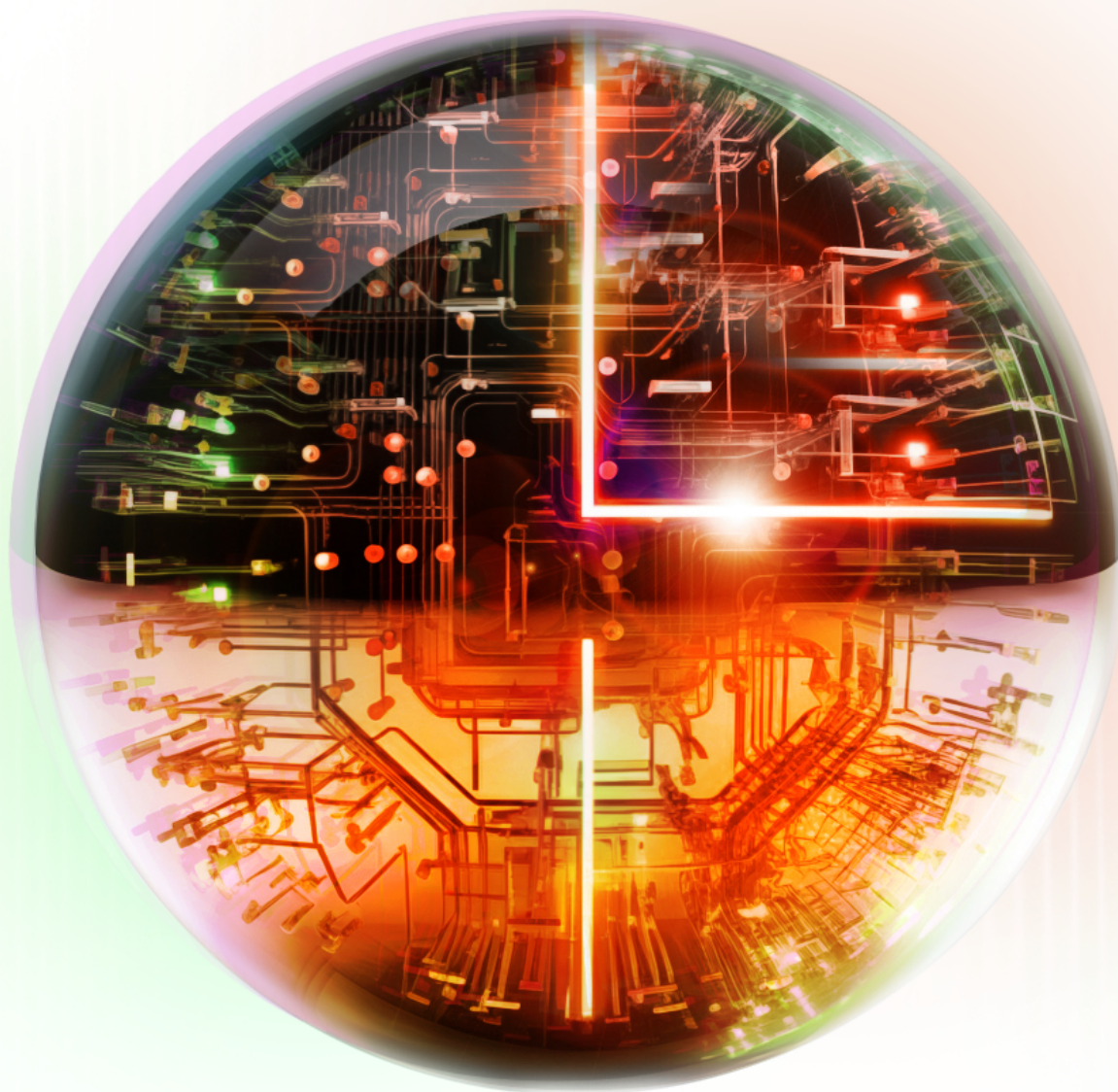


Deloitte.



The Quantum Countdown
Preparing for a new
tech revolution

Foreword	03
Introduction	04
What is quantum computing?	07
Quantum mechanics:	12
the magic behind the machines	
Quantum solutions:	15
supercharging problem solving	
The quantum threat:	21
why organisations need to act now	
How to be revolution ready	26
Endnotes	32
Authors	33

Foreword

Quantum computing has emerged as a potential technological gamechanger, allowing us to solve highly complex, large-scale problems quickly as a result of significant advances over many years.

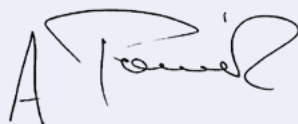
It's particularly exciting to see the widespread opportunities quantum computing presents to solve previously unsolvable problems across diverse domains including healthcare, climate change, agriculture and transportation.

But we also need to proactively address the risks and ethical considerations associated with quantum computing in fields such as privacy, security and fraud.

Australia has a chance to be a global leader in quantum computing if we are thoroughly prepared, willing to be bold, and clearly understand the key opportunities and risks.

Our report helps guide organisations towards a confident quantum future. The clock is ticking and we need to get ready for the possibilities ahead.

Adam Powick
Chief Executive Officer



Introduction

Bursting onto the scene in late 2022, generative artificial intelligence (Gen AI) caught many by surprise with its potential to revolutionise both daily tasks and the more complex aspects of our lives.

The world is still adapting to the benefits and risks of this disruptive tech, but before we can catch our breath, a conceivably more powerful force — quantum computing — could soon be upon us. The transformation and disruption could go far beyond anything we've experienced with AI.

Quantum computing isn't merely an emerging technology, it's a groundbreaking shift poised to redefine the fabric of computing, ushering in a new era of incredible problem-solving capabilities.



The quantum age is looming

No longer an aspiration confined to science-fiction, the first quantum computer with the power to surpass today's most powerful supercomputers could be available as soon as 2029¹, and research using quantum principles to solve complex problems has been happening for years.

Governments, organisations, and researchers are investing in building quantum computers, bracing for the transformative impacts, both positive and negative, it could unleash – while harnessing its principles to conquer intricate challenges that elude conventional technology. An estimated US\$30 billion was spent globally on quantum technology in 2022, with Australia contributing more than A\$130 million of this.^{2,3} By 2028, the conservative forecast is that US\$50 billion will be spent globally on quantum computing.⁴

Awe-inspiring opportunities and risks

The opportunities presented by this quantum leap are undeniably awe-inspiring and vast. From potentially eradicating different life-limiting medical conditions, to understanding the contributors to climate change and the solutions to slow, stop or reverse its effects, to finding practical solutions to global food scarcity issues. It's no wonder quantum computing is viewed as a revolution in technology and science.

However, this frontier isn't without its perils. The very same power that renders quantum computing a game-changer for good also poses significant risks, notably in cybersecurity. Current encryption methods that safeguard sensitive information could theoretically be rendered obsolete by the sheer computational muscle of quantum machines, leaving data vulnerable to breaches and exploitation on an unprecedented scale.



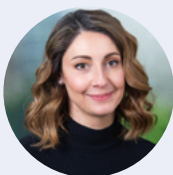
Preparing for the leap

Governments and regulators around the world have already started their quantum security journeys, with agencies such as the National Institute of Standards and Technology (NIST) in the US, outlining guidelines on how organisations can equip themselves for the potential threats ahead.

The technological changes and advancements made by quantum computing are set to impact most industries and most parts of our lives, so organisations should start planning now. Security specialists will need to rethink strategies, the C-suite will need to reimagine their products and services and explore new opportunities, while board members, risk professionals and regulators must be prepared to challenge organisations on readiness and the ethical implications of technological advancements.

It's time for Australian leaders to start their own quantum journeys. We're ready to help your organisation strategically leap into the quantum age to maximise the opportunities and minimise the risks of this game-changing tech.

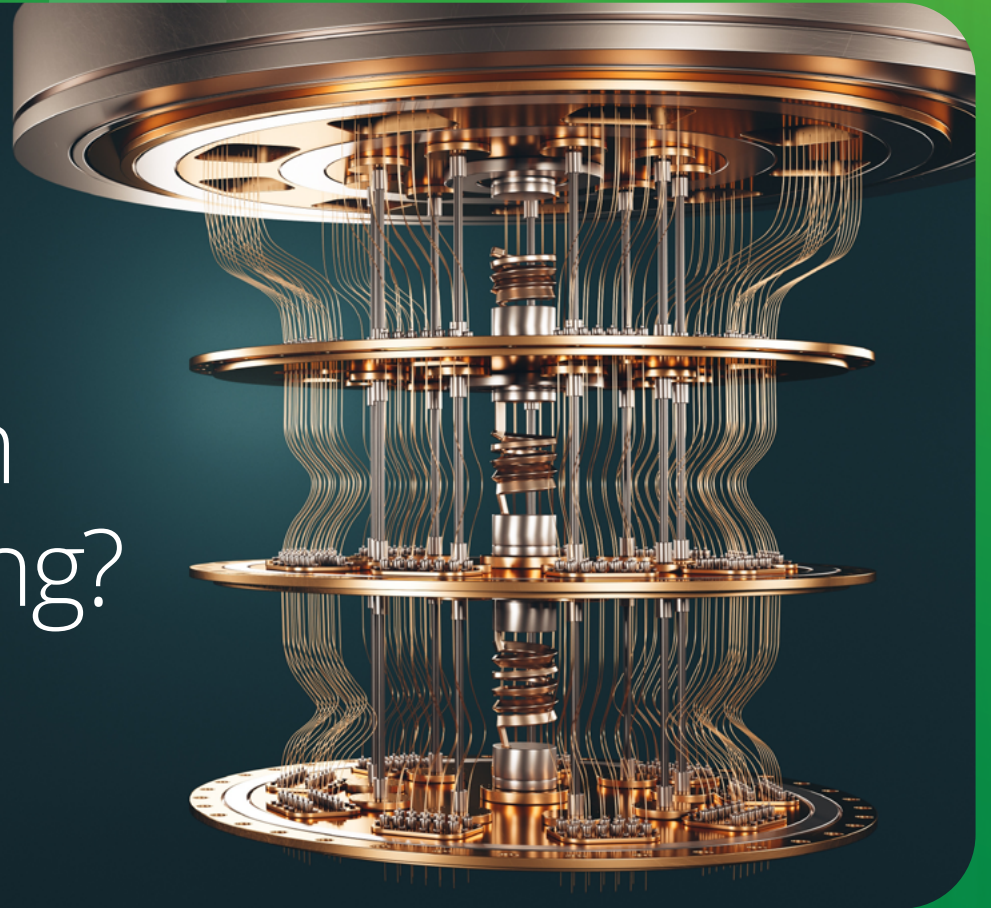
**The quantum era is waiting.
Don't let it catch you by surprise.**



Rita Gatt

Lead Partner | Regulation, Security and Risk
rigatt@deloitte.com.au

What is quantum computing?



At its core, quantum computing is a fundamentally different way of computer processing compared to today's 'classical computing' methods currently used in our iPhones, laptops or even supercomputers.

Quantum computers use quantum bits (**qubits**) that rely on the principles of quantum physics to unleash an immensely more powerful processor. The two most important principles used to achieve this power are **superposition** and **entanglement**.

Superposition explains how a quantum system can exist in multiple states simultaneously, allowing quantum computers to perform multiple complex calculations and process millions of operations at once.

How? While classical computers process information using bits that are either 1 (on) or 0 (off) and can only be in one state: 1 or 0, qubits can exist in a combination of both 1 and 0 (multiple states), unlocking the power of quantum algorithms and making quantum computers exponentially more powerful than classic computers.

Classic computing

Classical bit



On **or** off

Superposition

Quantum bit (qubit)

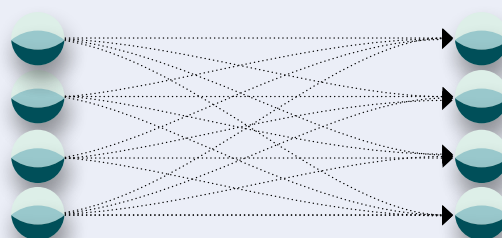


On **or/and** off

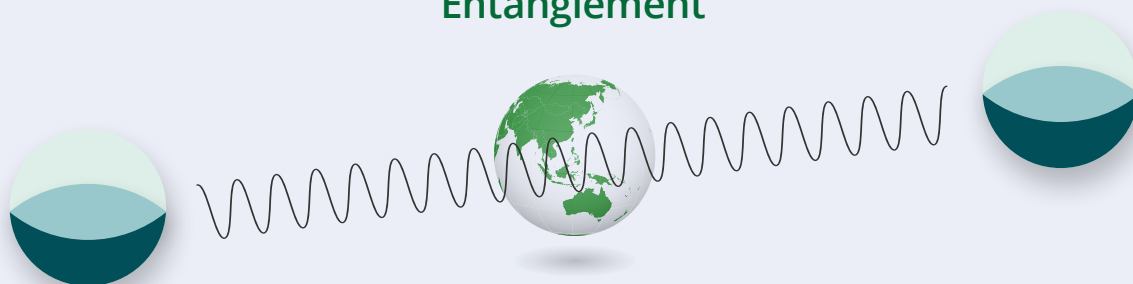
Linear process

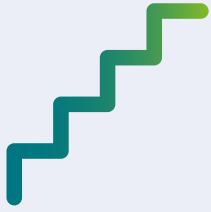


Parallel process



Entanglement





Entanglement is whereby an object or system such as electrons or photons, are connected regardless of their physical distance and are 'entangled', meaning if you measure the state of one, you can predict the state of the other. Einstein called this spooky science. This principle allows quantum computers to solve more complex problems and at a faster rate.

Quantum supremacy: surpassing impossible

Using the principles of quantum physics in computing unlocks a power unlike anything seen to date. To put it into perspective, consider this: in a range of scenarios, a quantum computer is estimated to be more than 150-million times faster than even our fastest supercomputer of today.⁵

Tasks once deemed unfeasible due to their complexity—ones that would have taken classical computers more than 40 years to crack— can potentially be unravelled in a matter of seconds thanks to the prowess of quantum computation.⁶ The term for this milestone is 'quantum supremacy', signifying the moment when a quantum computer performs a computation that's practically impossible for classical computers to solve within a reasonable timeframe.

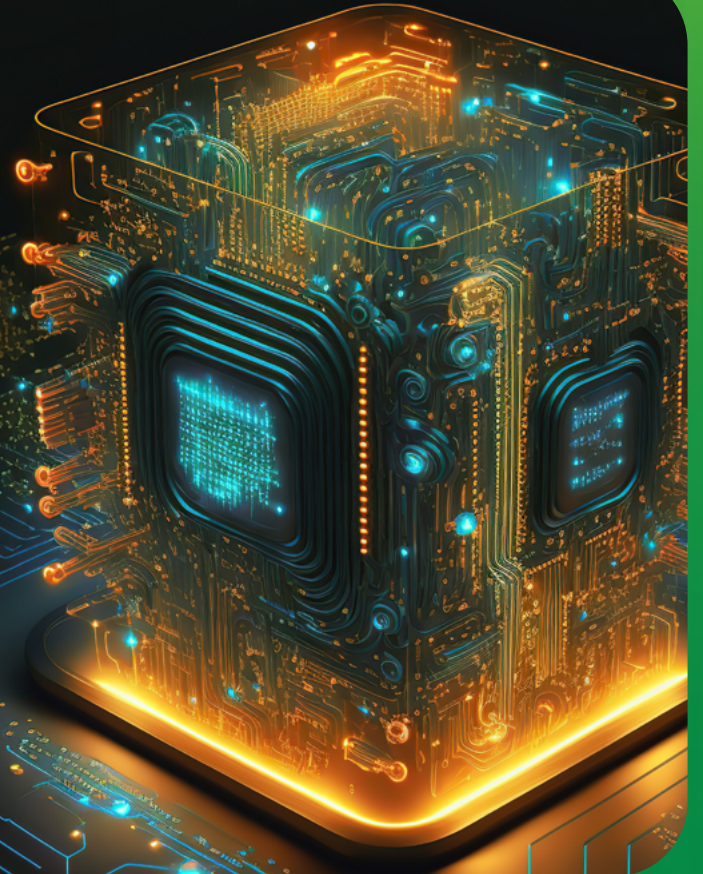
In 2019, Google claimed to have achieved quantum supremacy with their 53-qubit processor named Sycamore. This quantum computer performed a complex computation in just 200 seconds — a task, it was claimed, that would have taken the most advanced classical supercomputer approximately 10,000 years to complete. However, it's important to note their achievement was related to a specific problem set and does not signify universal quantum supremacy across all computational tasks.^{7,8}

Computer says no: conquering quantum computing limitations

In recent years, pioneers in quantum computing, including IBM, Google, and Harvard, to name a few, have made ground-breaking strides to create functioning quantum computers, albeit with inherent limitations. Quantum systems are sensitive to disturbances, such as 'decoherence', where quantum information becomes corrupted due to interactions with the environment (e.g. exposure to certain temperatures) or errors that occur during operations on qubits. Decoherence poses a significant threat to building and maintaining stable and reliable quantum computers.

Researchers are actively exploring ways to mitigate these limitations. To minimise decoherence specifically, efforts often focus on error detection and correction techniques as well as isolation from the environment. Other methods to preserve the delicate quantum information within the computer system include improved hardware with better designed qubits that can withstand external disturbances and noise.

Quantum mechanics: the magic behind the machines

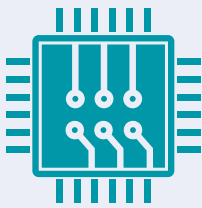


The concepts behind quantum mechanics trace back to 1901 with the trailblazing work of renowned physicists Neils Bohr and Max Plank, before initial attempts to build a quantum computer nearly 100 years later in 1998. In 2016, IBM made the first quantum processor publicly accessible on the cloud for experimentation and then in 2019 unveiled the world's first commercial quantum computer.⁹

Subsequent years have seen exponential developments, progressing quantum computing beyond inspiration for sci-fi content to receive significant investment with real tech advancements.

From IBM, Google, AWS and Microsoft to D-wave, Quantinuum and Rigetti, there are more players than you may expect working in this space, each with different timeframes and approaches to achieving success. Several universities and governments are also building their own quantum computers for research purposes.

Numerous types of quantum computers are currently under construction; some of the design methods being used include:



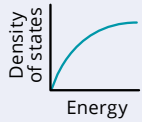
Superconducting circuits: this design uses superconducting materials, which generate electricity with zero-resistance at very low temperatures. Superconducting qubits are created in these circuits, leveraging quantum mechanics to process information.



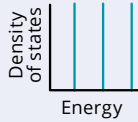
Trapped ions: individual ions (charged atoms) are trapped using electromagnetic fields and cooled by lasers. These ions act as qubits manipulated by lasers to perform quantum operations.



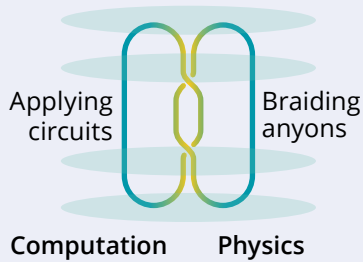
Bulk



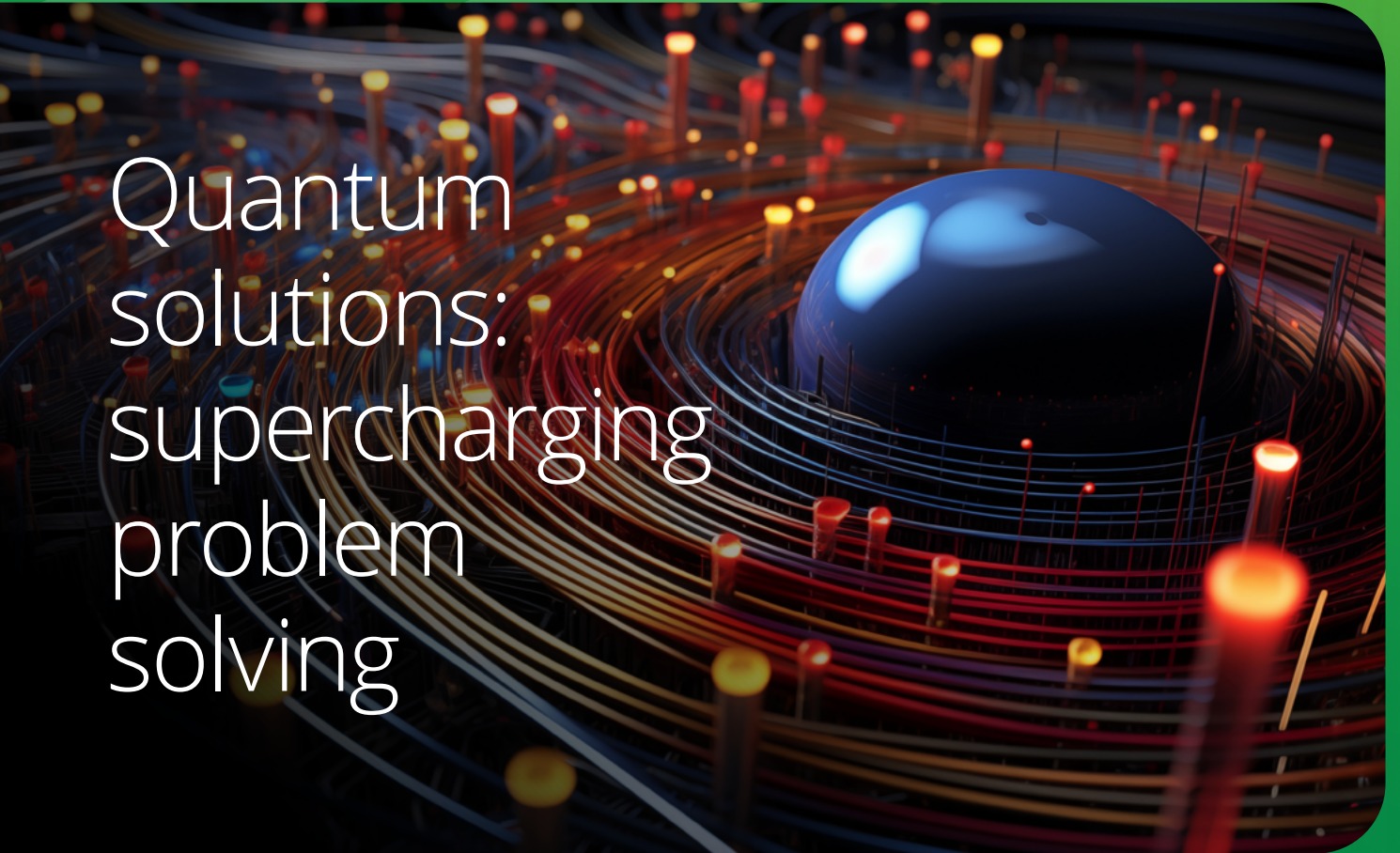
Quantum dot



Quantum dots: semiconductor nanocrystals — tiny light-emitting particles — are used to create quantum dots. These dots trap single electrons with ‘spin states’ — a form of angular momentum — that can be controlled and measured, in turn creating qubits.



Topological quantum computing: this stores and manipulates quantum information using anyons, unique quasi-particles existing in two dimensions. By manipulating their paths through ‘braiding’, anyons’ properties and ‘collective memory’ can create an error-resistant platform for quantum computing.



Quantum solutions: supercharging problem solving

With unparalleled computational power and the ability to process vast amounts of data, quantum computing holds immense potential for addressing complex global challenges. But how, exactly? We explore current quantum-inspired technologies and explore the future of innovative problem-solving.

The quantum advantage: using tomorrow's tech today

There's already a wide range of quantum-inspired technologies that draw inspiration from the principles of quantum mechanics without strictly using quantum computing itself. These quantum-inspired computing solutions and algorithms optimise classical computing tasks and enhance performance in various domains by mimicking quantum behaviour to solve problems faster and more effectively, here are some current examples:

Quantum-inspired computing solutions and algorithms

Classical computing solutions can be optimised or inspired by quantum principles to perform tasks more efficiently, even if they don't fully leverage quantum effects. Similarly, classical algorithms can use quantum concepts to enhance performance in certain tasks, such as optimisation and cryptography. These solutions and algorithms mimic quantum behaviour or advantages to solve problems faster or more effectively than their classical versions could.

Organisations are using quantum-inspired computing solutions and algorithms in various areas:



Optimisation: quantum-inspired algorithms that help solve complex optimisation problems like supply chain, portfolio, and logistics planning more efficiently.



Financial services: quantum-inspired computing solutions aid risk analysis, fraud detection, and portfolio management by processing large data volumes more effectively for more informed decisions.



Drug discovery: quantum-inspired computing techniques expedite the drug discovery process by efficiently simulating molecular interactions and identifying potential drug candidates, reducing time and costs.

Quantum key distribution (QKD), cryptography and post-quantum cryptography (PQC)

QKD uses quantum mechanics principles to create secure communication channels by transmitting encryption keys encoded in quantum states. It ensures the security of data transmission by detecting any attempts at interception. Similarly, quantum cryptography involves developing secure communication protocols using quantum principles, ensuring encrypted data remains protected against potential attacks from other quantum computers. PQC, on the other hand, is not based on quantum mechanics but aims to develop cryptographic algorithms that can resist attacks from quantum computers.

QKD, quantum cryptography and PQC are being researched and developed for various applications, including:



Secure communication: QKD can be used to establish secure communication channels between parties, ensuring transmitted data remains confidential and tamper-proof.



Privacy and security: the financial industry, government agencies, defence organisations, and the healthcare sector are exploring the use of QKD, quantum and PQC to bolster security measures; this includes enhancing security around financial transactions, protecting sensitive customer and patient data, securing sensitive communications, and safeguarding classified and national security interests, all while ensuring privacy and preventing unauthorised access.



Quantum sensing: quantum-inspired techniques can improve the precision of measurements. Quantum sensors and devices are used to achieve this across various fields, from timekeeping to geolocation. For instance, quantum-enhanced imaging and sensing technologies can detect minute changes in magnetic fields, light or gravitational forces.

Organisations are exploring the use of quantum sensing in various applications, including:



Security and defence: quantum sensors boost security measures by detecting and analysing signals like electromagnetic radiation and gravitational waves. They can be applied in threat detection, surveillance, and encryption to enhance security and defence.



Medical imaging: quantum sensors can enhance medical imaging techniques like MRI and PET, offering improved resolution and sensitivity for more accurate diagnoses and treatment plans.



Precision measurements: quantum metrology enables highly accurate measurements in fields like timekeeping, geodesy, and atomic clocks, and used in industries such as telecommunications, navigation, and scientific research.



Environmental monitoring: quantum sensors can detect and measure environmental parameters like magnetic fields, gravity, and temperature. This data is valuable for monitoring climate change, conducting geological surveys, and controlling pollution.

The future of problem solving

Looking beyond quantum-inspired solutions, once quantum computing is unleashed on the world the future of problem solving holds immense promise. Although quantum computers aren't yet commercially available, research is already underway to understand its potential and possibilities for critical challenges we're grappling with today. We're also seeing partnerships between quantum computing players with organisations and institutions to explore potential proof-of-concept demonstrations and applications.

Medical breakthroughs

When it comes to finding a cure for terminal or debilitating medical conditions, researchers often need to work through millions of iterations of ideas to see what works. Quantum computers may have the ability to simulate these ideas and responses, and not just process the trials and errors at massively increased speeds, but process these in parallel, meaning a significant shortening of time to discover treatments and cures. But it's not just about finding the right way to treat ailments, it's also about preventing them.

Imagine if we could discover the exact root cause, not just the likely contributors, to some of today's biggest medical challenges like Alzheimer's or cancer.

Quantum computers have the potential to help us understand our bodies right down to the atomic level and gain a much deeper understanding of how we work and what drives us to fall ill. In fact, one hospital in the US is already using a quantum computer for healthcare research into molecular biology and innovative cancer treatment methods.¹⁰

Climate and pollution solutions

Much research is underway to use quantum computers to better understand the contributors of climate change and to evolve practices in high-polluting industries. For example, the agricultural industry is already working on ways to use quantum computing-inspired techniques to reduce the amount of energy used to produce ammonia used in making fertilisers.¹¹ There's also work going into the analysis of land used for farming to optimise food production resulting in not just less waste and pollution but helping to solve the looming global issue of food scarcity.¹²

Finance and recession predictions

It was recently announced that quantum mechanics was used to reveal hidden patterns in the stock market.¹³ This technique was processed on a regular computer demonstrating how the fundamental principles of quantum computing are already making an impact on the industry. With quantum computing's ability to process and make sense of vast amounts of information and the finance industry's work with a large and complex number of variables, there's a huge opportunity to solve problems such as forecasting, risk and threat detection and even the prediction of mass events such as recessions.



The quantum threat: why organisations need to act now

The excitement around quantum computing and its extraordinary potential is tempered by the need to address accompanying security risks and it's a challenge demanding our immediate attention.

In less than a decade, quantum computing is projected to unravel the security of certain cryptographic algorithms. This imminent risk spans across various digital realms, affecting encryption, code signing, and signature validation that rely on digital certificates. The implications are vast, potentially compromising the confidentiality of data in transit and at rest, the integrity of software, and the authenticity of authorised connections.

'Harvest now, decrypt later' attacks are a threat we're already seeing play out. This is where adversaries collect encrypted data today with the aim of decrypting it with advanced quantum computing in the future. Innovations in PQC aim to protect against these quantum threats.

Bodies like NIST are leading the development of PQC standards for enduring data security in the quantum age.

The quantum threat also extends far beyond cryptographic algorithms, with potentially extensive ripple effects. Cyber leaders are deeply concerned about infrastructure breakdowns, ranking this threat among the most daunting challenges for businesses in the future.

The quantum safety switch

Transitioning to quantum-safe technology in response to the quantum threat is a major switch for organisations and governments worldwide. Looking at previous encryption advancements, it could take more than ten years for large organisations with complex data and processes to make the transition and ensure safeguards are in place.

NIST has been at the forefront of developing approved PQC standards, initiating this process back in 2016.^{14,15} Their efforts aim to future-proof cryptographic practices against the potential threats posed by quantum computing capabilities.

Also in the US, the National Security Agency (NSA) has set a significant milestone by establishing a 2035 deadline for PQC to be implemented across national security systems, underscoring the urgency and importance of transitioning to quantum-resistant cryptographic methods.¹⁶

Upgrade required: industry-specific challenges

The transition to quantum-safe algorithms will necessitate substantial updates across industries. In banking, the infrastructure will need significant overhauls to integrate PQC algorithms. This includes updating encryption methods for customer data, securing transactions, and fortifying communication channels between financial institutions. Additionally, industries like healthcare and telecommunications will face similar challenges, needing to update their systems to ensure patient data confidentiality and secure communication networks.

The adjustment won't be confined to software or network upgrades alone; it will also extend to hardware modifications. For example, in banking, point-of-sale terminals, ATMs, and backend servers will need hardware updates to accommodate new quantum-safe algorithms. Similarly, in the healthcare sector, medical devices and data storage systems will require hardware modifications to ensure compatibility with updated encryption standards. Telecommunication networks, including satellites and communication towers, will also necessitate hardware adjustments to secure data transmission using quantum-safe protocols.



On a collision course: urgent action required

Worryingly, the disruption caused by quantum computing to our current encryption methods is approaching within the next 5–10 years, but the transition to quantum-safe infrastructures for organisations and governments could potentially span more than a decade.

Quantum computing timeline

2024

2029

5-years' time

2034

10-years' time

2039

15-years' time

Organisation migration

Estimated ten-year migration roadmap

Ten-year migration roadmap

The number of years needed to properly and safely migrate to a quantum-safe solution.

Quantum computing readiness stage in 10 years, if organisations act now

Quantum threat

Quantum computing ready

Threat timeline The number of years before the relevant threat actors will be able to break the quantum-vulnerable systems.

Quantum computers may render encryption useless



We need to act now and plan strategically.

The collision between the fast-approaching threat and the time-consuming migration shows how urgent it is to take proactive, collaborative measures, and invest decisively in quantum-safe technologies. We need to strengthen ourselves against the fast-approaching challenges.



How to be revolution ready

With the impending collision between the rapidly advancing quantum threat and the essential but time-consuming migration of technology, organisations must urgently focus on strengthening cyber defences and making data quantum-secure now, not later.

To prepare for the changes more broadly and to make the most of the endless opportunities for quantum technologies, organisations should consider the following:



- Understanding the impact of quantum technology on industry
- Scanning the horizon for quantum disruption
- Exploring the intersection of quantum technology and business goals
- Assessing the organisational readiness for change
- Developing an ecosystem of partners in the quantum space
- Developing a quantum strategy
- Experimenting with quantum technologies.

Groups such as the NSA and NIST are also urging organisations to start acting now to develop secure future-proof quantum readiness plans.¹⁷

A structured approach to quantum readiness for organisations could involve the following roadmap:

Create a readiness roadmap

1. 

Create a task force

Plan your quantum resilience approach.

Understand that this will likely be a journey, not a sprint, and a major program of transformation. It should be aligned with other hardening objectives.

2. 

Plan discovery activities

Software applications can automate discovery, create and maintain a cryptographic catalogue. Surveys and interviews might also help.

3. 

Execute discovery gradually

Consider starting with a low impact Proof of Concept (POC) to commence building a cryptographic catalogue that can change dynamically as your environment changes.

4. 

Engage with software vendors and supply chain

To understand their embedded cryptography other dependencies and potential exposure.

5. 

Engage across the enterprise

Synchronise quantum readiness planning with other hardening and upgrade activities, including zero-trust uplifts.

6. 

Prioritise

Assign risk and priority to discovery outcomes. Continue to monitor and adapt.

Inaction or delaying the initiation of quantum readiness and resilience planning comes with a steep price tag. With each passing moment, the vulnerability to quantum threats compounds exponentially and necessitates immediate and sustained action by organisations and governments to safeguard digital assets.

Every organisation must conduct a thorough evaluation of the cost and impact of quantum-risk management in comparison to other strategic cybersecurity initiatives. This assessment, with the following table as a guide, will help prioritise the most effective scenarios and set allocating budgets accordingly.

Do nothing

Organisations that believe quantum computing is still at an early stage and the benefits of inviting and embarking on the quantum transition are yet to be defined.

Potential impacts

- No protection from quantum; full impact on the digital infrastructure
- Disruption of business operations and processes
- High risk of requiring a reactive, direct changeover when the threat materialises.

Potential opportunities

No upfront financial outlay.

Adopt a hybrid approach

As standards are created, it's possible to have classical, quantum and PQC solutions in a hybrid mode. The security of the complete solution is as good as the strongest element.

Potential impacts

- Vulnerability of classical solutions
- Low to medium financial impact.

Potential opportunities

- Provides legacy support to old solutions
- Allow agility and flexibility to adapt quickly to new solutions
- Provides classical protection while PQC algorithms being further stress tested.

Follow a phased approach

Phase investment to adopt quantum security solutions to replace impacted solutions.

Potential impacts

- Vulnerability of classical solutions
- Low-to-medium financial impact.

Potential opportunities

- Prioritisation of solutions based on inventory
- Phase-based improvement learnings
- Phased budget spending following quantum's evolution.

Direct changeover

Make a replacement of all impacted solutions, replacing them with quantum and post-quantum cryptography.

Potential impacts

- High financial impact – large migrations can have higher costs
- Large disruption of business operations and processes.

Potential opportunities

Direct enhancement of security against quantum risks for smaller, novel and less complicated environments.

Get ready to ride the quantum computing wave

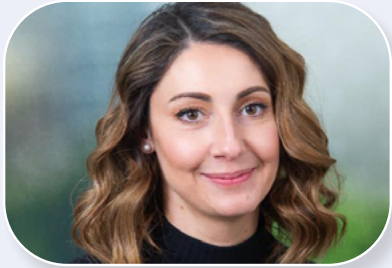
Despite perceptions that quantum computing may be daunting and complex, embarking on a journey in this space and learning how to limit its disruption doesn't need to be difficult. Organisations have a chance to proactively prepare for the use of quantum computing by identifying potential impacts on their businesses and taking practical steps to assess, educate and respond to the challenges, while optimising the opportunities. Unlike the relatively swift arrival of Gen AI that caught many by surprise, the advance notice of quantum computing provides organisations and governments time and resources to get ready for the impending wave of technological change and developments.

As we wait for quantum computing to have its moment in the sun, there's plenty for leaders to get on with. The quantum era is almost here, this is your chance to seize the opportunity, ride the quantum wave and position your organisation at the forefront of a technological revolution.

Endnotes

- 1 [When will quantum computers finally break into the market?](#) James McKenzie, Physics World, 3 Apr 2023
- 2 [The world is heading for a 'quantum divide': here's why it matters](#), World Economic Forum, 18 January 2023
- 3 [State of Quantum Computing: Building a Quantum Economy](#), World Economic Forum, September 2022
- 4 [Quantum technology market by computing, communications, imaging, security, sensing, modeling and simulation 2023–2028](#), Research and Markets, April 2023
- 5 [Quantum computing: Definition, facts & uses](#), Mark Smith, Live Science, March 19, 2022
- 6 [Supercomputer makes calculations in blink of an eye that take rivals 47 years](#), James Titcomb, The Telegraph, 2 July 2023
- 7 [Computing takes a quantum leap forward](#), Hartmut Neven, Google Quantum AI Team, 23 October 2019
- 8 [Quantum supremacy using a programmable superconducting processor](#), F Arute, K Arya, R Babbush et al, Nature 574, 23 October 2019
- 9 [An IBM quantum computer will soon pass the 1,000-qubit mark](#), Charles Q Choi, IEEE Spectrum, 24 December 2022
- 10 [Cleveland Clinic, IBM to lead new quantum computing for health projects](#), Andrea Fox, Healthcare IT News, 25 October 2023
- 11 [Atomically isolated copper on titanium dioxide for ammonia photosynthesis via nitrate reduction with unprecedentedly high apparent quantum yield](#), Hyun Sik Moon, Byeongju Song, Jiwon Jeon, Ting-Hsuan Lai, Yu-Peng Chang, Yi-Dong Lin, Jun Kue Park, Yan-Gu Lin, Yung-Jung Hsu, Hyeyoung Shin, Yongju Yun, Kijung Yong, Applied Catalysis B: Environment and Energy, Elsevier, 15 December 2023
- 12 [The Use of Quantum Technology in Agriculture](#), Ilamaram Sivarajah, AZoQuantum, 23 January 2023
- 13 [Quantum mechanics model unveils hidden patterns in stock markets](#), Chinese Academy of Sciences, 9 January 2024
- 14 [Post-Quantum Cryptography: Digital Signature Schemes](#), NIST, 2024,
- 15 [Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms](#), NIST, 20 December 2016
- 16 [National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems](#), The White House, 4 May 2022
- 17 [Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now](#), National Security Agency/Central Security Service, 21 August 2023

Authors



Rita Gatt

Lead Partner – Regulation,
Security and Risk

rigatt@deloitte.com.au

[LinkedIn profile](#)



Michael Puckridge

Principal – Cyber
and Strategic Risk

mpuckridge@deloitte.com.au

[LinkedIn profile](#)



Julie Gleeson

Principal – Cyber, Identity
and Strategic Risk

jgleeson@deloitte.com.au

[LinkedIn profile](#)



Tim Scott

Director – Cyber
and Strategic Risk

timsconfig@deloitte.com.au

[LinkedIn profile](#)

Are you ready to quantum-proof your organisation? Start the conversation today.

Connect with us: quantumready@deloitte.com.au

Huge thanks to
our contributors

Richard Hughes
Robert Lindwall
Matt Cowley
Nerida Shackleton

Kate O'Brien
Emily Emmerson
Yawen Jang

Deloitte.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

About Deloitte

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.com.

About Deloitte Asia Pacific

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Australia

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 10,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www2.deloitte.com/au/en.html

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

© 2024 Deloitte Touche Tohmatsu

1262655108_Designed and produced by The Agency | Deloitte Australia_3/24