF, August 25, 2021.

Ultimately, this has led to the very well-known problem of the quantum talent shortage, whereby governments and companies in the quantum technologies space have been struggling to find individuals with the appropriate level of quantum-relevant skills. One report claimed that the number of quantum physicists and engineers was estimated at only a few thousand worldwide — and there is certainly no guarantee that they would all end up in any of the quantum technology industries.[105] Many feel this talent shortage risks becoming a significant hurdle to the growth of quantum computing in the long run, with "a lack of talent" ranking third in a 2021 survey among all the possible barriers to the development of the technology.[106] In fact, it has been reported that the skills shortage in quantum computing could even harm the UK economy unless universities begin to recruit more students.[107] However, thankfully, there appears to be a changing tide in the educational requirements to join the quantum computing workforce.

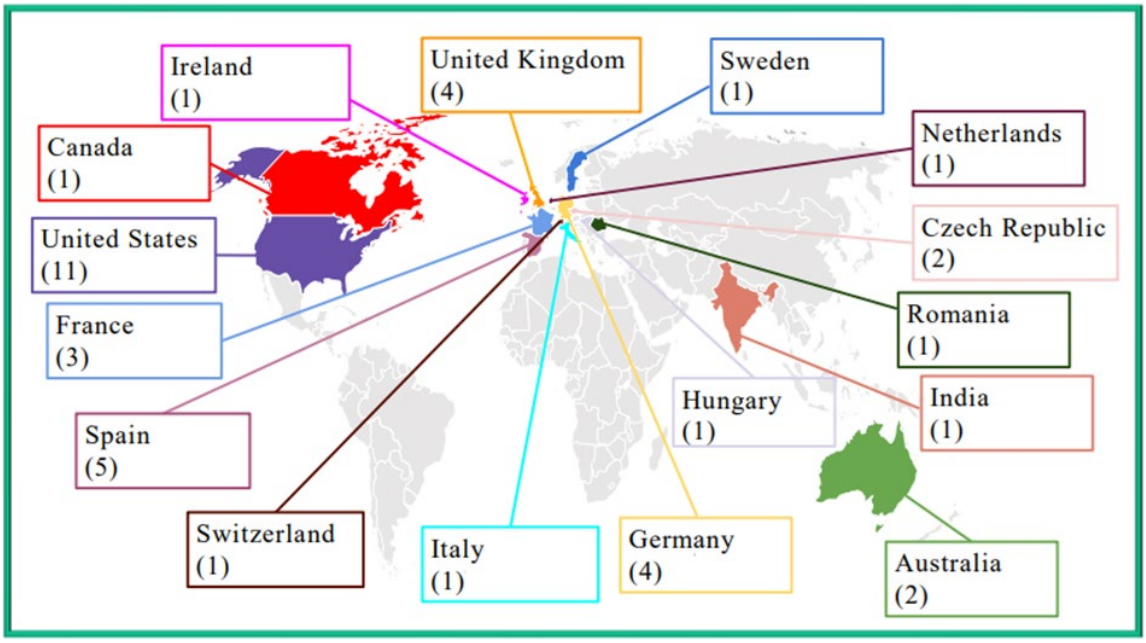
An Evolving Educational Landscape

There seems to be an overwhelming consensus from all the experts we spoke to that, for the quantum computing industry to scale at speed over the coming years, a more holistic approach to hiring needs to be taken. As Professor Sougato Bose put it when we interviewed him (see earlier in this report): "Quantum mechanics itself is typically taught, at least in the form needed for quantum computation, to undergraduates taking physics as a major, only in the last or third year. It has not spread out to the curriculum of other disciplines, as well as to earlier levels of physics curriculum in terms of the very fundamentals such as qubits and gates. I think this will be a change that will be necessary to have a larger volume of educated workforce in this area…"

This goes someway to further explaining demand for PhDs in the quantum computing industry — as a PhD has often been the first real point at which a student could begin to specialize in quantum technologies and gain the industry-specific knowledge needed by employers. Fortunately, it seems that universities around the world are recognizing this, and increasingly offering Master's degrees specifically in quantum technologies.

[105] Laura G. Converso, "How to Build a Quantum Computing Workforce," Accenture, November 9, 2020.
[106] Brian Lenehan, "Quantum Talent — Shortages and Tactics," Quantum Strategy Institute, December 3, 2021.
[107] Mark Piesing, "'How Can We Compete With Google?' The Battle to Train Quantum Coders," *The Guardian*, January 15, 2020.

Figure 41. Number of Master's Programs Focused on Quantum Technologies Across The World



Source: Kaur and Venegas-Gomez (2022)

It is important to note that these are still rare, with most countries only having one to two relevant Master's degrees in their entire graduate-level educational system, but nonetheless is a step in the right direction to lowering the academic barriers to entering the industry. The United States and the United Kingdom seem to again be leading in this respect with 11 and four Master's courses respectively, as of the time of publication. However, even with the increasing prevalence of Master's programs, there remains numerous challenges. There has been criticism of some curriculums merely packing courses relevant to quantum computing together without giving serious thought on the integration of these separate subjects, and ultimately requiring companies to do extra training. This may be contributing to why employers are requesting 3+ years of industry experience in 50% of Master's-level job openings, as mentioned above.

There have also been increasing calls for more engineering talent to be generated to supply the individuals who will be able to turn early and low-TRL (Technology Readiness Level) quantum experiments into commercial quantum products and services. In 2019, a symposium of 50 quantum experts noted that the knowledge required by existing quantum-related academic curriculums was not practical enough for graduates to apply in the industry.[108] These concerns are requiring educational providers to increasingly have to think about more practical quantum engineering skills, and as the industry becomes more mainstream, we are more likely to see dedicated undergraduate programs in this area. In fact, there is already work underway in designing courses from the ground up to meet the practical needs of working in the quantum technologies industry. These include educational opportunities offering more hands-on training with quantum hardware, including those relevant to different modalities of optics, ions, nanofabrication, and different tools required in the industry.[109]

[108] CyberTalk, "Closing The Quantum Computing Talent Gap," August 4, 2021.
[109] Abraham Asfaw et al., "Building a Quantum Engineering Undergraduate Program," *IEEE Transactions on Education*, Vol. 65, No. 2, May 2022.

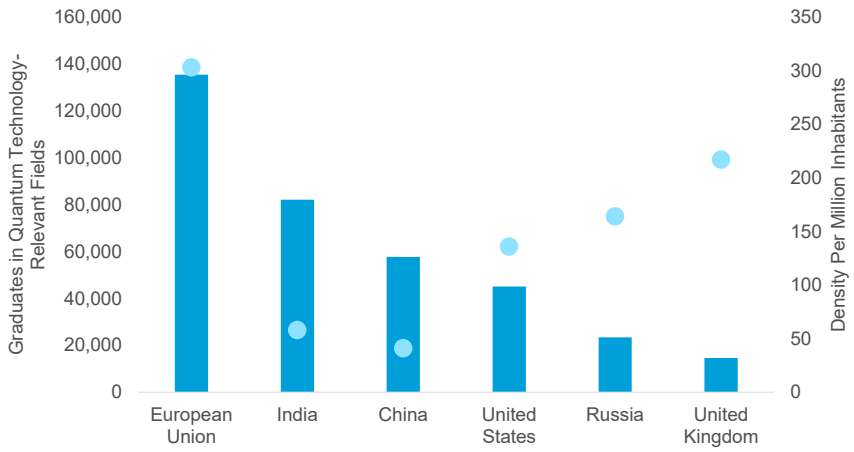
Nonetheless, this is still a far higher barrier to entry than for many other industries, and there is much work to be done to make the prospect of a career in quantum computing more accessible for much of the workforce. Nation-states are increasingly realizing this and incorporating the matter of workforce education into their national strategies. The U.S. has already begun this process and suggested ways to develop a quantum-ready workforce. This includes actions that intend to introduce broader audiences to quantum technologies through public outreach and education materials, address quantum-specific gaps in professional education and training opportunities, and make careers in quantum technologies more accessible and equitable.[110]

All this, however, will take time to implement. Even without the need for a PhD (which, as discussed above, most jobs still require), given it typically takes 3-5 years to train a new student and meet the employment expectations to work in the field, such initiatives are unlikely to provide a solution to the quantum computing skills shortage in the near term.

Training Those with Adjacent Skills

To meet the near-term demand for talent in quantum technologies, it will be increasingly necessary to train those with adjacent skills. Workers will likely be generalists with backgrounds in disciplines such as computer science or engineering, rather those educated specifically in quantum technologies.[111] One study found that there could be as many as 350,000 Master's-level graduates globally in fields that are relevant to quantum technologies, with over 100,000 in the European Union alone.[112]

Figure 42. Number of Graduates in Fields Relevant to Quantum Technologies



Number of graduates of master's level or equivalent in 2019 in biochemistry, chemistry, electronics and chemical engineering, information and communications technology, mathematics and statistics, and physics. High-level estimates are represented for China. The actual U.S. talent pool may be larger, as bachelor's programs are longer and master's programs are less common.

Source: McKinsey Digital, Citi GPS

[110] U.S. National Science & Technology Council, "Quantum Information Science and Technology Workforce Development National Strategic Plan," PDF, February 2022.
[111] Chuck Leddy, "Q&A: The Talent Shortage in Quantum Computing," MIT News, January 23, 2019.
[112] McKinsey Digital, "Quantum Technology Sees Record Investments, Progress on Talent Gap," April 24, 2023.

Such graduates would still need training to adapt their skills to make useful contributions to quantum engineering-related work. Numerous one-year supplementary curriculums are being considered to help with switches to quantum-related roles, but also several short courses are beginning to emerge to allow the transfer of skills to the quantum computing industry.

Multiple public and private entities are engaged in these efforts. For instance, MIT offers a number of online courses, ranging from those providing an introductory understanding of quantum computing fundamentals, to more specialist courses looking at different types of quantum algorithms. There are also efforts by various organizations, such as The Quantum Strategy Institute, to educate future graduates on the requirements of quantum engineering roles.[113] Other examples include Q-CTRL's Black Opal learning tool which offers a training portal that individuals can use to transfer their skills to quantum computing, and IBM's quantum developer certification program.[114]

In addition, meaningful internship and training programs that last at least 3-4 months can also help expand quantum computing candidate pools. IBM has been running a quantum computing internship with an annual intake of well over 100 people for several years.[115] Furthermore, hiring agencies are already building their own quantum computing candidate pools.

Of course, it is important to note that not all types of jobs in quantum computing need quantum-specific skills. In all likelihood, as the industry matures into a phase driven less by research and more by product and service delivery, the proportion of jobs in the industry that require more commercial and industrial skills, such as project management or marketing, is likely to grow. Some in the industry have suggested that roles that do not need quantum-specific skills (e.g., general software developers, non-technical roles such as product sales, etc.) are already becoming as in-demand as those requiring quantum-specific skills (e.g., experimental physicists, quantum algorithm developers, etc.).

Fundamentally, the upskilling and re-skilling of people with adjacent skills will play a critical role in meeting the demands of the quantum computing industry. However, as the Director of the National Science Foundation (NSF) described in a recent quantum technologies conference, there may not even be enough trainers in the quantum computing industry to upskill or re-skill a quantum-relevant workforce. One report suggests that less than 50% of quantum computing jobs will be filled by 2025.[116] As such, the talent shortage is likely to persist for some time, with wage inflation and competition for talent seeming likely — yet another reason why nation-states wishing to adopt the technology need to plan ahead.

---

[113] Amrita Manzari, "Roadmap to Quantum Engineering," Quantum Strategy Institute, October 26, 2021.
[114] Jeffrey Burt, "Q-TRL Black Opal: Quantum Learning for the Masses, QControl's Black Opal Learning Tool" The New Stack, December 3, 2021; Abe Asfaw, Kallie Ferguson, and James Weaver, "IBM Offers Quantum Industry's First Developer Certification," IBM, March 29, 2021.
[115] IBM, "IBM Quantum Internship Applications for Summer 2022 Are Still Open," September 7, 2021.
[116] Niko Mohr et al., "Five Lessons from AI on Closing Quantum's Talent Gap — Before It's Too Late", McKinsey Digital, December 1, 2022.

National Security Concerns

Finally, one particularly challenging issue for nation-states is that much of the talent in the field comes from foreign countries. A report from the White House Subcommittee on Economic and Security Implications of Quantum Science (ESIX) emphasized the indispensable role foreign talent and international companies play in the U.S. quantum ecosystem.[117] However, despite this, due to the fact that quantum computing has been recognized as an area of strategic significance to many countries, even if these foreign experts agree to join a company in the U.S., they must go through immigration reviews conducted by the government to be officially onboarded.

The ESIX report underscored that the U.S.'s domestic quantum computing talent supply fell short of domestic workforce demands by a large margin. With the competition to deliver large-scale quantum computers getting increasingly fierce, this shortfall of talent is only likely to increase in the near term. Issues like this present both a challenge and an opportunity for nation-states, as governments can help foster the needed collaboration between academia and industry.

We spoke to Dr. Stefano Gogioso, a leading computer scientist and researcher in quantum computation at Oxford University, about some of the challenges in educating a workforce in quantum computing.

[117] Nick Flaherty, "U.S. Summit On Quantum Industry Highlights Skills Shortage," *EE News Europe*, October 11, 2021; National Science & Technology Council, "The Role of International Talent in Quantum Information Science," PDF, October 2021.

Expert Interview with Computer Scientist and Researcher, Dr. Stefano Gogioso, at Oxford University

Dr. Stefano Gogioso
Computer Scientist and Researcher in Quantum Computation, Oxford University

Q: What are the biggest challenges when it comes to educating a workforce in quantum computing?

Dr. Gogioso: Quantum computers are exotic machines. They are fundamentally different from the computers we use today and scaling them beyond small prototypes has proven challenging. Such development efforts often dominate the quantum news cycle, but they are not actually a concern for the workforce at large: Figuring out which hardware architectures scale best, among the ten or so major ones currently in development, is a task for highly specialized physicists and engineers.

When it comes to educating and training professionals, the biggest challenge is that the exotic nature of these machines extends beyond their hardware, to the problems they can solve and the way in which they solve them.

Quantum computing is going to be a truly differentiating factor for businesses and nation-states only in the presence of custom applications: In any such adoption scenario, professionals are inevitably faced with an entirely different way of computing and solving problems. Unfortunately, the language used by quantum specialists is decades old and heavily reliant on advanced mathematics, making it inaccessible to the wider public: As a first step, we need to rephrase the same concepts in new and relatable ways. Then, we need to develop programming tools that use these ideas to make quantum computing accessible to professionals from a broad variety of backgrounds. The only way to educate a workforce at scale is to give them the means to truly understand how quantum computing works, to easily experiment with it, and to quickly prototype new applications.

Q: What level of upskilling is expected for professionals wishing to join the quantum computing workforce?

Dr. Gogioso: The simplest scenarios for quantum adoption involve the solution of problems from a pre-defined class, using a pre-packaged quantum computing service (D-Wave's quantum annealing is an example). Here, professionals are only required to moderately upskill, learning to recognize suitable problems (for D-Wave, constraint satisfaction and combinatorial optimization) and being trained to formulate such problems for submission to the service (for D-Wave, this happens in the form of quadratic unconstrained binary optimization — QUBO). Existing domain-specific knowledge remains the primary driver for the origination of interesting problems, as well as the creation of new value using solutions obtained from the quantum computers.

More sophisticated adoption scenarios instead require the formulation of custom applications for quantum computers: These could range from novel uses of established quantum algorithms to the development of brand-new ones through a continuum of proprietary modifications. For professionals wishing to develop such applications, the upskilling is significant but progressive. In the chemical, biomedical, and materials sectors, for example, one could start by learning about relevant quantum simulations and how to tailor them for execution on quantum computers.

For machine learning and artificial intelligence professionals, one could instead learn about quantum neural networks, where they are expected to outperform their classical counterparts, and the idiosyncrasies of their usage. Specific training is first required to write effective quantum programs, then to make efficient use of expensive computing resources, and finally to squeeze the most out of available quantum hardware. Experimentation and the drive to extract value will, in time, lead to the customization and optimization of existing quantum techniques, and then to the development of new ones, informed by domain-specific knowledge and business needs.

Supply Chains

Supply chain challenges have become familiar to nearly all large corporations over the past two years. In particular, the silicon chip shortage has shown just how fragile the global supply chain is, and how unexpected events can disrupt what many would consider one of the world's most heavily invested in and broadly interconnected industries — classical computing.

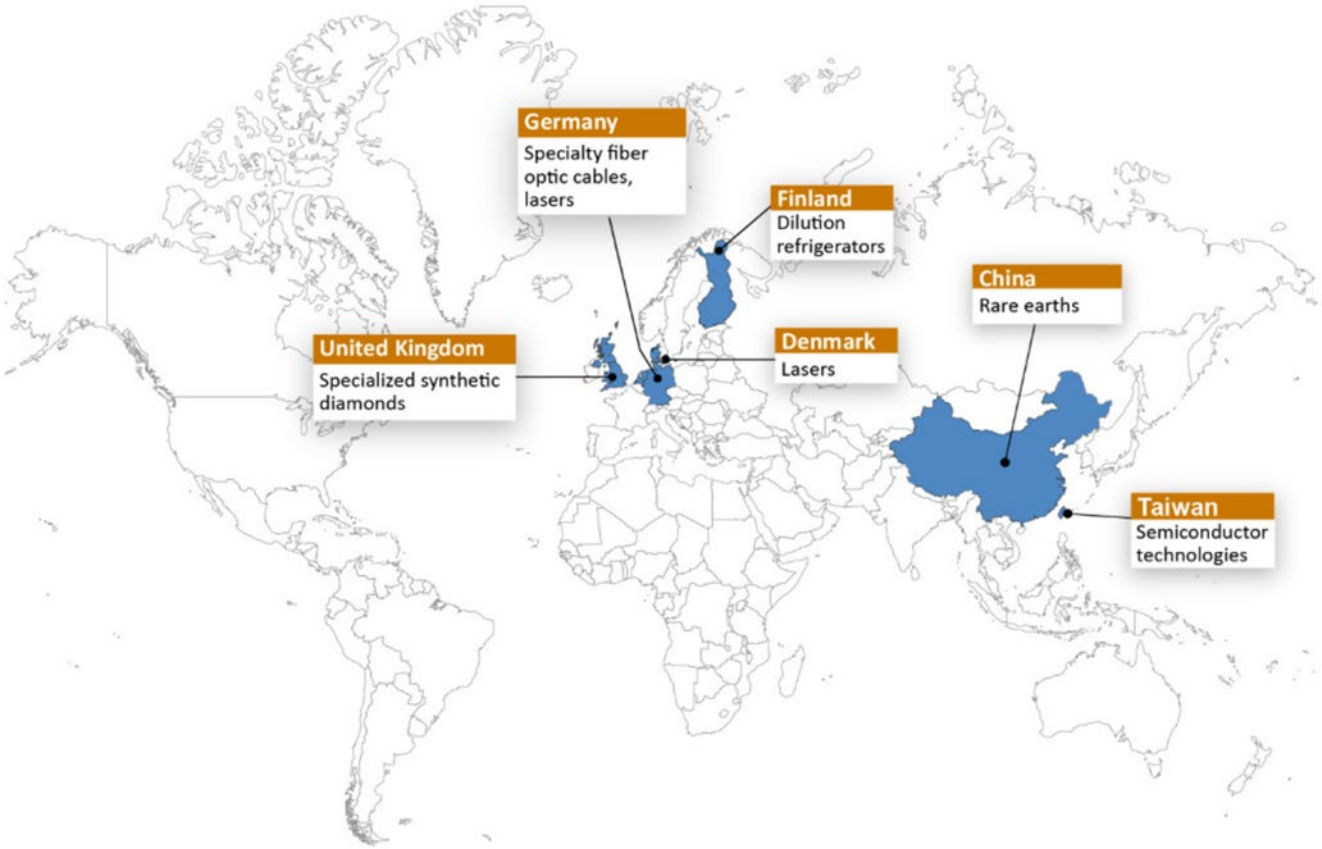
What Makes the Quantum Computing Supply Chain Different

Like that of classical computing, quantum computing's supply chain is global, but even more highly specialized and complex. As highlighted in a July 2016 report by the National Science and Technology Council titled *Advancing Quantum Information Science*, the additional needs of quantum computers over classical computers involve the development of novel qubit technologies, as well as other technologies needed to control a quantum computer. All these various quantum technologies could result in supply chain bottlenecks of strategic importance to nation-states. Complicating this further is the fact that different types of quantum computers with different qubit technologies are currently being pursued.

On the one hand, the large variety of qubit technologies could make it more difficult for manufacturers to achieve the economies of scale reached by the classical computing industry, thereby inhibiting manufacturers' ability to lower prices. On the other hand, this same breadth of approaches to building quantum computers could mitigate the increase in prices that could arise from a global quantum computing "gold rush." Right now, it is too early to say if there will even be a winning qubit technology that achieves adoption across the world (in the same way that the silicon chip became predominant in the manufacturing of classical computers), or to predict the impact this may have on a still-developing quantum computing supply chain.

Novel qubit technologies are just one part of the overall quantum computing supply chain, which countries are already beginning to evaluate more holistically. The U.S. Government Accountability Office (GAO), for instance, produced the chart shown in Figure 43 highlighting some of the components needed to make a quantum computer that are supplied from outside of the U.S.

Figure 43. Select Examples of Quantum Technology Component Parts Around the World



Source: U.S. Government Accountability Office

As Figure 43 shows, in addition to rare earth materials from China and the semiconductor technologies from Taiwan that already present significant bottlenecks for the classical computing supply chain, components specific to the quantum computing supply chain are produced all over the world. One example identified above is the manufacturing of dilution refrigerators in Finland (although notably, since the production of this map, numerous other countries have begun looking into building their own).

The Need for Extreme Cooling

Originally proposed by Heinz London in the 1950s, dilution refrigerators are able to cool their contents to near "absolute zero."[118] Absolute zero is the coldest possible temperature of any material; at that point, the material contains in effect zero energy and corresponds to around −273.15 °C on the Celsius temperature scale. The reason reaching this temperature is important for the manufacturing of quantum computers is because, as discussed earlier in the report, qubits are susceptible to noise, which comes in the form of ambient thermal energy. Thus, quantum computing technologies, such as superconducting qubits, need to be supercooled to these extremely low temperatures to prevent decoherence.

[118] Graham Batey and Gustav Teleberg, *Principles of Dilution Refrigeration: A Brief Technology Guide*, Oxford Instruments NanoScience, PDF, September 2015.

When discussing temperatures this low, most people refer to the Kelvin (K) scale — an absolute temperature scale obtained by shifting the Celsius scale by −273.15 °C so that absolute zero coincides with 0 K.[119] In fact, the temperatures needed by quantum computers are sometimes measured in milli-Kelvin, or mK, only a few thousands of a degree above absolute zero. For context, the temperature of outer space is often quoted as being around 2.7 K.[120] Ultimately, this need for extreme cooling presents a potential additional bottleneck for the already complex quantum computing supply chain.

Figure 44. Quantum Computing Dilution Refrigerator

Source: Shutterstock

We spoke to Dr. Anthony J. Yu, Vice President of Silicon Photonics Product Management at GlobalFoundries, a semiconductor foundry that is collaborating with industry leaders to produce photonic-based quantum computers, about some of the unique characteristics of the quantum computing supply chain.[121]

[119] Encyclopedia Britannica, "Temperature: Physics," last updated December 1, 2022.
[120] Philip Ball, "Space: How Cold Does It Get When We Leave Earth?" BBC, September 19, 2013.
[121] Prableen Bajpai, "An Overview of the Top 5 Semiconductor Foundry Companies," Nasdaq, October 1, 2021; GlobalFoundries, "GlobalFoundries Announces Next Generation in Silicon Photonics Solutions and Collaborates With Industry Leaders to Advance a New Era of More in the Data Center," March 7, 2022

Expert Interview with Dr. Anthony J. Yu, Vice President of Silicon Photonics Product Management at GlobalFoundries

Dr. Anthony J. Yu
Vice President of Silicon Photonics Product Management, GlobalFoundries

Q: What are the key differences in the quantum computing supply chain compared to the classical computing supply chain?

Dr. Yu: The key difference in quantum-based compute is that most, if not all, implementations involve dilution cooling to 4 degrees Kelvin (K) or less, require 3D semiconductor packaging compatible with large form factors and very low temperatures (<4K to reduce phonon noise), and tend to use non-standard semiconductor materials (e.g., yttrium, magnesium, niobium nitride, barium tantalum oxides, and nitrides) for either single ion sources or single photon detection.

Semiconductor lasers have been used in strong attenuation mode as single photon sources and should be included in the supply chain (III-V lasers). Novel/rare materials are covered by the GAO map — advanced low temperature 3D semiconductor packaging is not. The ideal form factor for a quantum system would be to fit within a 2U or 4U datacenter rack — which drives extremely miniaturized cooling systems (first solutions will be dedicated cabinets and not 2Us).

Q: What do you think are the key challenges to the quantum computing supply chain?

Dr. Yu: This is, by definition, a low temperature application — every quantum system that we are aware of requires cooling of the source and the detection to somewhere between 4 millikelvins (mK) and 4K — the strongest supply chain disruption would be access to cooling solutions.

A business challenge with developing the quantum supply chain is volume — these solutions are in their embryonic stage at the present time, they will need volume drivers to move from new product introduction (NPI) to full production. To facilitate this transition, due to the uniqueness of the quantum solutions, capital investment will be needed ahead of time — with strategic vision — or the volume ramp and the promise of quantum compute will be delayed. In this sense it is no different than any other 300mm investment opportunity — aside from the very early product maturity.

Q: What do you think stakeholders should be aware of about the quantum computing supply chain?

Dr. Yu: The packaging and 3D wired or wireless interconnect to quantum compute elements is fundamentally different than mainstream compute. This requires dedicated investments (usually IDMs) to implement the specialized systems. There is little to no economy of scale due to the uniqueness of the approaches to quantum compute — targeted investment ahead of the need is required.

Ethics

With great power comes great responsibility. Quantum computers have the potential to reshape our world by enabling breakthroughs in medicine, material science, finance, and other industries. This implies, however, that they could unleash equally great terror if used improperly. With breakthroughs in medicine design come potential breakthroughs in the design of chemical weapons, for example.

The Need for Ethics

Such risks underscore the importance of players in the quantum computing field to proactively consider the ethical dimensions of building such machines. In particular, as nation-states race to be the first to build a fault-tolerant quantum computer, having a set of ethics, rules, and guidelines may be critical to ensuring that quantum computing remains a boon to, and not a burden on, humanity.

The U.S. government has been an early champion of ethical considerations in the field of quantum computing. Alongside dedicated R&D funding, multiple branches of government have taken action to ensure that the quantum programs and grants incorporate ethical considerations in their structure.

Figure 45. Ethical and Legal Considerations

Source: Shutterstock

Integrating Ethics into Legislation

One year after the 2019 National Defense Reauthorization Act (NDAA) authorized the Department of Defense (DoD) to create a Quantum Information Science (QIS) research, development, and deployment program, Congress added a mandate for ethical considerations in the NDAA.[122] This provision requires the DoD to develop a plan for the "development of ethical guidelines for the use of quantum information science technology."[123]

[122] U.S. Congress, "H.R. 5515," PDF, accessed March 8, 2023.
[123] U.S. Congress, "National Defense Authorization Act for Fiscal Year 2020," PDF, accessed March 8, 2023; Congressional Research Service, *Defense Primer: Quantum Technology,* updated November 15, 2022.

Ethical considerations have also been embedded in new government programs from their inception, for example in the recently signed CHIPS and Science Act. This legislation mandates that the Director of the National Science Foundation (NSF) revise proposal instructions — within 24 months — to require that ethical considerations are included in applicable proposals for funding, and to instruct that these ethical considerations be factored into award decisions.[124] This provision begins with the notion that emerging areas of research present potential ethical concerns, and other sections of this law identify quantum technology as an key technology focus area for the authorized programs. Therefore, it is likely that the NSF Director will apply the requirement for ethical considerations to be included in quantum computing grant proposals.[125]

The CHIPS and Science Act also includes ethics in its creation of the new NSF Directorate for Technology, Innovation, and Partnerships (TIP), the $81 billion program designed to spur "translational and use-inspired" research and development in the ten listed key technology focus areas, which include quantum information science and technology.[126] This provision mandates the Director to ensure that ethical considerations are "taken into account in the priorities and activities of the [TIP] Directorate, including in… the awards-making process and throughout all stages of supported projects."[127]

These two examples of recent statutory and regulatory action on quantum computing ethics provide a sense of current quantum computing ethical priorities in the U.S. government, and hint at what we can expect in the near future from other governments. First, the above authorized programs need to be implemented in full, which will likely involve consultation with non-government stakeholders and could involve notice and comment rulemaking. Other federal agencies not described in detail here, such as the National Institutes of Standards and Technology (NIST) may join the NSF and DoD in establishing ethical standards or guidelines for quantum computing. Finally, the 2018 National Quantum Initiative (NQI) Act is due for reauthorization this year, and the inclusion of quantum ethics in the NDAA as well as the CHIPS and Science Act suggests that Congress may look to include ethical considerations in the NQI reauthorization.

In addition, many within the field of quantum computing itself have begun to consider the ethics of building such machines. Fundamentally, the earlier that nation-states begin legislatively addressing the issue of ethics in quantum computing, the better we can prevent ethical issues arising from the technology's use in the future.

We spoke to Nick Farina, CEO of EeroQ and quantum ethics advocate, about how the issue of ethics in quantum computing is being addressed.

[124] U.S. Congress, "H.R. 4346," PDF, accessed March 8, 2023.
[125] Ibid.
[126] Ibid.
[127] Ibid.

Expert Interview with Nick Farina, CEO of EeroQ

Nick Farina
CEO, EeroQ

Q: Why should we consider ethical guidelines for quantum computing, despite the relative immaturity of the technology?

Nick: Quantum computing will open entirely new frontiers of processing power, which we are only now beginning to understand. To create ethical guidelines for the use of this technology, we must first focus on understanding all of the potential applications (both positive and negative) of quantum computing. This is a nontrivial task, involves both quantum researchers and end-users of the technology, and will always be a work in progress as new applications are discovered. Second, once we understand the potential applications, we then need to think carefully about developing ethical frameworks around them. This is a process that will take multiple years and involve coordinating agreement among myriad stakeholders, both corporations and governments. Thus, the process should begin now and in parallel with quantum computer development.

Q: How can companies engage in federal policy around quantum computing ethics and regulation?

Nick: It is our view that quantum computing needs a multidisciplinary approach to regulation, as it will impact such a broad swath of society. Regulation at the federal level is inevitable and has already begun with pending export controls and the requirement for the Department of Defense to develop ethical guidelines in the 2020 National Defense Authorization Act. For companies looking to make the most of quantum computers while ensuring their usage minimizes harm, this formative time of legislative activity provides a chance to have an outsized voice in the dialogue. Ideally, regulation will avoid overly onerous restrictions on commercial use, while still preventing either clear misuse of the technology by bad actors or accidental abuse of the technology by those with good intentions but no regulatory frameworks.

Q: How can novel types of quantum computing designs (such as neutral atoms, photonics, or electrons on helium) change the expected timeline of quantum computing's impact and related ethical concerns?

Nick: If we assume the progress of quantum computing power to be linear, then one might expect it will be 10 or more years before we have applications requiring ethical considerations. However, we have many points of evidence that the technology will develop at a faster, more nonlinear pace than expected. One particular "X factor" is the rise and funding of new types of quantum computers that offer the potential to "leapfrog" the technologies currently furthest ahead. For example, the first two-qubit gate of an ion trap was in 1995, and ion traps are still in the range of dozens of qubits. While this has not been physically realized yet, there are multiple credible and well-funded academic and industry efforts that may be able to scale from the order of two to 10,000 qubits much faster than today's most well-known technologies. If one of these technologies begins to work, we will face ethical challenges much sooner than expected.

How to Prepare: A Holistic Quantum Computing Policy

In conclusion, quantum computing offers nation-states an opportunity to capitalize on the potential next leap in computing. While the best-positioned countries are the ones investing in the infrastructure and educating their workforces now, there is still considerable opportunity left given the early stage the industry is in. What is clear, however, is that any nation-state wishing to build its quantum computing industry needs to establish a holistic policy that supports both the underlying technology infrastructure and the overall quantum computing ecosystem.

As discussed earlier, government investment is often key to getting a nascent technology off the ground. This is especially true of quantum computing given the technology's specialized nature and the fact that quantum advantage has yet to occur. As the technology develops further, the talent shortage is likely to worsen in the short term — similar to how many countries have experienced a shortage of software engineering talent in recent years. However, unlike in that shortage, gaining the skills to become a quantum-computational engineer or scientist is likely to take many years. This means that nation-states need to start thinking ahead, and in order to meet future demand, begin to design curriculums at much earlier academic stages than is currently the case. This will require collaboration between different governmental agencies, academia, and ideally, industry.

Of course, bottlenecks in the quantum supply chain are a big risk, as components are sourced from all over the globe (see Figure 43). Hence, strategic initiatives between countries in this decade may be crucial to a nation-state's ability to capitalize on quantum computing in the decades ahead. Finally, forward-thinking nation-states should be considering quantum computing's attendant ethical concerns before we reach the era of quantum advantage.

The 2021 Citi GPS report *Holistic Digital Policy: Nation States Must Lead in Building Equitable Human-Centric Digital Economies* analyzed the digital transformations of 11 countries and effectively created a toolkit that governments around the world could use in designing their own national digital policies. It then looked into the approaches individual countries could take around digital policy based on their unique strengths and provided a framework for implementing a holistic policy. Given the strategic significance of quantum computing to nation-states — not just in terms of the potential economic opportunity, but also from a defensive cybersecurity perspective — quantum computing could be a technology for which the report's framework could apply. Proactively designing and implementing a holistic quantum computing policy could enable nation-states with sufficient infrastructure — including those that may not have led the way in the current classical computing paradigm — to potentially leapfrog their competitors.

We spoke to Celia Merzbacher, Executive Director of the U.S. Quantum Economic Development Consortium (QED-C), about some of the aspects nation-states should consider when developing a quantum computing policy.

Expert Interview with Celia Merzbacher, Executive Director of the U.S. Quantum Economic Development Consortium (QED-C)

Celia Merzbacher
Executive Director, U.S. Quantum Economic Development Consortium (QED-C)

Q: What are the greatest challenges to realizing the potential of quantum computing?

Celia: There are three main barriers that need to be addressed: The hardware must be improved and scaled up; new "quantum computer science" is needed, including algorithms and error correction schemes; and demonstrated use cases must be established that have substantial market potential. Overcoming these challenges will require a lot of engineering R&D by the private sector and investment in fundamental scientific research by the public sector. Identification of use cases requires engaging end users in depth and can be greatly aided by consortia like QED-C, which brings together the entire innovation ecosystem.

Q: What lessons can governments that wish to develop their own quantum computing strategies learn from the development of the quantum computing industry over the past 10-20 years?

Celia: A lesson from the early development of the quantum computing industry is that it is still early! There is not yet a clear winner among the several technologies that are being developed — and more than one may be successful for specific applications. Therefore, governments can assess their nation's strengths, whether in theoretical aspects, engineering, manufacturing, or something else, and then partner and invest strategically.

Q: How should a quantum computing strategy be different than a classical computing strategy?

Celia: When classical computing was being developed, government (in the U.S. in particular) was the primary customer and was willing and able to pay a premium to support that development for government missions, including in the military and space. Today, computing applications are largely driven by customers in the private sector, for example finance, chemicals and drug development, logistics, entertainment, and games. To accelerate the development of quantum computing that will have applications in both government and commercial sectors, government should help reduce the risk of early-stage technologies and provide sound export controls that do not hamper innovation.

Q: To what extent are the leaders of the quantum computing era likely to be the same nations that have led the classical computing era?

Celia: Nations where there is a robust ecosystem that supports classical computing have the benefit of infrastructure that could be important for the development and manufacture of quantum computing systems. However, many advances will emerge from academic research institutions where researchers have access to the scientific literature and can collaborate more easily than in the past with colleagues worldwide. Therefore, breakthroughs — especially in theory and software engineering, which are less dependent on costly infrastructure and equipment — could emerge from any corner of the globe.

Corporates

For corporates, the opportunity that quantum computing presents will be far more specific than for nation-states, so corporates' actions will be highly specific to their particular industries and business strategies. From our discussions with numerous quantum computing companies and the corporate clients they serve, we identified three key areas that corporates should be aware of when attempting to understand the quantum computing landscape:

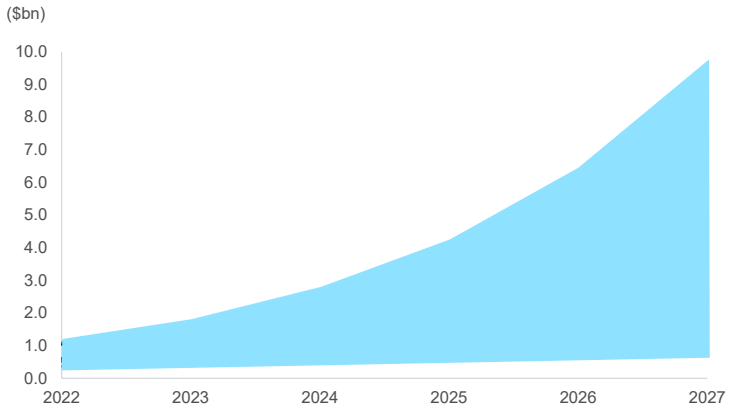
- What forecasts exist for total addressable market (TAM).
- What value creation could look like.
- Why collaboration and the cloud are key to corporate adoption.

Our discussions also showed us that the guidance corporates need depend on their goals with respect to quantum computing. Hence, we put together two separate sections with our conclusions for corporates — "How to Prepare: For Quantum Advantage" and "How to Prepare: For the Quantum Threat."

Market Forecasts

One broad way of gauging the size of the quantum computing opportunity is to look at forecasts for its total addressable market (TAM). To do this, we identified 10 reports with perspectives on the market, and using these reports, pulled together a consensus estimate of the quantum computing TAM through 2027. Based on the literature, the average market size estimate puts the quantum computing TAM at just under $650 million in 2022, growing at an average CAGR of around 30% to just under $3 billion in 2027 (see Figure 46). However, this is only part of the story.

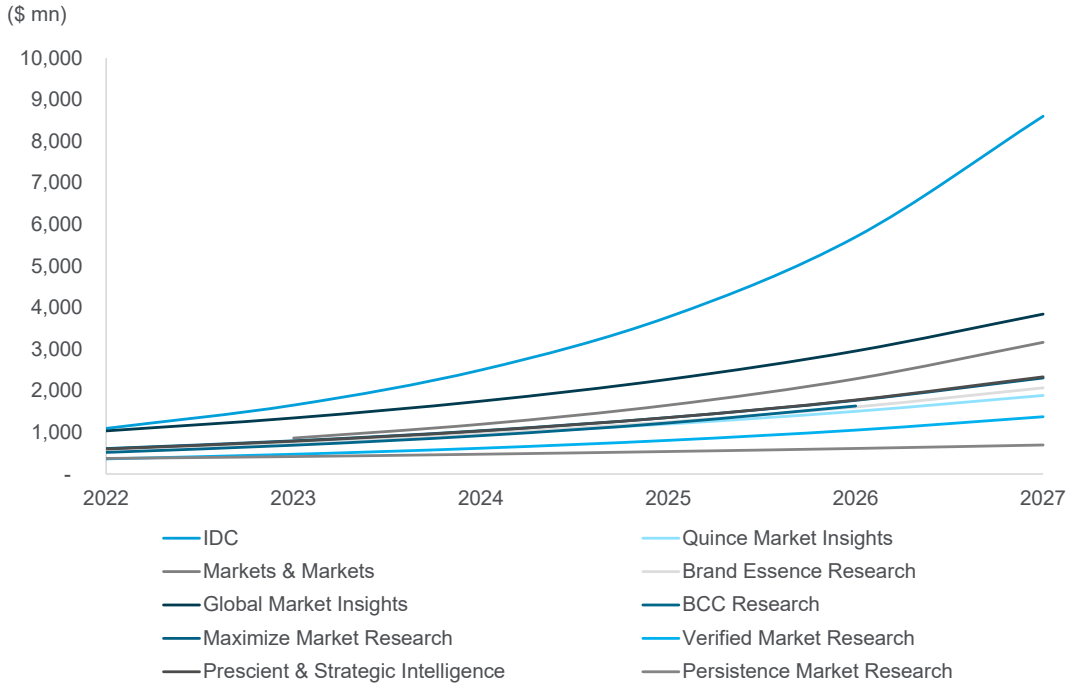
Figure 46. Range of Current TAM Forecasts (2022-27)



Source: Multiple TAM Forecasts, Citi GPS

There does not seem to be any agreed-upon size for the current TAM for quantum computing, with 2022 estimates ranging by a factor of 3, spanning anywhere from around $370 million to $1.1 billion. However, the literature seems to agree the industry is poised for exponential growth over the current decade, with CAGR estimates ranging from around 15% on the lower end to more than 50% on the upper end. Given the large variations in both the current TAM and the growth rate, this understandably leads to increasingly diverging forecasts (by a factor of over 10) as we enter the latter part of the decade, as noted in Figure 47.

Figure 47. Current TAM Forecasts (2022-27)



Source: IDC, Quince Market Insights, Markets & Markets, BCC Research, Maximize Market Research, Verified Market Research, Prescient & Strategic Intelligence, Global Market Insights, Fortune Business Insights

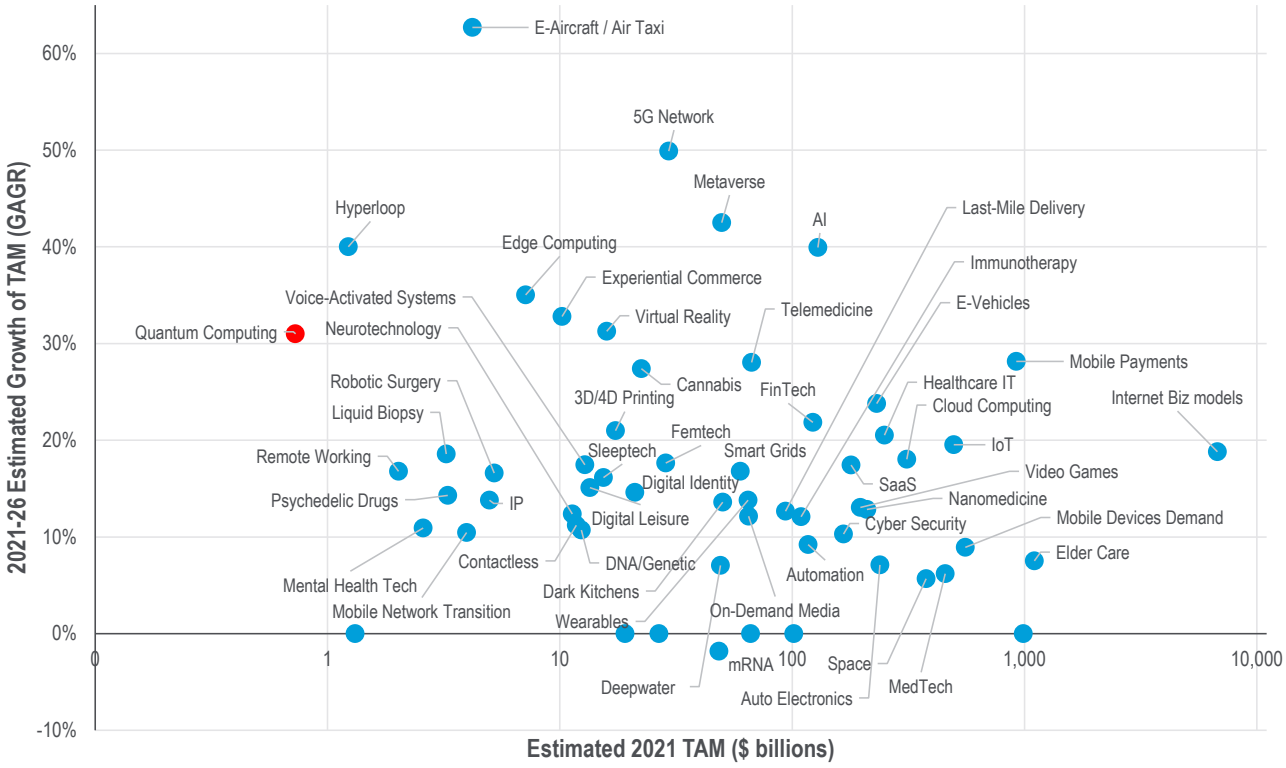
Comparing Quantum Computing to Other Areas of Innovation

Of course, in isolation, these TAM forecasts have limited meaning. As part of our ongoing analysis of the innovation and technology space as a whole, we analyzed the TAM forecasts for 100+ different areas of innovation, including almost 60 technology-orientated innovations that are often compared to quantum computing.

Our quantitative analysis enabled us to objectively compare different areas of innovation — something that is otherwise typically very challenging. Our findings were quite stark, TAM forecasts for various technological disruptions can vary by as much as 10,000x, with very broad areas of innovation such as Internet Business Models being several orders of magnitude larger than more narrowly labeled ones such as Remote Working or Mental Health. Our analysis found that Quantum Computing was somewhat of an outlier, with one of the lowest TAM estimates out of all the areas of innovation we looked at.

This makes sense, as the industry is still maturing, and most end-users today use the technology for research purposes. It also suggests that solely using the quantum computing TAM to analyze the market opportunity may not necessarily be the best way forward, which we discuss further in our next section “Value Creation.”

Figure 48. TAM Against 2021-26 Estimated Growth of TAM



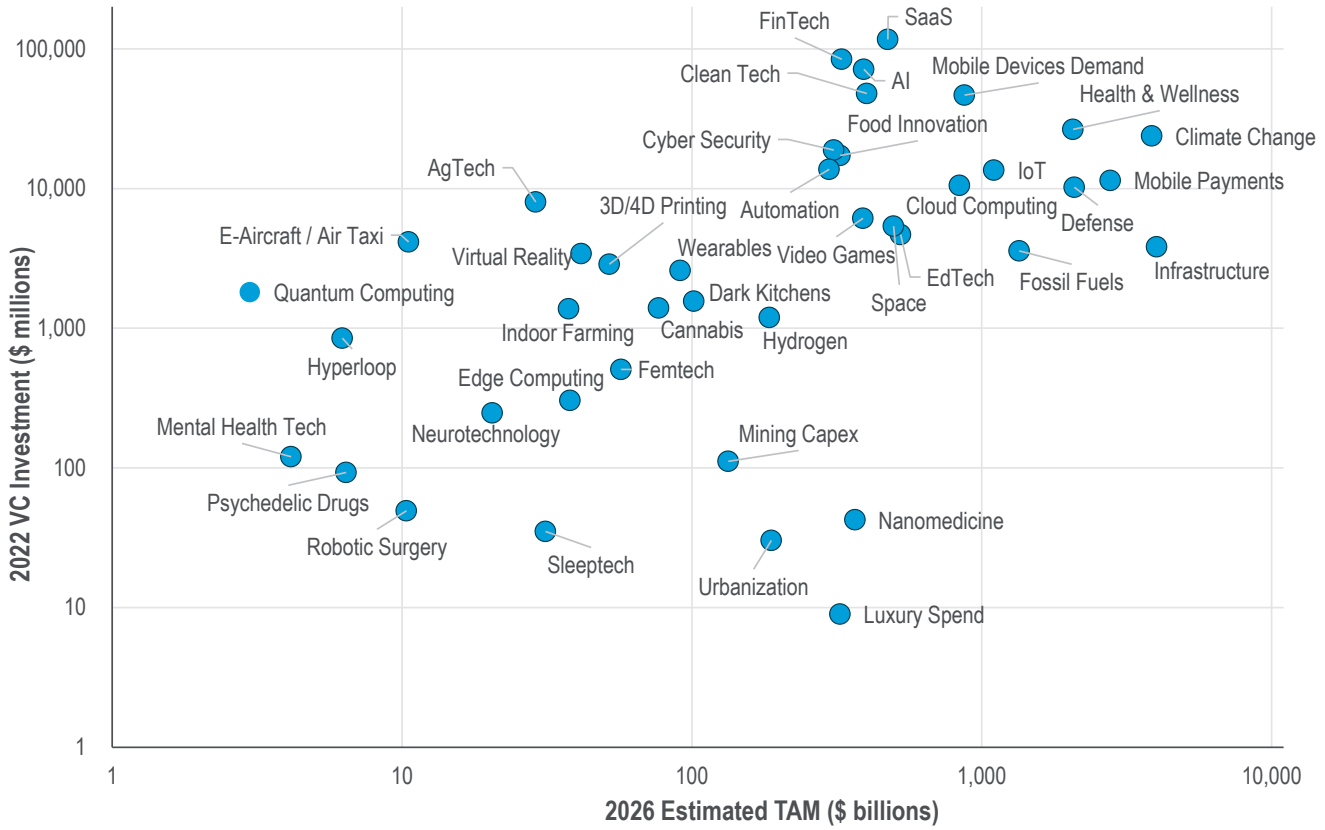
Source: Multiple TAM Forecasts, Citi GPS

Our analysis also showed that most areas of technological innovation had broadly similar estimated CAGRs over the period 2021-26, with a clustering around the 10-20% range. As can be seen from Figure 48 above, Quantum Computing is somewhat of an outlier in that it is on the upper end of this spectrum (at an estimated 31% CAGR), with a similar estimated growth to other innovations such as Edge Computing and Virtual Reality.

Notably, it has lower estimated CAGRs than other more topical areas of innovation that have gained mainstream traction in recent years, such as the Metaverse or Artificial Intelligence (AI). Again, this is not unexpected given the point above about quantum computers yet to be providing a commercial advantage to businesses. We anticipate this is likely to change relatively sharply, however, once the technology reaches the point of quantum advantage — also discussed further in the next section "Value Creation."

The above notion of quantum computing being an outlier is further supported when looking at Figure 49 below — arguably one of the most interesting lenses to evaluate the quantum computing market.

Figure 49. 2022 VC Investment Against 2026 Estimated TAM



Source: Multiple TAM Forecasts, PitchBook Data Inc., Citi GPS

When we compared the forecast 2026 TAM to the levels of 2022 VC investment in private companies, we found that quantum computing was the most densely invested area of innovation, with an average 2022-VC-Investment to 2026-Forecast-TAM ratio of over $600 million per $1 billion. For context, the next most densely invested areas were E-Aircraft at just under $400 million, Agricultural Technology (AgTech) at just under $300 million, Financial Technology (FinTech) at just over $250 million, Software as a Service (SaaS) at just under $250 million, and Artificial Intelligence (AI) at just under $200 million of VC investment in 2022 for every $1 billion of forecast TAM in 2026.

One interpretation may be that VCs are predicting the quantum computing industry to grow at a much faster rate than current estimates. Another interpretation is that VCs may anticipate a potentially oligopolistic market structure occurring in quantum computing, as was the case with classical computing, and are attempting to position themselves early by investing in some of the key players. We dive deeper into VC trends in the “Market Participants” section of this report below. Fundamentally, our analysis allowed us to put the quantum computing TAM and its projected growth into context. Nonetheless, as we discuss in the next section, the quantum computing TAM may not necessarily be representative of the whole quantum computing opportunity.

We spoke to Alex Challans, CEO of The Quantum Insider, about some of the challenges involved when assessing the quantum computing TAM.

Expert Interview with Alex Challans, CEO of The Quantum Insider

Alex Challans
CEO, The Quantum Insider

Q: What are the challenges when trying to determine the realistic total addressable market (TAM) for quantum computing, compared to other nascent technologies?

Alex: While we have a reasonable (but not perfect) idea of the potential use cases of a future quantum computer, there are numerous engineering challenges to overcome before we start to see devices that will enable this future. Contrary to some other nascent technologies, there is still significant uncertainty around the shape of future business models, as well as scarce existing data points demonstrating current revenue metrics. Most revenue-generating contracts signed by quantum computing companies today comprise joint research initiatives underpinned by a heavily consultative element, and they often do not reflect mature subscription or license revenue models of a mature industry. Indeed, there is still an important debate around how the revenue or cost savings generated from quantum use cases should be split between the quantum computing companies and their end-users. The current TAM estimates are therefore best treated as broad guiderails.

Q: In your opinion, what is the best way to gauge the TAM for quantum computing?

Alex: At The Quantum Insider, we saw the high degree of variability in the quantum computing TAMs already available in the market and wanted to anchor our estimates to numbers that are publicly available today. We therefore focused on the quantum computing as a service (QCaaS) market where companies such as AWS and Microsoft Azure were sharing the pricing of access to quantum computers. This meant that we could focus on utilization rates and the number of existing live quantum computers as the key estimated variable. We also liked BCG's way of looking at "value creation potential," which does a better job of highlighting the opportunity presented by quantum across different verticals.

While the TAM is an interesting area to investigate for organizations exploring new markets, we would encourage corporates to avoid getting fixated on precise percentages and numbers of billions of dollars; instead, they should focus on inflection or trigger points. By this, we mean proof points and technological breakthroughs, such as achieving a consistent enterprise use case for an early-stage (NISQ) quantum computer, which will demonstrate progress toward opening up significant market potential. Our expectation is that the gradual growth charts presented in most TAM predictions may end up being more exponential in character once these proof points have been hit.

Value Creation

An alternative way to gauge the quantum computing opportunity would be to look at the amount of value creation the technology could provide. To do so appropriately, however, it is important to be aware of misconceptions in the space.

Recognizing Adjacent Quantum Technologies

Quantum computing often receives much of the attention from the media — so much so, that, when people hear the word "quantum" they often just assume it is in reference to "quantum computing." But, as we have mentioned on a couple of occasions in this report, quantum computing is just one type of quantum technology. This presents somewhat of a challenge, as the quantum computing opportunity is often conflated with the much larger opportunity of quantum technologies, especially when talking about the broader notion of value creation.

Consequently, despite these adjacent quantum technologies being beyond the scope of this report, we feel it is important to recognize them. For instance, quantum communication harnesses the laws of quantum mechanics to protect data and offers the prospect of creating ultra-secure communication networks, and is something nation-states are already investigating.[128] Quantum sensing, on the other hand, is a form of advanced sensor technology that can detect changes in motion and electromagnetic fields, for instance. It offers the prospect of significant improvements in areas such as measurement and navigation, and quantum sensors are often described as potentially starting a revolution in a variety of areas from brain science to air-traffic control.[129]

Figure 50. Relevant Markets for Quantum Technologies

Sectors	Systems	Components
Cyber Security	Network Equipment	Photonics (lasers, photonic crystals, integrated circuits, imaging, communications)
Brain Diagnostics	Spectroscopy	MEMS Devices
North Sea Oil Reserves Recovery	Accelerometers Gyroscopes and Inertial Measurement Units	Cryogenic Equipment
GPS Navigation Devices	Sensors	
	Semiconductors	

Source: UK Government Office for Science (November 2016)

There are various synergies in the technical developments between these other quantum technologies and quantum computing, meaning that, from the perspective of nation-states, it makes sense to view quantum computing as often just one pillar of the broader quantum technologies opportunity.[130] For instance, the UK government previously outlined certain sectors, systems, and components in which quantum technologies represent an opportunity for companies (see Figure 50).[131]

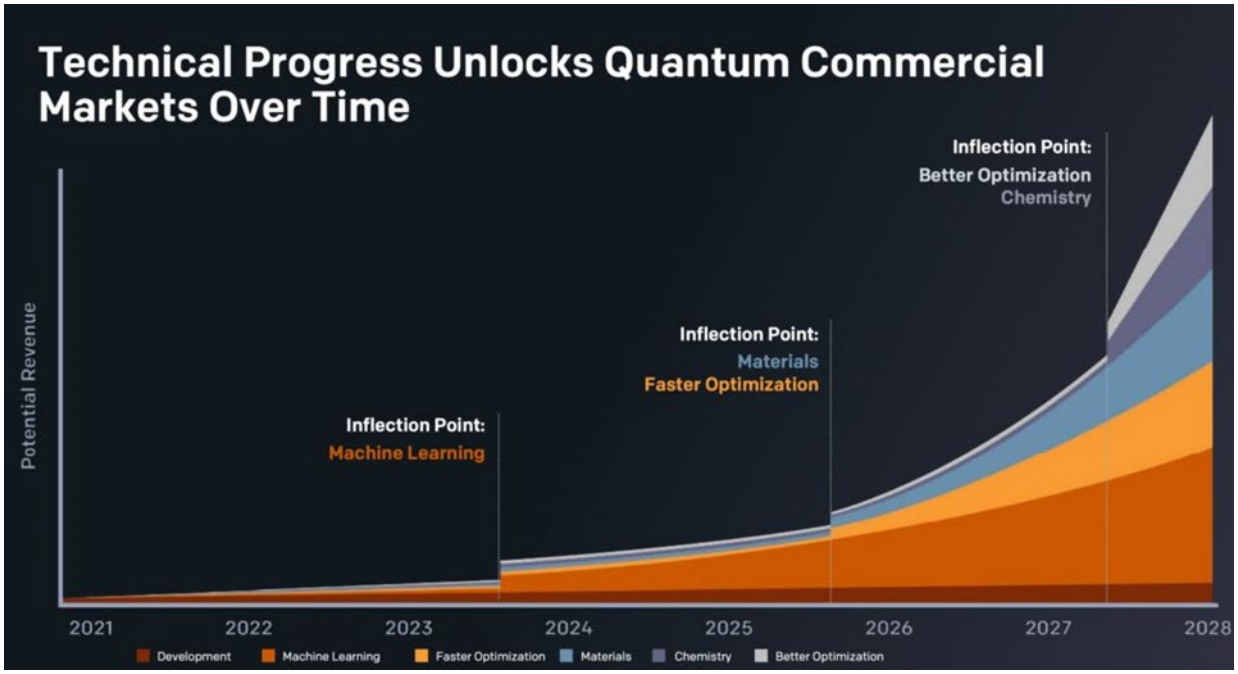
[128] Martin Giles, "Explainer: What Is Quantum Communication?" *MIT Technology Review*, February 14, 2019; UK National Quantum Technologies Programme, "UK Quantum Networks," accessed July 20, 2023.
[129] BAE Systems, "What Is Quantum Sensing?" accessed July 20, 2023; Kai Bongs, Simon Bennett, Anke Lohmann, "Quantum Sensors Will Start a Revolution — If We Deploy Them Right," *Nature*, May 24, 2023.
[130] Ofcom, *Quantum Communications: New Potential for the Future of Communications: Executive Summary*, July 28, 2021.
[131] UK Government Office for Science, *The Quantum Age: Technological Opportunities*, November 2016.

Being aware of these synergies helps put quantum computing into the broader context of quantum technologies (which itself may have other sizable opportunities not yet known). At the same time, it is important to note that on a business level, for corporates, the value creation quantum computing may offer will likely be distinctly different than those from these adjacent quantum technologies.

The Granular Nature of Quantum Advantage

When looking at the quantum computing opportunity specifically, one of the challenges with using the forecasts shown in Figure 51 is that all the estimates used one CAGR value for the duration of the forecast period. However, our discussions with experts in the quantum computing field (ranging from academics and governmental bodies to the CEOs of quantum computing companies) indicate it is unlikely for one CAGR value to apply to quantum computing. This is because value creation from quantum computing is unlikely to come all at once.

Figure 51. Step Changes in Potential Revenue Arising from New Use-Cases

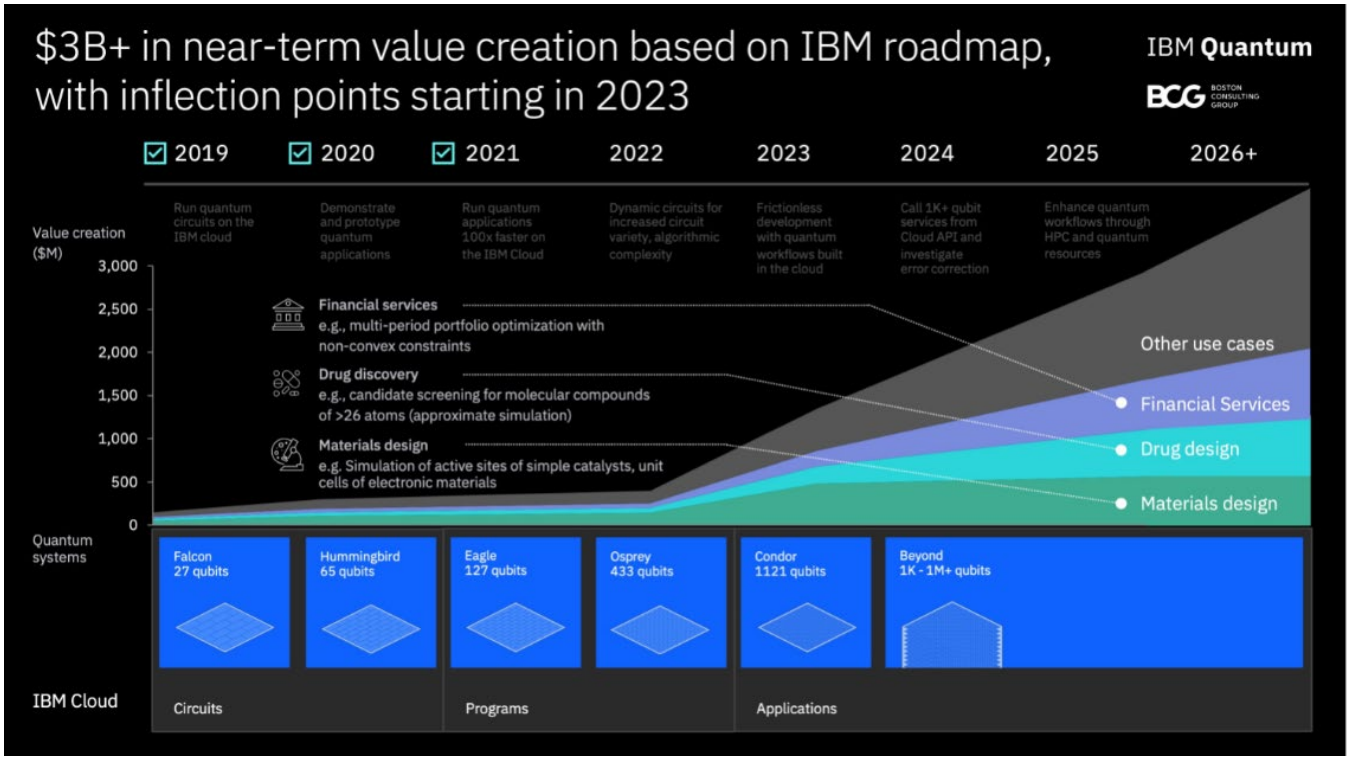


Source: IonQ

As discussed earlier, instances of quantum advantage will most likely be one of the key catalysts for commercial adoption and hence, higher potential revenue. Given the nature of progress in the quantum computing field and the suddenness with which quantum advantage may manifest itself, numerous inflection points will likely occur following each specific area of quantum advantage. Figure 51 above provides an example of such inflection points and the likely step-changes in TAM that may follow. It is these step-changes, or inflection points, allowing for value creation in industries that rely on the four areas most impacted by quantum computing: optimization, machine learning, simulation, and cryptography.

Figure 52 shows how value could be created in areas relating to financial services, drug discovery, or material design, to name a few. The amount of value creation is expected to increase as the ability to build larger and more powerful quantum computers, and run purpose-built applications on these machines, develops.

Figure 52. Value Creation Forecasts Based on a Quantum Computing Roadmap

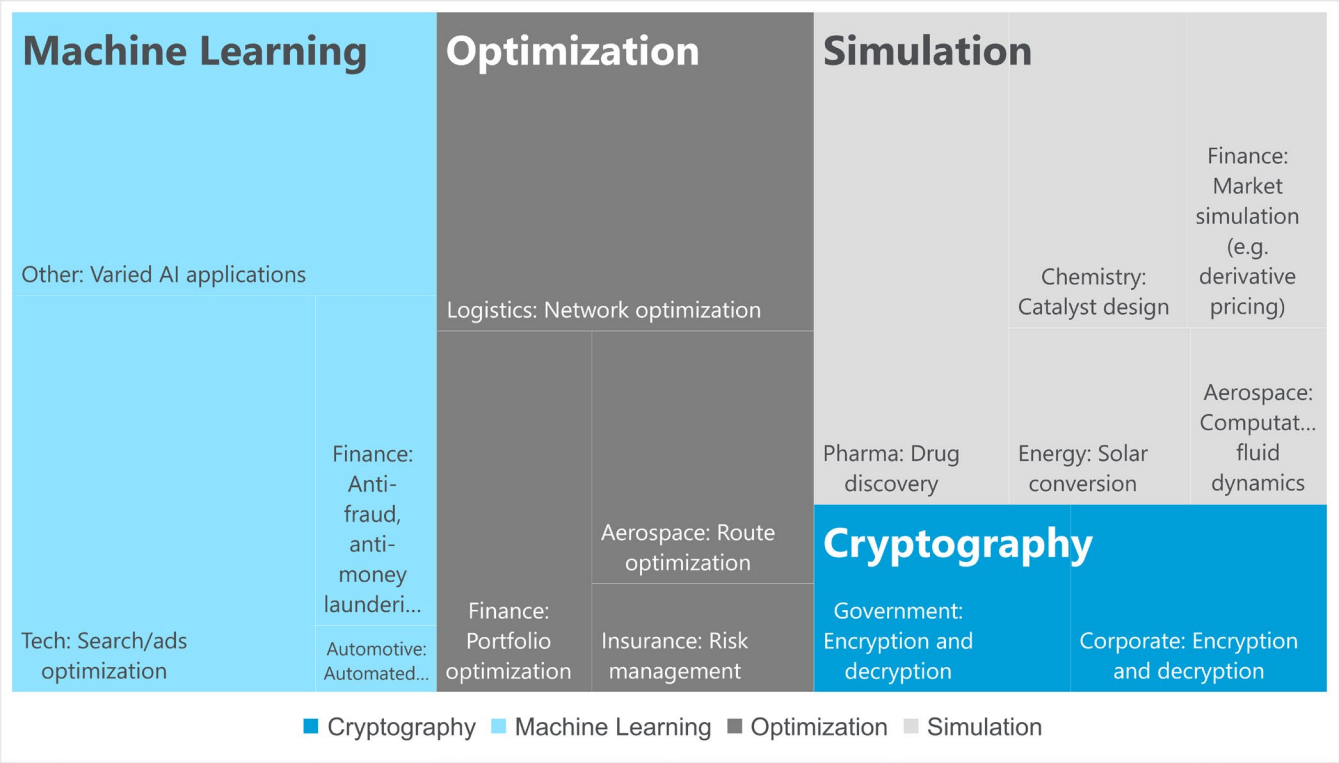


Source: IBM

Another useful aspect, shown in Figure 52, is how much of quantum computing's value creation may be in "other use cases." As discussed in the UK government's *The Quantum Age: Technological Opportunities* report, not all applications of the technology may be clear at this point in time or aligned with any particular industry. IBM estimated there may be over $3 billion in near-term value creation if the inflection points noted in Figure 52 begin in 2023.[132] However, it is almost impossible to tell exactly where, when, or by how much value creation there will be in each sector. For instance, BCG estimates the total annual value creation for end-users in the NISQ era (which they define as pre-2030) as $5 billion to $10 billion.

[132] IBM, "The IBM Quantum Development Roadmap," accessed April 10, 2023.

Figure 53. Potential Use Cases for Four Main Quantum-Advantaged Problem Types



Source: Boston Consulting Group, Citi GPS

Figure 53 provides some relative context to the value creation potential of quantum computing at the technology's maturity, which BCG estimates to be around $450 billion to $850 billion in the next 15-30 years.[133] Regardless of the precise total value, the key takeaways are that (1) value creation will likely be divided into the four broad areas of quantum advantage and (2) each area of quantum advantage will manifest itself in a highly granular way.

We spoke to William Hurley (better known as "whurley"), CEO of Strangeworks, about what value creation in quantum computing could look like.

[133] Jean-François Bobier et al., "What Happens When 'If' Turns to 'When' in Quantum Computing?" BCG, July 21, 2021.

Expert Interview with William Hurley, CEO of Strangeworks

William Hurley
CEO, Strangeworks

Q: How do you think value creation in the quantum computing industry will manifest itself?

William: The initial value creation will center around efficiencies in computing — time, cost, and quality. Large-scale problems that can experience marginal improvements in efficiency can lead to large savings. But the true value creation will come from problems and applications we haven't even thought of yet. No one in the '50s and '60s imagined social media and advertising as a use of computers at the time. The creation of entire industries is waiting for us when quantum computers become useful.

Q: Is there a particular area of quantum software that excites you the most?

William: This is admittedly biased, but our work at Strangeworks around the software infrastructure for quantum computers is incredibly exciting. The quantum software stack is currently very fragmented. Best-in-class solutions are available from different hardware and software players. The goal at Strangeworks is to bring all of these together and allow partners and customers to develop services that draw from all of these capabilities.

Q: Which problems does Strangeworks believe have the most potential for quantum advantage?

William: I have a slightly different view on this one. Many have suggested things like quantum chemistry and drug discovery as potential areas from which quantum advantage will first emerge. I think quantum has much broader applications. As an example, one of the first areas of quantum advantage we've seen is machine learning experiments. Recently, a team published a white paper on arXiv demonstrating that substantial quantum advantage can be realized using today's relatively noisy quantum processors. However, where I see the real opportunity is in any computational problem where you slightly increase the number of variables and the evaluation time of the problem increases exponentially. The traveling salesperson is used a lot as an example, but I believe there are a host of similar examples across industries.

Q: With more players entering the quantum computing market every year, what will give some players a competitive advantage?

William: Players that can effectively educate the customer about the promise of quantum computing as it relates to their industry and existing workflow will gain traction more quickly than those waiting for industries to come around. Many potential customers begin by asking us what the potential use cases are in their industry vertical — even those with quantum computing teams! The challenge is to get past the decision maker and connect to the subject matter expert or end user, discover their bottlenecks, and give them the resources to become advocates in their organization.

Collaboration and the Cloud

We feel that collaboration and the cloud will be key to the corporate adoption of quantum computing.

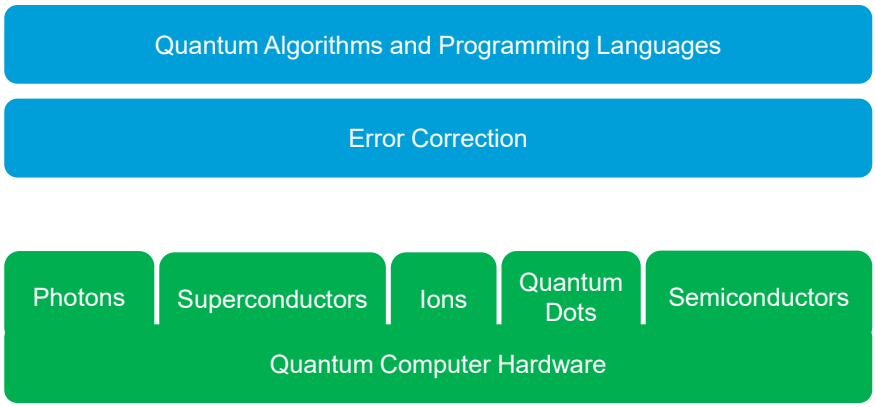
Understanding the Need for Collaboration

As we touched on in the "Nation-States" section at the beginning of this chapter, collaboration is likely key in developing a quantum computing ecosystem. Analogous to how building quantum computers will require collaboration between experts in fields such as physics and computing, commercializing quantum computing for corporate adoption will require collaboration between quantum computing companies themselves to build an efficient infrastructure — and most importantly, one that enables corporates to extract value.

Quantum computing companies will likely need to work together to standardize the technology. One of the easiest ways to understand this is to consider the role collaboration has historically played. For example, it was only with the advent of the universal serial bus (USB) protocol — a standardized connector agreed upon by industry players — that computer peripherals could be moved efficiently from machine to machine. Removing this friction allowed for a focus on the consumer experience.

Hence, on top of the needed collaboration between the academic and private sectors (as much of the theory behind quantum computers comes from academia), collaboration between quantum computing hardware and software companies will accelerate the path to quantum advantage. This is in part because, for many of the complex quantum algorithms and programming languages to run efficiently, they will need sufficient error-correction, which itself is an engineering problem that needs to be addressed in conjunction with the manufacturers of quantum computing hardware.

Figure 54. Breakdown of Layers Between Quantum Computing Hardware and Algorithms



Source: UK Government Office for Science (November 2016)

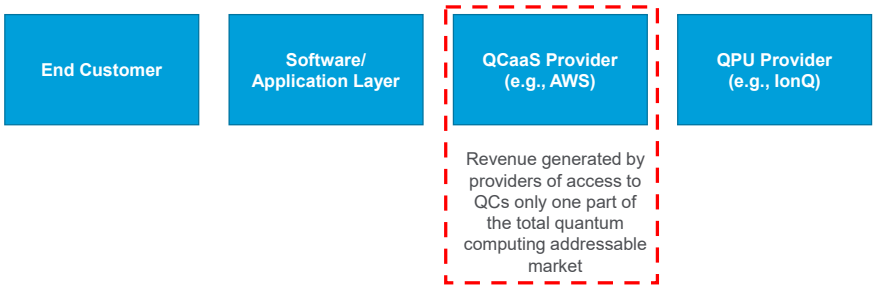
The Role of the Cloud

A number of competitors have begun offering access to their quantum computers via the cloud, dubbed Quantum Computing as a Service (QCaaS). There was consensus among experts we spoke to that quantum computing will mostly be a cloud-based service in the immediate to medium-term future. And in that sense, quantum computing's starting point will likely continue from classical computing's apparent endpoint.

The cloud is expected to accelerate the adoption of quantum computing, reducing the costs and challenges faced by corporates to maintain their own infrastructure and have a quantum computer on-premise (for example, the need for refrigeration and a team of engineers to maintain the quantum computer). A report by The Quantum Insider estimated the QCaaS market to be less than $50 million in 2020 and to consist mainly of research projects, consulting projects, and experimental access to platforms such as IBM Quantum and Amazon Braket.[134] They expect the QCaaS market to achieve an 80% CAGR over the forecast period of 2021-30. They estimate the TAM reaches $4 billion by 2025 and $26 billion by 2030, driven by what they refer to as "the realization of useful applications starting to emerge midway through this decade." As Figure 55 below shows, however, the revenue generated by QCaaS providers is expected to only form one part of the overall quantum computing TAM.

Figure 55. Breakdown of Different Layers Between End Customers and QPU Providers

Excludes Layers of Enabling Hardware and Software



Source: The Quantum Insider[135]

QCaaS providers are uniquely positioned between the software layer and the Quantum Processing Unit (QPU) to identify trends in corporate quantum computing usage. Using quantum computing cloud services also provides the end-user the flexibility to access different types of quantum computing technologies, such as quantum annealing or gate-based quantum computers, depending on their needs at the time. This is likely to play a particularly important role in the coming years, as corporates investigate different use cases and potentially experiment with different qubit technologies, ahead of the industry achieving quantum advantage (which we describe earlier as the point at which QCs can offer practical advantages in solving a valuable problem, whether that is by enabling faster, cheaper, or more efficient solutions than classical computers).

We spoke to Professor Simone Severini, Director of Quantum Computing at Amazon Web Services (AWS), about the role collaboration and the cloud will play in the progress and adoption of quantum computing.

[134] The Quantum Insider, "Report: Quantum Computing as a Service Market to Hit $26 Billion by End of Decade," August 12, 2021.
[135] The Quantum Insider, "Quantum Computing as a Service Market Sizing – How We Did It," August 19, 2021.

Expert Interview with Professor Simone Severini, Director of Quantum Computing at Amazon Web Services (AWS)

Professor Simone Severini
Director of Quantum Computing, Amazon Web Services (AWS)

Q: What role will collaboration with hardware providers play in the adoption of quantum computing?

Prof. Severini: AWS has the largest and most dynamic community, with more than 100,000 Partners from over 150 countries. From a quantum standpoint, hardware providers are critical for expanding access to quantum computing through Amazon Braket, our managed quantum computing service. With Braket, we are giving our customers access to a variety of approaches when it comes to trying quantum hardware — all delivered through our hardware partners.

We believe there is no "right" path to exploring quantum. The truth is, it is too early to know which approach will become the standard, which is why we are focused on providing access to a range of different approaches, such as gate-based ion-trap processors, superconducting processors, and photonic quantum computers.

Q: How does the cloud enable collaboration in the quantum computing space more generally?

Prof. Severini: First and foremost, the cloud enables access. Customers are choosing AWS over other providers because it has a lot more functionality, the largest and most vibrant community of customers and partners, the most proven operational and security expertise, and the business is innovating at a faster clip — and this extends to AWS' quantum computing portfolio and services.

The magic of Amazon Braket is that it's running on AWS, where our customers data already lives, alongside storage, analytics tools, and all of the other services our customers are already using to run their business. Amazon Braket is fully integrated with AWS, providing a seamless experience for customers to leverage quantum and classical resources together for the first time. This will be critically important in the future where classical and quantum will work together to solve problems.

Q: What are the advantages of quantum computing on the cloud vs on-premises?

Prof. Severini: There are five reasons companies are moving so quickly to the AWS cloud, and by extension, Amazon Braket: (1) agility, (2) cost savings, (3) elasticity, (4) the ability to innovate faster, and (5) the ability to deploy globally in minutes. Amazon Braket is just like any other of AWS's services, and our customer experience reflects that. By running on AWS, our customers will always have access to the latest hardware vs. an on-premises system that could potentially be out of date before it's even implemented. In addition, they don't need to worry about reconfiguring their data centers, or worse — having to manage such delicate machines and the overhead that comes with it.

Q: What are the most important technological developments needed for the continued adoption of quantum computing on the cloud?

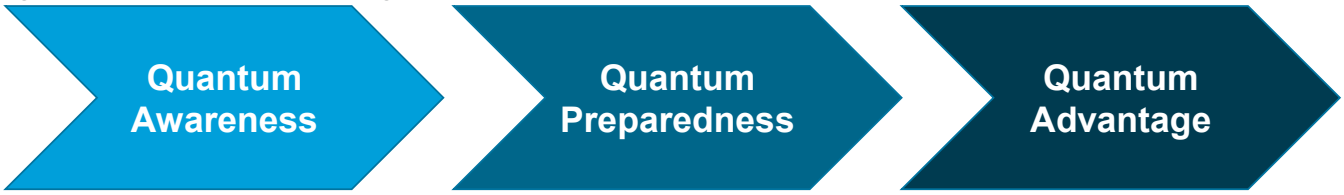
Prof. Severini: Quantum computing is still in the very early stages of research. With that in mind, the primary technological development that needs to be improved is error rate, or how accurately we can perform quantum gates. Quantum devices available today are noisy and are as a result limited in the size of circuits that they can handle (a few thousand of gates is the best we can hope for with NISQ devices).

This in turn severely limits their computational power. There are two ways that we are approaching making better qubits at the AWS Center for Quantum Computing: (1) by improving error rates at the physical level, for example by investing in material improvements that reduce noise; and (2) through innovative qubit architectures, including using Quantum Error Correction to reduce quantum gate errors by redundantly encoding information into a protected qubit, called a logical qubit.

How to Prepare: For Quantum Advantage

With the cloud providing a means of access to quantum computing, and with many quantum computing companies mapping out when and where they feel quantum advantage will occur this decade, the question turns to what corporates can do now to capitalize on quantum advantage when it occurs.

Figure 56. The Path to Quantum Advantage



Source: Citi GPS

Phase 1: Quantum Awareness

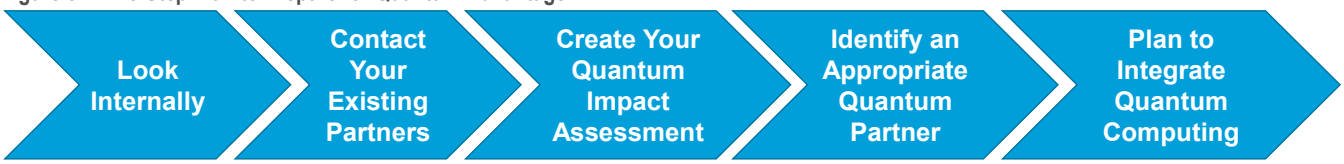
Our conversations with both corporates and industry experts revealed that while there is awareness of quantum computing among corporates, it is often considered a distant future technology or associated with previously-promised unrealistic timelines in delivering an advantage over current classical computing methods.

To that end, there are a lot of misconceptions about what quantum computers can and cannot do, and often little awareness of the specific areas that quantum computing will have an impact. It is also important to be aware of the tangible impact quantum computing may have on the particular industry or industries that a corporation operates in.

Phase 2: Quantum Preparedness

Given the diversity of corporations, not only in the industries in which they operate, but in their size, budget, and ambitions, no two corporates are likely to follow the exact same path toward quantum advantage. Figure 57 illustrates a general five-step process that companies can look to in preparing for the age of quantum advantage.

Figure 57. Five-Step Plan to Prepare for Quantum Advantage



Source: Citi GPS

Step 1: Look internally

Given that quantum computing is a complicated topic, spans numerous academic disciplines, and faces a shortage of specialists, companies will need to identify a primary point person to deal with outside partners and address workforce education requirements. As identified earlier in this report, talent shortages and upskilling the existing workforce will also be challenges. One solution may be to train employees to read technical papers, to help them better understand and decipher technical claims when they are made.

Step 2: Contact your existing partners

It is important to look among existing partners and identify individuals with specific quantum expertise. These may be IT partners, security vendors, cloud providers, research houses, or consultants. Existing partners will each have their own domain expertise in how a business operates, as well as their own unique perspective on where value in quantum computing may first occur. They may also help to identify the operational weak links which could be susceptible to quantum attacks.

Step 3: Create your quantum impact assessment

Armed with both the expertise of an internal workforce and existing strategic partners, the impact quantum computing may have on your business can be gauged. This includes identifying specific problems and opportunities and determining their materiality. It should also involve creating a business timeline and ideally should include discussions with the C-suite and at the board level.

When putting together a quantum impact assessment, it is important to be aware of what existing corporate partners do not know. Many will likely consider quantum computing as still in its infancy and will not necessarily be prepared for it or be able to provide guidance on the future services required. As such, depending on the knowledge gained from the two prior steps, it may be appropriate to swap Step 3 in Figure 57 with Step 4 to gain an agnostic view on the impact quantum computing may have on a corporate.

Step 4: Identify an appropriate quantum partner

Identifying the kind of partner needed is complicated: Some quantum computing companies focus primarily on providing access to hardware, some operate only on the software side, and others aim to offer a full-stack solution across all elements. Each provider will notably have their own limitations in terms of services they can provide. For instance, some full-stack quantum computing providers may not be agnostic to the hardware of competitors. Alternatively, software providers may be biased toward using the hardware modality they specialize in. And even within these different areas of focus, there is considerable variation among quantum computing companies in terms of their expertise and services. There are numerous criteria to examine in this regard, but some questions to ask may include:

- How deep are they in the science?
- How much can they integrate with my company's existing enterprise architecture?
- Can they work across multiple hardware types?
- What types of problems can they solve and on what time horizons?

For instance, in terms of hardware, gaining access to quantum annealers in the future may be particularly beneficial if capitalizing on quantum advantage in the area of optimization is a priority. On the other hand, gate-based quantum computers may be better if future plans involve more general-purpose quantum computing applications such as machine learning or molecular simulations. Be aware, however, that the two types of technology are at different stages of development. In terms of software, the availability of different quantum computing partners reflects the diversity of the industries that quantum computing will impact. Some software providers aim to provide a general-access software solution, whereas other providers will focus on providing the optimal software package for a specific industry, such as finance.

Something else to consider when identifying a quantum computing partner is how fast quantum computing is expected to be integrated within business workflows and infrastructure. From speaking to industry experts, this can vary significantly, and take anywhere from 12 to 36 months. One of the key questions to ask at this stage centers around the motivation for adopting quantum computing technology. Is it to secure an early competitive advantage ahead of the expected exponential increase in quantum computing capabilities? Or is it to ensure not being left behind when competitors eventually adopt this technology?

Step 5: Plan to integrate quantum computing

After identifying the appropriate quantum computing partner or partners (many corporates are opting to engage with more than one), the focus should shift to incorporating a means of access to quantum computing into the existing tech stack. This is unlikely to be "plug and play," given that the foreseeable future is a hybrid one in which corporates will need both quantum and classical computing depending on the task at hand.

Part of the integration process is to start building solutions to actual business problems that will force an integration into existing classical computing systems. Engaging in a "proof of concept" in this manner will allow for a better determination of a long-term quantum computing strategy. Notably, however, the proof-of-concept stage is often constrained to a research environment, so a true pilot would need to use real data and operate in the constraints of the particular business unit. Only then could one truly test the feasibility of outperforming existing classical-only solutions.

Engaging in such a process should mean that corporates are not caught off-guard by a lack of technical integration or skills within teams when the time comes to benefit from quantum advantage.

Phase 3: Quantum Advantage

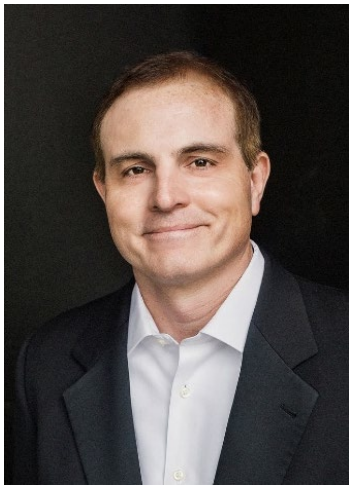
Notably, the path to quantum advantage will not necessarily be easy or cheap — especially for those playing to win. There are two key levels at which to explore adopting quantum computing. The first is simply to investigate and become familiar with a platform; for example, gaining access to a low-qubit quantum computer to understand how quantum algorithms work or may fit into your workflow. The second is to invest significantly in the technology and obtain access to a higher-qubit quantum computer to run the cutting-edge algorithms needed to position yourself for quantum advantage.

In 2022, Zapata Computing commissioned their second annual survey of 300 senior executives at large global enterprises with estimated revenues of over $250 million and computing budgets of over $1 million.[136] They found that 71% of quantum-adopting enterprises had a quantum computing budget of $1 million or more — considerably higher than in 2021 (28%). Also, 33% of respondents were what Zapata classified as "early or most advanced" tech adopters. Additionally, the percentage of respondents indicating they had no plans to adopt quantum computing fell from 31% in 2021 to 26% in 2022.

We spoke to Dr. Christopher Savoie, CEO of Zapata Computing, about their findings and what they are seeing from corporates today.

[136] Zapata Computing, *The Second Annual Report on Enterprise Quantum Computing Adoption*, January 11, 2023.

Expert Interview with Dr. Christopher Savoie, CEO of Zapata Computing



Dr. Christopher Savoie
CEO, Zapata Computing

Q: What are the earliest use cases that could provide an advantage for quantum computing over classical computing?

Dr. Savoie: Zapata believes the fastest path to quantum advantage could be with quantum-enhanced generative AI. Here, quantum computers are used as sampling devices to generate candidate solutions that classical computers cannot generate. We've used this approach to generate new solutions for optimization problems, for example optimizing assembly line scheduling as we recently demonstrated in work with BMW. Drug discovery is another promising near-term use case. We just published a study with Insilico Medicine and Foxconn that showed quantum-enhanced generative models can outperform classical generative models at generating small molecules. But we don't have to wait for quantum computers to mature. The same quantum methods can run on current classical devices to outperform best-in-class algorithms today — albeit, with less power than large-scale, error-mitigated quantum computers will provide.

Q: What is the role of classical computing with quantum applications?

Dr. Savoie: Quantum solutions will likely involve mostly classical computing, with a few powerful quantum computing steps. This includes processing data before it goes in the quantum algorithm as will any post-processing needed to turn the quantum outputs into actionable insights. Applications must orchestrate across the quantum and classical systems in the context of complex, hybrid-cloud, customer-specific architectures. At Zapata, we're solving for all the complexities of classical analytics and quantum in one integrated solution.

Q: What are the greatest barriers organizations face when adopting quantum computing?

Dr. Savoie: The largest barriers are the complexity of integrating quantum into the existing IT stack and the shortage of quantum talent, which is much scarcer than data science talent. But more importantly, customers are not clear on which use cases are most viable near-term. Some ecosystem players promote use cases that are helpful to customers only as research proofs of concepts (POCs): For example, variational quantum eigensolver (VQE) for molecular simulation is 7-10 years from outperforming current methods. The truth is that quantum-enhanced generative AI can add value today and should be the first place enterprises look for use cases.

How to Prepare: For the Quantum Threat

As discussed earlier in the "Cybersecurity" and "Cryptocurrency" sections, quantum computing poses a risk to existing industries. One report estimated the value at stake in finance, automotive, pharmaceutical, and chemical use cases to be potentially approaching $700 billion by 2035.[137]

As investigated in detail in earlier chapters, quantum computers (QCs) will excel at a specific set of problems, some of which push the boundaries of math, science, and technology. They will also be exponentially better at solving problems involving linear algebra, prime factorization, and discrete logarithms — keys to modern cryptography. Since much of the world's current cryptographic infrastructure relies on classical computers' inability to solve these problems efficiently, the advent of quantum computing presents a significant threat. This section intends to expand on our work in Chapter 2 to outline the problem and address what large organizations can do right now and in the future.

Understand Symmetric Encryption and the Threat to It

Think about encryption like a lock on a door. Many locks have been designed, but over time, a particular shape and style of lock is used fairly universally on all doors. This "standard" lock format represents an encryption algorithm, which is the mathematical function that "locks" or "unlocks" the metaphorical door. In this metaphor, the security of the lock is primarily based on each lock requiring a different key, not a different lock design. The key for the lock is like an encryption key. Since a locksmith or burglar cannot see inside of a lock to know which key will fit, they use special tools like lockpicks to "feel" inside the lock until they work out the shape of the correct key. Once they are successful, the lock opens.

Modern cryptography and attacks against it are similar. Although the locking mechanism is known via published algorithms, the security of the system is based on maintaining the secrecy of the encryption key. To bypass the encryption, an attacker must try many keys to find the one that fits or attempt to figure out what the lock expects and create a key that will open the door.

In symmetric encryption algorithms like AES (Advanced Encryption Standard) and its predecessor DES (Data Encryption Standard), the same encryption key is used to encrypt and decrypt through the same algorithm. In our door lock analogy, the locksmith is going to need to work out what key will fit with almost no information about the shape of it. They will need to test lots of possible keys until one fits. This type of attack, known as brute-force, creates a random encryption key value which is then used to attempt to decrypt the data.

If our lock only had a couple of pins on it, then working out the right key would be easy. The same is true in symmetric encryption. If there were only a small number of potential encryption keys, even into billions or trillions, then a traditional computer would eventually be able to guess the right key. This concept is known as "key size." The larger the key size, the more difficult it is for an attacker to guess the right key. AES, for example, has key sizes of 128, 192, and 256 bits available. If we use a 128-bit key, there are around 340 undecillion unique keys that would need to be attempted to brute-force decrypt the data — that is 340 with 36 zeros after it! Even leveraging the fastest modern classical computers in the world would take millions of years to brute-force that key.

[137] Matteo Biondi et al., "Quantum Computing Use Cases Are Getting Real—What You Need to Know," McKinsey, December 14, 2021.

In 1996, Lov Grover devised an algorithm to run on quantum computers making it significantly easier to perform an unstructured search. That is, his algorithm could determine much more efficiently what unknown value should be fed into a mathematical function to produce a particular output. This obviously causes some concern around the continued viability of symmetric key encryption, which relies on the difficulty in determining which key in the massive potential pool is correct.

However, Grover's algorithm only provides about four times the speed of a traditional searching algorithm. So, systems like AES are not completely broken. The number of potential keys available simply need to increase to maintain the security of symmetric algorithms. Many organizations are suggesting the adoption of 256-bit keys as a standard to protect against attacks from Grover's algorithm. This is based on the understanding that today, a 128-bit key is considered safe for protecting sensitive information up to the Top-Secret level, and doubling the key length is considered sufficient to provide the same level of protection in a post-quantum environment.

Understand Asymmetric Encryption and the Threat to It

Imagine a treasure chest that is locked with one key but can only be unlocked with a different key. A pirate could store away some treasure for their buddy and be sure that only the person who has the unlock key can retrieve it. Cryptographers would call this system an asymmetric (or two-key) algorithm — also known as public-key encryption. In these algorithms, there is a public and private key pair that are mathematically linked. So, our locksmith here could analyze the public key to determine the private key, in theory. Public-key encryption (such as RSA, discussed earlier in the report) makes this difficult by using mathematical features like prime factorization to make that analysis incredibly difficult for traditional computers to solve.

Peter Shor, a MIT mathematics professor, published a paper in 1994 that outlined a quantum algorithm for solving a set of problems that traditional computers found exceedingly difficult. His algorithm "solves" for prime factorization — in other words, it can find the prime numbers that, when multiplied together, give a particular value. Since asymmetric algorithms have a public part of their key, Shor's algorithm can effectively determine the private key part very quickly. The mathematical relationship between the two key pieces means that current asymmetric algorithms can be considered broken once Shor's algorithm can be run against large enough numbers. Simply increasing the key size will not fix this issue; new quantum-safe algorithms will be required.

Recognize the Threat Timeline

Cryptography underpins the security of every computer system we interact with. Symmetric algorithms protect our data in storage, in backup tapes, on disks, and over the network. Asymmetric algorithms are used for establishing secure network connections (like SSL, TLS, and VPN), maintaining strong identities, and exchanging symmetric encryption keys. Generally speaking, asymmetric algorithms protect data in transit while symmetric algorithms protect data in storage. Web security, digital identities, encrypted phones and laptops, web servers, encrypted databases, and more would all be fundamentally broken by quantum implementations of Grover's and Shor's algorithms.

While Grover's and Shor's algorithms are known, they cannot be run on today's quantum computers in a way that would significantly impact our current encryption systems. However, there are a few problems. First, the point at which the required size of quantum computers will be ready is unknown. Current estimates from "friendly" companies and researchers suggest anywhere from five to 10 years, but there could be significant advances by our adversaries that we do not know about. Also, our encrypted communications and data are likely already being archived by our adversaries for a future date when they can be decrypted — known as a "Harvest Now, Decrypt Later" (HNDL) attack. If any of our data could be exploited in five to 10 years, then we need to take steps to protect it today.

Develop an Enterprise Approach to Cryptography Modernization and Agility

We see two main approaches to cryptography, which can be done in parallel: cryptography modernization and cryptography agility.

Single-key (symmetric) encryption systems that are in use today will need larger keys to ensure they stay effective once quantum computers are available. Current standards and implementation need to be enhanced to establish a 256-bit key length as the default for AES and use similar-strength keys for other symmetric encryption systems. This will ensure today's encrypted data cannot be broken in the future.

When current public-key encryption algorithms can be completely broken by quantum computers, those algorithms will need to be replaced with quantum-safe solutions, known as Post-Quantum Cryptography (PQC). NIST and other organizations are already determining which new algorithms should be adopted. Once available, those new algorithms will need to replace today's public-key encryption in every platform that uses it. This will be a huge undertaking, similar in scope to the Y2K problem, as every technology developer and company will need to participate.

For some corporates, the best approach may be to start working on a plan that will allow quick and easy identification of which systems are impacted, develop ways to swap out algorithms efficiently, and collaborate with vendors and partners to ensure their systems are also updated. This will become even more difficult when corporates move to the stage of using End of Life and End of Vendor Support systems (e.g., older versions of computers that do not receive the latest software patches), as these will not likely be patched to support new algorithms. The same is true for traditional cryptographic protocols that have been superseded — they will almost certainly not support the new encryption paradigms required.

Regardless of the approach taken, for most large corporates, cryptography modernization will require a multi-year strategy that will impact policies and standards and potentially lead to technology program changes and partnerships.

Quantum-resistant algorithms are being developed on today's classical computers, meaning one does not need a quantum computer to design quantum-resistant algorithms. However, there are also quantum cryptography algorithms that could be adopted in the future that, by design, would be quantum-proof. A determination on how widely these technologies are adopted is necessary before deciding on implementing quantum cryptography.

NIST began formally investigating PQC in 2016. In addition to knowledge-sharing and presentations around the topic, their primary focus has been in identifying algorithms to adopt and replace those identified as vulnerable and is expected to release draft standards. Given the preexisting shortage of cybersecurity experts, companies need to be mindful of the likely talent shortage in quantum computing as well, as discussed in the “Workforce Education” section of this report.

We spoke to Professor Deeph Chana, Chair of the NATO Advisory Group on Emerging and Disruptive Technologies, about what organizations should consider when it comes to the threat of quantum computing.

Expert Interview with Professor Deeph Chana, Chair of the NATO Advisory Group on Emerging and Disruptive Technologies

Professor Deeph Chana
Chair, NATO Advisory Group on Emerging and Disruptive Technologies

Q: What should organizations take into consideration when evaluating the quantum threat to cryptography?

Prof. Chana: We can say with some confidence that the current situation is characterized by a significant lack of technical literacy and competence within the majority of organizations where security issues related to quantum technology should be of concern. Such skills are simply hard to attain and are in scarce supply.

Furthermore, well before we get to the highly advanced topic of quantum computing, we already have evidence, through countless studies and real-world events, that significant issues persist with respect to the base competencies needed to deal with more conventional forms of cybersecurity risk, not to mention the threats that might be posed by a quantum computer. That this is a global issue has been revealed by recent incidents such as the WannaCry ransomware attack, the SolarWinds supply-chain software hack, the myriad of cybersecurity issues related to the COVID-19 pandemic, and the modus operandi in cyber-warfare used in the Russia-Ukraine war.

In each case, governments and industry leaders appeared to be caught by surprise, in many cases claiming, incorrectly, that such risks were previously unknown when in reality they had been openly highlighted by experts, in some cases for over a decade. In the short term, therefore, it seems that most companies will have to rely on external expertise to understand the importance of quantum computing risks. Ideally, however, their needs will be best served by a blend of internal competence collaborating with external expertise, and this is what they should plan for.

Q: Why should organizations be thinking about future quantum attacks right now?

Prof. Chana: It is not necessary for quantum computing to be a commercial reality in order for considerations of its security risk potential to be undertaken. More importantly, with such an analysis in hand, it is feasible to start taking action through pre-emptive implementations of technical and non-technical mitigations. Security preparedness through designed resilience rather than a policy of reaction, therefore, is the posture I'm advocating for.

However, related to my points on expertise above, this requires competent technology risk analysis to be well established and available to an organization, which, currently, is generally not the case. The major issue with not taking a stance of preparedness may be summarized by the idea of accumulation of *security debt*; where the impact of a quantum computing-driven threat would be greatly multiplied in future systems that evolve and grow in scale, complexity, and reach without designed-in mitigations.

We can, for example, consider scenarios where large amounts of *conventionally* encrypted data might suddenly become accessible due to the arrival of a quantum computing-enabled decryption system — this should be motivation for taking action on advanced encryption and data security methods now. The idea of stealing data today for the purposes of decrypting it tomorrow is a threat scenario that needs consideration across a range of industries.

Market Participants

Overview

This past decade has seen increasing amounts of private investment into quantum computing. As it is no longer just an esoteric technology of governments and university departments, private markets are taking note of the increasing number of spin-offs and start-ups making inroads in the area.

While there are, of course, examples of consolidation occurring in the space, there is not yet a consistent level of M&A activity, which is why we focus on the capital invested in the private primary markets.

The two broad areas market participants need to be aware of are (1) venture capital (VC) trends and (2) the company and funding environment.

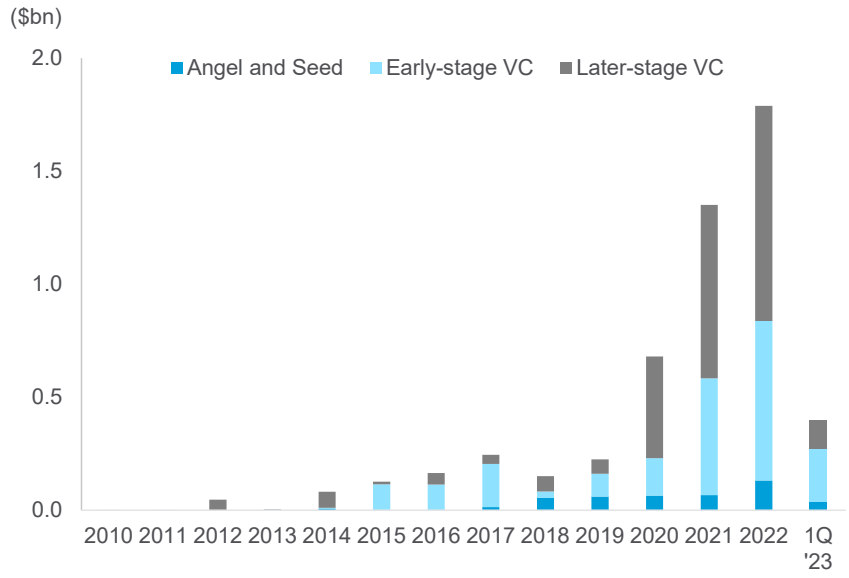
Venture Capital Trends

VC Investment

The dollar amount of capital invested in quantum computing has increased sharply in recent years. 2020 seems to have been a breakout year for VCs in the sector, with over $700 million invested, almost as much as the five prior years combined (Figure 58)

While some may attribute this to the so-called “spec-tech boom” following the global interest rate cuts in light of the COVID-19 pandemic, 2021 saw this trend continue with over $1.3 billion invested (Figure 58), accounting for almost half (around 44%) of all the capital ever invested by VCs in quantum computing at the time.

Figure 58. VC Investment in Quantum Computing (2010-1Q 2023)



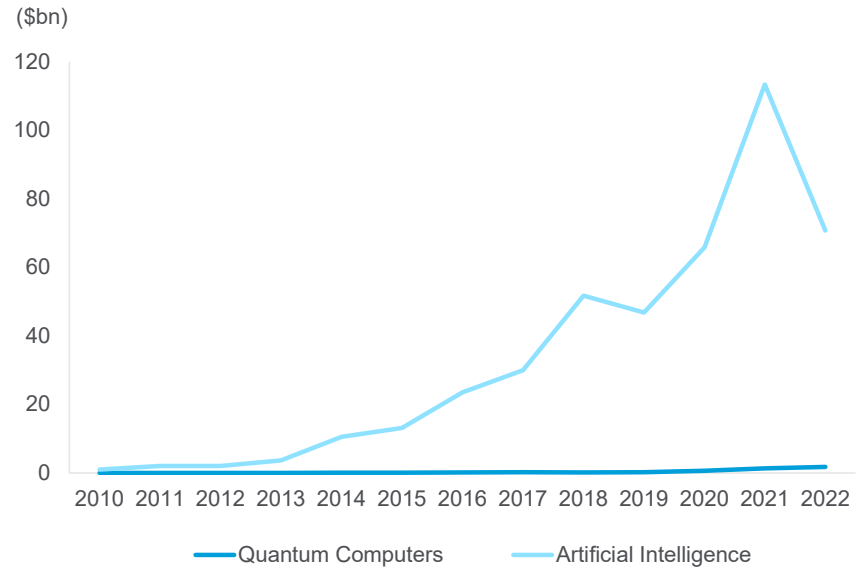
Source: PitchBook Data Inc., Citi GPS

Another potential catalyst for investment in recent years could have been the claims of quantum supremacy in 2019, which brought quantum computing to the attention of the public. In the three years leading up to this announcement, VC investment in quantum computing saw only a 29% CAGR, rising from $105 million in 2016 to $227 million in 2019, whereas the three years since has seen a CAGR of more than 150%.

Despite the market turmoil of the first half of 2022, quantum computing received strong investment of nearly $1.8 billion (Figure 58), equating to around a third of all VC investment to date. In fact, 80% of the VC investment in quantum computing has occurred since the start of 2020, and 95% has been since the middle of the past decade. Looking at VC investment by stage over the period starting from 2016, we find that 9% was categorized as angel and seed investment, whereas 41% was early-stage investment and 50% was later-stage investment. Looking at the average deal size by investment stage also shows that deals have grown across all investment stages in recent years, but particularly in the more mature end of the investment spectrum, such as later-stage investment.

Assessing a nascent technology such as quantum computing by looking solely at levels of VC investment growth on its own may not tell the full story, especially given the small starting levels of VC investment in the quantum computing industry. One technology, however, that quantum computing is often compared to in terms of its potential impact is artificial intelligence (AI).

Figure 59. VC Investment in Quantum Computing vs. Artificial Intelligence (2010-22)



Source: PitchBook Data Inc., Citi GPS

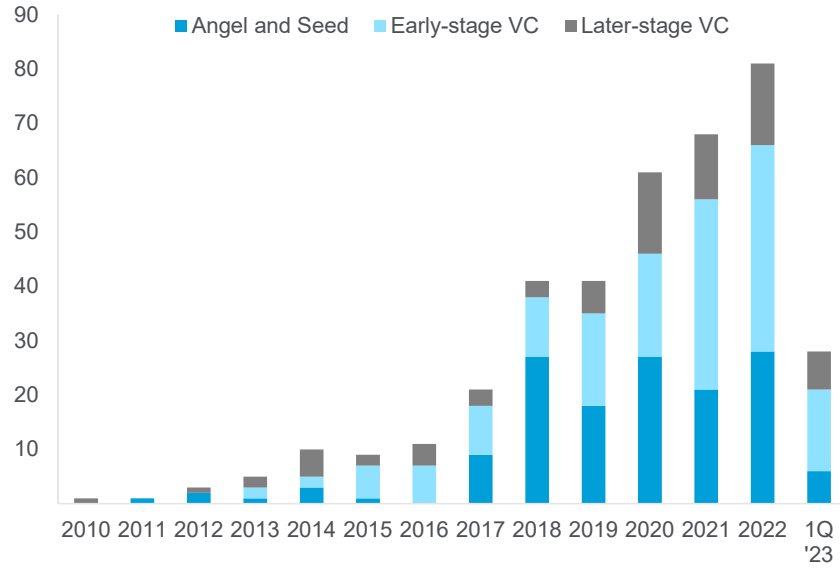
When compared to AI, based on PitchBook data, we find that the level of investment in quantum computing is very much still a drop in the ocean, with AI having averaged almost 90 times more investment than quantum computing in the past two years, with $66 billion and $113 billion invested in 2020 and 2021, respectively. The recent decline in AI investment $71 billion in 2022, per PitchBook data, alongside increasing capital flowing into quantum computing as the industry matures, puts the multiple nearer to 40.

While AI is by no means a perfect comparison to quantum computing, it does show that, despite quantum computing being one of the most densely invested sectors (see the "Market Forecasts" section), there is considerable scope for further investment flows.

VC Deal Activity

In contrast to VC investment, VC deal activity in quantum computing has been on a steady rise for most of the past decade. Looking at deal count by year, for instance, deal activity in the space started to take off in the middle of the past decade — climbing from an average of five deals annually for the period 2010-15 to around 65 in 2020-21. We also see that many of the deals are still in the Angel and Seed stages (reflecting the nascency of the quantum computing sector as a whole), although recent years show a trend towards more typical Early-Stage and Later-Stage investments. 2022 was another record-breaking year, with 81 deals, suggesting that more players are entering the maturing market.

Figure 60. VC Deal Activity in Quantum Computing (# of Deals, 2010-1Q 2023)

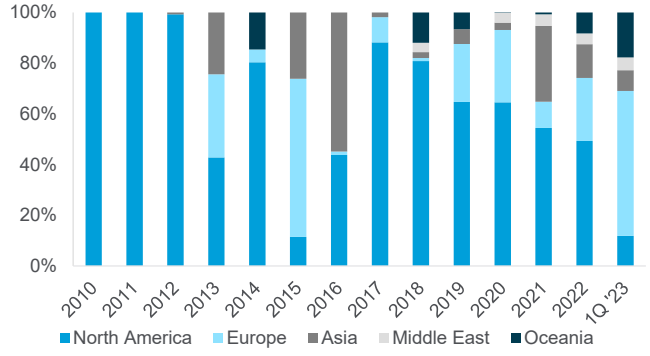


Source: PitchBook Data Inc., Citi GPS

Regional Divides

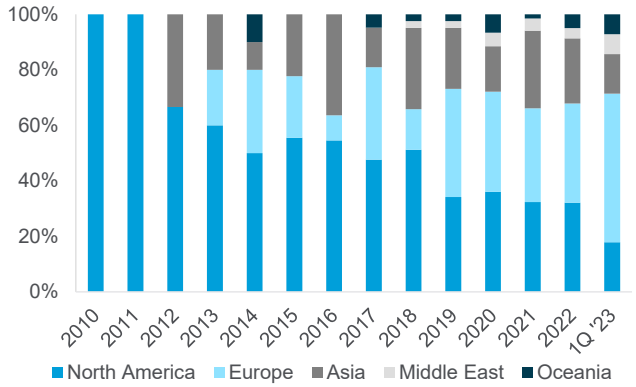
In terms of regions, the North American and European markets accounted for 73% of all deal activity over the ten-year period from 2012 to 2021 (the first two years of the 2010s had so few deals that the data on regional divides for that period is unlikely to be meaningful). Since that time, however, when looking at the capital invested, despite the North American market having had 1.3 times as many deals as the European market, it has had 3.7 times the amount of capital invested. Combined, the North American and European markets have been responsible for around 80% of the total capital invested by VCs in quantum computing worldwide over the past decade.

Figure 61. VC Investment in Quantum Computing by Region



Note: 2023 figures through end of 1Q
Source: PitchBook Data Inc., Citi GPS

Figure 62. VC Deal Activity in Quantum Computing by Region



Note: 2023 figures through end of 1Q
Source: PitchBook Data Inc., Citi GPS

As we can see from Figure 61 and Figure 62, Asia has made notable progress in recent years. According to PitchBook data, 2015 was the first year in which the region had more than one deal. Since then, deal activity has increased to an all-time high of 19 in 2021, accounting for 26% of all deal activity. Deal activity has been a leading indicator for the amount of capital invested, as the VC capital invested in Asia grew from just over $13 million in 2019 to just over $400 million in 2021.

We spoke to Stuart Woods, Chief Operating Officer of Quantum Exponential, about some of the VC trends he is seeing in quantum computing.

Expert Interview with Stuart Woods, Chief Operating Officer of Quantum Exponential

Stuart Woods
Chief Operating Officer, Quantum Exponential

Q: What do you think will be the main driver of VC investment in quantum computing over the next decade?

Stuart: The incentives for VC investing in quantum computing have evolved quite significantly over the last few years. Initially, investment was in pure quantum computing as it related to encryption, and then it was quantum computing for "supremacy" over classical alternatives.

It may be in the middle- to long-term future that quantum technologies are integrated into the fabric of much of our infrastructure, but not necessarily fronted by the quantum buzzword. They will just be services, accepted as standard, that happen to use and rely on quantum technologies. In the near term, I think installing quantum computers in data centers for their revenue-generating new services will become ever more familiar.

Q: What do you think will be the impact of the recent downturn in markets in terms of raising funds for quantum computing companies?

Stuart: The first key point is that quantum technology is not just quantum computing. The current global geopolitical environment highlights even further that quantum is a much broader market than the computing element for which it has attracted most attention. Quantum sensing, for example, will have varied applications across timing, GPS and navigation systems, brain imaging, and measuring ground movement and subsidence. The effect of the downturn is to focus the market more broadly on other applications needed by governments, for example, smart infrastructure, clocks for timing financial transactions and sensing applications for government climate change policies.

Q: What makes investing in quantum computing different from investing in other areas of Deep Tech?

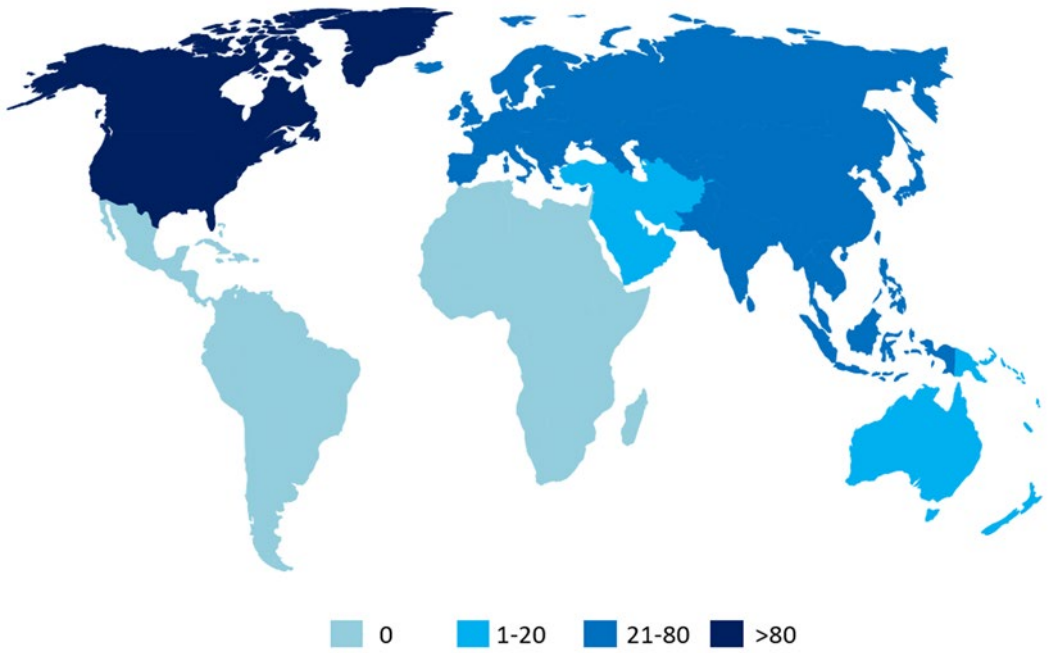
Stuart: Quantum is more technically challenging, although it is becoming increasingly mainstream and a must-have asset class. I am wary of parts of the market that are labelled "quantum-inspired." This is a misnomer which is highly ambiguous and has the potential to distort the actual standing and successes of companies in the quantum ecosystem.

Naturally, technical due diligence and robust intellectual property are key. I also think understanding the channel to market with quantum is essential; almost all quantum activities can be spun up into services, but sometimes founders (misguidedly) want to — or feel they should — sell products. Similarly, not every quantum company needs to build a quantum computer. We have to remember that and encourage each facet of the market to nurture and fine-tune its areas of expertise — not everyone can do everything all at once.

The Company and Funding Environment

It is not just in VC investment and deal activity that a geographical divide exists, but also in the number of quantum computing companies headquartered by global region. When looking at company count by geography, we found that, as of the end of 2022: 45% of companies were headquartered in North America and 34% were in Europe, followed by 14% in Asia and 3% in the Middle East.

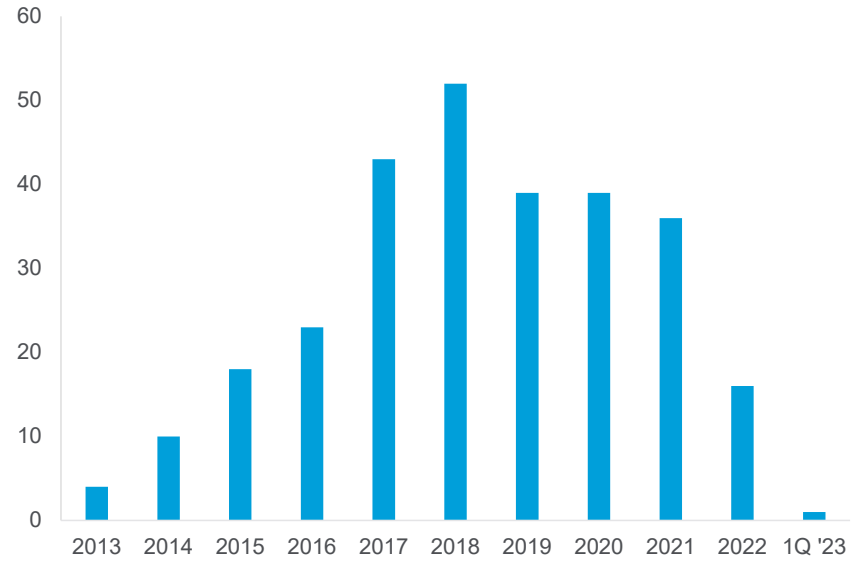
Figure 63. Quantum Computing Company Count by Region (as of end-2022)



Source: PitchBook Data Inc., Citi GPS

Despite the increase in both VC investment and deal activity over the past decade, according to PitchBook data, the number of quantum companies founded over time has varied considerably. From an average of three companies founded per year at the start of the decade to a peak of just over 50 in 2018, there has been a steady decline over the past few years. For context, 2022 saw just 16 companies founded.

Figure 64. Number of Quantum Computing Companies Founded (2013-1Q 2023)



Source: PitchBook Data Inc., Citi GPS

Figure 65 gives some examples of recent VC deals within the quantum computing sector listed on PitchBook. It is clear that capital is being raised by quantum computing companies across the globe.

Figure 65. Largest Quantum Computing VC Deals in 2Q 2023

Deal Size (US$)	Country	Deal Type	Deal Date
51.65	United Kingdom	Later Stage VC	April 18, 2023
30.00	Germany	Later Stage VC	June 22, 2023
14.00	Finland	Early Stage VC	June 2, 2023
5.83	Denmark	Early Stage VC	June 1, 2023
5.81	France	Early Stage VC	May 23, 2023
5.42	Netherlands	Later Stage VC	April 13, 2023
4.52	Denmark	Later Stage VC	May 11, 2023
4.00	United States	Seed Round	June 6, 2023
3.86	South Korea	Early Stage VC	June 28, 2023
0.85	Sweden	Early Stage VC	June 20, 2023

Source: PitchBook Data Inc., Citi GPS

As shown in Figure 66, governments are also investing in quantum computing companies. For instance, the likes of Innovate UK (part of the UK Research and Innovation agency) and the National Science Foundation (a U.S. governmental organization that helps start-ups through grants and seed funding) are also making a large number of investments.

Figure 66. Most Active Investors in Quantum Computing Companies (1Q 2023)

Investors	Investments	Investor Type	Country
Innovate UK	42	Government	United Kingdom
Company A	24	Venture Capital	France
European Innovation Council Fund	23	Government	Belgium
Creative Destruction Lab	18	Accelerator/Incubator	Canada
Company B	17	Venture Capital	United States
Company C	11	Venture Capital	United States
Oxford Science Enterprises	11	University	United Kingdom
National Science Foundation	10	Government	United States
Company D	9	Corporate Venture Capital	United States
Company E	9	Venture Capital	United Kingdom
Company F	9	Venture Capital	Germany
Company G	8	Venture Capital	Singapore
Company H	8	Venture Capital	United States
In-Q-Tel	8	Not-For-Profit Venture Capital	United States

Source: PitchBook Inc., Citi GPS

We spoke to David Moehring, General Partner at Cambium Capital, about some of the challenges quantum computing companies face in raising capital in the current funding environment.

Expert Interview with David Moehring, General Partner at Cambium Capital

David Moehring
General Partner, Cambium Capital

Q: What are the important characteristics you look for when investing in a quantum computing company?

David: Quantum computing is a highly complex and multi-faceted technology. There are many important characteristics, but more important than any one metric in isolation is the interdependence of that metric to others. Most companies will strongly highlight one specific area where they excel, but it is critical to understand where they do not, and to make sure there are no single points of failure. In such a complex industry, it is far more important to understand a company's weaknesses than their advertised strengths. This is true not just with quantum computing, but with advanced-computing architectures as a whole.

Q: Can you give some examples?

David: From the engineering perspective, some technologies work very well at small scale, and may even have years of documented success in a university setting, but many have insurmountable hurdles to scaling. From the business perspective, many companies build hardware without a bona fide use-case in mind. Further, even if the compute infrastructure is matched to a business case, it is also important to offer a practical compiler and software stack for the solution to reach its full potential. The mismatch of building hardware that isn't viable for end-user applications often creates inefficiencies in the full value chain that completely negates the effort and cost of building the computer in the first place.

Q: What are the different types of quantum computing companies?

David: While our fund has only invested in companies building quantum computing hardware, our partnership has firsthand research and development experience in academia, government, and industry, as well as in building startups and funding all aspects of the quantum- and advanced-computing ecosystem. As with classical computing, no one company can accomplish everything, and thus also with quantum computing it is important to have a robust industry spanning design, fabrication, manufacturing, software, and application development. Some companies encompass multiple of these aspects, but regardless, all must be addressed to unlock the full potential for quantum computing.

How To Prepare: A Deeper Understanding

Understanding quantum computing companies brings its own set of challenges. With the industry itself arguably just coming out of its own start-up phase, and only a handful of quantum computing companies in the process of going public, it is hard for market participants to assess the longer-term opportunity.

One key thing to recognize is that quantum computing itself is highly nuanced. As such, understanding quantum computing companies requires a genuine understanding of the technology, the industry use cases, and the landscape at large.

For instance, when assessing a hardware company, an understanding of each of the different qubit technologies and the unique challenges it faces in terms of reaching scale would be beneficial — and this is before any consideration of whether the management team's approach to solving it is the best. Similarly, on the software side, as we touched on earlier in the report, understanding how quantum computing algorithms work requires at least some understanding of how quantum hardware and software interact.

Furthermore, while quantum computing is potentially a genuinely transformational technology, its status as such makes it difficult to separate bold claims from hype. While there are numerous established companies in the space, there are also many start-ups, and it is difficult to independently verify their specific actions, achievements, or the ramifications of their findings. For instance, companies often compare the results of their quantum computers to those of powerful — but not necessarily the best — classical computers. Another approach companies take is to benchmark quantum computers on highly specific tasks that are designed to test hardware from an academic perspective. While this may be scientifically valid, it does not necessarily translate into generating commercial value.

Fundamentally, quantum computing is an industry facing high expectations, as reflected in the high CAGRs predicted by almost all third-party market forecasts we identified in the "Market Forecasts" section. In addition to some of the deep science areas mentioned above, numerous quantum computing-related services are provided via cloud companies, IT service companies, supply chain, and education providers.

We spoke to Mark Danchak, Partner at General Innovation Capital, about what market participants should consider when it comes to investigating quantum computing.

Expert Interview with Mark Danchak, Partner at General Innovation Capital

Mark Danchak
Partner, General Innovation Capital

Q: What information is important for understanding the quantum computing investing space?

Mark: I have spent six years building an information matrix that we can cross-reference to readout who we think the most likely winners will be in the quantum computing (QC) space. Each underlying substrate that is being explored to build scaled systems has its own unique advantages and disadvantages, both for building systems and running algorithms. That level of nuanced understanding is difficult to see without having spent a great deal of time with these companies. It is not easy for the traditional venture fund to pick winners in the space.

Q: What are the main vectors of development you are tackling?

Mark: The QC industry will take off when three vectors of progress intersect: (1) scaled hardware systems, (2) error-correction methodologies, and (3) algorithm development. If you can get a handle on these, you can start to factor in one of the most important elements of venture investing, which is the question of when customers will start to show up meaningfully. I hear people throw out statements such as "quantum is always five years away," which is an old trope people have used for many technologies, but I can tell you 95% of the people looking at this space today barely heard the words quantum computing four or more years ago.

Q: Which industries do you think will benefit first from quantum computing?

Mark: The industries that we believe will see the early use cases for quantum computing will be one of two archetypes: (1) companies that deal in the quantum mechanical realm as a fundamental part of their everyday business, such as pharmaceuticals, advanced materials, and chemicals; and (2) companies that can achieve large gains by leveraging small gains in computational areas, such as (perhaps primarily) finance.

Closing Statement

The newness and complexity of quantum computing is a challenge for stakeholders, but fostering awareness of what these machines can achieve could help with preparation and execution. We hope this report shines a brighter light on some of the opportunities, issues, and timelines around the technology. The debate around the arrival of quantum advantage will continue, and it will appear at different times for different use cases. When it does, despite the upskilling and technology integration that will be necessary, quantum computing is likely to scale exponentially.

Appendix: How Quantum Computers Work

We recognize that understanding the physics underpinning quantum computing is not necessary in order to appreciate the potential impact it may have on the world, in the same way that users of classical computers do not need to understand how a transistor works. However, quantum physics is often portrayed as an esoteric and almost mystical area of science in the media. For that reason, we felt it would be diligent to provide a basic conceptual grounding for some of the terms that are often used when describing quantum computing, including the likes of "superposition," "entanglement," and "interference."

The Basics of Quantum Physics

Quantum physics is, in essence, the study of energy and matter at the smallest of scales, and its aim is to understand the properties and behavior of the building blocks of nature. One analogy would be to imagine the world around you as a digital image made up of trillions of pixels; in such a case, quantum physics would be the investigation of what happens in between those pixels. We could easily write a book just on the history of quantum physics, but for the purposes of this report, we will focus on giving you a brief history and what you need to know from it to get a grasp on how a quantum computer works.

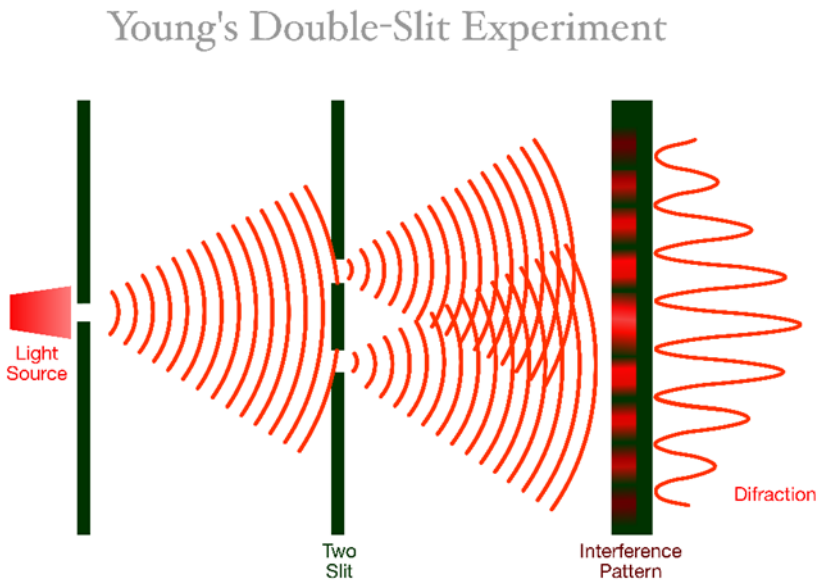
The field of quantum physics began in the early 1900s following experimental observations of atoms that seemed to contradict the then classical physics paradigm. One of the realizations was that energy and matter on the smallest of scales can be thought of as discrete packets, or "quanta," each with their own associated minimum value. In the case of light, energy is delivered by particles of light known as "photons." Each photon of a particular frequency delivers the exact same amount of energy and, most importantly, cannot be broken down into smaller units. The same applies for an electrical current, in which the "electron" is a fundamental carrier of charge.

The Two-Slit Experiment

If there is one experiment that can provide a conceptual understanding of quantum physics, it is the famous two-slit experiment.

The experiment shows that when light waves reach two narrow slits positioned very close to each other, the light waves interfere with one another and result in what we refer to as an interference pattern of light and dark areas on the screen behind. This is because light waves, like all waves, are characterized by peaks and troughs, and "interference" simply refers to how these light waves combine.

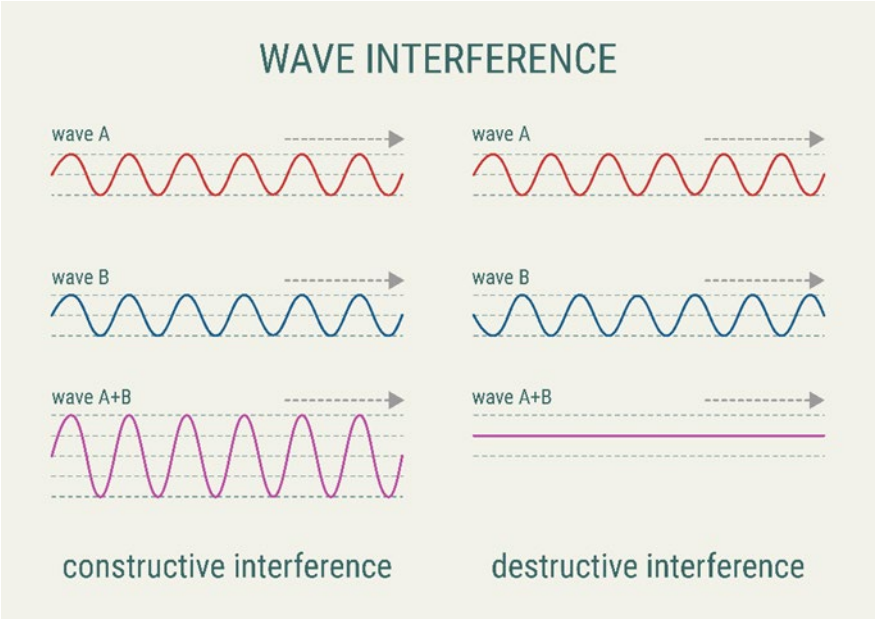
Figure 67. Double-Slit Experiment (with Light Waves)



Source: Shutterstock

Constructive interference is when two light waves meet in-phase — that is to say, when the peaks of two waves meet one another. This results in the two waves combining "constructively," increasing the size of the resultant wave's peaks and troughs, and in the case of light, resulting in an area of greater brightness. Destructive interference is when two light waves meet out-of-phase — that is to say, when the peak of one wave meets the trough of the other. This results in the two waves combining "destructively," cancelling out each other's peaks and troughs, and in the case of light, resulting in an area of darkness.

Figure 68. Constructive vs. Destructive Interference

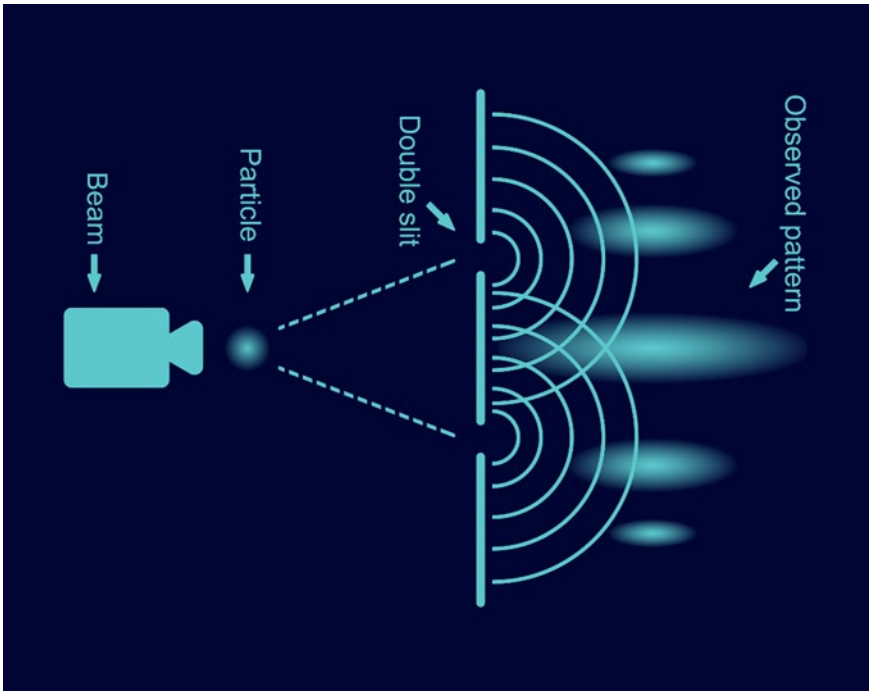


Source: Shutterstock

These patterns of light and darkness reflect areas of constructive and destructive interference, in the same way you see ripples from two separate waves overlapping combining to create peaks and troughs in a pond.

If we repeat the experiment with a beam of electrons — something once believed to be a point particle — we find that we observe the same interference patterns.

Figure 69. Double-Slip Experiment (with Electrons)

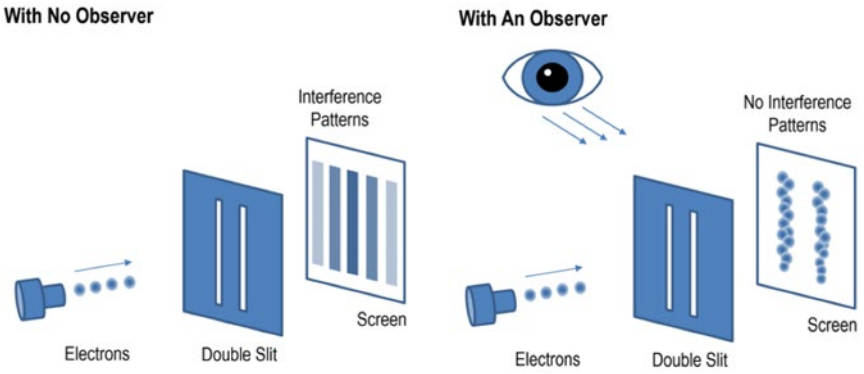


Source: Shutterstock

While the natural assumption would be that the particles are colliding with one another after going through the two slits, even when we fire one electron at a time at the double-slit, we eventually obtain the same interference patterns. This leads us to one of the key principles of quantum mechanics: the idea of wave-particle duality, meaning that on an atomic scale, matter can behave as both a particle and a wave.

The wave-particle duality of nature explains what actually happens — that the electron behaves as a wave at the point that it reaches the double-slit and, in fact, takes both paths at the same time and interferes with itself. This notion of an electron taking multiple paths at the same time is what we know as the principle of "superposition." Superposition is a term used to describe an object in a combination of multiple position states at the same time. This effect contributes to the power of quantum computing, as it means multiple computations can be carried out in parallel.

Figure 70. How the Act of Observation Collapses a Superposition



Source: Citi GPS

However, things get weirder still in the world of quantum mechanics. When attempting to observe this superposition of states of an electron, scientists found that the electron began to behave as a point particle, with the rear-screen showing only two distinct areas where the electrons had made contact and without any of the interference pattens seen before. This leads up to another key concept in quantum computing, which is that the act of observing a superposition in fact collapses it. Thus, with respect to quantum computing, though many computations can be carried out in parallel, you can observe only one of the results at a time. This is why separate computations have to be combined in a clever way before an observation is made from a quantum computer, ultimately ensuring that the correct answer has a high probability of being measured.

The Basics of Computing

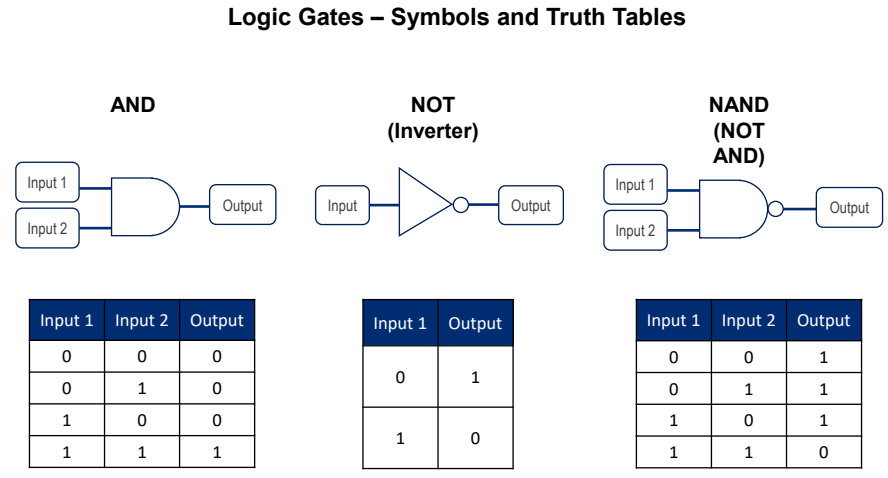
How Classical Computers Work

To help understand what makes a quantum computer special, a basic understanding of how our current "classical" computers work is beneficial. As noted in our "Understanding Quantum Computers" section, classical computers rely on bits that are only ever in one state at a time — either on or off. You can imagine it almost like a light switch, with "on" corresponding to a 1 and "off" corresponding to 0.

Next is to understand the concept of a logic gate, which undertakes simple mathematical calculations. The easiest to understand is probably the "AND gate," which simply outputs a "1" if both the first input AND the second input are equal to 1. These logic gates are formed from transistors. Consequently, the more transistors we can place on a computer chip, the more logic gates we can have and the more calculations a computer can undertake in a given time (i.e., the faster it gets).

Furthermore, modern classical computers have come a very long way in the past 70 years, and part of their progress is attributable to their standardized design. While of course that period has seen countless innovations in computers' underlying architecture, all have used the same exact material — the silicon transistor — to facilitate the computation.

Figure 71. Logic Gates: Symbols and Truth Tables



Input 1	Input 2	Output
0	0	0
0	1	0
1	0	0
1	1	1

Input 1	Output
0	1
1	0

Input 1	Input 2	Output
0	0	1
0	1	1
1	0	1
1	1	0

Source: Citi GPS

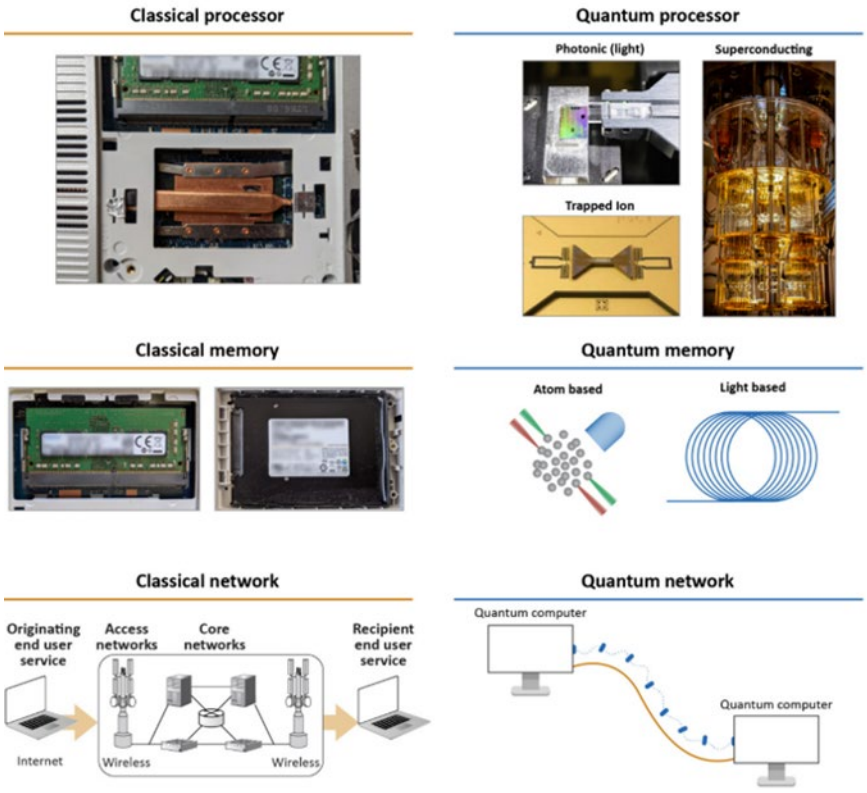
Quantum computers, on the other hand, come in two different structural models and use an even greater variety of qubit technologies (see the "The State of the Quantum Computing Market" section).

Comparing Quantum Computers to Classical Computers

In contrast to the highly standardized way we build classical computers, quantum computers are created in many different ways. First proposed as a concept by famed physicist Richard Feynman in the 1980s, the quantum computer relies instead on a quantum bit, or "qubit." Unlike classical bits that can only be in either 0 or 1, qubits can also be in a superposition of 0 and 1. Furthermore, each additional qubit added to a system results in an approximate doubling of its power (for certain applications).

Since quantum physics is observed across multiple different forms of energy and matter, there is currently no standardized way of creating a qubit. Figure 72 below shows the main similarities and differences between classical and quantum computers.

Figure 72. Classical Hardware vs. Quantum Hardware



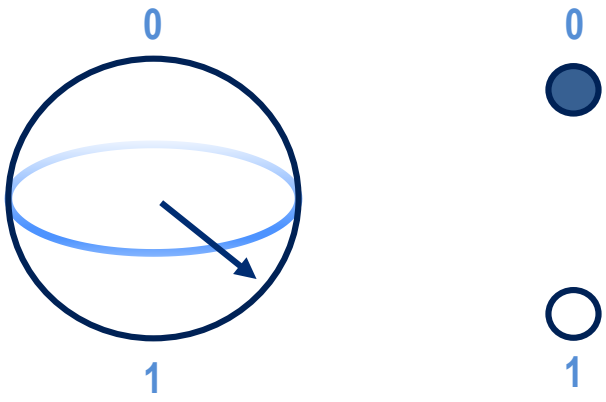
Source: Citi GPS

How Qubits Make Quantum Computers So Powerful

The best way to imagine a qubit is through the conceptual idea of a Bloch sphere, which is a geometric representation of a qubit and the various states it can occupy.

The best way to imagine a qubit is through the conceptual idea of a Bloch sphere, which is a geometric representation of a qubit and the various states it can occupy.

Figure 73. Qubits vs. Bits



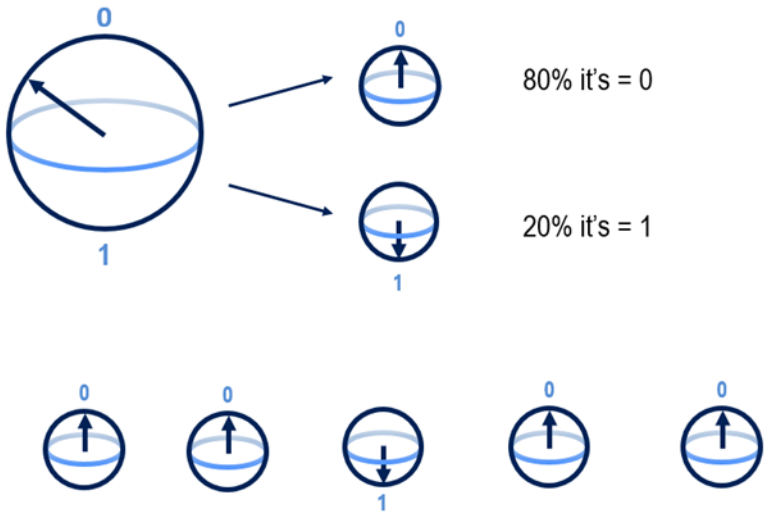
Source: Citi GPS

Just like how a classic bit has two states of either 0 or 1, a qubit has two computational basis states positioned on opposing poles of the Bloch sphere, as shown in Figure 73.

These two basis states are the only values returned when measuring the qubit, analogous to how the electron travels through only one of the two slits in the two-slit experiment as a particle when being observed (because any observation or measurement of a quantum state collapses its superposition). The rest of the time, when the qubit is not observed or measured in any way, it remains in a superposition of states, which can be visualized as an arrow pointing to a position on the surface of the sphere other than the north or south poles.

The surface of the sphere represents all possible states that the qubit can be in. In our example, the arrow points to a specific state. The latitude of the tip of the arrow indicates the likelihood of measuring a 0 or 1.

Figure 74. Measurement of One Qubit



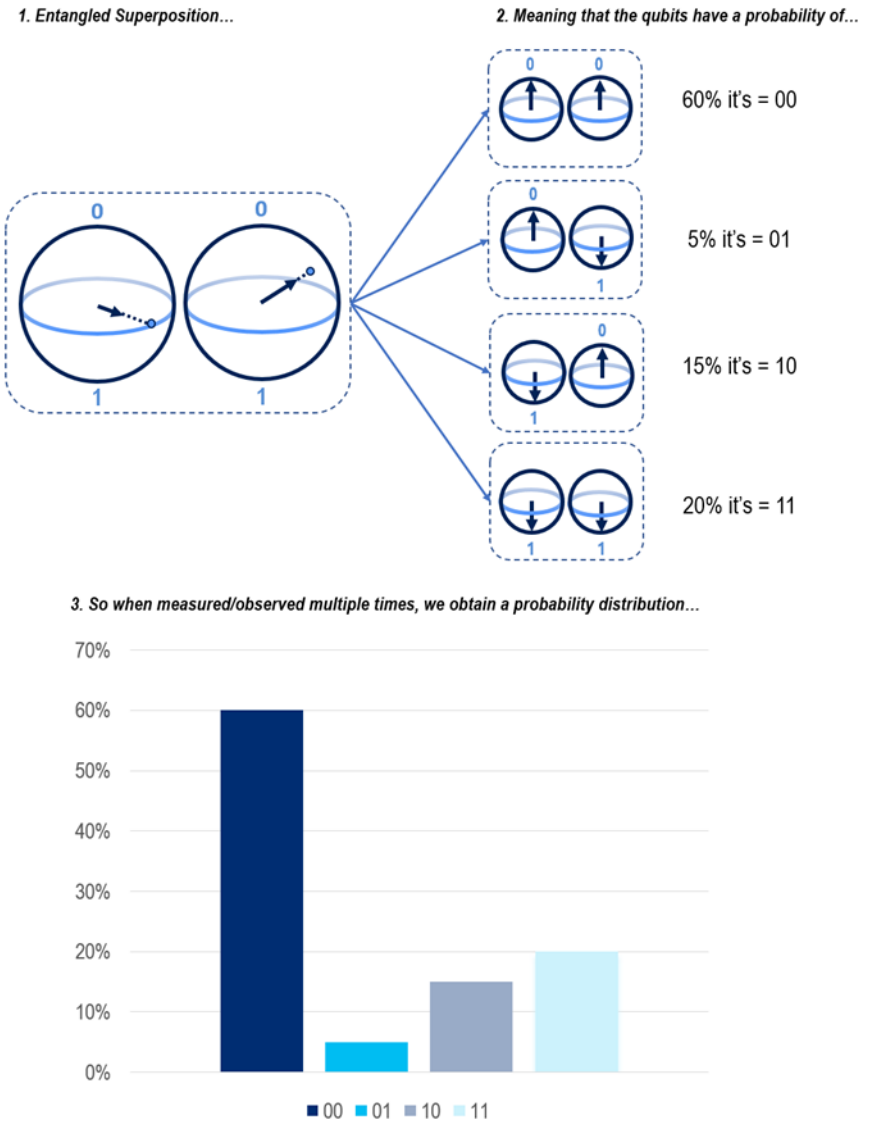
Reading No.	1st	2nd	3rd	4th	5th
Qubit Measurement	0	0	1	0	0

Source: Citi GPS

Another key difference between classical computers and quantum computers is that all classical bits are independent of one another, meaning that the state of one bit does not impact the state of another bit. What makes quantum computers so powerful are not just the qubits used, but also the ability to "entangle" the qubits.

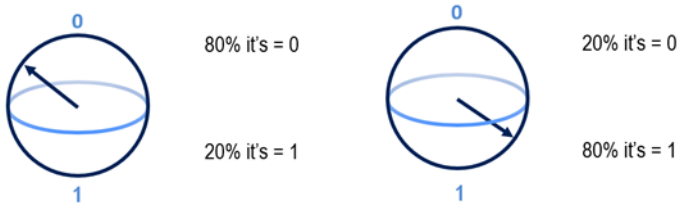
Qubits display a special phenomenon known as entanglement, whereby individual qubits can become intrinsically linked and thus no longer act independently of one another. What this means in practice is that each of the two constituent qubits no longer has its own precise individual state, indicated by the arrow not reaching the surface of the sphere in Figure 75showing two qubits in an entangled state, but instead part of their identity resides in the link between them. This manifests in the appearance of correlations in the joint probability distribution for the two measurement outcome bits.

Figure 75. Two Qubits in an Entangled State



Source: Citi GPS

Figure 76. Two Qubits Not in an Entangled State



And consequently, the measured states are independent of one another also…

Reading No.	1st	2nd	3rd	4th	5th
Qubit 1 Measurement	0	0	1	0	0

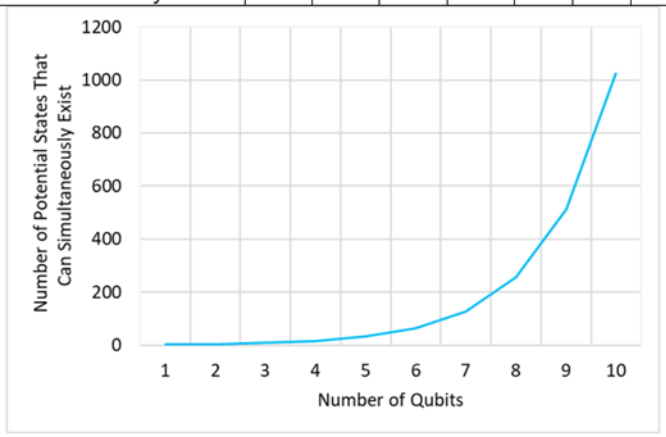
Reading No.	1st	2nd	3rd	4th	5th
Qubit 2 Measurement	1	1	1	0	1

Source: Citi GPS

And for specific problems, this is one of the keys to the power of quantum computers — that through the process of entanglement, just by adding one additional qubit (which, when measured, still only provides either a 0 or 1), you can actually double the total number of states the quantum computer can be in at a time and thus approximately double the calculating power for the entire system.

Figure 77. Number of Potential States That Can Simultaneously Exist

Number of Qubits	1	2	3	4	5	6	…	N
Number of potential states that can simultaneously exist	2	4	8	16	32	64	…	2^N

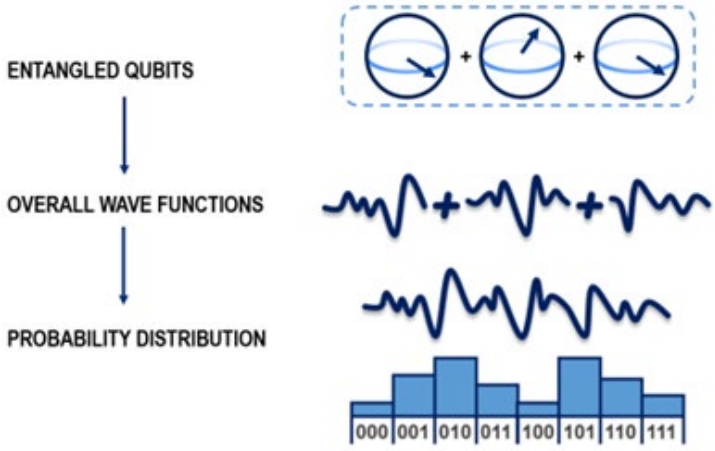


Source: Citi GPS

As with any exponential relationship, the higher the number of qubits, the greater the rate of increase in capabilities (or the steeper the curve, in the case in Figure 77). But to actually harness this power, you need to design a clever algorithm.

Altering the states of individual qubits in this entangled system allows us to alter the overall state, and thus the probability distribution of the measured outcome. Ultimately, while a quantum computer can be in a superposition of thousands or millions of computational basis states at the same time, measuring the qubit state collapses the superposition to one resultant individual outcome. In addition, one can use “constructive interference” to increase the likelihood of finding the right answer, and “destructive interference” to decrease the likelihood of getting the wrong answer.

Figure 78. How Entangling Qubit Results Generates a Probability Distribution

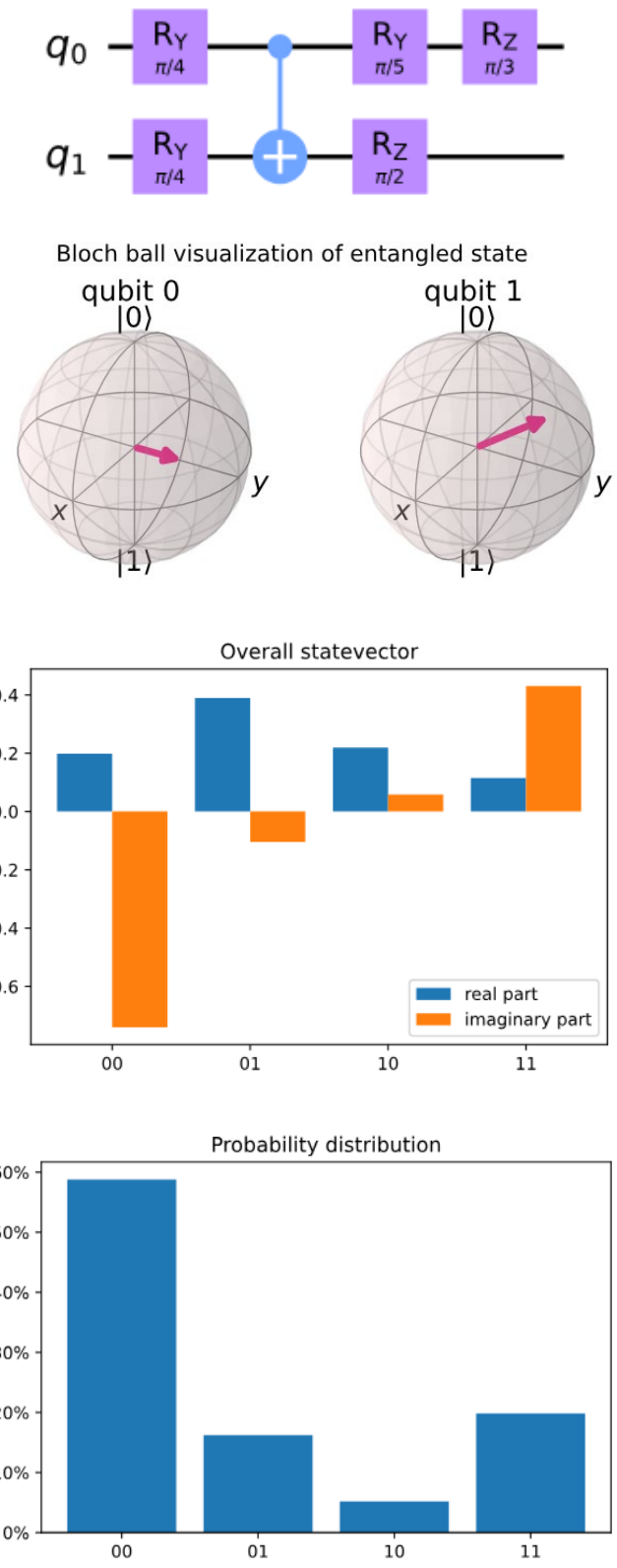


Source: Citi GPS

It is very important to note that quantum computers, unlike classical computers, do not provide exact answers, but rather probability distributions. If created well, these distributions will identify the most probable answer. This can be useful since quantum computers enable the solving of problems that would otherwise be intractable on classical computers. The most famous example is Peter Shor's algorithm, which showed it was possible to break current encryption techniques. However, not all problems will necessarily be solved faster with a quantum computer, and there is a field of study known as quantum complexity theory that addresses this issue specifically — something we discussed in the “A Hybrid Approach to Computing Is Inevitable” section earlier in the report.

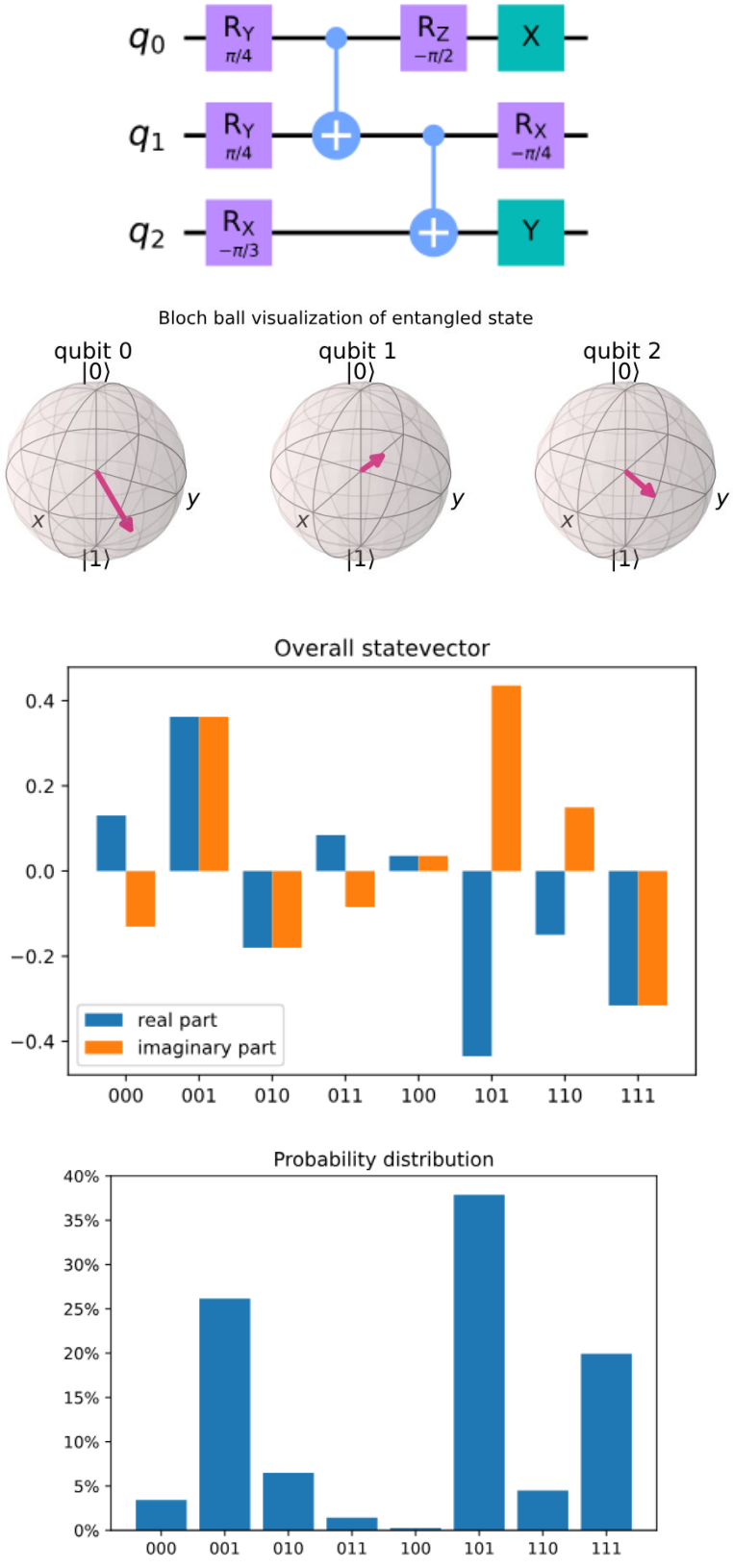
Figure 78 provides only a very high-level overview of how entangling qubits results in a probability distribution. Rather, the measurement of such an entangled state of qubits results in both imaginary and real parts — as can be seen in Figure 79 and Figure 80 below, which show entangled systems of two and three qubits, respectively.

Figure 79. Probability Distribution Generated from Observations of Two Entangled Qubits



Source: Citi GPS

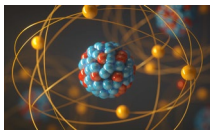
Figure 80. A Probability Distribution Generated from Observations of Three Entangled Qubits



Source: Citi GPS

As our premier thought leadership product, **Citi Global Perspectives & Solutions (Citi GPS)** is designed to help readers navigate the most demanding challenges and greatest opportunities of the 21st century. We access the best elements of our global conversation with senior Citi professionals, academics, and corporate leaders to anticipate themes and trends in today's fast-changing and interconnected world.

All Citi GPS reports are available on our website www.citi.com/citigps



Future of Nuclear Energy in a Low-Carbon Environment
Fission and Fusion Advanced Reactors to Prevail
July 2023

Voluntary Carbon Market
A Critical Piece of the Net Zero Puzzle
July 2023

Economic and Social Mobility
The Role of Business in Improving Outcomes
June 2023

Sustainable Ocean Economy
Charting a Prosperous Blue Future; Risk to Resilience
June 2023

Asia as a Time Machine to the Future
Seven Areas Where Asia Gives Insights Into the Future
May 2023

Money, Tokens, and Games
Blockchain's Next Billion Users and Trillions in Value
March 2023

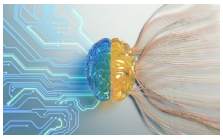
The Cyber Problem
Causes and Consequences of the Rise in Cyber Skill Demand
March 2023

The Creator Economy
Getting Creative and Growing
March 2023

Generative AI
ChatGPT and Search
February 2023

Supply Chain Finance
Uncertainty in Global Supply Chains Is Going to Stay
January 2023

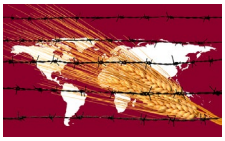
State of Global Electric Vehicle Adoption
A Trip Around the World
January 2023



Disruptive Innovations IX
Ten More Things to Stop and Think About
December 2022

Antimicrobial Resistance
The Silent Pandemic
December 2022

Climate Finance
Mobilizing the Public and Private Sector to Ensure a Just Energy Transition
November 2022



Food Security
Tackling the Current Crisis and Building Future Resilience
November 2022

Energy Transition: Vol 1
Mixed Momentum on the Path to Net Zero
November 2022

Energy Transition: Vol 2
Building Bridges to Renew Momentum
November 2022

China's Inward Tilt
The Pursuit of Economic Self-Reliance
October 2022

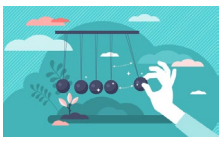
Philanthropy v2.0
Reinventing Giving in Challenging Times
October 2022

Food and Climate Change
Sustainable Foods Systems for a Net-Zero Future
July 2022

Home of the Future 2
PropTech – Towards a Frictionless Housing Market?
June 2022

Global Supply Chains
The Complexities Multiply
June 2022

Space
The Dawn of a New Age
May 2022



Investing for Outcomes
Why Impact Is Relevant Beyond Impact Investing
April 2022

Metaverse and Money
Decrypting the Future
March 2022

Global Art Market Disruptions
Pushing Boundaries
March 2022

Women Entrepreneurs
Catalyzing Growth, Innovation, and Equity
March 2022

Eliminating Poverty
The Importance of a Multidimensional Approach
February 2022

Global Supply Chains
The Complicated Road Back to "Normal"
December 2021

Philanthropy and the Global Economy
Opportunities in a World of Transition
November 2021

Education: Learning for Life
Why L&D Is the Next Frontier in Global Education
November 2021

Home of the Future
Building for Net Zero

October 2021

Global Carbon Markets
Solving the Emissions Crisis Before Time Runs Out
October 2021

Disruptive Innovations VIII
Ten More Things to Stop and Think About
October 2021

Holistic Digital Policy
Nation States Must Lead in Building Equitable Human-Centric Digital Economies
October 2021

Biodiversity
The Ecosystem at the Heart of Business
July 2021

If you are visually impaired and would like to speak to a Citi representative regarding the details of the graphics in this document, please call USA 1-888-800-5008 (TTY: 711), from outside the US +1-210-677-3788

IMPORTANT DISCLOSURES

This communication has been prepared by Citigroup Global Markets Inc. and is distributed by or through its locally authorised affiliates (collectively, the "Firm") [E6GYB6412478]. This communication is not intended to constitute "research" as that term is defined by applicable regulations. Unless otherwise indicated, any reference to a research report or research recommendation is not intended to represent the whole report and is not in itself considered a recommendation or research report. The views expressed by each author herein are his/ her personal views and do not necessarily reflect the views of his/ her employer or any affiliated entity or the other authors, may differ from the views of other personnel at such entities, and may change without notice.

You should assume the following: The Firm may be the issuer of, or may trade as principal in, the financial instruments referred to in this communication or other related financial instruments. The author of this communication may have discussed the information contained herein with others within the Firm and the author and such other Firm personnel may have already acted on the basis of this information (including by trading for the Firm's proprietary accounts or communicating the information contained herein to other customers of the Firm). The Firm performs or seeks to perform investment banking and other services for the issuer of any such financial instruments. The Firm, the Firm's personnel (including those with whom the author may have consulted in the preparation of this communication), and other customers of the Firm may be long or short the financial instruments referred to herein, may have acquired such positions at prices and market conditions that are no longer available, and may have interests different or adverse to your interests.

This communication is provided for information and discussion purposes only. It does not constitute an offer or solicitation to purchase or sell any financial instruments. The information contained in this communication is based on generally available information and, although obtained from sources believed by the Firm to be reliable, its accuracy and completeness is not guaranteed. Certain personnel or business areas of the Firm may have access to or have acquired material non-public information that may have an impact (positive or negative) on the information contained herein, but that is not available to or known by the author of this communication.

The Firm shall have no liability to the user or to third parties, for the quality, accuracy, timeliness, continued availability or completeness of the data nor for any special, direct, indirect, incidental or consequential loss or damage which may be sustained because of the use of the information in this communication or otherwise arising in connection with this communication, provided that this exclusion of liability shall not exclude or limit any liability under any law or regulation applicable to the Firm that may not be excluded or restricted.

The provision of information is not based on your individual circumstances and should not be relied upon as an assessment of suitability for you of a particular product or transaction. Even if we possess information as to your objectives in relation to any transaction, series of transactions or trading strategy, this will not be deemed sufficient for any assessment of suitability for you of any transaction, series of transactions or trading strategy.

The Firm is not acting as your advisor, fiduciary or agent and is not managing your account. The information herein does not constitute investment advice and the Firm makes no recommendation as to the suitability of any of the products or transactions mentioned. Any trading or investment decisions you take are in reliance on your own analysis and judgment and/or that of your advisors and not in reliance on us. Therefore, prior to entering into any transaction, you should determine, without reliance on the Firm, the economic risks or merits, as well as the legal, tax and accounting characteristics and consequences of the transaction and that you are able to assume these risks.

Financial instruments denominated in a foreign currency are subject to exchange rate fluctuations, which may have an adverse effect on the price or value of an investment in such products. Investments in financial instruments carry significant risk, including the possible loss of the principal amount invested. Investors should obtain advice from their own tax, financial, legal and other advisors, and only make investment decisions on the basis of the investor's own objectives, experience and resources.

This communication is not intended to forecast or predict future events. Past performance is not a guarantee or indication of future results. Any prices provided herein (other than those that are identified as being historical) are indicative only and do not represent firm quotes as to either price or size. You should contact your local representative directly if you are interested in buying or selling any financial instrument, or pursuing any trading strategy, mentioned herein. No liability is accepted by the Firm for any loss (whether direct, indirect or consequential) that may arise from any use of the information contained herein or derived herefrom.

Although the Firm is affiliated with Citibank, N.A. (together with its subsidiaries and branches worldwide, "Citibank"), you should be aware that none of the other financial instruments mentioned in this communication (unless expressly stated otherwise) are (i) insured by the Federal Deposit Insurance Corporation or any other governmental authority, or (ii) deposits or other obligations of, or guaranteed by, Citibank or any other insured depository institution. This communication contains data compilations, writings and information that are proprietary to the Firm and protected under copyright and other intellectual property laws, and may not be redistributed or otherwise transmitted by you to any other person for any purpose.

IRS Circular 230 Disclosure: Citi and its employees are not in the business of providing, and do not provide, tax or legal advice to any taxpayer outside of Citi. Any statements in this Communication to tax matters were not intended or written to be used, and cannot be used or relied upon, by any taxpayer for the purpose of avoiding tax penalties. Any such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

NOW / NEXT

Key Insights regarding the future of Quantum Computing

INNOVATION

There is currently no known efficient algorithm that can run on a classical computing to decrypt public-key cryptographic standards. / Through Shor's algorithm and Grover's algorithm, advanced quantum computers can attack symmetric encryption standards and in the next 15 years, could break 2048-bit RSA encryption.

LABOR MARKET

With only a few thousand quantum scientists and engineers estimated worldwide in 2020, lack of talent could be a hindrance to the technology's growth. / Short course and professional development courses are emerging to allow the transfer of skills to the quantum computing industry.

TECHNOLOGY

High R&D costs, high failure rates, and long development cycles are commonplace in the healthcare industry. / Quantum computers, with their expected future advantages in optimization, machine learning, and molecular simulation, will provide the computational toolkit required to some of these entrenched problems.