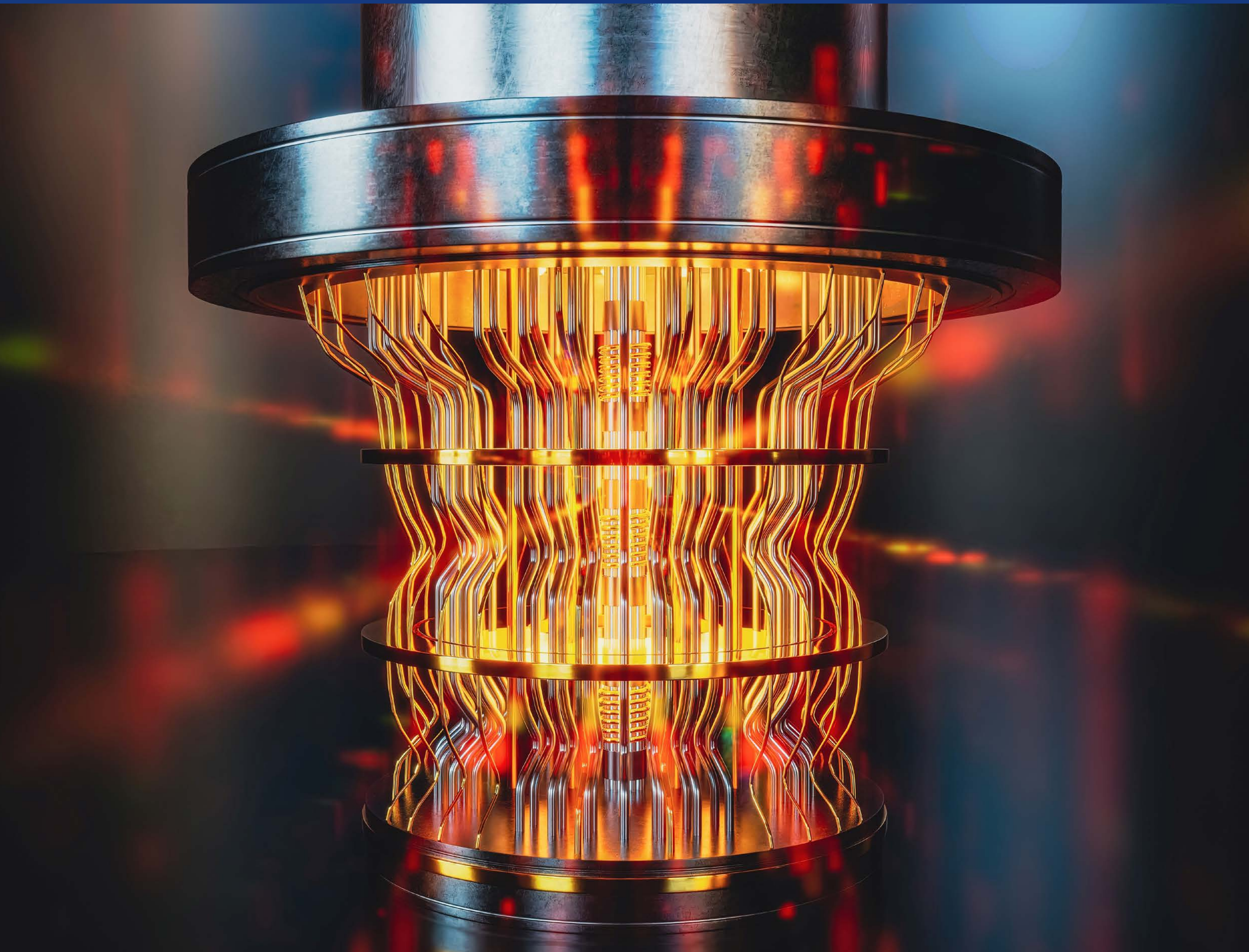
Office of the NSW Chief Scientist & Engineer

Quantum Algorithms and Applications

March 2024

Authors Prof Michael Bremner and A/Prof Simon Devitt, University of Technology Sydney
Editor Dr Eser Zerenturk, Office of the NSW Chief Scientist & Engineer



Fitzroy Falls, New South Wales

The Department of Enterprise, Investment and Trade acknowledges, respects and values Aboriginal peoples as the Traditional Custodians of the lands on which we walk, live and work. We pay our respects to Elders past and present.

We acknowledge the diversity of Aboriginal people and their ongoing connection to their country, waters and seas. We also acknowledge our Aboriginal and Torres Strait Islander employees who are an integral part of our diverse workforce.

Contents

Disclaimer - Third Party Reliance
This report is solely for the purpose set out in the executive summary and for the NSW Government's information. It has been prepared as a summary of more extensive data and information collection, analysis and synthesis, interim reports, observations and findings for a specific NSW Government purpose which may not relate to any single reader's specific situation. The NSW Government does not take responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility. We shall not be liable for any losses, claims, expenses, actions, demands, damages, liability or any other proceedings arising out of reliance by any third party on this report.

This report has been prepared for the Office of the NSW Chief Scientist & Engineer by Prof Michael Bremner and A/Prof Simon Devitt from the University of Technology Sydney.

Executive summary

Quantum algorithms and software development represent a significant commercial opportunity for NSW.

Quantum computers have a broad range of potential applications in industry, most prominently as a potential tool for scientific discovery. By simulating complex systems that are impossible to model with classical computers, quantum computers could help researchers develop new materials, chemicals and processes for advanced manufacturing. Over longer timescales, quantum computers may be used much more broadly, bringing advancements and efficiencies to artificial intelligence (AI), finance, transport and logistics.

However, the journey to commercial utility of quantum computing is far from over. There are many aspects of this technology that are in the early stages of development, from the hardware that powers computations, to the stack of software technologies that deliver the instructions. This presents opportunities for new businesses that work on both the development of the technology and how it can best serve the needs of industry and society.

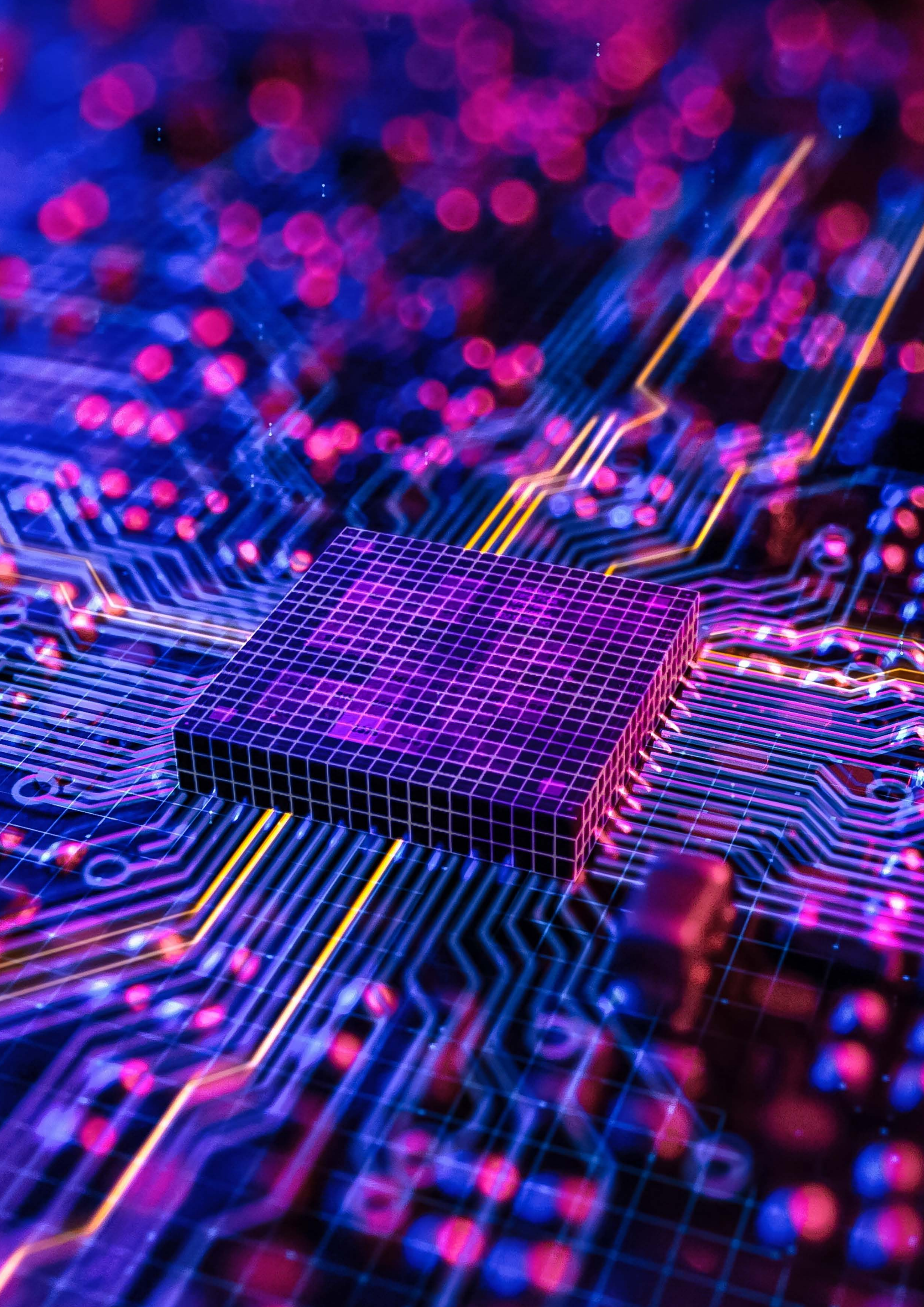
Especially pressing is the need for new algorithmic and software tools that can bring forward the opportunities presented by quantum computers. Improvements in quantum algorithms and software can shave decades off the potential time to utility for quantum applications.

An ongoing process of discovery and collaboration between the researchers at universities and industry will be vital for these discoveries — retention and creation of specialised talent is essential for success.

In this report these challenges and opportunities are detailed. Comprehensive discussions of the past and potential future progress of quantum hardware and software are provided, alongside high-level descriptions of the known possibilities and limitations of quantum computing applications.

NSW has built a strong quantum computing research ecosystem in Sydney. From the early days of quantum computing, NSW institutions have seen the potential for Australia to play a leading role in the development of this new technology. Key initiatives, such as the Sydney Quantum Academy, have positioned NSW for ongoing success. NSW universities have spun-out significant startups and researchers at these institutions are working with many of the leading industry-based teams in the world.

This report concludes with three recommendations for NSW to ensure that it benefits from the economic opportunities that will come from quantum computing and capitalises on the investments it has made in an increasingly competitive international environment.



Acronyms

ACQAO	ARC Centre of Excellence for Quantum-Atom Optics
AIST	National Institute of Advanced Industrial Science and Technology (Japan)
ANU	Australian National University
AQT	Alpine Quantum Technology
ARC	Australian Research Council
ARO	Army Research Office
AI	Artificial Intelligence
AQSN	Australian Quantum Software Network
ATIQ	Trapped-Ion Quantum Computer for Applications
AUSMURI	Australian United States Multidisciplinary University Research Initiatives
AWS	Amazon Web Services
CACI	California Analysis Center, Incorporated
Caltech	California Institute of Technology
Cambridge	Cambridge University
CAS	Chinese Academy of Sciences
CES	Centre in Exciton Science
CLOPS	Circuit Layer Operations per Second
CMO	Complementary Metal-Oxide-Semiconductor
CNBP	Centre for Nanoscale BioPhotonics
CoE	Centre of Excellence
CQB	Centre for Quantum Biology
CQCT	Centre for Quantum Computing Technology
CQC2T	Centre for Quantum Computing and Communications Technology
CQT	Centre for Quantum Technologies
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CUDOS	Centre for Ultra-high bandwidth Devices for Optical Systems
CWI	Centrum Wiskunde & Informatica (Netherlands)
DARPA	Defence Advanced Research Projects Agency (USA)
DISR	Department of Industry, Science and Resources
ENS	École normale supérieure (France)
EQUS	Centre for Engineered Quantum Systems
ETH	Federal Institute of Technology Zurich
EuroHPC JU	European High Performance Computing Joint Undertaking
FAU	Fraunhofer Institutes
FLEET	Future Low-Energy Electronics Technologies
GE	General Electric
GeQCoS	German Quantum Computer based on Superconducting Qubits
HDR	Higher Degree Research
HPC	High Performance Computing
IMEC	Interuniversity Microelectronics Centre (Belgium)
IP	Intellectual Property
IQC	Institute for Quantum Computing (Canada)

IQuAn	Ionen-Quantenprozessor mit HPC-Anbindung (Germany)
KIT	Karlsruhe Institute of Technology (Germany)
MIT	Massachusetts Institute of Technology
MRI	Magnetic Resonance Imaging
MQCQE	Macquarie Centre for Quantum Engineering
NCCRs	National Centres for Competence in Research (Switzerland)
NEC	Nippon Electric Company
NII	National Institute of Informatics (Japan)
NISQ	Noisy Intermediate Scale Quantum
NIST	National Institute of Standards and Technology (USA)
NMR	Nuclear Magnetic Resonance
NQIT	Networked Quantum Information Technologies Hub (UK)
NQTP	National Quantum Technology Program (UK)
NTT	Nippon Telegraph and Telephone (Japan)
NUS	National University of Singapore
OECD	Organisation for Economic Co-operation and Development
OIST	Okinawa Institute of Science and Technology (Japan)
QAST	Quantum Algorithms, Software and Theory
QCCF	Quantum Computing Commercialisation Fund
QEC	Quantum Error Correction
QRAM	Quantum Random Access Memory
QSI	Centre for Quantum Science and Information
QSIT	Quantum Science and Technology
RAM	Random Access Memory
RCS	Random Circuit Sampling
Rigetti	Rigetti Computing
RMIT	Royal Melbourne Institute of Technology
RSA	Rivest–Shamir–Adleman
RSG	Resource State Generators
RWTH	Aachen: Rheinisch-Westfälische Technische Hochschule Aachen (Germany)
SME	Subject Matter Expert
SRC	Special Research Centre
SQA	Sydney Quantum Academy
SQC	Silicon Quantum Computing
UK-NQS	United Kingdom National Quantum Showcase
UQ	University of Queensland
USTC	University of Science and Technology China
UTS	University of Technology Sydney
UWA	University of Western Australia
VTT	Technical Research Centre of Finland
WMI	Walther-Meißner-Institut (Germany)
Zapata	Zapata Computing

Key definitions

Quantum technology: A controllable system that owes its properties and behaviours directly to the dynamics described by quantum physics.

- **First-generation quantum technology:** Quantum technology that is governed by properties and behaviours that emerge from the bulk quantum mechanical effects of a very large number of quantum particles. First-generation quantum technologies include semiconductor materials (digital transistors), coherent light (optical lasers) and nuclear magnetic resonance (magnetic resonance imaging, MRI). Each of these technologies was responsible for a technological revolution in the 20th century: the digital computer, the high-speed optical internet and non-invasive medical imaging.
- **Second-generation quantum technology:** Quantum technology that directly exploits the behaviour of quantum mechanical particles or objects. Unlike first-generation quantum technology, which exhibits classical behaviour – such as the ability to be used as a switch (transistors) – due to its quantum mechanical properties, second-generation quantum technology actively manipulates and utilises the quantum mechanical effects to perform tasks that have no classical analogue.

Quantum computing: A computational device that uses quantum particles as the basic unit of information. The most common instance is a device containing many two-level quantum systems as quantum bits (qubits), with computational gate operations allowing qubits to interact.

- **Algorithmic complexity:** A computational algorithm can be parameterised with respect to its algorithmic complexity, sometimes referred to as 'Big-O' notation. This parameterisation characterises an algorithm in terms of the number of qubits required to execute a program and the number of distinct time steps as a function of the size of the input. For example, in Shor's factoring algorithm, the input is a number that can be represented using n-bits. The quantum algorithm to factor using Shor's algorithm would require $O(n)$ qubits – i.e. the number of qubits grows linearly with the input size, n, and a number of gate steps that grows as $O(n^3)$ – i.e. the number of steps grows cubically with n. A quantum algorithm is generally considered 'efficient' if these resources grow *polynomially*, i.e. if qubit or time complexity scales as $O(n^B)$, where n is the size of the problem and B is a positive real number. A quantum algorithm is generally considered inefficient if qubit or time complexity scales *exponentially*, i.e. scales as $O(B^n)$, where n is the problem size and B is a positive real number greater than one. Shor's algorithm is therefore considered computationally efficient.
- **A per shot pricing system:** Cloud-based pricing models for quantum computing access. Generally parameterised by a single use charge for a particular circuit with an additional smaller charge for each individual run (or shot) of that particular circuit. For example, in the AWS pricing model for a Rigetti quantum computer, the cost of running an algorithm is[1] $\$ = 0.3 + 0.00035S$
Where S is the number of times this circuit is executed. For many quantum algorithms (on noisy devices), S will be large to generate statistically significant results. If the noise on the device is above 1%, S can be exponentially large in the size of the algorithm, leading to large compute costs. For example, for a $N = 40$ qubit quantum circuit that is very noisy, S could be as large as $S = 2^{40}$, leading to a computer cost of $\$ = 0.3 + 0.00035 \times 2^{40} = \$384$ *million*. For a fast quantum computer, that operates with gate speeds of 100ns (for example, superconductors), this would take approximately 30 hours.

[1] https://aws.amazon.com/braket/pricing/.

- **Coherence:** A term describing how well a quantum state is maintaining its quantum properties. It can also describe operations that are successfully occurring between two quantum objects. A fully coherent quantum state is where a quantum system's wavefunction is completely described without correlations between inaccessible environmental variables. A coherent operation between quantum systems is where two or more quantum systems interact, inducing constructive or destructive interference between components of the wave-function describing the combined system.
- **Circuit Layer Operations per Second (CLOPS):** A secondary metric derived by IBM that effectively divides the quantum volume by the total execution time of the quantum circuit.[2] i.e. *CLOPS ~ QV/t*, where *t* is the physical gate time of the quantum computer. Derived due to ion-trap computers being able to achieve larger quantum volumes than IBM's own superconducting qubits.[3] By renormalising quantum volume to CLOPS, IBM's quantum computing systems could remain superior with this new metric as superconductors run between 1,000x and 10,000x faster than ion-trap computers.[4]
- **Fault-tolerant quantum computer:** A quantum computing system implementing full error-correction protocols to enable low error rate operations. A fault-tolerant quantum computer may consist of only one error-corrected qubit, or it may contain millions.[5]
- **Fidelity:** A general measure as to the accuracy of preparing a particular quantum state or performing a gate operation. State fidelity is a measure between zero and one that describes how accurately a quantum state can be prepared in a quantum computer with respect to a desired reference state – where a fidelity of zero means that the states are completely dissimilar (orthogonal) and a fidelity of one means the prepared state is identical to the reference state. Gate fidelity is a measure between zero and one that describes how accurately an operation is applied on a quantum state. Gate fidelity is measured by comparing the unitary matrix (or a linear mapping) describing the gate operation against a target operation. Alongside fidelity, sometimes error rate is used. Generally, error rate is defined as $error = 1^{-Fidelity}$.
- **Interference:** The general state of a quantum computer is a linear vector space of complex numbers. Each basis state — corresponding to a possible binary output of the quantum computer — has an associated 'amplitude', represented by a complex number. As the state of the quantum computer is manipulated via gate operations, these complex amplitudes can add together or cancel each other out. This is known as interference. The goal of quantum algorithms is to manipulate these amplitudes such that the 'incorrect' answers destructively interfere — i.e. add together to equal zero such that the incorrect answer is never observed when the quantum computer is measured — and the 'correct' answers constructively interfere, such that there is a high probability of obtaining the correct answer when the quantum computer is measured.
- **Noisy Intermediate Scale Quantum (NISQ):** A quantum algorithm small enough to be faithfully executed on near-term quantum hardware without requiring resource-intensive quantum error correction protocols.[6]
- **Optimisation problem:** Optimisation problems aim to find the extremal values of a mathematical object. There are many different types of optimisations that depend on the nature of the mathematical data type to be optimised.
- **Polynomial time (P) and Nondeterministic Polynomial time (NP):** P and NP are two well-studied computational complexity classes that characterise many commonly encountered computational problems. A problem is said to be in P if the run time required by the computational algorithm to solve it increases as a polynomial function in the size of the problem, i.e. if the input of the algorithm can be represented by n-bits, then the space or time required for the algorithm scales as $O(n^B)$, where B is a positive real number. An NP problem is one where, if the solution is known, the run time to *verify* that the solution grows polynomially with the size of the problem. However, computing the solution to the hardest problems in NP is believed to take exponential time. Arguably, the most famous unsolved problem in theoretical computer science is if P vs NP i.e. for every problem that can be efficiently *verified* can it also be efficiently *solved*?

[2] Wack A et al. (2021) 'Quality, Speed, and Scale: three key attributes to measure the performance of near-term quantum computers', arXiv:2110.14108 [quant-ph].

[3] https://www.quantinuum.com/news/quantinuum-h-series-quantum-computer-accelerates-through-3-more-performance-records-for-quantum-volume-217-218-and-219

[4] https://quantumcomputing.stackexchange.com/questions/26769/speed-of-superconducting-qubit-architectures.

[5] Devitt S J et al. (2013) 'Quantum error correction for beginners', Reports on Progress in Physics, 76(7):076001.

[6] Preskill J (2018) 'Quantum Computing in the NISQ era and beyond', *Quantum*, 2:79.

- **Quantum advantage:** A computational algorithm that has superior performance to its classical equivalent without strict theoretical proofs of supremacy. Metrics of advantage can be broader than computational execution time or hardware resources and can include the total economic cost of the quantum vs classical solution.[7]
- **Quantum algorithm:** An algorithm specifically designed to be run on a quantum computer. They differ from classical algorithms in that they are composed of operations that are fundamentally quantum mechanical in nature.
- **Quantum complexity theory:** The study of the resource requirements and limitations of solving problems via quantum algorithms, often in contrast to classical algorithms.
- **Quantum error correction:** The process of redundantly encoding a piece of quantum information across a collection of individual quantum systems. Physical errors on the constituent qubits move the information between these distinct regions in ways that are detectable and correctable, maintaining the fidelity of the encoded information.[8]
- **Quantum supremacy:** A computational algorithm that can be theoretically proven to be implementable using a quantum computer and not using a classical computer at any reasonable scale. The first claimed demonstration of quantum supremacy occurred in 2019 from Google using a 53-qubit quantum chip.[9] Supremacy claims are now debated due to improved classical methods for emulating the quantum protocol run on the Google chipset. Supremacy now likely requires at least a 90-qubit chipset to be unequivocal.[10]
- **Quantum volume:** A metric developed by IBM to classify the power of their quantum chipsets.[11] Consider a random quantum circuit that contains n-qubits and n-timesteps. If a quantum computer can successfully execute this circuit and replicate the classical emulation of this circuit, quantum volume is defined as $QV = 2^n$. An error-free, classical emulator, containing 64GB of RAM (standard in current state of the art laptops) can emulate a quantum circuit perfectly, and achieve an equivalent quantum volume of $QV = 2^{32} = 4{,}294{,}967{,}296$. The most advanced quantum chipsets can currently achieve a quantum volume[12] of $QV = 2^{19} = 524{,}288$.
- **Random circuit sampling:** A quantum algorithm that consists of a random group of single and two qubit gates, designed to take the computational state of the computer to a random point within the exponentially large state space (Hilbert space) accessible to the computer. By measuring the quantum computer after the application of a random circuit, you can sample from the probability distribution defined by the random circuit. It has been shown that for quantum circuits containing approximately 80-100 physical qubits and approximately 80-100 layers of random gates, sampling from this probability distribution on a classical computer is likely to not be possible using current or expected future semiconductor technology.[13]

Quantum Algorithms, Software and Theory (QAST): Research that is focused on the theoretical aspects of quantum information science. This may be in developing and analysing new or existing quantum algorithms, communications or sensing protocols, developing tools for quantum error correction or error mitigation, building compilers or performance analytics tools or developing new programming interfaces, languages or new ways to interact with quantum computers. QAST also includes more fundamental theoretical research regarding the nature of quantum computing, communications or sensing technology, including what this technology can do and how it relates to more foundational concepts in physics, mathematics, computer science and chemistry.

[7] Hoefler T (2023) 'Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage', arXiv:2307.00523 [quant-ph].
[8] Devitt S J et al. (2013) 'Quantum error correction for beginners', *Reports on Progress in Physics*, 76(7):076001.
[9] Arute F et al. (2019) 'Quantum supremacy using a programmable superconducting processor', *Nature*, 574:505–510
[10] Zhang M et al. (2023) 'Noisy Random Quantum Circuit Sampling and its Classical Simulation', Advanced Quantum Technologies, 6(7):2300030.
[11] Cross A W et al. (2019) 'Validating quantum computers using randomized model circuits', *Physical Review A*, 100(3):032328.
[12] https://www.quantinuum.com/news/quantinuum-h-series-quantum-computer-accelerates-through-3-more-performance-records-for-quantum-volume-217-218-and-219.
[13] Boixo S et al. (2018) 'Characterizing quantum supremacy in near-term devices', *Nature*, 14:595-600.

1. A history of quantum computing

1.1 A brief history of quantum computer development

While the theoretical foundations for quantum computing started in the late 1960s and early 1970s,[14,15] more serious discussions about building such a device occurred in the mid-1990s. The first significant results detailing how a quantum computer could be built came in 1995.[16,17]

More concrete proposals emerged for quantum computing systems towards the end of the 1990s and some initial demonstrations of actual quantum computers, most notably liquid-state nuclear magnetic resonance (NMR) systems[18,19] and photonics approaches.[20,21] Photonic demonstrations piggybacked off well-established work into entanglement theory and foundational issues in quantum mechanics,[22,23] that led to the Nobel Prize for physics in 2022, including the first demonstrations of quantum teleportation in 1997.[15] NMR quantum computers were some of the first to demonstrate primitive quantum gate operations and algorithms,[24] even though it was clear to the community that liquid-based NMR approaches for quantum computing were intrinsically unscalable beyond these initial small-qubit number demonstrations.[25,26]

From 1995, there was an increase in initial system proposals for several different quantum computing hardware architectures.[27] This was followed by proposals for superconducting quantum computers,[28] quantum dot-based computers,[29] spin-donor systems,[30] optical quantum computers,[31] quantum computers that utilise topological states of matter,[32] non-gate based models such as quantum annealers[33] and measurement-based quantum computing.[34]

At least eight primary hardware modalities for quantum computing took shape over the next ten years. These systems demonstrated the ability to manufacture quantum bits (qubits) in a semi-reliable manner, received substantial funding from universities or national programs, and featured a prominent experimentalist advocating their particular hardware modality as a scalable platform for quantum computation.

[14] Holevo A S (1973) 'Bounds for the quantity of information transmitted by a quantum communication channel', *Problems of Information Transmission*, 9(3):177–183.
[15] Wiesner S (1983) 'Conjugate coding', ACM Sigact News, 15(1):78-88
[16] DiVincenzo D (1995) 'Quantum Computation', *Science*, 270(5234):255-261
[17] Lloyd S (1996) 'Universal Quantum Simulators, *Science*, 273(5278):1073-1078.
[18] Cory D G et al. (1997) 'Ensemble quantum computing by NMR spectroscopy', *Proceedings of the National Academy of Sciences*, 94(5):1634–1639.
[19] Gershenfeld N A and Chuang I L (1997) 'Bulk Spin-Resonance Quantum Computation', *Science*, 275(5298):350–356
[20] Bouwmeester D et al. (1997) 'Experimental quantum teleportation', *Nature*, 390(6660):575–579
[21] Boschi D et al. (1998), 'Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels', *Physical Review Letters*, 80(6):1121–1125.
[22] Aspect A et al. (1981) 'Experimental tests of realistic local theories via Bell's theorem', *Physical Review Letters*, 47:460.
[23] Aspect A et al. (1982) 'Experimental test of Bell's inequalities using time-varying analyzers', *Physical Review Letters*, 49:1804
[24] Vandersypen L M K et al. (2001) 'Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance', *Nature*, 414: 883-887.
[25] https://en.wikipedia.org/wiki/Nuclear_magnetic_resonance_quantum_computer.
[26] Jones J A (2001) 'Quantum Computing and Nuclear Magnetic Resonance', arXiv:quant-ph/0106067.
[27] Cirac J I and Zoller P (1995) 'Quantum Computations with Cold Trapped Ions', *Physical Review Letters*, 74:4091.
[28] Divincenzo D P (1997) 'Topics in Quantum Computers', Mesoscopic Electron Transport, NATO ASI Series, accessed December 2023, Topics in Quantum Computers | SpringerLink.
[29] Loss D and DiVincenzo D P (1998) 'Quantum computation with quantum dots', *Physical Review A*, 57:120.
[30] Kane B E (1998) 'A silicon-based nuclear spin quantum computer', *Nature*, 393:133-137
[31] Knill E et al. (2001) 'A scheme for efficient quantum computation with linear optics', *Nature*, 409:46-52.
[32] Kitaev A Y (2003) 'Fault-tolerant quantum computation by anyons', *Annals of Physics*, 303(1):2-30.
[33] Kadowaki T and Nishimori H (1998) 'Quantum annealing in the transverse Ising model', *Physical Review E*, 58:5355.
[34] Raussendorf R and Briegel H J (2001) 'A One-Way Quantum Computer', *Physical Review Letters*, 86:5188.

These eight major systems are:

- Donor-Based system,[35] including phosphorus in silicon systems
- Ion Traps[36]
- Neutral Atoms[37,38]
- NV-Diamond and other colour centres[39]
- Superconductors[40]
- Photonics, discrete variable, single photon[41] and continuous variable coherent laser pulses[42]
- Quantum Dots,[43] including silicon quantum dots
- Topological states of Matter.[44]

These eight systems remain the dominant systems under development for quantum computing today, even though during the 2000s, they were part of a much more extensive list of proposed hardware modalities. By the early to mid-2010s, each of these systems (except for topological states of matter) could claim to be able to routinely fabricate and control physical qubits, perform universal gate operations at moderate to high fidelity and even run small-scale test protocols such as quantum algorithms, and error-correction codes or communications protocols.[45]

At this time, quantum computers began to move out of the laboratory and into the commercial world.

[35] Kane B E (1998) 'A silicon-based nuclear spin quantum computer', *Nature*, 393: 133-137.
[36] Cirac J I and Zoller P (1995) 'Quantum Computations with Cold Trapped Ions', *Physical Review Letters*, 74:4091.
[37] Brennen G K et al. (1999) 'Quantum Logic Gates in Optical Lattices', *Physical Review Letters*, 82:1060.
[38] Jaksch D et al. (2000) 'Fast Quantum Gates for Neutral Atoms', *Physical Review Letters*, 85:2208.
[39] Shahriar M S et al. (2002) 'Solid-state quantum computing using spectral holes', *Physical Review A*, 66:032301.
[40] Divincenzo D P (1997) 'Topics in Quantum Computers', Mesoscopic Electron Transport, NATO ASI Series, accessed December 2023, Topics in Quantum Computers | SpringerLink.
[41] Knill E et al. (2001) 'A scheme for efficient quantum computation with linear optics', *Nature*, 409:46-52.
[42] Lloyd S and Braunstein S L (1999) 'Quantum Computation over Continuous Variables', *Physical Review Letters*, 82:1784.
[43] Loss D and DiVincenzo D P (1998) 'Quantum computation with quantum dots', *Physical Review A*, 57:120.
[44] Kitaev A Y (2003) 'Fault-tolerant quantum computation by anyons', *Annals of Physics*, 303(1):2-30.
[45] https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.

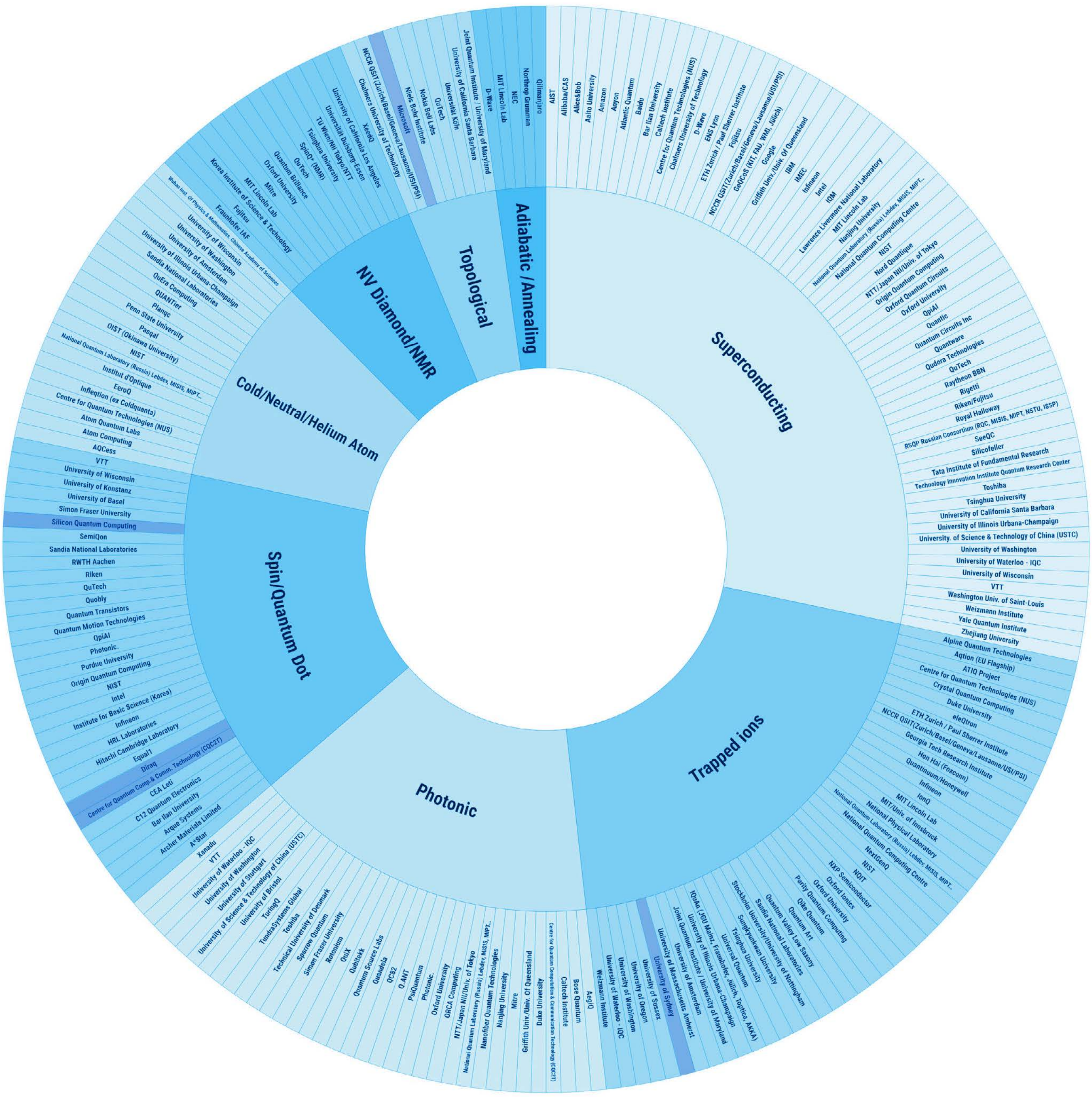


Figure 1. Global summary of the companies and academic programs developing the eight major quantum hardware technologies. Sourced from the Michel Kur, CEO of Multiverse Systems SAS,[46] and modified to highlight companies and academic efforts specific to NSW. ■ Companies specific to NSW

Figure 1 is a graphical summary of effort on each of these systems worldwide. This includes university research groups, national efforts, corporations, and startups. Superconductors still dominate the landscape, but each system is well represented, and so far, no technology is 'leading the race'. Each of these systems still has significant barriers before they reach the scale needed to solve commercially relevant problems and each of these systems will require an extensive fabrication base if they intend to manufacture and deploy quantum computers at commercial and global scales.

1.2 The dawn of quantum algorithms

Quantum computers were first theorised to be more powerful than existing models of computing in the early 1980s, building on breakthroughs in the foundations of information sciences and theoretical physics that occurred in the 1960s and 1970s. The initial concept was driven by the observation that simulating quantum mechanical systems appeared to be a fundamentally difficult task for classical computers – however, advances in quantum control made it possible for some quantum mechanical systems to mimic or simulate the behaviour of others in a way that classical computers could not.[47]

[46] https://www.linkedin.com/feed/update/urn:li:activity:7018614672098541569/

[47] Feynman R P (1982) 'Simulating Physics with Computers', *International Journal of Theoretical Physics*, 21:467–488.

This idea was built into a formal model of computing[48,49,50] which made it possible to begin studying how algorithms might work on such devices if they were ever to be built.

A series of breakthroughs in quantum algorithms saw quantum computing transform from a philosophical and academic curiosity to a potentially revolutionary idea by the mid-1990s. Key observations by David Deutsch, Australian scientist Richard Jozsa[51] and Daniel Simon[52] suggested that quantum computers might exponentially outperform classical computers in certain settings. Building on these observations, Peter Shor discovered the now famous 'Shor's algorithm', which showed that quantum computers could *efficiently*, that is with relatively low cost, solve the 'factoring' problem – the problem of finding the prime factors of a composite number.[53] This problem is notoriously difficult for classical computers to solve, and its difficulty underlies the *still* ubiquitous Rivest–Shamir–Adleman (RSA) cryptographic system which is used extensively for secure online communications.[54]

The potential cybersecurity implications of Shor's discovery led to initial efforts worldwide to determine how hard it would be to build a quantum computer. This saw increased expenditure by government defence and intelligence agencies on developing quantum computers and the theory underpinning them.[55] Within a few years, multiple proposals for developing the basic building blocks of quantum circuitry appeared.[56,57,58] However, the intricate accuracies required to build quantum computers meant they were more susceptible to errors than the semiconductor technologies at the core of classical computing. In another landmark discovery, Shor and others developed quantum error correction (QEC), establishing software methods for dealing with errors in quantum computers if sufficiently sophisticated quantum circuitry could be built.[59]

The dual discoveries of the quantum factoring algorithm and quantum error correction created a significant challenge to much of the conventional thinking of computer science. While classical computers have continued to improve, the underlying mathematical model for computing has remained largely consistent since the 1930s. Throughout the history of computing, there have been many attempts to invent new models of computing that offer a transformative increase in more computing capability.[60] These models have usually been either equivalent to existing models or physically limited, and ultimately, errors would overwhelm the accuracy of the devices. Shor's discoveries established that quantum computers were likely both a distinct model of computing and potentially physically feasible.

In parallel with these advancements, Lov Grover discovered the quantum 'unstructured search' algorithm, an algorithm that provides for a *provable* quantum speedup over classical unstructured search problems.[61] Unlike Shor's algorithm, which provides *exponential* improvement over classical computers, Grover's algorithm provides a more modest *polynomial* advantage. Such advantages could disappear, for instance, due to error correction costs or other architectural constraints. However, Grover's algorithm was critical because it suggested that quantum computers could be superior to classical computers for a broader range of high utility problems, including functions that are common on classical computers.

The discovery of Grover's algorithm also provided a better understanding of the nature of quantum advantage. Bennet, Bernstein, Brassard and Vazirani proved that Grover's algorithm is optimal for unstructured search, and in doing so, also showed that quantum computers are likely to encounter many of the same problems classical computers encounter for NP-complete problems and are unlikely to have a simple one-size-fits-all approach to many optimisation problems.[62] As such, quantum advantage is subtle and depends on the mathematical structures that underlie key problems. Consequently, theoretical research plays an important role in revealing quantum algorithms with an advantage over classical computers.

[48] Deutsch D (1985) 'Quantum theory, the Church-Turing principle and the universal quantum computer', *Proceedings of the Royal Society A*, 400:1818.

[49] Yao A C (1993) 'Quantum circuit complexity', *Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science*, Palo Alto, CA, USA, 352-361.

[50] Bernstein E and Vazirani U (1993) 'Quantum complexity theory', *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing* (pp. 11-20).

[51] Deutsch D and Jozsa R (1992) 'Rapid solution of problems by quantum computation', Proceedings of the Royal Society A, 439:1907.

[52] Simon D R (1994) 'On the power of quantum computation', *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 116-123.

[53] Shor P W (1994) 'Algorithms for quantum computation: discrete logarithms and factoring' *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 124-134.

[54] https://cra.org/ccc/wp-content/uploads/sites/2/2018/11/CCC-Identifying-Research-Challenges-in-PQC-Workshop-Report.pdf.

[55] Many initial programs run by DARPA or the ARO are not archived online anymore but examining acknowledgements from papers of the time (*https://arxiv.org/abs/quant-ph/9705052*), illustrate early US Department of Defence spending on the topic.

[56] Vedral V (1996) 'Quantum networks for elementary arithmetic operations', *Physical Review A*, 54:147.

[57] Steane A (1998) 'Quantum computing', *Reports on Progress in Physics*, 61:117.

[58] Nielsen M A and Chuang I L (2000) 'Quantum Computation and Quantum Information', *Cambridge University Press*, United Kingdom.

[59] Shor P W (1995) 'Scheme for reducing decoherence in quantum computer memory', *Physical Review A*, 52:R2493(R).

[60] Aaronson S (2013) 'Quantum computing since Democritus', *Cambridge University Press*, New York.

[61] Grover L K (1996) 'A fast quantum mechanical algorithm for database search', *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, 212-219.

[62] Bennett C H et al. (1997) 'Strengths and Weakness of Quantum Computing', *SIAM Journal on Computing*, 26:1510-1523.

2. The scale of quantum computers

Quantum computing has rapidly evolved over the past few years, with the first cohorts of quantum leaders transitioning from academic research to commercial ventures. As technology advances, a crucial question emerges: what can be expected in terms of the scale of quantum computers in the next 10 and 20 years?

2.1 Current state

Before looking into the future, it is essential to understand the current state of quantum computing. Today, quantum computers are still nascent, with small-scale, error-prone devices dominating. Major players in the industry, such as IBM, Google and others, offer cloud-based quantum computing access to researchers and developers. These systems typically consist of around 50 to 100 physical qubits.

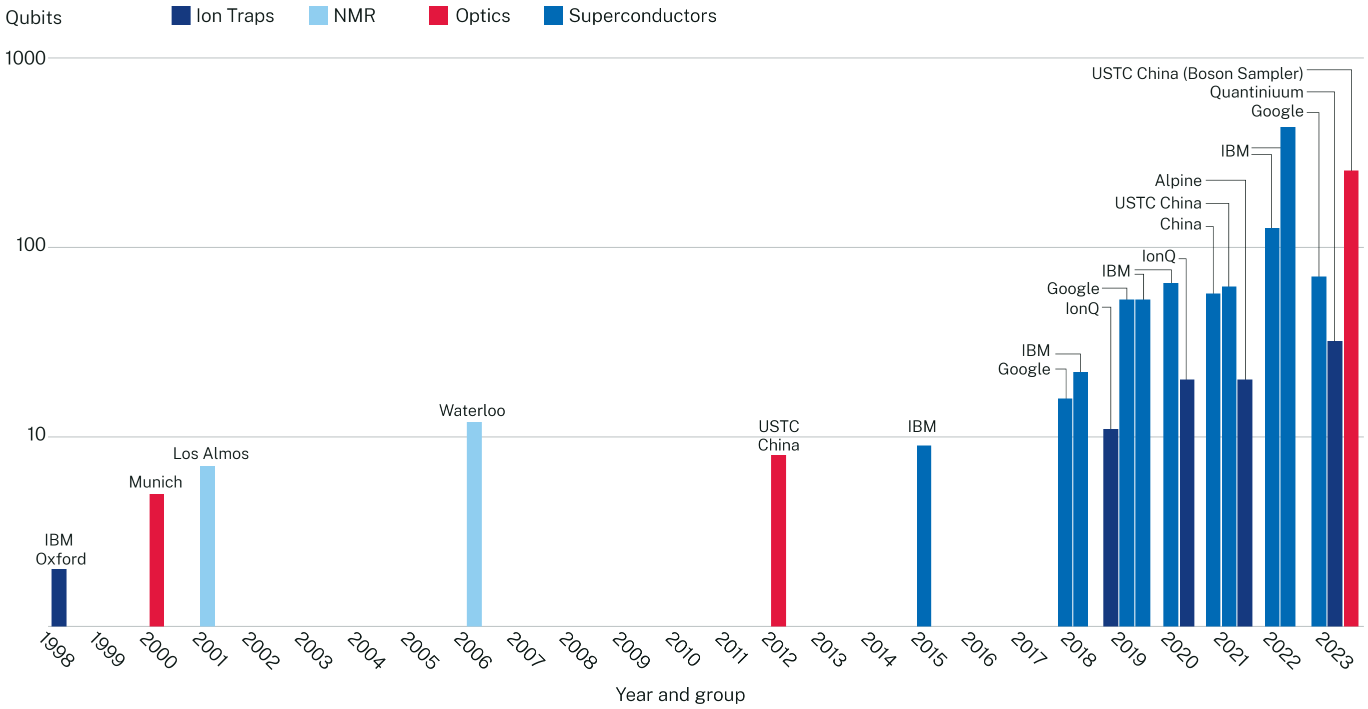


Figure 2. Historical size of quantum chips. Changes in quantum computer size over the past 26 years, illustrated as the number of qubits across ion-traps, optical quantum computers, nuclear magnetic resonance and superconductors from 1997 to 2023. This is a non-exhaustive list.

Figure 2 shows quantum computer sizes across, historically, four of the most common hardware modalities.[63] The most significant increase in qubit numbers is from IBM, pushing forward a roadmap to build a 100,000-qubit chipset by the end of this decade,[64] with 127-qubit devices available on their cloud service today and a 433-qubit system announced in 2022.[65]

[63] Arguably a missing modality in Figure 2 is neutral atoms, whose progress has seen rapid advancement in the past 12-24 months. There are still issues surrounding the most well-known deployment of a neutral atom computer, the 256-qubit QuEra Aquila device as it is not a universal gate based system (https://www.quera.com/aquila). The details of a newly announced 1000+ qubit neutral atom device from Atom computing are still not available. Hence, neutral atoms have been omitted from this plot.

[64] https://research.ibm.com/blog/100k-qubit-supercomputer.

[65] https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two.

While these chipsets are getting larger, error rates are not decreasing at a comparable rate to allow these computers to perform larger and larger computations. Figure 3 shows data from the IBM superconducting systems.[66] This data illustrates the best 2-qubit gate error rate as a function of the system. IBM has demonstrated approximately a factor of 10 reduction over the past six years. However, this data does not look at the average error rate over a single chipset that may contain dozens or hundreds of 2-qubit gates and does not plot the average over many different chips of the same generation architecture. Figure 3 examines the best individual gate operation that exists across all the gates on all the chipsets that have been tested.

When various qubit systems were first experimentally demonstrated starting in the late 1990s, 20-30% error rates were not uncommon.[67,68] Since then, research and development across most major platforms have decreased these physical error rates to 1% and sub-1%, depending on the type of quantum operation and hardware system. It is now standard across several qubit platforms to reliably fabricate and control qubits with high fidelities, in some cases above 99%.[69,70]

However, while these fidelities are extraordinarily high from a scientific or engineering point of view, they must be higher to implement quantum algorithms at scale successfully. A rough unit of measure to determine the error rates necessary to implement a quantum algorithm or quantum circuit successfully is to calculate the inverse circuit area,[71] *1/(KQ)*, where Q is the number of qubits in your algorithm/circuit and K is the number of gate steps. This quantity provides a reasonable bound for the physical error rate required on hardware. Consequently, for a 100-qubit quantum computer, a quantum algorithm/circuit requires 10 elementary gate steps, and the error bound for the physical hardware is less than 0.1%; this is approximately the error rate achievable using new generation qubit chip designs in 2023 in ion-traps, neutral atoms and superconductors.[72,73,74]

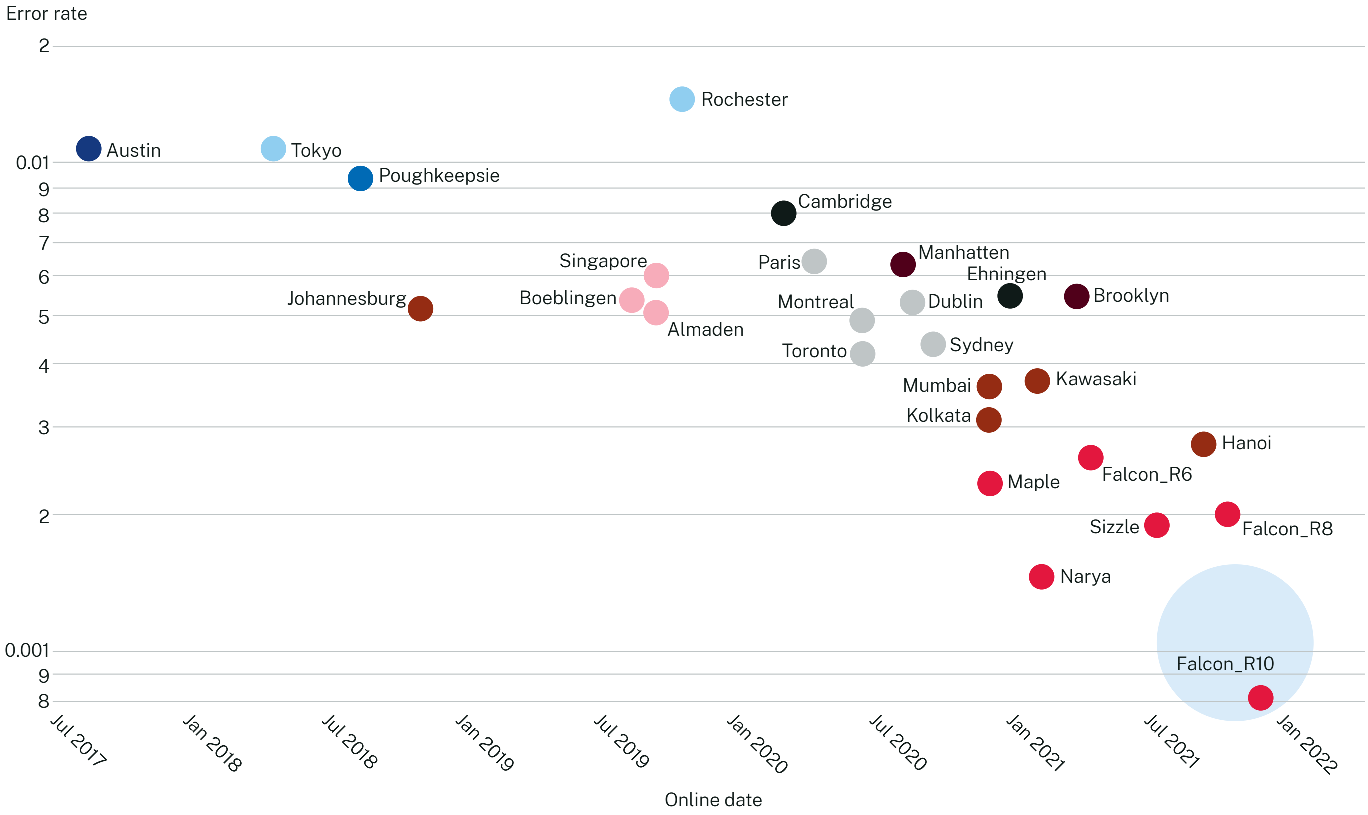


Figure 3. Gate fidelities. Best CNOT error rate as a function of system revision. Data from IBM examining the best CNOT gate fidelity across multiple generations of their superconducting quantum processors. Best CNOT represents the highest fidelity 2-qubit gate across all gates and all manufactured chipsets of a particular name.[75]

[66] https://www.hpcwire.com/2021/12/13/ibm-breaks-100-qubit-qpu-barrier-marks-milestones-on-ambitious-roadmap/.

[67] Monroe C et al. (1995) 'Demonstration of a Fundamental Quantum Logic Gate', *Physical Review Letters*, 75:4714.

[68] Nakamura Y et al. (1999) 'Coherent control of macroscopic quantum states in a single-Cooper-pair box', *Nature*, 398:786-788.

[69] Barends R et al. (2014) 'Superconducting quantum circuits at the surface code threshold for fault tolerance', *Nature*, 508:500-503.

[70] Wang Y et al. (2020) 'High-Fidelity Two-Qubit Gates Using a Microelectrochemical-System- Based Beam Steering System for Individual Qubit Addressing', *Physical Review Letters*, 125:150505.

[71] Brandhofer S et al. (2021) 'ArsoNISQ: Analyzing Quantum Algorithms on Near-Term Architectures', *IEEE European Test Symposium*, Bruges, Belgium, 1-6.

[72] Ding L et al. (2023) 'High-Fidelity, Frequency-Flexible Two-Qubit Fluxonium Gates with a Transmon Coupler', *Physical Review X*, 13:031035.

[73] Moses S A et al. (2023) 'A Race Track Trapped-Ion Quantum Processor', arXiv:2305.03828 [quant-ph].

[74] Evered S J et al. (2023) 'High-fidelity parallel entangling gates on a neutral-atom quantum computer', *Nature*, 622:268-272.

[75] https://www.hpcwire.com/2021/12/13/ibm-breaks-100-qubit-qpu-barrier-marks-milestones-on-ambitious-roadmap/.

Due to the limited functionality of current quantum computing systems, researchers have spent significant time developing core theory surrounding the concept commonly known as quantum supremacy.[76] This area of research focuses on designing a quantum algorithm/circuit that is difficult for a classical computer to simulate/emulate. Multiple authors showed[77] that a classical computer cannot efficiently emulate this sampling procedure as the number of qubits increases.[78,79] These sampling algorithms/circuits were explicitly designed to be the smallest possible quantum algorithm/circuit that could be proved to not be effectively simulated or emulated on classical computers, but importantly, their purpose is not to produce an algorithm of any particular scientific or commercial utility.

This challenge of quantum supremacy was taken up by the Google Quantum Artificial Intelligence (AI) team, who, in 2019, published a paper that claimed to have demonstrated random circuit sampling in a chipset of 53 superconducting qubits.[80] The result sits on the threshold of what is potentially simulatable with a classical machine rather than clearly in the supremacy regime (which would need approximately 90 physical qubits to be unequivocal). However, the work demonstrated many highly beneficial aspects of the technology, including suppressing complex error channels and fabricating, testing and calibrating an extremely complex quantum chip. In 2021, Chinese researchers unveiled the Zuchongzhi-2 superconducting chip, which realised random circuit sampling over 56 qubits. Compared to the 2019 Google result, this was a more explicit demonstration of supremacy using random circuit sampling.[81] In 2023, Google achieved a 70-qubit demonstration.[82]

There is a significant effort within the theoretical quantum community and across many subject matter experts (SMEs) to identify new domain problems that require enhanced computational power, benchmark the utility of quantum computing for these applications and provide rigorous estimates for the size of a quantum computer needed to run these new algorithms.[83,84,85]

The major bottleneck is related to the additional physical resources required to effectively error-correct quantum chipsets. Quantum algorithms are susceptible to errors during computation. QEC protocols are needed to reduce the errors in the chipsets and require resources of their own.[86]

For a suitably large-scale quantum computer to be of utility, the QEC would constitute the vast majority of the computation performed by the system; that is, the principal computation performed by a large-scale quantum computer is to correct its own errors. For example, factoring a large composite number using Shor's algorithm is one of the most impactful applications of a quantum computer due to its utility to compromise RSA public-key cryptosystems. Without error correction, a quantum computer consisting of approximately 5,000 physical qubits would be sufficient to break[87] RSA-2048. However, each of these qubits would require an effective error rate of less than 10^{-15}.[88] This is not possible using current technology. To perform enough error correction to allow this algorithm to run successfully requires a machine containing 20 million physical qubits – 4,000 times more than the algorithm requires. This overhead is solely required to reduce the error in the system from 0.1% at the physical level to the 10^{-15} needed to implement the algorithm successfully.[89] Error-correction overhead thus becomes significant when examining the utility of quantum algorithms for any application.

Figure 4 summarises what is currently available from a selection of quantum hardware vendors.[90,91] Some of these machines are deployed either for access via the cloud or direct sales to HPC centres (AQT, IQM), some have been detailed in academic papers[82,83,92] (IonQ, Google, USTC) and some have been announced by companies but have yet to appear as either deployed systems or academic papers (IBM, Atom Computing, Infleqtion). The systems are now dominated by Superconducting, Ion-Traps and Neutral atom quantum computers, and each of them demonstrates various errors on their fundamental gate operations.

[76] Preskill J (2012) 'Quantum computing and the entanglement frontier', arXiv:1203.5813 [quant-ph].

[77] Boixo S et al. (2018) 'Characterizing quantum supremacy in near-term devices', *Nature*, 14:595-600.

[78] Bremner M et al. (2010) 'Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy', *Proceedings of the Royal Society A*, 467:459-472.

[79] Bremner M J et al. (2016) 'Average-Case Complexity Versus Approximate Simulation of Commuting Quantum Computations', *Physical Review Letters*, 117:080501.

[80] Arute F et al. (2019) 'Quantum supremacy using a programmable superconducting processor', *Nature*, 574:505–510.

[81] Wu Y et al. (2021) 'Strong Quantum Computational Advantage Using a Superconducting Quantum Processor', *Physical Review Letters*, 127:180501.

[82] Morvan A et al. (2023) 'Phase transition in Random Circuit Sampling', arXiv:2304.11119 [quant-ph].

[83] https://learn.microsoft.com/en-us/azure/quantum/intro-to-resource-estimation.

[84] https://www.quantumresource.org/.

[85] https://qce.quantum.ieee.org/2023/workshops-program/.

[86] Devitt S J et al. (2013) 'Quantum error correction for beginners', Reports on Progress in Physics, 76(7):076001.

[87] 2048-bit RSA keys are commonly assumed to be large enough to be secure against all classical crypto-attacks.

[88] Devitt S J et al. (2004) 'Robustness of Shor's algorithm', *Quantum Information and Computation*, 6(7):616-629.

[89] Gidney C and Ekera M (2021) 'How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits', *Quantum*, 5:433.

[90] https://ianhellstrom.org/quantum.html.

[91] https://www.qusecure.com/qubit-scorecard/.

[92] Chen J-S et al. (2023) 'Benchmarking a trapped-ion quantum computer with 29 algorithmic qubits', arXiv:2308.05071 [quant-ph].

In general, none of these systems can claim to have reliable, reproducible gate error rates for a universal set of operations below 0.1% – the highest error rate practically required for QEC protocols to be implemented – and, in general, average error rates for these systems across a universal gate set is approximately 1%.[93]

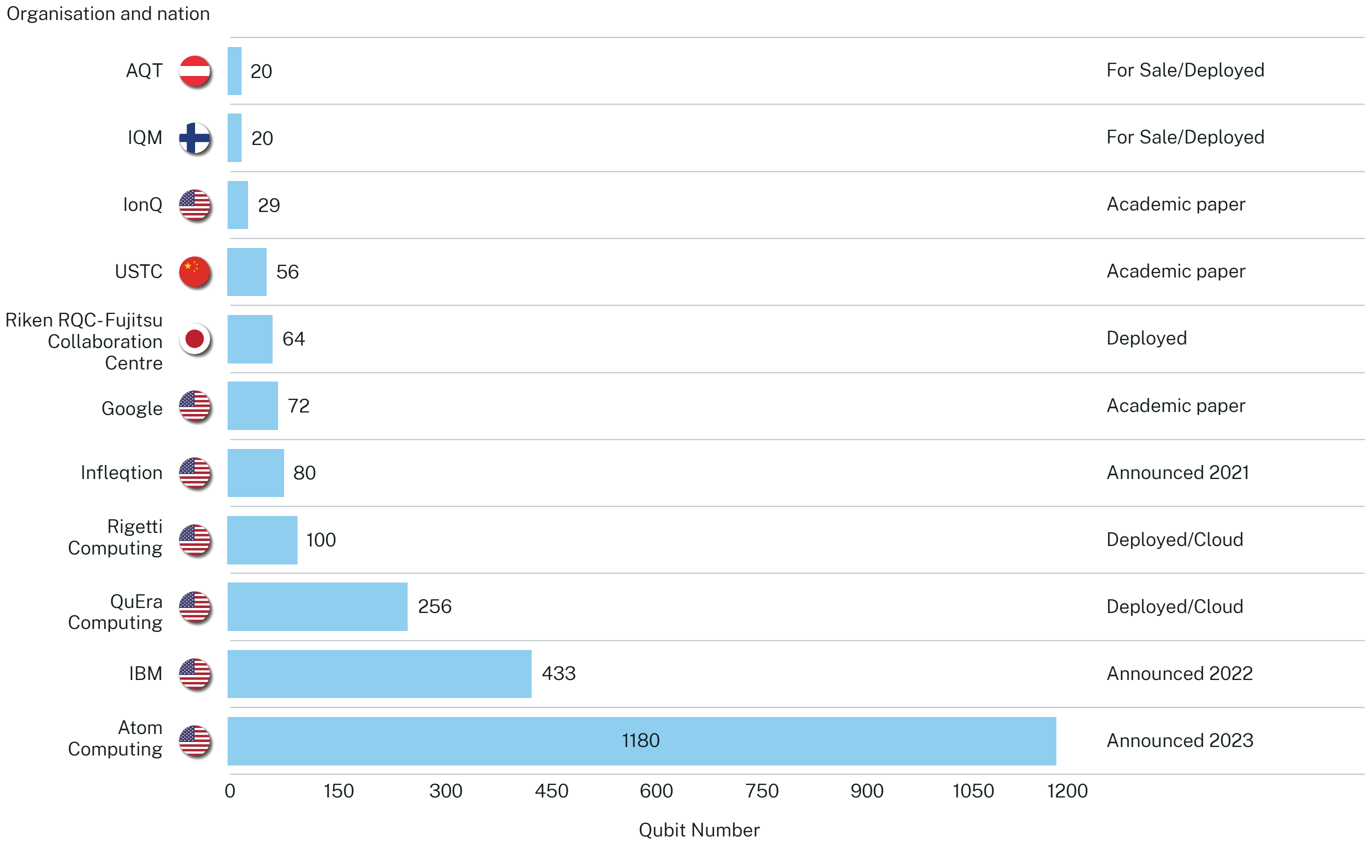


Figure 4. Announced or deployed systems from a variety of providers available today or announced to be available in 2024. Many performance metrics, including error rates, are not yet available.

2.2 Ten years out

In the next 10 years, it is reasonable to expect a gradual but significant improvement in quantum computing technology. Researchers and engineers will continue to focus on improving error rates, gate fidelities and qubit stability. QEC techniques will become more sophisticated, allowing error rates to decrease. Quantum algorithms will also undergo continuous refinement, leading to more efficient and practical applications.

By the end of this decade, it is anticipated that quantum computers with several hundred to a thousand qubits will be accessible on the cloud. These machines will offer improved reliability and enhanced performance, with a potential bifurcation in the community between companies that wish to push to high qubit numbers without focusing on the realisation of reliably low error rates versus companies that spend more capital on making qubits better and improving assembly line techniques for manufacturing and packaging at the cost of only providing quantum computing systems containing a few hundred qubits. However, even with these advancements, the development of large-scale, fault-tolerant quantum computers capable of solving complex problems at an industrial scale is not imminent.

The companies, however, do have arguably highly optimistic plans. Along with the systems that are either deployed now, or announced to be deployed within the next 6-12 months, several companies have touted ‘roadmaps’, describing their targets for the next 8-10 years. Figure 5 illustrates qubit targets for these roadmaps.[94,95,96,97,98]

[93] https://ianhellstrom.org/quantum.html.
[94] https://www.ibm.com/quantum/roadmap.
[95] https://www.qusecure.com/qubit-scorecard/.
[96] https://quantumai.google/learn/map.
[97] https://finance.yahoo.com/news/rigetti-computing-reports-first-quarter-200500204.html.
[98] https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap.

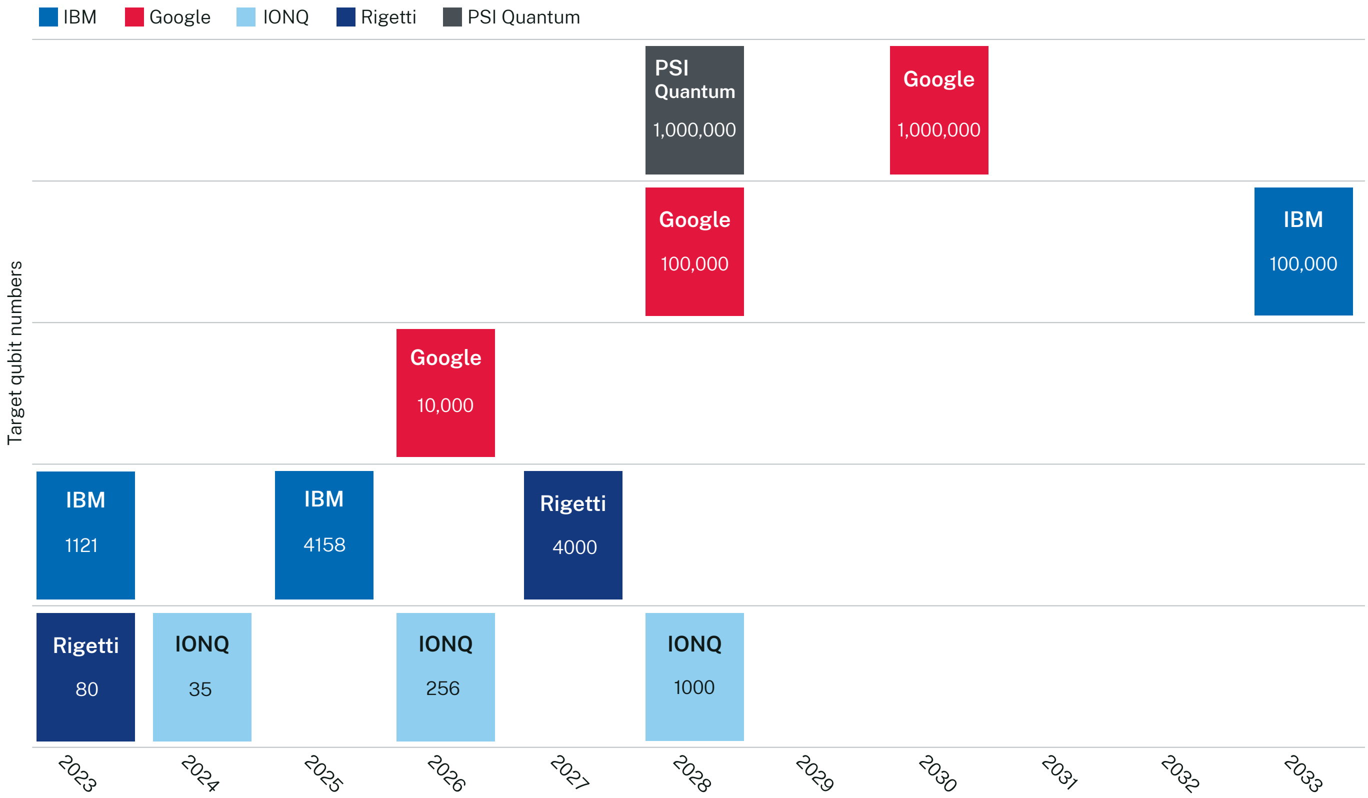


Figure 5. Declared longer term roadmaps for several quantum computing hardware companies. These hardware roadmaps are arguably optimistic and focus only on qubit counts. Contextualising what these qubit counts mean requires making several assumptions. In the case of non-solid-state architectures, such as PsiQuantum's photonic approach, even more extrapolation and interpretation is required to understand the claim of 1 million qubits by 2028.

The vast majority of the hardware roadmaps benchmark the size of their respective systems in terms of qubit counts. There is little discussion surrounding 'fidelity roadmaps' or how the quality of qubits is expected to increase moving from 2024 to 2034. The current target for scalable quantum computing systems, in order for QEC to be effective in further reducing error rates to the levels required for large-scale algorithms, is for a universal set of physical gate operations to be reliably at the 0.1% level or lower.[99] Reliability in this context refers to the ability of hardware manufacturers to produce qubit chipsets that reach this 0.1% error rate level with minimal to no deviation, device-to-device. Error rates for effective QEC need to be 0.1% or lower. Manufacturing variability above 0.1% will significantly impact performance. Hence, the assumption is that the variance from this 0.1% will either be very low or biased such that individual qubits do not suffer noise above this 0.1% bound, but variances could allow for lower error rates.

Reliability reducing errors will be a significant challenge for all major hardware platforms for at least the next 10 years. While it is expected that error rates of 0.1% will be achievable across many systems (several systems are approaching these error rates in prototype devices today), ten more years of research and development to ensure that these error rates are *reliably* at the 0.1% or lower is not an unreasonable assumption given the history of qubit technology.

Assuming that error rates on these technologies, in ten years, can reliably be realised at 0.1% or lower, how can qubit counts be quantified in these roadmaps? This can get quite complex, given the specifics of an architecture. But a guideline is:[100]

- the total number of physical qubits in a system is approximately 1000 times more than the number of encoded qubits
- the encoded clock rate of the system is approximately 1000 times slower than the physical speed of the particular qubits.

At this overhead, it is estimated that the TeraQuop regime will be reached, where one trillion logical operations can be performed before the error correction fails. This means that the error correction is taking an effective 0.1% error rate at the physical layer and reducing it by approximately a factor of 1 billion.

Consequently, the number of encoded qubits, clock rates and effective error rates for major systems can be estimated *if* they successfully reach their roadmap targets over the next ten years (Table 1).

[99] Devitt S J et al. (2013) 'Quantum error correction for beginners', Reports on Progress in Physics, 76(7):076001.
[100] https://www.riverlane.com/blog/what-is-a-teraquop-decoder.

Table 1. Approximate size and speed metrics for quantum hardware architectures if they achieve scales indicated in their roadmaps.

	Physical qubits/Devices	Logical qubits	Logical Clock Rate
Google (2030)	1,000,000	~1000	~60KHz
IBM (2033)	100,000	~100	~60KHz
PsiQuantum (2028)	1000 RSGs @ 58MHz	~1000	~4.2KHz
Rigetti (2027)	4000	~4	~60KHz

Table 1 is an approximation, as the specific hardware architecture needs to be considered in detail.[101] Comparing solid state architectures like superconductors or ion-traps against architectures such as photonics is difficult. However, if targets are met from these roadmaps, it is expected that approximately 1000 encoded qubits with lifetimes extended by a factor of 1 billion is possible. Note that this does not mean a quantum algorithm of 1000 qubits can actually be executed, as many of these encoded qubits in the hardware will be utilised for other ancillary protocols needed to maintain a fault-tolerant machine. Optimising this level of error-corrected compilation is a major focus of research today, but as a very rough approximation, between 20-30% of the logical qubits in Table 1 may be available to the algorithm. This leads to the following outlook for the next ten years.

If Quantum computing roadmaps are realised by the end of the 2020s, quantum computers will have approximately the same number of error corrected qubits as there are physical qubits today. This will allow algorithms to be run at effective error rates of one part in one trillion, rather than one part in one thousand, but with the same effective number of qubits.

2.3 Twenty years out

The scale of quantum computing hardware, estimated by the companies themselves, is likely to be too optimistic, and the true state of the quantum ecosystem by 2044 will be somewhere between systems containing on the order of a thousand reliable qubits, moving towards million qubit scale systems, embedding full error-correction protocols.

Assuming the most optimistic scenario, where roadmaps are largely realised by hardware companies and systems exist that have the same number of effective qubits as are available today but with reliably low effective error rates, allows us to treat quantum computers as essentially error free devices but still limited to only of the order of 100 qubits of processing power. Assuming this is successful, moving from 2034 to 2044 will be about realising a true Moore's law type scaling for quantum and doubling the effective number of qubits available to a quantum computing system – while maintaining low error rates due to the error-correction – every 18 to 24 months. On these timelines, estimates of the ecosystem become much more speculative.

[101] For Google, IBM and Rigetti's superconducting architecture, it is assumed a distance, d~22 surface code, a physical code cycle time of approximately one microsecond. Logical qubits assumes all physical qubits are utilised in surface code patches containing approximately 1000 physical qubits, which is approximately the TeraQuop regime (https://www.riverlane.com/blog/what-is-a-teraquop-decoder). PsiQuantum is a more difficult architecture to contextualise with their 1,000,000 qubit claim by 2028 due to the nature of photonic qubits. Strictly speaking,1,000,000 photons in their architecture which exit Resource State Generators (RSGs) operating at GHz speed, outputting six photons per cycle, would only correspond to 160 microseconds of operation of a single RSG. arXiv.2306.08585 [quant-ph] gives benchmarks for breaking elliptic curve cryptography that can be extrapolated from. Using 6,000 RSGs, operating at 58MHz with ~3km of optical delay line interleaving for 9.7min, a quantum algorithm operating at an equivalent logical clock rate of ~4.2KHz, containing the equivalent of ~6,000 logical qubits can be executed. By simply counting photons, this would be approximately 1.2 x 1015 individual photonic qubits produced by the RSGs. Clearly, this is not what PsiQuantum means when it says 1,000,000 qubits. The numbers in Table 1 are produces when trying to extrapolate and balance the number of effective logical qubits in a PsiQuantum architecture compared to a superconducting architecture.

By 2044, the development of quantum computing will have reached a more mature stage. By this time, many experts expect quantum error rates to have been reduced significantly through effective error-correction and more effective fabrication and manufacturing techniques. Quantum computers with thousands or tens of thousands of qubits may become accessible for research and specialised commercial applications. Quantum algorithm and software development will move onto these platforms and away from pen and paper techniques that are currently used, and it is probable that advances in error-correction will allow for more dense encoded qubits, lowering effective error rates further while maintaining the same number of physical qubits.

The years 2034-2044 will also involve advancements in the hardware front, with the expected emergence of new qubit technologies that are more stable and easier to manipulate. Quantum coherence times will extend, allowing more complex quantum algorithms to run with minimal interference. Further, continuous optimisation of algorithms and error-correction techniques will lead to quantum computers that can effectively outperform classical supercomputers for specific tasks.

2.4 Issues and caveats

Several challenges must be addressed throughout the next two decades to reach these predictions. Error correction will remain a major hurdle, as large-scale quantum computers will require substantial overhead to maintain high fidelity. As such, quantum computers with millions of physical qubits may be necessary to support practical quantum algorithms.

Breakthroughs in quantum error correction and hardware technologies may revolutionise the field. Discovering more efficient error-correcting codes or discovering ways to protect qubits from environmental noise could reduce the required qubit overhead. Moreover, new qubit technologies, such as topological qubits or error-resistant qubits, might emerge, further advancing the scalability of quantum computers.

The scale of quantum computers over the next two decades will heavily depend on research investment and funding. Governments, private corporations and research institutions will play a vital role in driving the progress of quantum computing. Increased funding in research and development will expedite discoveries and innovations in the field.

Additionally, international collaborations and knowledge-sharing among researchers and organisations worldwide will significantly impact the growth of quantum computing. Cooperative efforts can accelerate breakthroughs and encourage the development of more powerful quantum computing systems.

Predicting the exact scale of quantum computers 10 and 20 years from now is challenging due to various factors, including technological limitations and unforeseen breakthroughs. However, based on the current trajectory, quantum computers with hundreds of qubits can be expected to become more accessible in the next 10 years. By the next 20 years, the field is likely to reach a more mature stage, with quantum computers possessing thousands or tens of thousands of qubits capable of tackling complex problems that are either computationally expensive or intractable for classical computers.

The future of quantum computing holds immense potential and promise. Continued research, investments and collaboration will pave the way for transformative advancements in computing, revolutionising industries and pushing the boundaries of what is scientifically possible.

3. Roadmap for the development of quantum algorithms

3.1 Current state

Quantum algorithm development is currently in an unusual place relative to classical algorithm application development, as it is being led almost exclusively through theoretical research. Because classical computers are ubiquitous and inexpensive, it is the norm that application development is driven by experimentation. This is in part because the theoretical understanding of classical computer science is very mature. Decades of discovery and deployment of advances in the mathematical understanding of algorithms and programming languages can be drawn on to engineer solutions.

For example, AI advancements are being driven by deploying learning models on large-scale datasets. One of the most critical aspects of AI development has been that computational power has crossed a threshold, allowing rapid progress by experimentally developing applications. This has significantly broadened access to advanced computing capabilities in many industries and led to the integration of AI into many technologies.

However, while experimental application development is the norm in classical computing now, it is expected that the rising cost of development of classical computers will hamper this progress and ultimately become a bottleneck to progress. It has regularly been argued that 'Moore's Law', which has fuelled continual improvements in classical computing power since the development of the first silicon transistors, is coming to an end.[102] If it is, then the costs of classical hardware improvements will rise, and the gains of the last decade will be harder to replicate. This means that theory, and the development of entirely new computing platforms will play a significant role in the coming years.

Unlike classical computers, theoretical development in quantum computing has been essential because, until the last few years, there has been no hardware capable of running or simulating quantum algorithms at a scale where they might have any advantage. Despite this, with decades of research, quantum algorithms and complexity theory have developed into a mature field by working closely with mathematical models to best determine how quantum computers will perform algorithmic tasks. To date, all the major discoveries in quantum algorithms[103] (see Section 5 for examples) have been made theoretically, leveraging theoretical tools from computer science, mathematics and physics and without the need to access quantum computing hardware.

The last decade has seen the emergence of online NISQ[104] quantum computing platforms and an increased exploration of the cost versus benefits of deploying quantum algorithms. Increasingly, research projects feature SMEs working with quantum computing researchers to explore potential applications aiming to generate valuable intellectual property in advance of deployment of larger and more capable quantum computers.

[102] https://www.cnbc.com/2022/09/27/intel-says-moores-law-is-still-alive-nvidia-says-its-ended.html.

[103] Quantum Algorithms Zoo contains a community driven list of known quantum algorithms developed since the beginning of quantum computing https://quantumalgorithmzoo.org/.

[104] Preskill P (2018) 'Quantum Computing in the NISQ era and beyond', *Quantum*, 2:79.

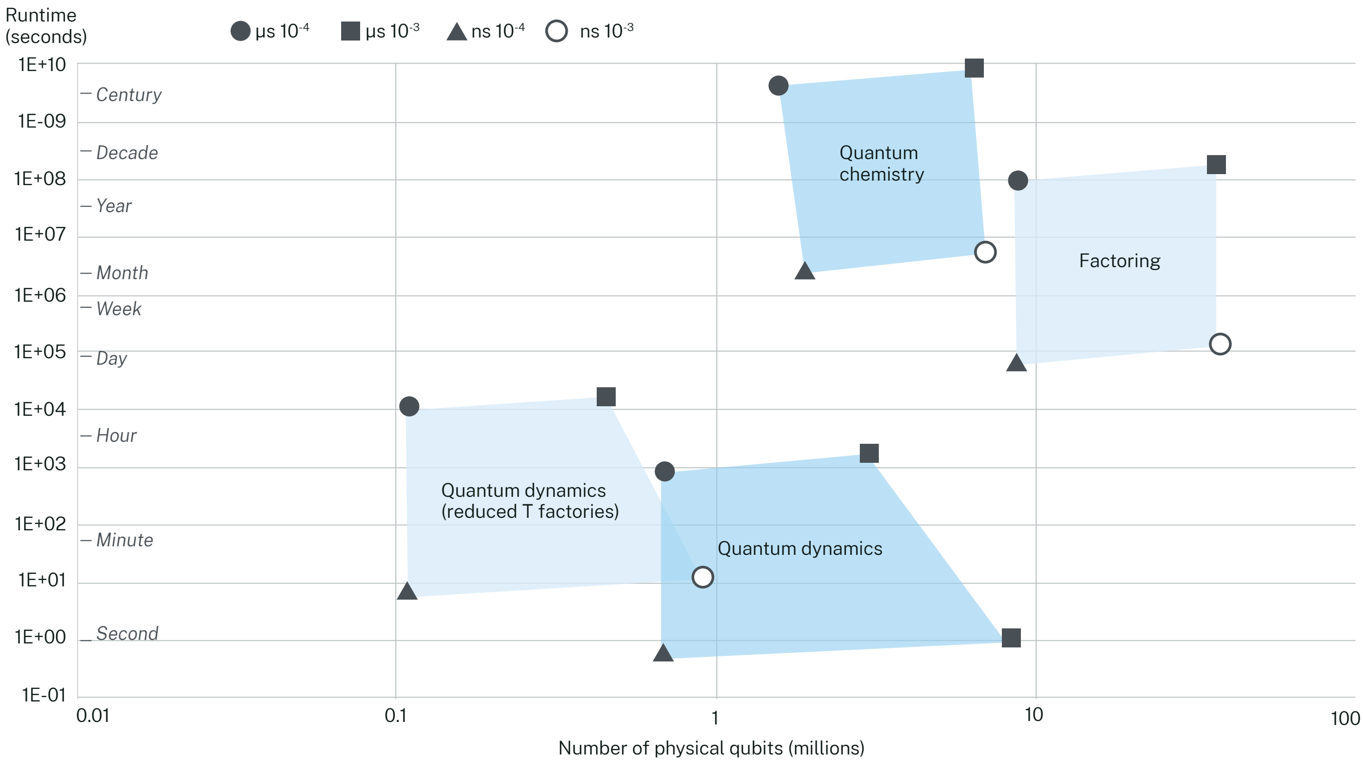


Figure 6. Runtime and qubit counts for early commercially relevant targets in quantum computing. Each coloured region represents approximate resource counts bounded by reasonable estimations of quantum processor speeds and error rates. Here quantum dynamics refers to the simulation of the dynamics of a complex magnetic system and it can be seen that by changing the compilation strategy for this application that the resource cost can change significantly. This is a common characteristic of many quantum applications where significant gains can be made through more sophisticated software compilation. Also included are resource estimates for an electronic structure problem related to carbon fixation and for the factoring problem of a scale relevant for cybersecurity applications. Data sourced from[105].

Much of the work in this space involves exploratory experiments that seek to determine how best to use small-scale NISQ devices. While such studies are increasing the ecosystem of researchers working in quantum computing and giving valuable knowledge around hardware performance, these studies are generally not yet producing applications or algorithms capable of outperforming classical computers for problems with commercial value. Experimental development of quantum algorithms is particularly hampered by the small, and noisy, nature of NISQ processors which make it difficult to encode real-world utility scale problems on these devices. The identification of an industrially useful application that can deliver a genuine quantum advantage on a NISQ device would be a huge breakthrough in light of these problems.

Significant value has been generated by detailed theoretical studies, examining the end-to-end complexities of industrial use cases. This is arguably most advanced for cryptographic applications (e.g. the factoring problem) and in the potential use cases for quantum simulation algorithms in industrial chemistry and materials science. In both of these areas quantum algorithms are believed to give an exponential improvement over the best known classical devices and so represent some of the nearest potential commercial targets for quantum computing (Figure 6).

Despite the hardware advances of recent years, theoretical development of quantum algorithms has been essential for determining the best use cases for quantum computing. Much of the technology required for utility-scale quantum computing is still an active area of research and has yet to reach a development phase. Not only is the physical hardware a significant engineering challenge, but tools that have long been ubiquitous in classical computing, such as programming languages and compilers are immature for quantum computers.

[105] Beverland M E et al. (2022) 'Assessing requirements to scale to practical quantum advantage', arXiv:2211.07629 [quant-ph].

3.2 Ten years out

Over the next ten years, experts expect that there will be an evolution away from theoretically developed pen-and-paper algorithms and an increased move towards the development of applications that are specifically targeted at high-value industry problems. As quantum hardware continues to scale, enabling software will begin to emerge that will aid in discovering and analysing quantum algorithms facilitating the emergence of sophisticated heuristic methods.

Arguably, the most important question for the quantum computing industry right now is what size of quantum processor is required to solve strategically important problems in industry and government? Currently, resource estimation and utility benchmarking for quantum algorithms is a time-consuming process that requires teams of experts in an application domain, quantum algorithms, and quantum error correction. A typical study takes months because the task of optimising computing resources required for a fault-tolerant implementation of a potential application requires a high level of training and subject-specific know-how. Even when a significant quantum advantage is expected, rarely does a study manage to determine the quantum computational cost beyond asymptotic scaling. This is due to the intertwined difficulty of optimising parameter regimes for an application and the costs of quantum error-corrected computation.

Quantum algorithms for simulation

The problem of simulating physical quantum systems is at the heart of quantum computing and it is widely expected that quantum computers will ultimately be better at this task than classical computers. There have been many quantum algorithms introduced for simulating a wide variety of different types of quantum systems including those that are common in chemistry, materials science, and condensed matter physics. While quantum computers are expected to be better at this task it does not necessarily mean that every quantum simulation task is easy for quantum computers, theory suggests that there are quantum simulation tasks that would take exponential time on a quantum computer[106] and so there is considerable effort to understand the best uses of quantum computing for simulation.

Increasingly SMEs from chemistry, materials science, and condensed matter physics are working closely with quantum computing theory teams to identify the best use-cases of quantum simulation algorithms. Generally, such studies have involved theoretically identifying molecules, materials, and the relevant parameter scales where quantum computers are likely to outperform classical computers and then optimising potential applications to determine the minimum quantum cost to outperform classical computers.

In NSW this has been a significant focus of theoretical research. For example, the Google Quantum AI team has worked closely with NSW researchers to develop quantum simulation applications.[107] A recent survey by Google Quantum AI[108] highlighted three studies examining use cases associated with quantum simulations relevant to the pharmaceutical industry, energy storage (a work in collaboration with A/Prof Dominic Berry from Macquarie University), and nuclear power reactor use cases.

Over the next decade, significant improvements to the tools for *compiling* quantum algorithms are expected. This will speed up and democratise the development process, allowing a broader range of scientists to undertake detailed studies of the use of quantum computing at scale. Software tools that assist and analyse the *compilation* of quantum algorithms at both the logical and physical level are under development and will be essential for algorithm optimisation at the scales where quantum computers will have significant utility.

[106] Kempe J et al. (2004), 'The Complexity of the Local Hamiltonian Problem', arXiv:quant–ph/0406180.
[107] https://blog.google/intl/en-au/company-news/technology/dfi-supports-quantum-researchers/
[108] https://blog.research.google/2023/10/developing-industrial-use-cases-for.html

In parallel, research on the theory of quantum algorithms and where quantum advantage will most likely occur will have increasing importance. Such research has the potential to give the essential scientific grounding for the continued development of quantum computing technologies and will form the backbone intellectual property (IP) for future applications.

The fields of quantum chemistry and quantum materials science are areas where quantum computers can have a significant advantage[109] and quantum algorithms for this task are already highly optimised.[110] Consequently, an increasing number of experts from these fields are engaging with quantum computing teams to examine in detail how best to use quantum computers and what opportunities they will unlock. There is already a significant amount of activity in this space, with large technology and manufacturing companies building teams to work on this area. Over the next decade quantum processors and specialized quantum simulation devices will increasingly play a role in scientific discovery in these areas.

Over the next decade, there will also be more study of the quantum security of post-quantum cryptography[111] –new classical cryptographic schemes that are constructed to be resistant to attacks by large-scale quantum computers. Currently, rigorous study of quantum attacks on these new schemes is limited by talent, both domestically and internationally. There are few research teams with sufficient expertise in cryptography and quantum algorithms to be able to robustly study the full potential of quantum attacks on newly developed post-quantum cryptosystems. As quantum hardware efforts expand, so too will the need to test the quantum security of these schemes.

In other areas where a quantum advantage is much more speculative or a long-term prospect, such as for optimisation problems or AI, more fundamental research is required to understand when and how quantum computing will play a role. The development of techniques for fine-grained analysis of the complexity of quantum algorithms that better accounts for real-world use cases will be increasingly important. This will also aid in the development of benchmarks for the community to test heuristic algorithms.

3.3 Twenty years out

Importantly, within the next two decades, it is expected that quantum computers capable of attacking current cryptographic systems will become available. This will have a transformative effect on internet security. While industry stands to benefit from many of the positive outcomes of quantum computing within the next twenty years, these opportunities will be balanced by the threat that they pose. Sovereign actors will likely have an increasing role to play in addressing both the threat and opportunity of quantum for society, industry and global security.

Once quantum computers can function at scale, they will be able to address high-value problems in quantum chemistry and materials science. At this scale, quantum computers will be able to run quantum simulation algorithms that are large enough to not only outperform classical devices but to begin to resolve the key scientific questions that are current high-cost bottlenecks for industry. For example, it will allow wholesale computational experimentation that will open the door to new manufacturing possibilities for energy intensive processes such as fertiliser manufacture.

The exploration of quantum heuristic algorithms will become commonplace, and the ongoing development of an application will be less reliant on guarantees of performance, but rather on experimentally derived advantages. Alongside the emergence of more heuristic techniques will be an increasingly blurred line distinguishing quantum and classical performance, and development cost will become the dominating mechanism for deciding whether to adopt a quantum versus classical solution for specific applications. This would first happen by addressing high-value materials science and chemistry problems that are difficult to simulate using classical computers but may increasingly be adopted to broad-utility algorithms in optimisation and AI.

By the end of the second decade, quantum application development will likely be much closer to classical application development. As quantum computers advance, the emergence of kernels and instruction set architectures will see quantum application development increasingly becoming the domain of software engineers, as opposed to computer science theorists. As is the case now in classical computing, theory will continue to have a role in developing the frontiers of the scientific development of new algorithms, but application development will increasingly be an engineering challenge.

[109] Feynman R P (1982) 'Simulating Physics with Computers', International Journal of Theoretical Physics, 21:467–488.
[110] https://scholar.google.com.au/citations?user=J__Dwl4AAAAJ&hl=en.
[111] https://csrc.nist.gov/projects/post-quantum-cryptography.

4. Quantum algorithms and general-purpose computing

Among the quantum algorithms research community, it is widely believed that the first commercially relevant applications of quantum computing will be in scientific discovery, most likely in chemistry and materials science.

Advances in these fields regularly impact critical areas of the economy such as healthcare and manufacturing. This is because of computationally challenging problems in the simulation of physical systems at the quantum scale and the relative ease with which quantum algorithms can improve on these techniques.

The utility of quantum algorithms for application to wider sectors of the economy is a much more complicated question. There are many critical areas where computational bottlenecks hinder progress, e.g. logistics are regularly challenging because optimisation problems are difficult, or AI may be inaccurate because data training was expensive. Quantum computers do show promise in such areas, but unlike the case for quantum simulation, the advantages offered by quantum algorithms are more subtle which makes the relative cost when compared to classical computing more difficult to gauge. In these areas, the role of performance benchmarking commonly used in classical application development is important.[112]

One of the largest research programs to try and find the appropriate utility for quantum computing systems is the US Defense Advanced Research Projects Agency (DARPA) Quantum Benchmarking project (2022-2025).[113] With over US$30 million in funding across seven project teams, the Quantum benchmarking project is designed to identify, characterise and benchmark the most commercially and scientifically useful quantum algorithms across various domain applications. Project partners include Boeing, General Motors, CACI and others. These companies collaborate directly with researchers looking to solve specific, high-value applications to understand how these problems are currently being addressed, how much value exists in solving a particular problem and what parts of the problem present the bottlenecks.

[112] For example, https://pacechallenge.org/2022/.

[113] https://www.darpa.mil/program/quantum-benchmarking.

5. Rigorous quantum advantage

In 2019, Google performed an experiment that demonstrated *quantum computational supremacy*, the first quantum computation that was beyond the reach of classical computers.[114]

They performed an algorithm dubbed Random Circuit Sampling (RCS)[115] on a 53-qubit superconducting processor that could not be simulated within a reasonable amount of time on the world's best supercomputer. Since then, improvements in supercomputing and classical algorithms have seen the frontier between classical and quantum computing for this problem move, with the requisite size to overcome classical computers now thought to be above at least 70 qubits.[116,117] However, the underlying theoretical argument that such problems are amongst the smallest quantum computations to push beyond classical computing has only gained weight over the years. The assertion that the RCS problem is beyond the reach of classical computers is grounded in two decades of breakthroughs in *quantum complexity theory*.

5.1 Quantum complexity theory

The cost of solving computational problems can vary widely (Figure 7). This key fact allows us to have safe internet security but also explains why it is difficult to optimise logistics. Complexity theory is a field at the intersection of mathematics and computer science that studies the resources or costs that are required for solving computational problems. It informs algorithms experts on where and how computational bottlenecks appear and the potential for avoiding them.

One of the biggest challenges in complexity theory, if not all of mathematics and computer science, is establishing definitive separations between the difficulty of computational problems. The famous 'P vs NP' problem dates to the 1950s and is a Millennium Prize Problem[118] that is at the core of understanding what problems can be solved with computers that remain unsolved alongside many variations of similar conjectures. For this reason, much of complexity theory and our understanding of computer science is relative to our belief in the cost of solving specific problems. For example, there are no known easy algorithms for finding the prime factors of large integers. This underlies the RSA cryptosystem that is widely used for internet security.

The capabilities of quantum computers relative to classical computers have been debated since the 1990s and are the central topic of quantum complexity theory. Given the challenges of complexity theory, there may never be a definitive mathematical proof that quantum computers are radically more powerful. Instead, computer scientists have worked to understand how quantum computing is distinct from classical computing and the consequences for classical computing if it is not. Such research provides evidence against the notion that humanity hasn't been 'smart' enough to develop classical algorithms that could replace quantum computers.

[114] Arute F et al. (2019) 'Quantum supremacy using a programmable superconducting processor', *Nature*, 574:505–510.

[115] Boixo S et al. (2018) 'Characterizing quantum supremacy in near-term devices', *Nature*, 14:595-600

[116] The quantum supremacy boundary in random circuit sampling has never been a clear line, but rather a region of clearly 'no', clearly 'yes' and 'depends on how good we can make the classical emulation algorithm'. While improvements in classical techniques may push this boundary by perhaps another 10 or 20 qubits, it is commonly assumed that if random circuit sampling could be performed over a 90 qubit chipset, no classical computer, present or future could ever emulate this experiment.

[117] Morvan A et al. (2023) 'Phase transition in Random Circuit Sampling', arXiv:2304.11119 [quant-ph].

[118] https://www.claymath.org/millennium/p-vs-np/

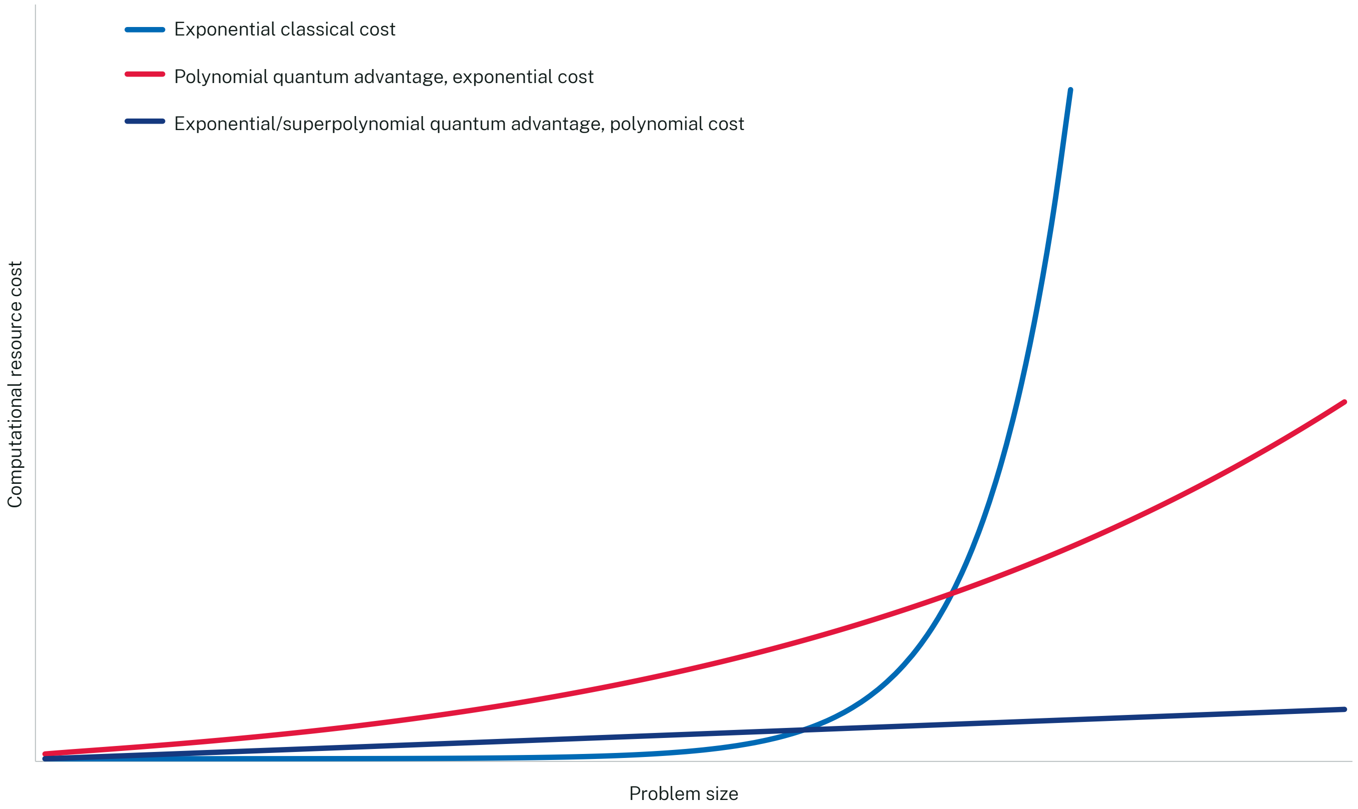


Figure 7. Classical and quantum resource costs relative to problem size. Note that the quantum advantage only appears at larger sizes due to the additional overheads of fault tolerance. Predicting exactly when the quantum cost becomes cheaper than the classical cost is a significant challenge and involves comparisons of the best performing algorithms relative to the predicted performance of hardware for specific problems.

Quantum complexity theory provides an insight into where quantum advantage may exist, and where it is unlikely to occur. Since the early days of quantum computing, it has been clear that any significant quantum advantage is not simply a matter of providing a speedup to or parallelising of arbitrary computations but is considerably more subtle and depends on the characteristics of the problem to be solved.[119] For this reason, many of the computational bottlenecks for classical computers remain computational bottlenecks for quantum computers. Understanding when and how these bottlenecks can be circumvented is one of the key skills in developing new quantum algorithms and one of the reasons why progress on quantum computing use-cases typically requires highly trained scientists.

As of 2024, it is generally well accepted amongst computer scientists that quantum computing is a distinct model of computation separate to ‘classical’ computing. Arguably, Shor’s quantum factoring algorithm[120] remains the best evidence of a separation between quantum and classical computing. Not only because it is one of the most studied problems in mathematics,[121] but also because there is a large separation in the quantum versus classical cost of solving this problem. It is an example of an *exponential* (or superpolynomial) separation in cost, which means that the cost of classical computation rapidly becomes much more expensive than the quantum algorithm. This makes it an attractive target for benchmarking the progress of quantum computing, essentially providing targets for improvements to algorithms, compilation, error-correction and hardware.

Shor’s algorithm is not the only evidence for quantum advantage. Quantum simulation algorithms, especially those for simulating the dynamics or evolution of a system in time, of quantum systems (such as those that appear in materials science or chemistry), appear to have a significant, exponential advantage over classical computers and are seen as the obvious category of problems that will yield commercially relevant benefits. Arguments for this are not simply phenomenological but have been made rigorous via the same methodology that support Google’s claims of quantum computational supremacy for RCS.[122]

[119] Bennett C H et al. (1997) ‘Strengths and Weakness of Quantum Computing’, *SIAM Journal on Computing*, 26:1510-1523.

[120] Shor P W (1994) ‘Algorithms for quantum computation: discrete logarithms and factoring’ *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 124-134.

[121] Given that almost the entirety of the classical financial system is underpinned by electronic transitions that are protected using variants of the RSA-algorithm, there is a tremendous financial incentive to find a classical solution to the factoring problem.

[122] B.oixo S et al. (2018) ‘Characterizing quantum supremacy in near-term devices’, *Nature*, 14:595-600.

The RCS problem is an extreme version of a typical quantum simulation problem that is especially difficult for classical algorithms at smaller sizes and leverages our understanding of the difficulty of simulating condensed matter and quantum optical systems. For this reason, quantum simulation applications will be the first to demonstrate the utility of quantum computers.

While quantum simulation is an attractive target, not every problem that chemists or material scientists would like to solve becomes easy with quantum computing. Many problems, such as understanding the stability of molecules or identifying high temperature superconductors, may not have the same scale of advantage as the quantum dynamics problem. One of the biggest areas of research in theoretical quantum computing right now is determining how best to utilise the advantages given by quantum simulation methods to resolve problems of commercial and scientific interest in this space.

More broadly, there is very strong evidence that quantum computers can outperform classical computers for many problems, albeit on longer timescales. Quantum computers have provable benefits over classical computers for algorithms with broad utility, especially in optimisation, equation solving and heuristics. The caveat to this is that the amount of advantage is more subtle than for problems such as code breaking or quantum simulation and is often only a polynomial improvement over classical algorithms. In many cases this means that the scale of the problem where quantum computers, given their considerable upfront cost, are much larger than near-term quantum processors are likely to manage, and hence are not viable in the near term. This is discussed at length in the section below.

5.2 Optimisation algorithms

Optimisation is a key subroutine or component of a vast number of computing applications. It is at the core of many high value problems in seemingly disparate areas from logistics, finance, AI, or even biochemistry. Optimisation algorithms are both very common, and regularly computationally expensive, on any given day occupying a vast quantity of the world's computing resources. Frequently, optimisation problems are NP-hard and algorithms for solving them have exponential scaling on classical computers. This also means that *in general, quantum computers cannot be expected to easily solve them*. However, real-world scenarios often have specific details, or structure, that might make a problem that seems intractable in the absence of structure, tractable. The search for structures and techniques to aid in the solution of optimisation problems is a constant activity across the computational sciences, and modest improvements can have significant impact.

Given the ubiquity and high value of optimisation problems there has been significant research on quantum algorithms for optimisation since the 1990s. One of the most important early discoveries in quantum computing was that quantum computers can have a *polynomial* advantage over classical computers for *unstructured search problems*.[123] This problem is of critical importance because it can be adapted to many optimisation problems, and it has opened the door to wide-reaching quantum-based improvements. Importantly, while quantum computers are more efficient at this task than classical computers, it is still considered a difficult problem for quantum computers and so, after accounting for quantum error correction, quantum advantage for general optimisation problems is not likely in the near-term.

While the quantum advantage that comes from unstructured search is comparatively well known, there are many quantum improvements to critical optimisation algorithms that are distinct, and arguably as important for real-world optimisation problems. Key examples include the quantum algorithms for *branch and bound*,[124] *divide and conquer*,[125] and *Monte Carlo*[126] methods. In each of these cases the quantum algorithm goes beyond the techniques used in the quantum search algorithm to yield a resource saving. However, like search, the broadly applicable advantage that emerges is polynomial unless there is further structure to the problem at hand.

[123] Grover L K (1996) 'A fast quantum mechanical algorithm for database search', *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, 212-219

[124] Montanaro A (2020) 'Quantum speedup of branch-and-bound algorithms', *Physical Review Research*, 2:013056.

[125] Childs A M et al. (2022) 'Quantum divide and conquer', arXiv:2210.06419 [quant-ph].

[126] Montanaro A (2015) 'Quantum speedup of Monte Carlo methods', *Proceedings of the Royal Society A*, 471:2181.

Table 2. Proven performance quantum combinatorial optimisation algorithms. Timeframe to utility is based on the current understanding of resource estimates for related problems. This table does not reflect heuristic approximation methods that, by their nature do not have rigorous performance bounds.

Algorithm	Rigorous performance improvement	Current expected time to utility	Application areas
Search	Polynomial[127,128]	20+ years	Machine learning, logistics, finance
Graph properties	Polynomial[129,130] to superpolynomial[131,132,133]	20+ years	Logistics, networking, AI
Backtracking	Polynomial[134]	20+ years	Heuristics, logistics
Branch and bound	Polynomial[135]	20+ years	Portfolio optimisation
Divide and conquer	Polynomial[136]	20+ years	Broad application
Markov chain Monte Carlo	Polynomial[137]	20+ years	Broad application

Constraint satisfaction and combinatorial optimisation

Constraint satisfaction problems are typical examples of NP-complete problems. Many combinatorial optimisation problems can be transformed via simple algorithms to constraint satisfaction problems, and so efficiency gains in constraint satisfaction can often carry over to many other problems. Grover's quantum search algorithm gives a quadratic improvement over classical search algorithms for solving constraint satisfaction, however in many cases more tailored algorithms can outperform general search. Ambainis' amplitude amplification gives a general quadratic improvement for the classic NP-complete satisfiability problem[138] and there are many other examples of more-tailored quantum algorithms that can be used for constraint satisfaction problems such as the quantum backtracking algorithm.[131]

While these algorithms give asymptotic improvements in general, whether these can be achieved in real-world scenarios depends heavily on the details of the real-world problem and the performance of the quantum processor.[139] Studies[134] have shown that quantum computers can offer multiple orders of magnitude improvements for commonly used constraint satisfaction problems such as k-colouring utilising the quantum backtracking algorithm. However, these improvements depend on the error-correction methods that are deployed. Quantum algorithms for approximate constraint satisfaction, such as those for quantum semi-definite programs[140] also offer polynomial advantage. Significant work is being conducted to determine the utility of heuristics such as the Quantum Approximate Optimisation Algorithm[141] and recent studies have identified potential benchmarks and challenges for this approach.[142]

[127] https://www.darpa.mil/program/quantum-benchmarking.
[128] Ambainis A (2005) 'Quantum search algorithms', arXiv:quant-ph/0504012
[129] Ambainis A et al. (2011) 'Quantum property testing for bounded-degree graphs' In Proceedings of RANDOM '11: *Lecture Notes in Computer Science* 6845:365-376.
[130] Durr C et al. (2006) 'Quantum Query Complexity of Some Graph Problems', *SIAM Journal on Computing*, 35(6):1310–1328. Earlier version in ICALP'04. arXiv:quant-ph/0401091
[131] Ben-David S et al. (2020) 'Symmetries, Graph Properties, and Quantum Speedups', *IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, Durham, NC, USA, 649-660.
[132] Montanaro A and Shao C (2020) 'Quantum algorithms for learning a hidden graph and beyond', arXiv:2011.08611 [quant-ph].
[133] Lee T et al. (2021) 'Quantum algorithms for graph problems with cut queries', *Proceedings of the Thirty-Second Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), Society for Industrial and Applied Mathematics*, Virtual Conference, 939-958.
[134] Montanaro A (2018) 'Quantum walk speedup of backtracking algorithms', *Theory of Computing*, 14(15):1-24.
[135] Montanaro A (2020) 'Quantum speedup of branch-and-bound algorithms', *Physical Review Research*, 2:013056.
[136] Childs A M et al. (2022) 'Quantum divide and conquer', arXiv:2210.06419 [quant-ph]
[137] Montanaro A (2015) 'Quantum speedup of Monte Carlo methods', *Proceedings of the Royal Society A*, 471:2181.
[138] Ambainis A (2005) 'Quantum search algorithms', arXiv:quant-ph/0504012
[139] Campbell E et al. (2019) 'Applying quantum algorithms to constraint satisfaction problems', *Quantum*, 3:167
[140] Brandão FGSL et al. (2020) 'Faster quantum and classical SDP approximations for quadratic binary optimization', *Quantum*, 6:62
[141] Farhi E et al. (2014) 'A Quantum Approximate Optimisation Algorithm', arXiv:1411.4028 [quant-ph].
[142] Abbas A et al. (2023) 'Quantum Optimization: Potential, Challenges, and the Path Forward', arXiv: 2312.02279 [quant-ph].

Such broad utility quantum algorithms have the potential to deliver significant economic and societal benefit if the cost of production of quantum computers can be reduced. Preliminary studies from Google, in collaboration with researchers at the UTS and Macquarie University, and other studies[143,144,145] indicate that the overhead required for dealing with quantum errors make it unlikely that quantum computers can outperform classical computers for such tasks in the near term. However, the software tools for performing optimisation of quantum algorithms on this scale are still under development, so reliable mid-to-long term estimates for quantum advantage in such cases are unknown.

While broadly applicable, and definitive, quantum advantage in optimisation is likely some way off, there is speculation that quantum computers might turn out to be useful for optimisation in the near term. Firstly, there are several approaches for polynomial improvements for combinatorial optimisation problems via adiabatic techniques[146] or adaptations to the Quantum Approximate Optimisation Algorithm.[147,148,149] However, in these cases, there is still much analysis to be performed.

Table 3. Proven performance quantum continuous optimisation algorithms. Timeframe to utility is based on the current understanding of resource estimates for related problems. This table does not reflect heuristic approximation methods that, by their nature do not have rigorous performance bounds.

Algorithm	Rigorous performance improvement	Current expected time to utility	Application areas
Zero-sum games	Polynomial[150]	20+ years	Finance, automated decision making
Interior point	Polynomial[151,152]	20+ years	Finance, logistics
Multiplicative weights update	Polynomial[153,154,155]	20+ years	Finance, logistics, machine learning, automated decision making
Convex optimisation	Polynomial[156,157]	20+ years	Broad application

[143] Sanders Y R et al. (2020) 'Compilation of Fault-Tolerant Quantum Heuristics for Combinatorial Optimization', *PRX Quantum*, 1:020312.

[144] Babbush R et al. (2021) 'Focus beyond Quadratic Speedups for Error-Corrected Quantum Advantage', *PRX Quantum*, 2:010103.

[145] Campbell E et al. (2019) 'Applying quantum algorithms to constraint satisfaction problems', *Quantum*, 3:167.

[146] Hastings M B (2018) 'A Short Path Quantum Algorithm for exact optimization', *Quantum*, 2:78.

[147] Farhi E et al. (2014) 'A Quantum Approximate Optimisation Algorithm', arXiv:1411.4028 [quant-ph].

[148] Boulebnane S and Montanaro A (2022) 'Solving Boolean satisfiability problems with the quantum approximate optimization algorithm', arXiv:2208.06909 [quant-ph].

[149] Shaydulin R et al. (2023) 'Evidence of Scaling Advantage for the Quantum Approximate Optimization Algorithm on a Classically Interactable Problem', arXiv:2308.02342 [quant-ph].

[150] Apeldoorn J van and Gilyen A (2019) 'Quantum algorithms for zero-sum games', arXiv:1904.03180 [quant-ph].

[151] Kerenidis I and Prakash A (2020) 'A Quantum Interior Point Method for LPs and SDPs', *ACM Transactions on Quantum Computing*, 1(1):1-32.

[152] Kerenidis I et al. (2021) 'Quantum algorithms for Second-Order Cone Programming and Support Vector Machines', *Quantum*, 5:427.

[153] Brandao F G S L and Svore K M (2017) 'Quantum Speed-Ups for Solving Semidefinite Programs', *IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, Berkeley CA USA, 415-426. Earlier version arXiv:1609.05537 [quant-ph].

[154] Brandao F G S L et al. (2019) 'Quantum SDP Solvers: Large Speed-Ups, Optimality, and Applications to Quantum Learning', *46th International Colloquium on Automata, Languages, and Programming (ICALP)*, Patras, Greece, 27:1-27:14. Full version arXiv:1710.02581 [quant-ph].

[155] Apeldoorn J van et al (2020) 'Quantum SDP-Solvers: Better upper and lower bounds', *Quantum*, 4:230. *Earlier version in 58th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, Berkeley, CA, USA. arXiv:1705.01843 [quant-ph].

[156] Chakrabarti S et al. (2020) 'Quantum algorithms and lower bounds for convex optimization', *Quantum*, 4:221. Earlier version arXiv:1809.01731 [quant-ph].

[157] Apeldoorn J van et al. (2020) 'Convex optimization using quantum oracles', *Quantum*, 4:220.

In another direction, there is a possibility that quantum heuristic algorithms may provide better or faster solutions than classical heuristics.[158] Given the level of noise in current hardware and the capabilities of classical heuristic methods there has been limited success in identifying new heuristic techniques that provide clear utility. However, improvements in hardware, and better characterisation of parameters that may lead to quantum advantage in these scenarios, may lead to new discoveries in the near future.

Finally, while not strictly optimisation problems, there is evidence of superpolynomial speed-ups for the problem of learning the mathematical properties of graphs[159,160,161] and for variations of the search problem.[162] In both of these cases the problems are related to difficult optimisation problems, and researchers have studied the interplay between structured and unstructured optimisation problems to show a superpolynomial advantage. While it is not known how such arguments can be extended to practical advantage, they represent an interesting line of study for future algorithm development.[163]

Quantum interior point methods for finance

Recent work[164] has estimated the quantum resources required to perform portfolio optimisation, a computationally intensive task often encountered in finance, via the quantum interior point method algorithm. Portfolio optimisation is concerned with determining the optimal allocation of funds across a portfolio to maximise returns. Portfolio optimisations can be cast as Second-Order Cone Programs, and the leading method for solving such programs for portfolio optimisation is the classical interior point method. The quantum interior point method algorithm provides an asymptotic polynomial advantage over the classical algorithm. However, the quantum interior point method algorithm requires access to a Quantum Random Access Memory (QRAM) which can be very costly physically. In recent work from from AWS, Goldman Sachs, Caltech and Rheinisch-Westfälische Technische Hochschule Aachen (RWTH Aachen)[160], the authors perform an end-to-end resource estimate, with realistic portfolio parameters with portfolios of up to 120 companies. This size portfolio optimisation is classically tractable within seconds on a laptop. They find that due to the requirements of QRAM together with quantum error correction that this calculation could take millions of years using the quantum interior point method algorithm and realistic quantum processor speeds. However, the authors stress that there could be significant improvements made with further optimisation.

[158] Farhi E et al. (2014) 'A Quantum Approximate Optimisation Algorithm', arXiv:1411.4028 [quant-ph].
[159] Ben-David S et al. (2020) 'Symmetries, Graph Properties, and Quantum Speedups', *IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, Durham, NC, USA, 649-660.
[160] Montanaro A and Shao C (2020) 'Quantum algorithms for learning a hidden graph and beyond', arXiv:2011.08611 [quant-ph].
[161] Lee T et al. (2021) 'Quantum algorithms for graph problems with cut queries', *Proceedings of the Thirty-Second Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Society for Industrial and Applied Mathematics, Virtual Conference, 939-958.
[162] Yamakawa T and Zhandry M (2022) 'Verifiable Quantum Advantage without Structure', *IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, Denver CO USA, 69-74.
[163] Aaronson S (2022) 'How much structure is needed for huge quantum speedups?', arXiv:2209.06930 [quant-ph].
[164] Dalzell A M et al. (2023) 'End-To-End Resource Analysis for Quantum Interior-Point Methods and Portfolio Optimization', *PRX Quantum*, 4(4):040325.

5.3 Equation-solving algorithms

In 2008, Harrow, Hassidim and Lloyd discovered a quantum algorithm with exponential advantage for solving linear systems of equations[165]. Typically, linear equation solving is characterised as an efficient problem for classical computers and forms the backbone of many other tasks.[166] It is an extremely common operation in many tasks such as machine learning, regression analysis and cryptography. However, the cost of linear systems of equations is proportional to the size of the linear system to be solved. Taking machine learning as an example, leveraging linear equation solvers on large data sets becomes more computationally expensive as the data sets get bigger.

Table 4. Key quantum equation-solving algorithms.

Category	Algorithm	Rigorous performance improvement	Currentexpected time to utility	Application areas
Equation solving	Linear equations	Superpolynomial[164]	10-20+ years	Broad application
Differential equations	Finite element method	Superpolynomial[167]	10-20+ years	Chemistry, materials science, energy, aerospace, advance manufacturing
Differential equations	Spectral methods	Superpolynomial[168]	10-20+ years	Chemistry, materials science, energy, aerospace, advance manufacturing
Differential equations	Coupled oscillators	Superpolynomial[169]	10-20+ years	Manufacturing, energy sector

The quantum linear equation algorithm provides a partial solution to this problem, with an exponential saving in the scale of the (linear) system. While this is a considerable advantage there is a drawback. The data must be input into a form that is appropriate for the quantum processor to access in superposition – a difficult prospect in the near term. It is also the case that the solution is encoded directly into a quantum state and cannot be directly read out. Instead, properties of the solution must be inferred. While this may not yield the equation solutions directly as is done in many classical algorithms, it does allow for a rapid characterisation of potential solutions, which is a very common task.

Quantum algorithms for equation solving is a relatively underdeveloped area in comparison to optimisation problems. Initial studies focused on extending the quantum linear equations solver to differential equations, building on classical techniques such as the frequently used finite difference method. Such techniques have seen quantum improvements to a range of algorithms for systems of linear ordinary and partial differential equations.

The research community is now focused on developing quantum algorithms for nonlinear equations, and examining how performance can be varied under different input parameter regimes, and application to commonly studied equation types e.g. recent work demonstrating an exponential advantage for systems of coupled oscillators.[170]

Given the ubiquity of linear systems in computing, and the fact they offer an exponential advantage, there is an increasing effort to understand when quantum equation-solving algorithms will have utility over classical algorithms. In some cases, it is anticipated that this might be possible in the not-too-distant future. Particularly challenging systems of equations, such as the Vlasov-Maxwell equation,[171] which have applications in particle physics are likely to outperform classical computers with relatively small problem size. Whereas quantum algorithms for nonlinear differential equations might provide a new path to solving problems that have been computational bottlenecks in areas such as fluid dynamics for decades, such as the Navier-Stokes equation,[172] given further research.

[165] Harrow A W et al. (2009) 'Quantum algorithm for linear systems of equations', *Physical review letters*, 103(15):150502.
[166] https://en.wikipedia.org/wiki/System_of_linear_equations.
[167] Montanaro A and Pallister S (2016) 'Quantum algorithms and the finite element method', *Physical Review A*, 93:032324.
[168] Childs A M and Liu J- P et al. (2020) 'Quantum Spectral Methods for Differential Equations', *Communications in Mathematical Physics*, 375:1427-1457. Earlier version arXiv:1901.00961 [quant-ph].
[169] Babbush R et al. (2023) 'Exponential quantum speedup in simulating coupled classical oscillators', *Physical Review X*, 13:041041.
[170] Babbush R et al. (2021) 'Focus beyond Quadratic Speedups for Error-Corrected Quantum Advantage', *PRX Quantum*, 2:010103.
[171] Engel A et al. (2019) 'Quantum algorithm for the Vlasov equation', *Physical Review A*, 100:062315.
[172] Liu J- P et al. (2021) 'Efficient quantum algorithm for dissipative nonlinear differential equations', *The Proceedings of the National Academy of Sciences*, 118(15):e2026805118.

5.4 Machine learning and AI

The use of classical machine learning and AI algorithms has exploded over the last decade, and they can be found practically everywhere. Driven by a decrease in the cost of high-performance computing, heuristic methods for development in these areas have become commonplace and have enabled solutions for difficult problems that would have typically required much more subject matter expertise to achieve. Naturally, many researchers, and much of the investment community, have asked how quantum computers can play a role in machine learning. Unlike other well-studied areas in quantum algorithms, such as cryptography, quantum simulation, optimisation and even equation solving, there is limited understanding as to how best to use quantum computers for AI and machine learning. One reason for this is that much of the research in AI and machine learning is driven by experimentation, whereas quantum computers have not developed to the point where experimentation on such algorithms yields any discernible advantage.

That quantum computers might be useful in machine learning is not simply driven by hype. The well-understood quantum advantages in optimisation and equation solving initially motivated research into quantum machine learning, with algorithms for these tasks at the core of many bottlenecks in machine learning applications.[173,174]
Many studies have shown that for particular types of data, with specialised mathematical properties, there exists a quantum advantage for learning problems. However, how best to use such subroutines to deliver a significant quantum advantage for more general, practical, machine learning problems remains an ongoing challenge. One of the biggest roadblocks is the difficulty of processing large data sets with quantum computers. Loading data in and out of quantum processors is currently a very expensive task and in many cases the cost of this erases any significant quantum advantage for quantum machine learning tasks.[175,176,177]

[173] Biamonte J et al. (2017) ‘Quantum machine learning’, *Nature*, 549:195-202.

[174] Cerezo M et al. (2022) ‘Challenges and opportunities in quantum machine learning’, *Nature Computational Science*, 2:567-576.

[175] Tang E (2019) ‘A quantum-inspired classical algorithm for recommendation systems’, *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, Phoenix AZ USA, 217-228. Earlier version arXiv:1807.04271 [cs.IR].

[176] Tang E (2021) ‘Quantum principal component analysis only achieves an exponential speedup because of its state preparation assumptions’, *Physical Review Letters*, 127:060503.

[177] Chia N- H et al. (2020) ‘Sampling-based sublinear low-rank matrix arithmetic framework for dequantizing Quantum machine learning’, *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, Chicago IL USA, 387-400. Earlier version arXiv:1910.06151 [cs.DS].

6. Transitioning to quantum – challenges for government and society

Quantum technology is likely to be a defining technology of the 21st century.

The first generation of quantum technology – the transistor, the laser and nuclear magnetic resonance – developed in the early to mid-20th century led to the digital revolution of the late 20th and early 21st century. The second generation of quantum technologies, built off the back of major scientific advances of the last 30 years, will likely lead to a similar technological leap forward as society moves towards the 22nd century.

Nations possessing the know-how to first identify and exploit the benefits of quantum technologies will be the first to reap the windfall of quantum. This has seen many countries accelerate spending and develop strategic plans for the adoption of quantum technologies beyond the usual research and development cycle.[178] [179] Increasingly, quantum technologies are categorised as a *critical technology* both from the perspective of national defence and ongoing economic security. In Australia, the Commonwealth has responded with the *National Quantum Strategy*,[180] and categorised quantum technologies as critical[181] and one of several technologies making up 'pillar two' of the AUKUS agreement, a trilateral security partnership for the Indo-Pacific region between Australia, the United Kingdom (UK) and the United States (US).[182]

6.1 Opportunities

The Australian National Quantum Strategy, like many others around the world,[183,184,185,186,187] identifies quantum sensing, quantum communications and quantum computing as the key application areas for new quantum technologies. Of these, quantum computing is predicted to have the largest economic impact both here in Australia and internationally over the next several decades. CSIRO conservatively predicts that quantum computing will create over 10,000 jobs in Australia by 2040 with revenues around A$2.8 billion.[188] This is based on the assumption that Australia captures 4% of the international market. The economic impact unlocked as a result of quantum computing applications is predicted to be significantly larger than the revenues of quantum computing. McKinsey predicted in 2021 that quantum computing use cases could generate between $300-800 billion worth of impact internationally across a variety of sectors, with the market for quantum computing use-case development alone worth approximately $80 billion.[189] Promising applications for quantum computing have been identified in many sectors: cybersecurity, chemical manufacturing, material science, optimisation problems (which can include for example transport logistics and financial modelling) and classical dynamics (such as computational fluid dynamics for aeronautics or climate modelling).

[178] https://qureca.com/overview-on-quantum-initiatives-worldwide-update-2022/.
[179] https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf.
[180] https://www.industry.gov.au/publications/national-quantum-strategy.
[181] https://www.industry.gov.au/publications/list-critical-technologies-national-interest/quantum-technologies.
[182] https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/.
[183] https://qt.eu/.
[184] https://www.quantum.gov/.
[185] https://sj.jst.go.jp/news/202205/n0523-03k.html.
[186] https://instituteq.fi/finnish-quantum-agenda/.
[187] https://uknqt.ukri.org/.
[188] https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/csiro-futures/future-industries/quantum.
[189] "Quantum computing use cases—what you need to know | McKinsey." 14 Dec. 2021, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know.

Determining the specific scientific or commercial utility for these applications is currently a hotly debated topic internationally. The largest government-funded program involved in benchmarking these applications is the Quantum Benchmarking program administered by the DARPA 2022-2025.[190] Australian participants include the University of Technology Sydney (UTS) and the University of Sydney.[191]

Preliminary analysis of applications for quantum computing in this program and other studies suggest that commercial utility may require quantum computers at least as large as those required to compromise public key cryptosystems (machines on the order of 1-20 million qubits).[192] Many applications will require machines that are even larger.[193] The best quantum computers currently have approximately 100 qubits in a complete and deployed system.[194] *Those who can find new algorithmic and software techniques that can bring down these numbers will be well positioned to reap the windfalls of these technological changes*. This means that Quantum Algorithms, Software and the Theoretical (QAST) research is critical for gaining competitive advantage and delivering the economic benefits of quantum computing.

The government will have a key role to play in ensuring that Australian industry benefits from the adoption of quantum computing technologies. In May 2023, the Australian National Quantum Strategy was announced,[195] centred on five themes which capture the key elements to be balanced as industry moves forward:

1. creating thriving research and development, investment in and use of quantum technologies
2. securing access to essential quantum infrastructure and materials
3. building a skilled and growing quantum workforce
4. ensuring our standards and frameworks support national interests
5. building a trusted, ethical and inclusive quantum ecosystem.

[190] https://www.darpa.mil/program/quantum-benchmarking.
[191] https://www.innovationaus.com/uts-usyd-join-us-quantum-yardstick-project/.
[192] Gidney C and Ekera M (2021) 'How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits', *Quantum*, 5:433.
[193] Dalzell A M et al. (2023) 'Quantum algorithms: A survey of applications and end-to-end complexities', arXiv:2310.03011 [quant-ph].
[194] https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor.
[195] https://www.industry.gov.au/publications/national-quantum-strategy.

6.2 The Australian context – government support for quantum computing

Ⓐ Have Australians designed the architectures and blueprints that are actively being built?	🟢 Yes
Ⓑ Do we have local talent to be highly competitive if resources are available?	🟡 Developing
Ⓒ Are we competitive in this space now?	🔴 No

TRAPPED IONS	SUPER CONDUCTING	PHOTONICS	NV DIAMOND/ COLOUR CENTRES	DONORS	SPIN/ QUANTUM DOTS
🟢 A Australians have designed a major architecture used by startups or corporates	🟢 A Australians have designed a major architecture used by startups or corporates	🟢 A Australians have designed a major architecture used by startups or corporates. Australia essentially invented the platform	🟢 A Australians have designed a major architecture used by startups or corporates	🟢 A Australians have designed a major architecture used by startups or corporates. Australia essentially invented the platform	🟢 A Australians have designed a major architecture used by startups or corporates
🔴 B Expertise within australia	🟡 B Expertise within australia	🟢 B World class expertise within australia	🟢 B World class expertise within australia	🟢 B World class expertise within australia	🟢 B World class expertise within australia
🔴 C Not competitive in the quantum computing space using this hardware	🔴 C Not competitive in the quantum quantum computing space using this hardware	🔴 C Not competitive in the quantum computing space using this hardware	🟡 C Potentially competitive in the quantum computing space using this hardware	🟢 C Highly competitive in the quantum computing space using this hardware	🟡 C Potentially competitive in the quantum computing space using this hardware

Figure 8. Of the eight major systems currently in development globally for quantum computing, Australia has made major contributions to at least six. Shown is a brief summary of Australian achievements for these systems and indicated in green, yellow and red are our contributions and domestic capacity to capitalise on our historical contributions to these platforms.

While quantum information science as an academic field can trace its origins to theoretical research in late 1960s and early 1970s,[196,197] it wasn't until the turn of the millennium that it was widely recognised that quantum computing, communications and sensing technology could be transformative.

In 1999, the Australian government began investing in the R&D of this technology and set up the Special Research Centre (SRC) for Quantum Computing Technology. This centre was one of the first nationally funded centres globally, set up specifically to accelerate the development of quantum technology. The work that emerged from the SRC and its successor, the Australian Research Council (ARC) Centre of Excellence (CoE) for Quantum Computing Technology (CQCT) in the 2000s was critical in shaping the field.[198,199,200,201]

In the early 2000s, the number of companies and startups in the quantum space was minimal,[202,203,204,205] and sovereign investment dedicated to quantum computing, communications and sensing were limited to Australia, Canada, the US, the UK, Singapore and Japan. The Australian centre was one of only three nationally funded research centres dedicated to quantum computing, along with the Centre for Quantum Technologies (CQT) in Singapore[206] and the Institute for Quantum Computing (IQC) in Canada.[207]

In terms of sovereign-level investment, from the 2000s to the early 2010s, Australia ranked sixth in the OECD and consequently, had a huge impact on the field. Australian researchers invented the fields of optical quantum computing[208,209] and Silicon-based quantum computing systems,[210,211,212] as well as pioneering foundational theory in almost all aspects

[196] Holevo A S (1973) 'Bounds for the quantity of information transmitted by a quantum communication channel', *Problems of Information Transmission*, 9:177–183.
[197] Wiesner S (1983) 'Conjugate coding', *ACM Sigact News, 15*(1):78-88P1
[198] Knill E et al. (2001) 'A scheme for efficient quantum computation with linear optics', *Nature*, 409:46-52
[199] O'Brien J L et al. (2003) 'Demonstration of an all-optical quantum controlled-NOT gate', *Nature*, 426:264-267.
[200] Lanyon B P et al. (2007) 'Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement', *Physical Review Letters*, 99:250505.
[201] Morello A et al. (2010) 'Single-shot readout of an electron spin in silicon', *Nature*, 467:687-691.
[202] https://www.dwavesys.com/
[203] https://www.nec.com/en/global/quantum-computing/index.html.
[204] https://www.fastcompany.com/90633843/1981-quantum-computing-conference-ibm-roadmap-mit.
[205] https://www.hpl.hp.com/research/about/quantum_processing.html
[206] https://en.wikipedia.org/wiki/Centre_for_Quantum_Technologies.
[207] https://en.wikipedia.org/wiki/Institute_for_Quantum_Computing.
[208] Knill E et al. (2001) 'A scheme for efficient quantum computation with linear optics', *Nature*, 409:46-52
[209] O'Brien J L et al. (2003) 'Demonstration of an all-optical quantum controlled-NOT gate', *Nature*, 426:264-267.
[210] Kane B E (1998) 'A silicon-based nuclear spin quantum computer', *Nature*, 393:133-137.
[211] Simmons M Y et al. (2003) 'Towards the atomic-scale fabrication of a silicon-based solid state quantum computer', *Surface Science*, 532-535:1209-1218.
[212] Zwanenburg F A et al. (2013) 'Silicon quantum electronics', *Reviews of Modern Physics*, 85:961.

of quantum technology,[213,214,215,216,217] and exported that knowledge base around the world[218,219] (Figure 8). Australia was recognised as an exemplary place to work, collaborate and participate in student exchange. Australia had become a powerhouse player in the quantum field and was recognised by the international community as one of, if not, the leading nation pushing the development of this technology.[220 221]

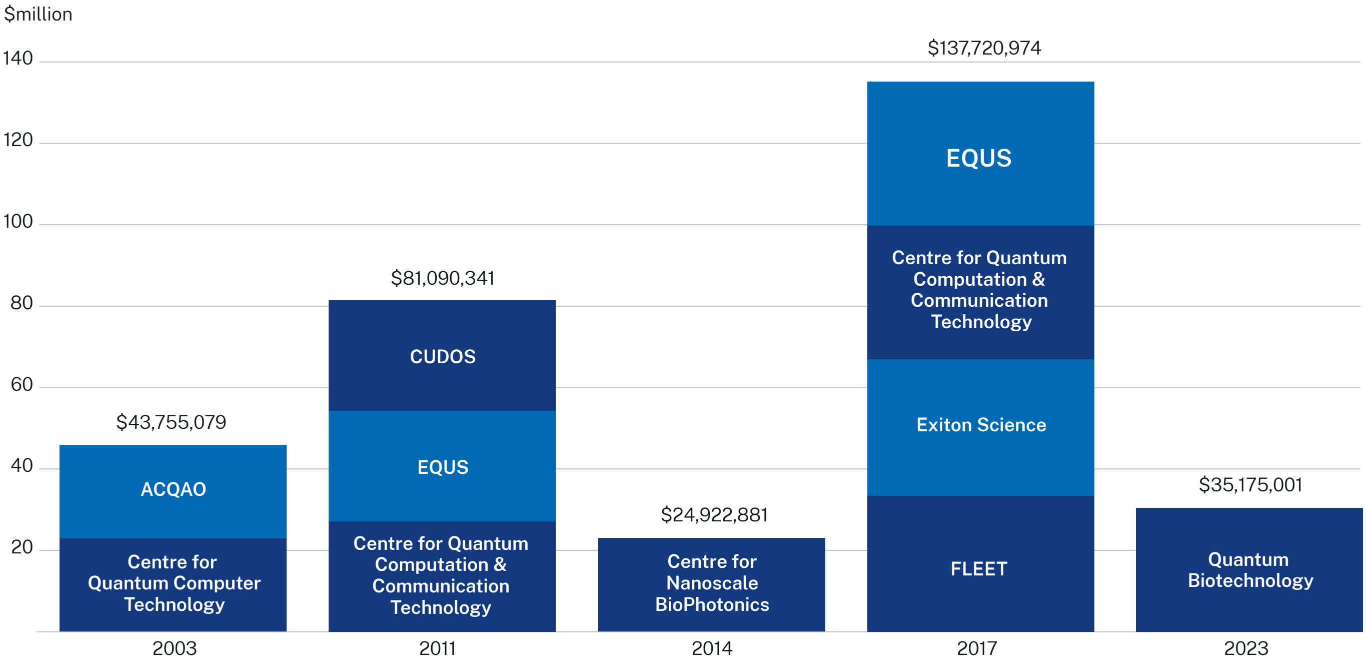


Figure 9. ARC funding for the Centres of Excellence program between 2000 and 2023. In total, eight CoEs have been established with direct or peripheral connections to the quantum technology field, totalling over A$320 million in funding.

The CoEs make up the majority of the ARC federal funding dedicated to quantum technologies. There have been eight CoEs with supporting quantum or quantum-related technologies (Figure 9). By liberally crediting the full total funding for all eight centres as directly contributing to quantum technology, the CoEs correspond to $323 million AUD (A$) – approximately 62% – of all funding dedicated to quantum (A$518 million total, since 2000). And by only including the Centres for Quantum Computing and Communications Technology (CQCT/CQC2T) and the Centre for Engineered Quantum Systems (EQUS), the two centres most directly focused on the development of quantum computing, communications and sensing technology, the CoEs account for approximately 43% of all funding (A$150 million for CoEs out of a corresponding total of A$348 million across all ARC schemes).

When understanding Australia's global leadership in quantum technologies the role of large-scale and long-term funding afforded through multiple ARC grant rounds cannot be understated. It is evident that these investments at the national scale have direct links to the prominence of the global quantum ecosystem and the emerging quantum industry in Australia. It is also clear that stable funding through the ARC CoE programs has allowed further growth in research capacity funding for the participating institutions, with UNSW Sydney (administering organisation of CQC2T), ANU (administering organisation of ACQAO and participant in CQC2T and EQUS), and UQ (administering organisation of EQUS) receiving significantly more funding than other Australian institutions (Figure 10). This is reflected in NSW, ACT and Queensland states receiving the most funding for quantum related research over the past 20 years (Figure 11).

[213] Fitzsimons J and Twamley J (2006) 'Globally Controlled Quantum Wires for Perfect Qubit Transport, Mirroring, and Computing', *Physical Review Letters*, 97:090502.
[214] Greentree A D et al. (2006) 'Quantum phase transitions of light', *Nature Physics*, 2:856-861.
[215] Bartlett S D et al. (2007) 'Reference frames, superselection rules, and quantum information', *Reviews of Modern Physics*, 79:555.
[216] Wiseman H M et al. (2007) 'Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox', *Physical Review Letters*, 98:140402.
[217] Berry D W et al. (2007) 'Efficient Quantum Algorithms for Simulating Sparse Hamiltonians', *Communications in Mathematical Physics*, 270:359-371.
[218] https://la-science.lanl.gov/lascience27.shtml.
[219] https://www.zdnet.com/article/aussie-it-research-hits-global-benchmark/.
[220] https://qist.lanl.gov/pdfs/qc_roadmap.pdf
[221] https://assets.publishing.service.gov.uk/media/5a7d647aed915d269ba8a61b/quantum-technologies.pdf.

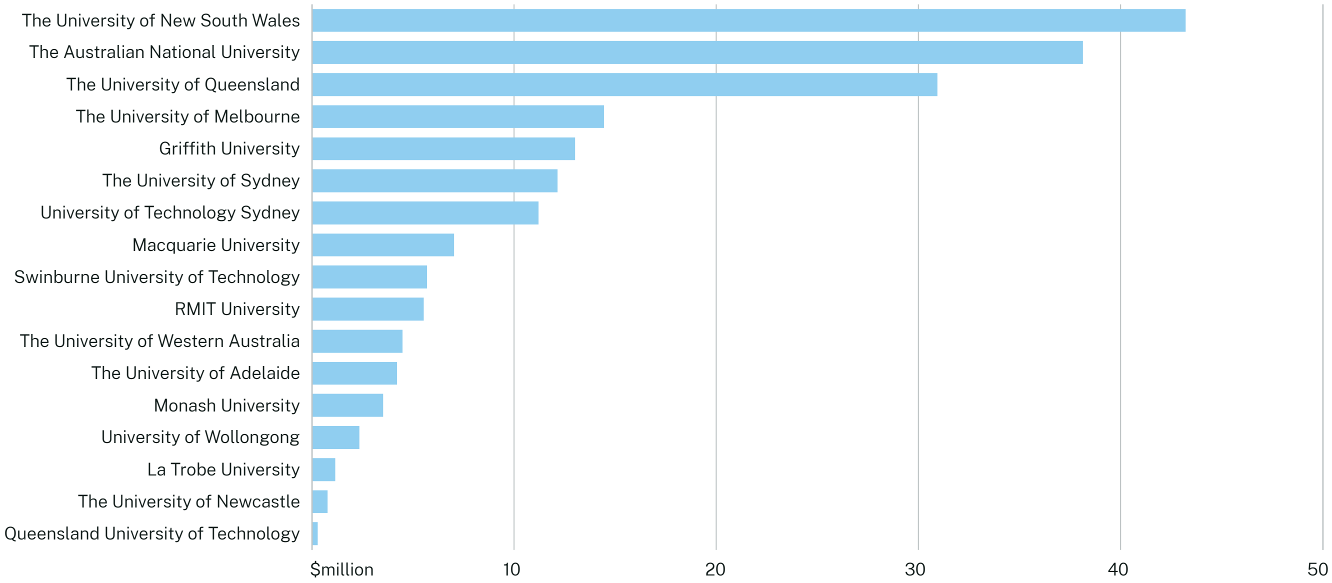


Figure 10. ARC funding of quantum technology-related projects across all ARC funding schemes from 2000-2023.[222] Funding categorised with respect to the administering organisation at the time of award.

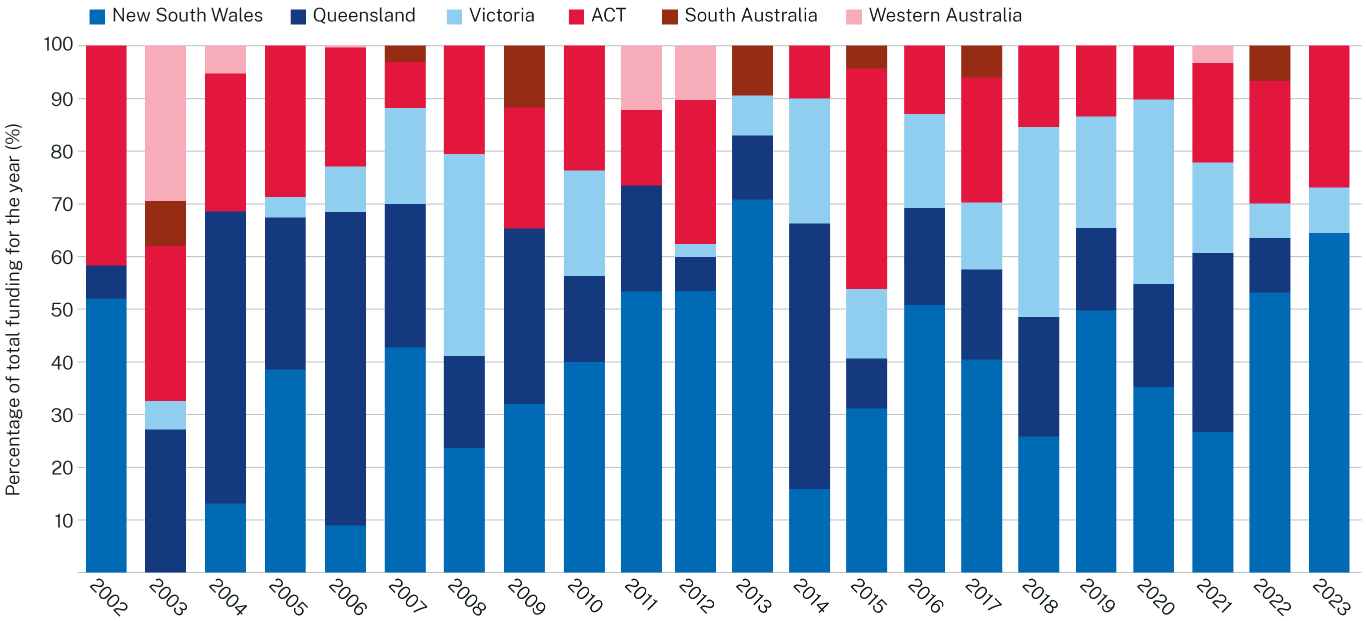


Figure 11. ARC funding of quantum technology-related projects across all ARC funding schemes from 2000-2023. Funding categorised in terms of states where the administering organisation is located.

When examining ARC and other Government funding across schemes, excluding CoEs it is evident that a significant majority of funding has gone to research focused on the development of quantum technology devices, and a comparatively small amount of funding has been allocated to quantum algorithms and the application of quantum computing technologies (Figure 12). It is expected that a detailed breakdown of CoE budgets would mirror this data, however these budgets are not publicly available.

[222] Raw data for this analysis can be found at https://github.com/devitt1/Funding-data.

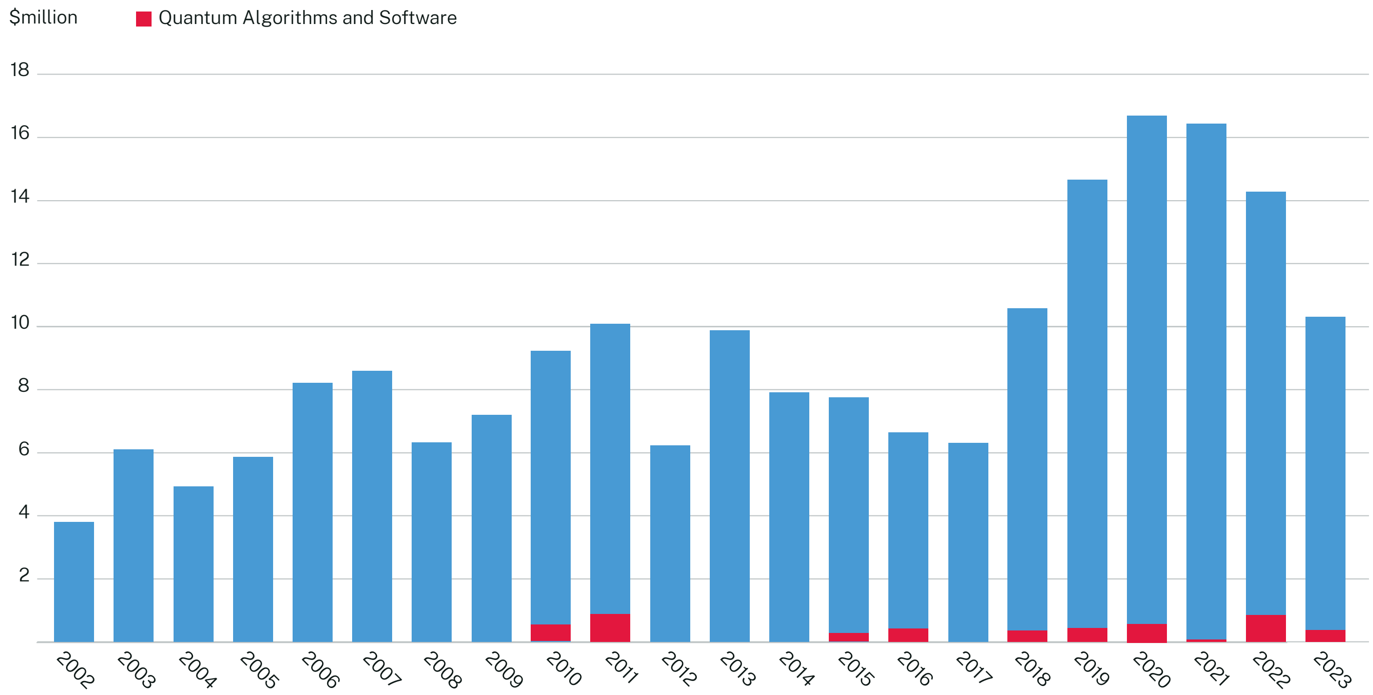
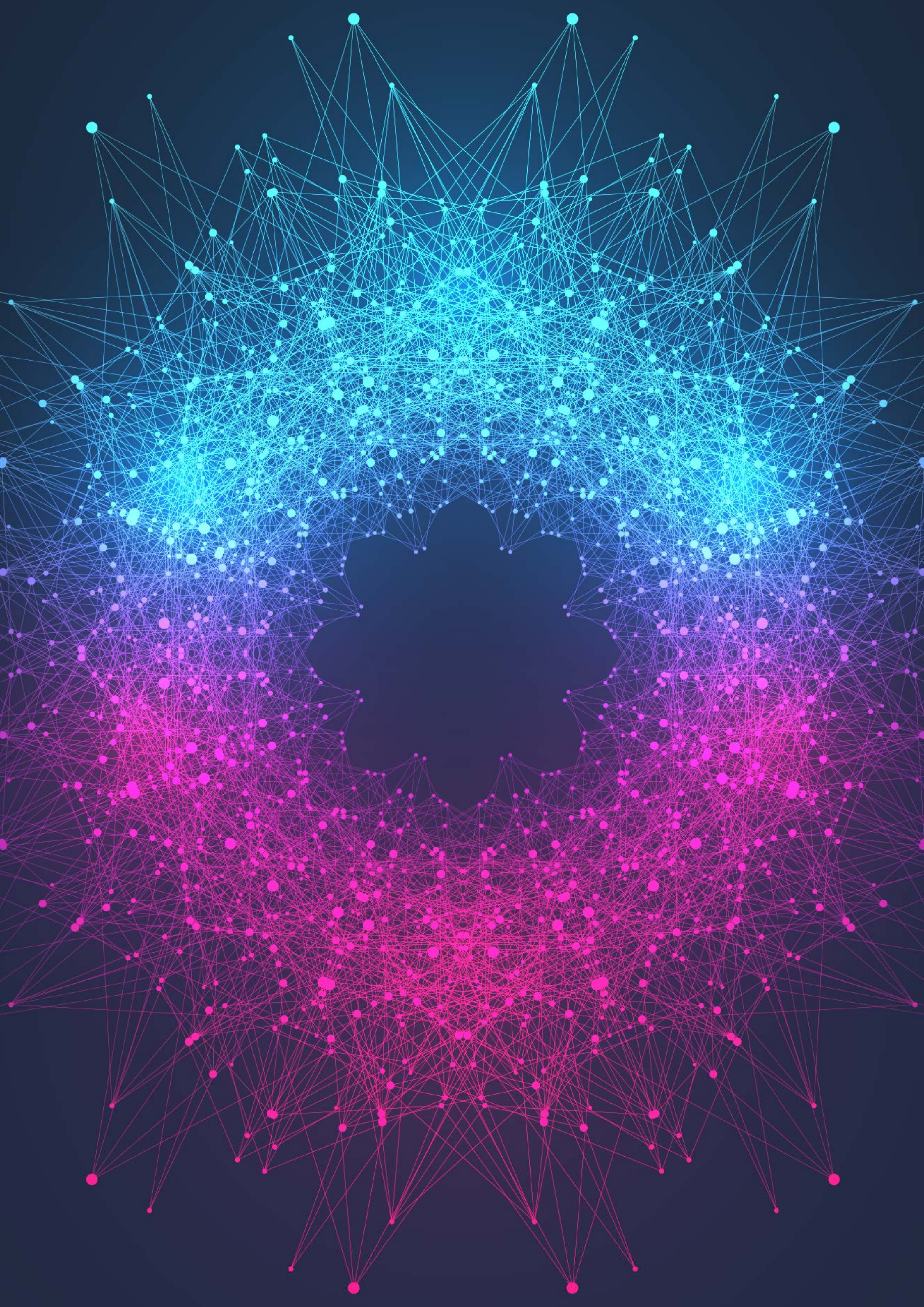


Figure 12. ARC funding of quantum technology-related projects across all ARC funding schemes from 2000-2023. Columns represent total funding as a function of the year. Funding for research focused on quantum algorithms and software is nested in columns (red).



Examining direct tenders from federal government sources, reveals that, in total, A$9.2 million was contracted, with the majority of this amount, A$6.2 million, awarded to Canberra quantum communications startup Quintessence Labs between 2017 and 2022, followed by A$1.5 million awarded to Sydney quantum software start-up Q-CTRL between 2021 and 2023.[223]

In 2023, the NSW Government launched the Quantum Computing Commercialisation Fund, a A$7 million program, for NSW-based quantum companies, on developing specific products or services related to quantum computing to bring a product to market.[224] Q-TRL, Diraq and Quantum Brilliance received funding through this program.[225]

6.2.1 The Australian National Strategy

In the 2023 budget[226] the Australian Government committed to delivering:

- A$40.2 million to deliver a Critical Technologies Challenge Program
- A$19.8 million to establish the Australian Centre for Quantum Growth.

The Federal Government ran a community consultation process on these initiatives in 2023 and both are expected to be launched in 2024. The Critical Technologies Challenge Program is intended to encourage the uptake of quantum technologies and to create stronger ties between quantum researchers and industry in Australia. Whereas the Australian Centre for Quantum Growth will “support research and development of a quantum technology industry”, “help catalyse demand for quantum technologies”, and “help Australian companies capture a share of the emerging global market”.

In addition, the Australian Government has committed A$1 billion to be invested across the range of critical technologies via the National Reconstruction fund.[227] However, to date no announcements have been made regarding any quantum-specific programs or investments emerging from the National Reconstruction Fund.

6.3 Challenges

Australia has a long and distinguished history in the quantum technology field, being one of the few research-heavy nations focused on quantum technology in the 2000s, adopting an early position to take advantage of the oncoming advances in quantum computing.

However, since the early 2010s, Australia has been overtaken by national initiatives and significant private-sector investments worldwide. While work is currently underway within the Commonwealth Department of Industry, Science and Resources (DISR) and the Australian Chief Scientist’s office to address this shortfall with the National Quantum Strategy delivered in May 2023, Australia is now competing with nations whose first major investments into an expansion of quantum technology started 8-10 years ago.[228] [229]

Australia still has the potential to be a significant part of the global supply chain for second-generation quantum technology (see Section 9 for detailed recommendations). This is unlike digital technology where Australia is, by and large, only a customer of a multi-trillion dollar industry.

To date, the focus of government and private investment in Australia has been in support of new hardware technologies in quantum computing, communications and sensing technology. These activities have generated a critical mass of quantum talent in NSW including in the surrounding fields of Quantum Algorithms, Software and Theory (QAST). These have been further bolstered by strategic investment by universities and NSW initiatives such as the Sydney Quantum Academy (SQA).

Given the maturity of hardware commercialisation in Australia,[230,231,232] QAST research is cheap – compared to experimental hardware programs. Additionally, because many of Australia’s most talented researchers in the QAST field are not aligned with pre-existing commercial efforts, QAST is a ripe area for Australia to build upon on the international stage.

Australia is in an advantageous position to capitalise on QAST research and development and establish itself as a major supplier of IP to the global quantum ecosystem. However, Australia needs to act now. The most critical element to establishing a globally competitive industry within the QAST space is to recruit and maintain a healthy talent pool of the best

[223] Public tender results from various federal departments was also surveyed, available through https://www.tenders.gov.au/, an online database of federal government public contracts database. All quantum technology-related tenders awarded between 2005 and 2023 were examined by searching under the keyword ‘quantum’.
[224] https://www.chiefscientist.nsw.gov.au/__data/assets/pdf_file/0009/549009/QCCF-Guidelines.pdf.
[225] https://www.nsw.gov.au/grants-and-funding/qccf.
[226] https://www.industry.gov.au/news/investments-grow-australias-critical-technologies-industries.
[227] https://www.industry.gov.au/news/national-reconstruction-fund.
[228] https://uknqt.ukri.org/our-programme/.
[229] https://www.jst.go.jp/inter/washington/quantumdcl2022.html.
[230] https://pitchbook.com/profiles/company/267810-76.
[231] https://pitchbook.com/profiles/company/498508-93.
[232] https://pitchbook.com/profiles/company/438743-44.

theorists and quantum software developers in the field. Other nations and/or companies are aggressively recruiting, including from Australia,[233] and the ability for Australia to capture a global market focused on QAST will diminish if world-class talent cannot be recruited or retained.

NSW has taken a tentative first step in founding the Australian Quantum Software Network (AQSN), coalescing research into QAST from around the nation under the umbrella of an AQSN that will be established formally as a non-profit, professional organisation. Smaller research groups and centres exist at multiple universities,[234,235,236] but there are no organisations or efforts within Australia aside from the AQSN that are attempting to coalesce QAST research more broadly.

6.4 Recent global investments

While non-academic activities in quantum technologies can be traced back to research efforts at corporations such as IBM,[237] Hewlett-Packard[238] and NEC[239] in the 1980s, 1990s and early 2000s, only in the period 2010-2015 did multinational corporations, the private equity and venture capital community and a variety of governments with no prior history in quantum[240,241,242,243,244] start to recognise the potential market and national security value of quantum. Subsequently, increased amounts of capital has come into the sector.

A summary of sovereign investment in quantum technology globally is provided in Figure 13.
A non-exhaustive list of major corporate, startup and sovereign investment, in 2023, include:[245]

- The UK announced a second **National Quantum Strategy**, doubling its commitment compared with the NQTP through a 10-year, A$4.8 billion (£2.5 billion) investment. The UK-NQS also indicates its intention to attract at least an additional A$1.9 billion (£1 billion) of private-sector investment, on top of the government commitment.[246]
- The German government announced a A$4.9 billion (€3 billion) *Quantum Technologies Action Plan* over the next three years to build a 100-500 qubit quantum computer.[247]
- The Canadian government announced a *National Quantum Strategy* in early 2023 supported by a A$405 million ($360 million CAD) incremental commitment. This is the first dedicated quantum investment by the federal government in Canada, who were, like Australia, an early and successful investor in the quantum space.[248]
- In October 2022, the *European High Performance Computing Joint Undertaking* (EuroHPC JU) announced the funding of six quantum computers to be built and installed in HPC locations in Barcelona (Spain), Munich (Germany), Ostrava (Czech Republic), Essonne (France), Bologna (Italy) and Poznan (Poland). With an investment of over A$260 million (€160 million), these six computers will be drawn from a variety of different systems being developed as part of the EU quantum flagship program.[249]
- South Korea, in June 2023, announced a strategic initiative with a A$3.5 billion (3 trillion KRW) investment into quantum technologies by the year 2035, with aims to increase its quantum workforce by a factor of seven, develop their own quantum computing infrastructure, and to capture 10% of the global quantum market by 2035.[250]
- The Indian government codified in April 2023 its A$1.4 billion (Rs 80B) *National Quantum Mission*, with the goal of building a 1000-qubit quantum computing system by 2031 and deploying satellite-based quantum communication links and quantum key distribution systems, and a multi-node quantum communications network.[251]
- In late 2021, Taiwan announced a four-year (2022-2026) A$378 million ($8 billion TWD) investment into an *Industry cooperation platform for quantum technology*.[252]

[233] https://twitter.com/hbar_consultant/status/1411247731067133952.
[234] https://www.griffith.edu.au/centre-quantum-dynamics.
[235] https://www.uwa.edu.au/research/ems-research-clusters/quantum-information-simulation-and-algorithms.
[236] https://www.uts.edu.au/our-research-archived/centre-quantum-software-and-information.
[237] https://www.fastcompany.com/90633843/1981-quantum-computing-conference-ibm-roadmap-mit.
[238] https://www.hp.com/hpinfo/newsroom/press_kits/2008/hplabsemea/demo-qkd.pdf.
[239] https://www.nec.com/en/global/quantum-computing/index.html.
[240] https://dst.gov.in/national-quantum-mission-unprecedented-opportunity-india-leapfrog-quantum-computing-technologies.
[241] https://www.businesskorea.co.kr/news/articleView.html?idxno=117287.
[242] https://www.gov.ie/en/publication/126b4-quantum-2030-a-national-quantum-technologies-strategy-for-ireland.
[243] Cao C et al. (2006) 'China's 15-year science and technology', Physics Today, 59(12):38-43.
[244] Zhang Q et al. (2019) 'Quantum information research in China', Quantum Science and Technology, 4:040503.
[245] For a summary of investments prior to 2023, see https://www.aspi.org.au/report/australian-strategy-quantum-revolution, https://www.standards.org.au/documents/quantum-computing-report.
[246] https://www.gov.uk/government/news/new-technologies-on-show-at-quantum-showcase-as-science-minister-drives-forward-uks-25-billion-quantum-strategy.
[247] https://qbn.world/eur-3-billion-action-plan-for-quantum-technologies-by-german-government/.
[248] https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy#
[249] https://eurohpc-ju.europa.eu/one-step-closer-european-quantum-computing-eurohpc-ju-signs-hosting-agreements-six-quantum-computers-2023-06-27_en.
[250] https://thequantuminsider.com/2023/06/29/south-korea-to-invest-2-33-billion-in-quantum-by-2035/.
[251] https://dst.gov.in/national-quantum-mission-unprecedented-opportunity-india-leapfrog-quantum-computing-technologies.
[252] https://english.ey.gov.tw/Page/61BF20C3E89B856/75a758cd-6b6c-4ae6-bf33-cfee41d6992b.

- The Danish government, in June 2023, announced a A$220 million (1 billion DKK) national quantum initiative up to 2027[253] where *"The primary objective of the National Strategy for Quantum Technology is to foster Danish quantum research, ensuring its continued global leadership and facilitating the translation of research findings into practical quantum solutions for global challenges."*
- In September 2023, the Finnish government announced a budget of A$117 million (€70 million) to scale up their domestic quantum computer systems to 300 qubits.[254]

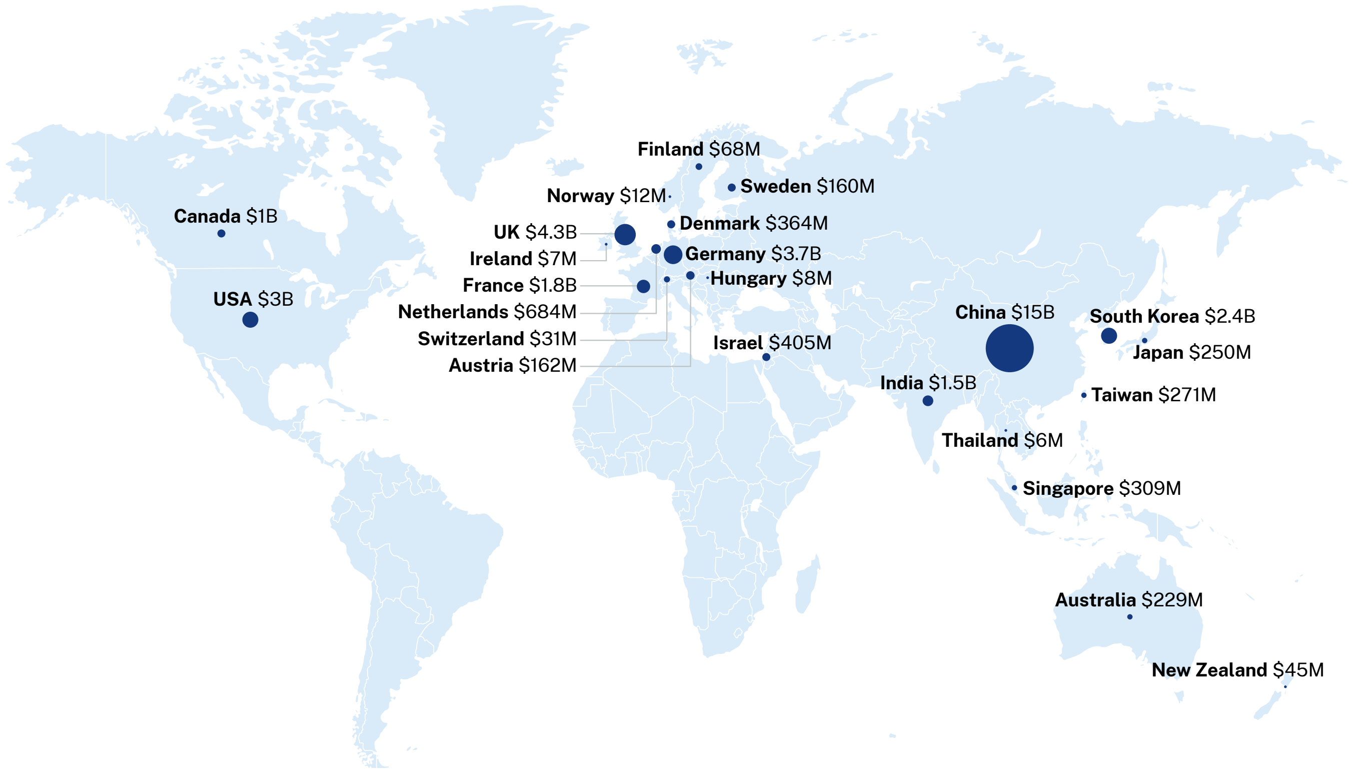


Figure 13. Sovereign investments into quantum technology programs to date. All figures in US$ million (M) or billion (B). Data sourced from the Quantum Insider Quantum Computing Market Data Platform.[255]

The quantum startup space has also continued to see large investments around the world, with the following notable examples from 2023:

- A$744 million ($500 million USD (US$) raised by SandboxAQ, a California-based post-quantum cryptography company that also focuses on 'the intersection of quantum and AI, optimisation and security'. A major investor into this company was former Google CEO, Eric Schmidt, with the company spinning out from X – a blue-sky research division of Alphabet Inc.[256]
- A$220 million (US$148 million) raised by Chinese startup, Origin Quantum: Origin is pursuing multiple types of quantum computing hardware, superconductors and semiconductors and several 'software solutions'. This raise was financed by domestic Chinese investors.[257]
- Photonic Inc. a Silicon-based quantum hardware startup out of British Columbia in Canada, raised US$100M as part of a major partnership with Microsoft.[258]
- Xanadu, a Canadian-based photonic quantum hardware company, founded by the University of Queensland graduate, Christian Weedbrook, raised A$148 million (US$100 million) from several investors in 2022 in a Series C[259] and in 2023 secured A$45 million ($40 million CAD) from the Canadian Government's (federal) Strategic Investment Fund.[260]

[253] https://investindk.com/insights/denmark-makes-decision-to-spend-1-billion-dkk-on-quantum-research-and-innovation-strategy.
[254] https://quantumzeitgeist.com/finland-unveils-second-quantum-computer-with-20-qubits-aims-for-50-qubit-device-by-2024/.
[255] https://thequantuminsider.com/data/
[256] https://www.sandboxaq.com/press/exclusive-alphabet-spinoff-sandbox-aq-raises-500m-for-cyber-security-other-quantum-work.
[257] https://www.quantumbusinessnews.com/deals-partnerships/chinese-quantum-startup-raises-148m-#
[258] https://photonic.com/news/photonic-raises-100m-for-quantum-technology/.
[259] https://www.prnewswire.com/news-releases/xanadu-closes-100m-usd-series-c-to-accelerate-development-of-fault-tolerant-quantum-computers-301672611.html.
[260] https://www.utoronto.ca/news/quantum-computing-startup-xanadu-receives-40-million-federal-funding-globe-and-mail.

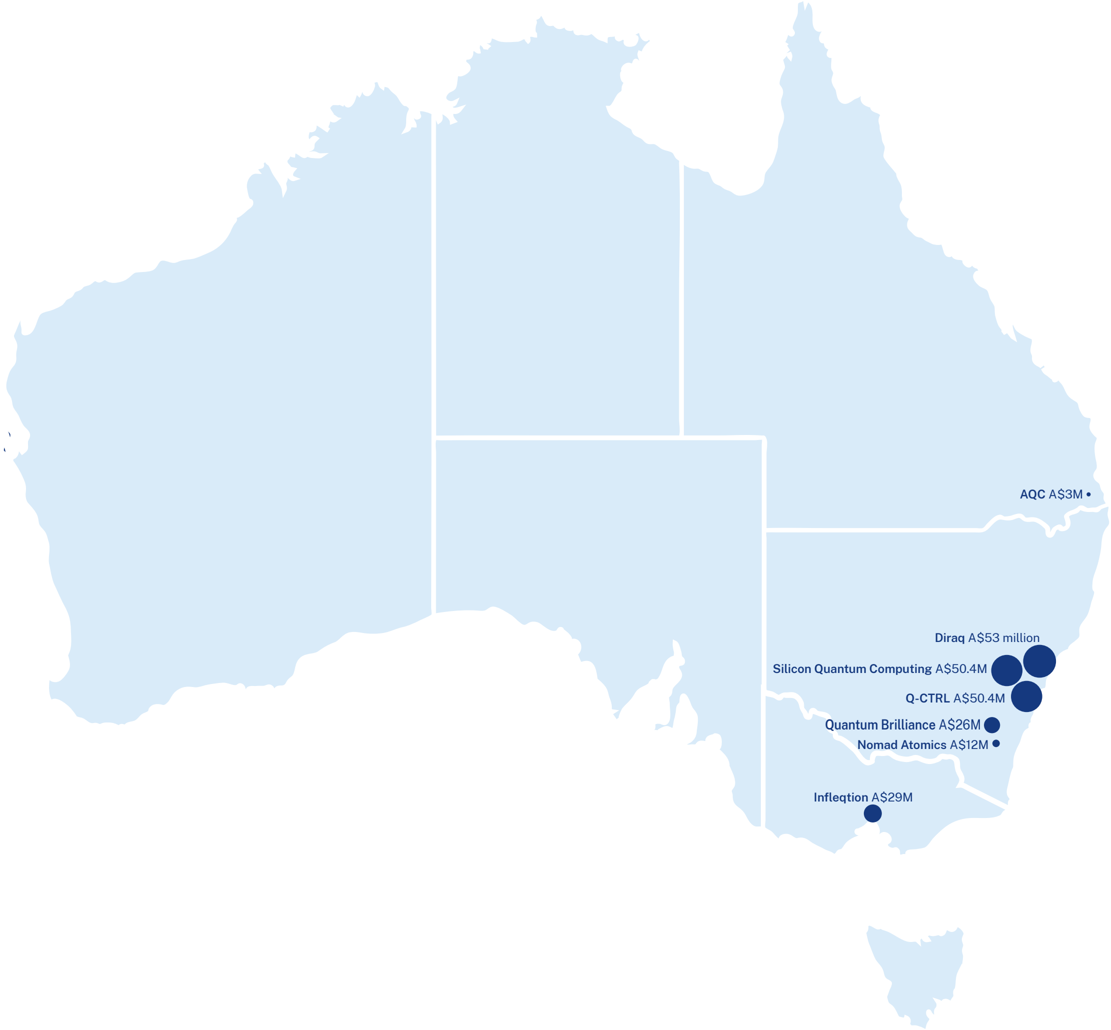


Figure 14. Investments into Australian quantum companies from January 2023 to February 2024.

In Australia, there has been additional investment into several startup companies in 2023 (Figure 14), including:

- Diraq, the second spinout from the silicon hardware groups at UNSW Sydney, was founded in 2022 with over A$53 million in Series A funding from Allectus Capital and Quantonation.[261]
- Q-CTRL, a quantum software and sensing company based in Sydney, which continued its expansion in 2023, closing its series B with an additional USD$27.4 million investment.[262]
- Infleqtion, a US-based company focused on cold-atom technology, received a significant investment of A$29 million from Breakthrough Victoria, establishing an Australian presence out of Swinburne University of Technology in Melbourne.[263]
- Quantum Brilliance, a diamond-based quantum hardware company based in Canberra also received investment from Breakthrough Victoria in 2023, with A$8 million invested as part of a A$26 million funding round that also included further investment from Main Sequence Ventures.[264]
- SQC, the first spin out from the silicon hardware groups at UNSW Sydney founded in 2017, received A$50.4 million in Series A funding in 2023.[265]
- Canberra-based quantum sensing startup, Nomad Atomics, secured a A$12 million in a Series A round.[266]
- Queensland-based hardware startup, Analog Quantum Circuits (AQC), secured an initial A$3 million investment from Uniseed to start developing superconducting components for quantum technologies.[267]

[261] https://thequantuminsider.com/data/
[262] https://q-ctrl.com/blog/q-ctrl-announces-expansion-of-industry-leading-series-b-for-quantum-infrastructure-software.
[263] https://breakthroughvictoria.com/stories/coldquanta-media-release/.
[264] https://breakthroughvictoria.com/stories/quantum-brilliance-media-release/.
[265] https://sqc.com.au/2023/07/25/silicon-quantum-computing-raises-50-4m/.
[266] https://www.businessnewsaustralia.com/articles/quantum-sensor-startup-nomad-atomics-raises--12m.html.
[267] https://www.startupdaily.net/topic/quantum-computing/uniseed-backs-queenslands-first-quantum-hardware-startup-with-3-million-round/.

Many major multinational corporations across multiple sectors are now involved in quantum technology. This includes companies such as Google,[268] Microsoft[269] and IBM[270] that are looking to build technology, but it also includes companies that are investing to determine how quantum computing, communications and sensing will change their industries. This includes companies such as Airbus,[271] Woodside,[272] GE,[273] Pfizer,[274] Goldman Sachs[275] and BMW,[276] to name a few. These companies are investing in and funding research in the quantum algorithms and software space, which presents opportunities for leading Australian researchers to secure research development contracts.

In the startup space, there has been an increase in the establishment of quantum companies worldwide. Two of the highest valued quantum computing startups in the world, PsiQuantum in Palo Alto[277] and Xanadu in Toronto,[278] are founded by Australian researchers, but they are not based in Australia. Australia has established six quantum hardware/software companies directly involved in developing quantum computing, sensing or communications technology. Compared to other nations, Australia now ranks joint 13th in startups to the US (72), the UK (38), Canada (34), Germany (24), France (16), Japan (15), Spain (12), China (11), The Netherlands (10), India (10), Poland (8), Switzerland (7), Singapore (6), Israel (6), Australia (6), Finland (6).[279]

[268] https://quantumai.google/.
[269] https://www.microsoft.com/en-us/research/research-area/quantum-computing/?
[270] https://www.ibm.com/quantum.
[271] https://www.airbus.com/en/innovation/disruptive-concepts/quantum-technologies/airbus-quantum-computing-challenge.
[272] https://www.woodside.com/docs/default-source/media-releases/12-nov-2019---woodside-joins-mit-ibm-watson-ai-lab-and-ibm-q-network.pdf.
[273] https://www.ge.com/research/project/quantum-computing.
[274] https://centerfordigitalinnovation.pfizer.com/quantum-computing-4-sequence-alignment-qc.
[275] https://www.goldmansachs.com/careers/possibilities/quantum-computing/.
[276] https://www.press.bmwgroup.com/global/article/detail/T0362463EN/bmw-group-quantum-computing-challenge:-the-winners-have-been-decided?language=en.
[277] https://pitchbook.com/profiles/company/235924-66.
[278] https://pitchbook.com/profiles/company/186555-43.
[279] https://quantumcomputingreport.com/privatestartup/

7. NSW capabilities in quantum algorithms, software and theory research

Strategic investments over the last 20 years by NSW universities and the NSW Government has established a critical mass of quantum computing research capability in NSW.

Research funding has been primarily driven through competitive grants programs (primarily the ARC), US defence funding (e.g. ARO, DARPA, AUSMURI), and strategic investment by Australia's universities over the last two decades. More recently, this has been enhanced by strategic funding from multinational corporations (especially Microsoft and Google) and private investment in startups including SQC, Diraq and Q-CTRL. This has seen NSW, and more broadly Australia's quantum ecosystem, develop two key advantages.

1. **A significant baseline of experimental infrastructure for quantum computing and communications hardware development.** This is most obvious for silicon-based quantum computing systems and optical quantum computing and communications, but reasonable infrastructure for other areas of development such as superconducting and ion-trap qubits also exists.
2. **A talent pipeline across all areas of quantum technologies.** This has meant that the experimental programs have been enhanced by the latest developments in QAST. Additionally, the close geographic proximity of QAST researchers within the NSW ecosystem has ensured that theoretical work is often kept grounded to the experimental realities of the hardware, leading to numerous collaborations across NSW between experimentalists, often working in industry, and those focused on QAST.

QAST research provides the vital link between quantum hardware development and value capture in industry. Importantly, talent is the key driving factor of ongoing QAST development. Over the last five years, NSW advantages in this area have been consolidated through the creation of the Sydney Quantum Academy (SQA), a joint venture enabled with co-funding from the NSW Government, UNSW Sydney, the University of Sydney, UTS and Macquarie University. With a focus on the early career talent pipeline and ecosystem growth the SQA has helped build new education pathways and outreach programs to bridge the gap between university-based research and industry.

Collectively, these initiatives have resulted in the high-quality QAST research output of NSW universities comparable to, and in many cases considerably better than, those of the top research destinations internationally.[280]

There is a considerable amount of industry collaboration and engagement between QAST research teams in NSW and internationally leading corporate and startup quantum industry players. A non-exhaustive list of industry collaboration in QAST research at SQA universities includes Google, Microsoft, IBM, AWS, Lockheed Martin, Boeing, BBN Raytheon, SQC, Diraq, Q-CTRL, Quantum Motion Technologies, BTQ, PsiQuantum, Rigetti, IonQ, Alpine Quantum Technologies, BTQ, Zapata and HRL Laboratories. Beyond these there is an extensive list of academic collaborations covering the world's best research institutions.

[280] For comparison, a case study is presented in Section 7.3 analysing publication statistics for the Conference on Quantum Information Processing, the leading, quantum-specific venue for the presentation of quantum algorithms research.

Australian Quantum Software Network (AQSN)

AQSN was established by UTS and launched by the Hon Ed Husic MP in December 2022. The aim of AQSN is to consolidate all QAST research across Australia and communicate the breadth and depth of QAST research both locally and abroad. The AQSN, upon launch, included:

- membership of 13 institutions across Australia, including:
  - 10 universities across NSW, Queensland, Victoria and Western Australia
  - the quantum information theory research at CSIRO
  - NSW Venture Backed Startup, Q-CTRL
  - NSW Quantum Education Startup, Eigensystems
- over 110 individual members including permanent faculty, industry researchers, students and postdoctoral researchers
- 30 research groups, making AQSN the largest collaboration of quantum software research talent in the world
- 6 external partner organisations, including Google Quantum AI, the Okinawa Science and Technology in Japan, Aalto University in Finland and Australian quantum hardware-based startups, SQC, Diraq and Quantum Brilliance.

This section provides a background on QAST-specific research efforts and capabilities in NSW.[281]

7.1 NSW QAST research

7.1.1 University of Technology Sydney

QAST research at UTS is mostly housed in the UTS Centre for Quantum Software and Information[282] (QSI) which is unique in Australia in that it is based in the School of Computer Science and focuses on quantum computing software. QSI has significant research programs covering the full stack of quantum software technologies: quantum algorithms and complexity, quantum programming theory, fault-tolerant architecture design, quantum control and characterisation, and quantum hardware development.

In addition to the QSI, there are researchers within the School Mathematical and Physical Sciences working in theoretical physics and hardware for quantum technology. This includes research into superconducting qubits, photonic sources for quantum communications and quantum materials.

Australian partnerships: UTS leads the quantum algorithms and complexity program of the CQC2T, is one of the partners in the SQA and a founding member of the AQSN.

Industry engagement: UTS has a strong history of industry engagement in quantum computing, including industry heavyweights such as Google and Lockheed Martin and key collaborations through multiple projects in DARPA's Quantum Benchmarking program including with HRL Laboratories, Boeing, General Motors, IonQ, Rigetti and Zapata.

History: QSI grew out of its predecessor, the UTS Centre for Quantum Computation and Intelligent Systems, which was founded in 2008. UTS initiated this research effort by recruiting Distinguished (Dist) Prof Mingsheng Ying, an early leader in the theory of quantum programming languages, and his team from Tsinghua University. In 2016, QSI was established with Prof Runyao Duan as the founding Director.

QSI aims to be an inclusive environment that encourages advanced research and the nurturing of talent. Past faculty members have gone on to senior leadership positions in the quantum industry, including Prof Runyao Duan who left Australia to lead the quantum computing program at Baidu, and A/Prof Min-Hsiu Hsieh who is currently the director of the Hon Hai (Foxconn) Quantum Computing Research Centre.

Current QAST senior faculty list: Prof Michael Bremner (Director), A/Prof Simon Devitt (Research Director), Prof Yuan Feng, A/Prof Christopher Ferrie, Dr Marika Kieferova, A/Prof Nathan Langford, A/Prof Troy Lee, Prof Sanjiang Li, Dr Luke Mathieson, A/Prof Youming Qiao, Dr Yuval Sanders, A/Prof Alexander, Solnstev, Dr Harley Scammell and Dist Prof Mingsheng Ying.

Scale: More than 45 faculty, honorary faculty, postdoctoral researchers and higher degree research (HDR) students.

7.1.2 The University of Sydney

The Quantum Science Group[283] research program at the University of Sydney ranges from fundamental physics and quantum information science through to experimental technology development which incorporates both atomic and condensed matter systems. The research program is a highly integrated effort of leading researchers in both quantum optical/atomic physics and condensed-matter physics, theory and experiment.

[281] The Australian Quantum Software Network (AQSN) website has more information on QAST research around Australia https://www.quantumsoftware.org.au/.

[282] https://www.uts.edu.au/our-research-archived/centre-quantum-software-and-information.

[283] https://quantum.sydney.edu.au/.

QAST research at the University of Sydney is predominantly within the Quantum Theory Group[284] in the School of Physics and the Kassal Group[285] in the School of Chemistry. The Quantum Theory Group research interests range from understanding the fundamental differences between classical and quantum information processing to designing the best quantum architectures for quantum computers. Their research strengths are in:

- quantum error-correcting codes
- quantum characterisation, verification and validation
- physical implementations of quantum computers
- many-body quantum optics
- foundations of quantum mechanics
- topological phases of matter.

The Kassal Group's QAST research is focused on developing quantum algorithms for chemistry applications.

Australian partnerships: The University of Sydney hosts a node of EQUS, is a member of the AQSN and is a partner in the SQA.

Industry engagement: The scientific pursuits of the Quantum Science Group are complemented by deep industry engagement and entrepreneurial activities. The group hosts a global research node of the Microsoft Station Q network (led by Prof David Reilly) and has led to the formation of Australia's first venture-capital backed quantum-tech startup, Q-CTRL (founded and led by Prof Michael Biercuk). They have collaborated extensively within industry including with PsiQuantum, Google, IBM and Diraq.

History: QAST research at the University of Sydney began in the mid-2000s with the recruitment of Prof Stephen Bartlett and Prof Andrew Doherty. A feature of the Quantum Science Group has been close collaboration with experimental teams at the University of Sydney and UNSW Sydney, and more generally with leading experimental quantum computing teams around the world.

Current QAST senior faculty: Prof Stephen Bartlett, Dr Clement Canonne, Prof Andrew Doherty and A/Prof Ivan Kassal.

Scale: More than 35 faculty, honorary faculty, postdoctoral researchers and HDR students.

7.1.3 Macquarie University

The Macquarie Centre for Quantum Engineering (MQCQE) works on a broad range of topics in QAST research, from the foundations of quantum mechanics through to the detailed optimisation of quantum computing applications. A unifying theme of MQCQE is the intersection of complex many-body physics and applications of quantum technologies.

The research strengths of the MQCQE include quantum simulations and algorithms, quantum many-body science, integrated nonlinear quantum photonics and fundamental quantum information.

Australian partnerships: Macquarie University hosts a node of EQUS, is a member of the AQSN and is a partner in the SQA.

Industry engagement: Macquarie University has had a long running collaboration with Google focusing on quantum algorithms for chemistry and materials science. They also have a close collaboration with BTQ[286] (Canada) working on post-quantum cryptography and Lockheed Martin.

History: QAST research at Macquarie University dates back to the early 1990s, with the appointment of Prof Barry Sanders (now at the University of Calgary). Since then the group has gradually expanded. Like the University of Sydney, they have traditionally had a broad cross section of interests in QAST research, often working closely with experimental teams around the world.

Current QAST senior faculty: Prof Gavin Brennen, A/Prof Dominic Berry, Prof Alexei Gilchrist, Prof Michael Steel and A/Prof Daniel Terno.

Scale: More than 38 faculty, honorary faculty, postdoctoral researchers and HDR students.

7.1.4 UNSW Sydney

UNSW Sydney has played a major role in the development of quantum computing since the 1990s and is well known for its research on quantum computing and quantum technologies more broadly. It has been the lead node of the CQC2T since its inception, which has led to a major focus on the development of silicon-based quantum computing. UNSW Sydney has spun-out the quantum computing companies SQC and Diraq, both of which employ QAST researchers and collaborate with QAST researchers at Australian universities and internationally. The focus of QAST research within the university mirrors these efforts with researchers focusing on new ways of designing quantum hardware in solid-state systems.

Australian partnerships: UNSW Sydney leads CQC2T, is one of the partners in the SQA and a member of the AQSN.

[284] https://quantum.sydney.edu.au/research/quantum-theory-group/.
[285] https://www.kassal.group/.
[286] https://www.btq.com/our-team.

Industry engagement: SQC and Diraq, both of which are primarily focused on hardware development, also have QAST teams. UNSW Sydney also has research collaborations with Google.

History: UNSW Sydney has a long history in quantum computing research, with a heavy focus on QAST[287] research in support of silicon-based hardware development. This research dates to the first proposals for solid-state quantum computers from Dr Bruce Kane (now at the University of Maryland).

Current QAST senior faculty: Prof Susan Coppersmith, A/Prof Dimi Culcer, Prof Robert Malaney and Dr Sushmita Ruj.

Scale: More than 10 faculty,[288] honorary faculty, postdoctoral researchers and HDR students.

7.2 Industry capability in NSW

7.2.1 Eigensystems

The quantum-related startup in the NSW ecosystem was spun out of QSI at UTS in 2023 and is currently based in NSW. Focused on the intersection of quantum technologies and education technology, Eigensystems[289] works to build tools and material to enable the training of a new, quantum-literate population. Just as digital literacy was crucial during the technological revolution of the late 20th and early 21st century, quantum literacy will be the next big shift in education. While Eigensystems is still in stealth mode, it is anticipated that in 2024 they will launch their first product.

7.2.2 Q-CTRL

The core focus of Q-CTRL is on developing quantum infrastructure software – control and characterisation software tools for quantum hardware. Q-CTRL is Australia's first venture-backed quantum computing company, with headquarters in NSW and led by CEO and founder Prof Michael Biercuk. Beyond quantum software, Q-CTRL is also working on quantum sensing technologies. Since inception, they have developed into a large team with significant backing by international venture capital companies. With approximately A$100 million in funding to date,[290] Q-CTRL has expanded with offices in Los Angeles and Berlin and has secured customers and contracts throughout the global quantum ecosystem.

Q-CTRL currently focus on three core business elements:

1. an online education platform that introduces individuals to foundational concepts in quantum information science
2. a software system that assists and optimises the design of control signals for low error rate quantum computing
3. a quantum sensing hardware division, attempting to build a new type of ultra-sensitive gravitational field sensors based on cold atom technology.

7.2.3 BTQ

BTQ, a Canadian venture-backed startup, whose primary focus is to develop solutions for post-quantum cryptography, has a significant presence in NSW, setting up a regional office at the Sydney Quantum Terminal.[291] In 2023, BTQ made two strategic hires from the Sydney ecosystem: Prof Gavin Brennan from Macquarie University, who was appointed as the head of Quantum Research, and Dr Peter Rohde from UTS. Their strategic recruitment led to new research that focuses on using quantum computing systems to provide the so-called 'proof of work' functionality that lies at the heart of many blockchain technologies.[292] The purpose of this work is to develop new cryptocurrencies that utilise quantum computing systems. This work has potential to solve one of the biggest criticisms of the blockchain, namely the massive amounts of power consumption needed by protocols such as Bitcoin to perform computational tasks that do nothing more than servicing the functionality of the blockchain.

7.2.4 Google

Under its Digital Future Initiative launched in 2021, Google Australia has dedicated A$1 billion in Australian infrastructure, research and partnerships, part of which is to propel Australia's position as a global quantum pioneer.[293] Their Australian headquarters are in NSW.

Google has invested in Australian quantum computing research by launching the following partnerships with field-leading researchers at NSW universities:

- A/Prof Dominic Berry (Macquarie University) to develop algorithms for quantum simulation
- Prof Susan Coppersmith (UNSW Sydney) to study properties of materials on an atomic scale

[287] https://q-ctrl.com/.
[288] There are more QAST researchers based out of UNSW Sydney who are employed by SQC and Diraq.
[289] https://quokkacomputing.com/.
[290] https://pitchbook.com/profiles/company/221852-44.
[291] https://thequantumterminal.com/
[292] Singh D et al. (2023) 'Proof-of-work consensus by quantum sampling', arXiv:2305.19865 [quant-ph].
[293] "Investing in Quantum computing to build a strong digital future." 28 Jul. 2022, https://blog.google/intl/en-au/company-news/technology/investing-in-quantum-computing/.

- A/Prof Ivan Kassal (University of Sydney) to develop new quantum algorithms for simulating chemical reactions
- Prof Michael Bremner (UTS) to explore mathematical structures to speed up computation with quantum computers.

These collaborations are coordinated by Dr Marika Kieferova, who holds a joint appointment between Google's Quantum AI team and UTS.

7.2.5 Diraq

Diraq is a quantum computing startup based in Sydney that is focused on the development of quantum computers based on complementary metal-oxide-semiconductor (CMOS) qubit technology. Led by CEO and founder Prof Andrew Dzurak, Diraq is a full-stack quantum computing company that was spun out of UNSW Sydney in 2022. While the company's focus is hardware, they have a growing team of QAST researchers working on topics ranging from device physics and quantum error correction, through to the software necessities of their devices.

7.2.6 Silicon Quantum Computing

Silicon Quantum Computing (SQC) is led by founder and CEO Prof Michelle Simmons and is focused on the development of phosphorus-doped silicon quantum processors. Based in Sydney, SQC was founded in 2017 and was the first quantum computing company to be spun out of CQC2T and UNSW Sydney. SQC is a full-stack quantum computing company, with most researchers working on hardware development. However, they have a growing team of QAST researchers working across quantum algorithms, error correction, architecture design, device physics and the software components of their technology stack.

7.2.7 Quantum Brilliance

Quantum Brilliance is building quantum processors based on nitrogen-vacancy centres in diamond. Their team is mostly working on hardware development, but they do have a QAST team that examines quantum computing applications and the software stack required for running their devices, including the software platform Qristal[294] which is used for programming their processors. Quantum brilliance has offices in Sydney, Canberra, Stuttgart, Singapore, and Chester (UK).

7.3 The Conference on Quantum Information Processing – a case study on research output

Research output comparisons are notoriously difficult to gauge and are highly dependent on the publication nuances of specific research fields. This is especially pronounced in QAST research as it is highly multidisciplinary. There are wildly differing standards for publication between theoretical physics and theoretical computer science. However, every year, the quantum information theory community attempts to reconcile these differences through the annual conference on Quantum Information Processing (QIP). QIP is the longest running annual conference in theoretical quantum computing and it seeks to bring together the top advances in QAST research that are relevant to quantum information processing. It is especially relevant for quantum algorithms, complexity, software and error correction – the key topics of this report. This conference has a stringent peer-review process, however, unlike many other conferences it does not produce proceedings, which allows research to be incorporated that would usually be published in a more traditional discipline-appropriate venue.

[294] https://quantumbrilliance.com/quantum-brilliance-qristal.

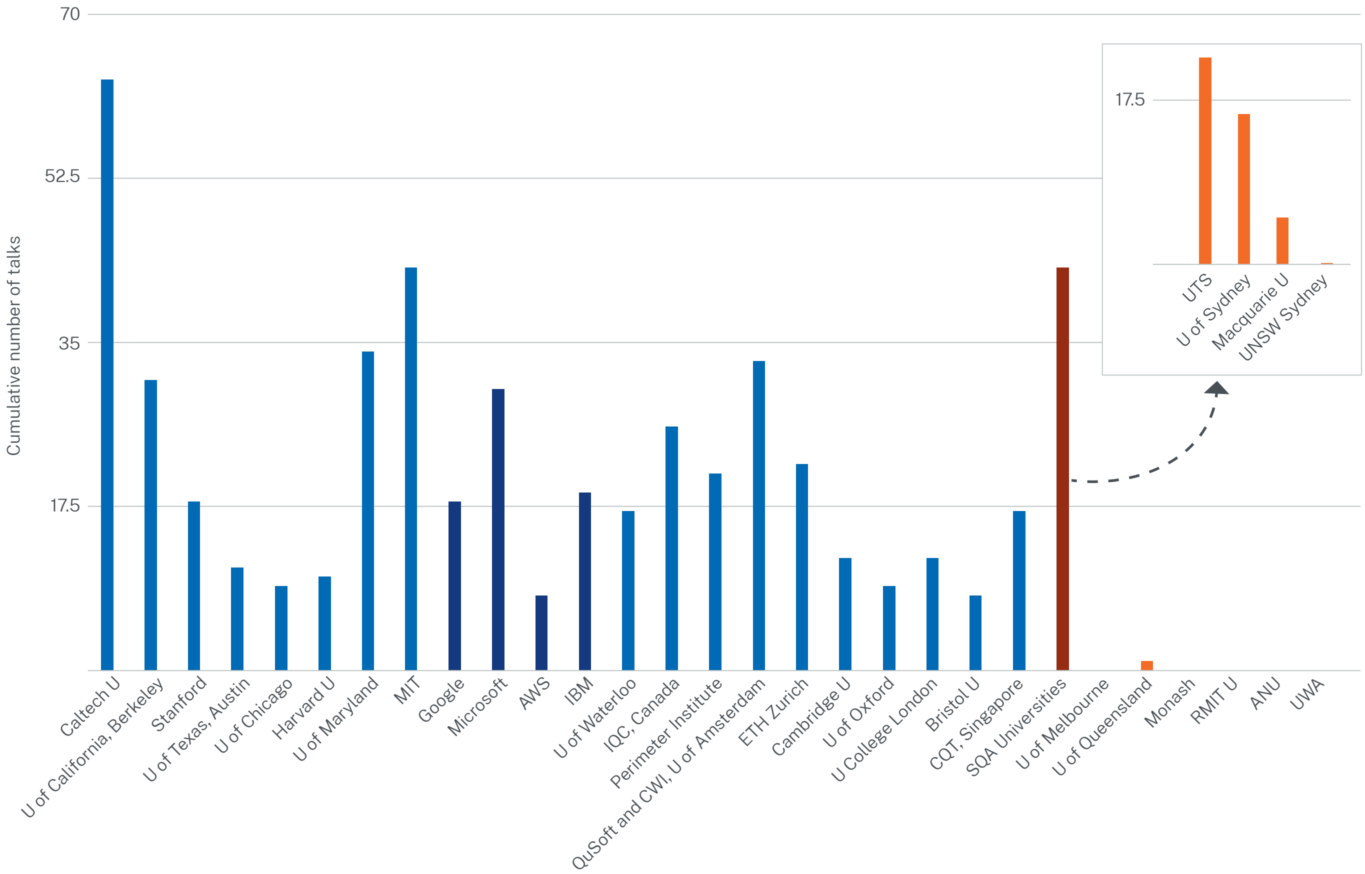


Figure 15. Cumulative paper acceptances at the most prominent QAST conference in the world, QIP, from 2017-2021, categorised by institution. The SQA universities in NSW rank joint second (with MIT) in the total number of papers accepted at QIP. University has been abbreviated to U in the figure.

Measuring the number of talks at QIP is a reasonable indicator of high-quality outputs of research in theoretical quantum computing, especially in the aspects of this research that overlap with the information sciences. It should be noted, however, that this is a clear bias of the data. It is much less likely to showcase research on quantum physics for the sake of physics or experimental implementation, which does exclude quite a lot of important research by the theoretical quantum physics community. However, for the purposes of this report, this bias is appropriate. Examining publicly available data on talks at QIP between 2017-2021, a count has been made of the number of times affiliations have appeared on these works and the scores have been plotted for the top universities as well as Google, IBM, Microsoft and AWS, which are the most featured corporations at QIP (Figure 15).

Examining this data, it can be seen that many of the world's leading universities are featured prominently, with the Caltech scoring considerably higher than every other institution and the Massachusetts Institute of Technology (MIT) ranking second. Collectively, the output of the SQA universities is equal to that of MIT and roughly comparable with the San Francisco Bay Area.

UTS ranks first amongst the Australian institutions and seventh overall. This has UTS ranked alongside leading research institutions such as ETH, Zurich (Switzerland) and the Perimeter Institute (Waterloo, Canada) and outperforming leading corporations IBM, AWS and Google, and world-renowned universities such as Stanford, Harvard, Cambridge and Oxford. The University of Sydney is a close second for Australian institutions and outperforms Harvard, Cambridge and Oxford. The only other Australian entities with talks at QIP were Macquarie University with five talks, and the University of Queensland with one.

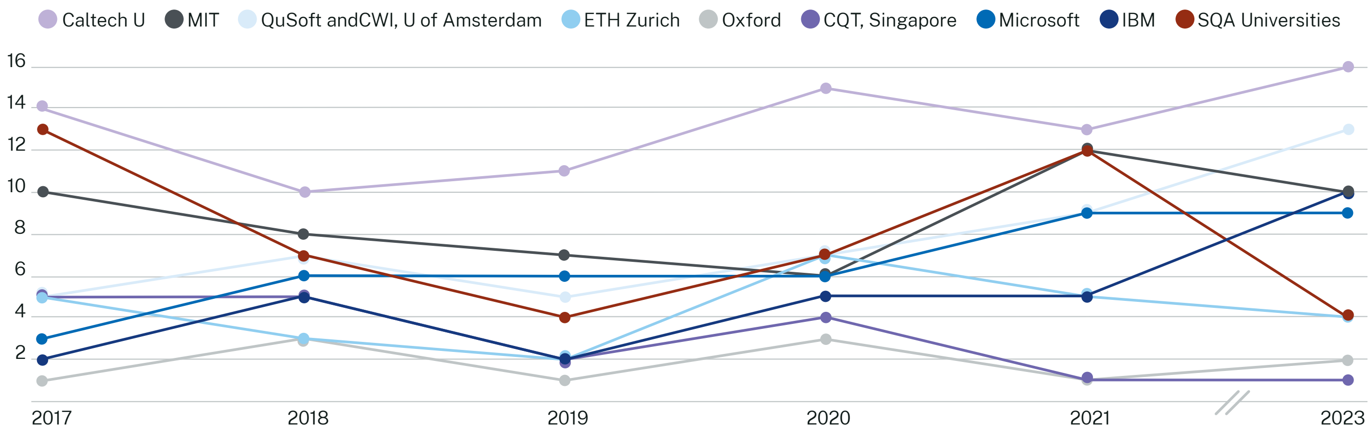


Figure 16. Accepted QIP talks from 2017-2023 for a subset of institutions. A decline in NSW and Australian-based institutions is observed as a function of time. This tracks with a general loss of senior expertise in QAST that began in Australia in approximately 2018-2019. Data is not available for QIP 2022.

Diving deeper, however, a more disturbing trend is noted for Australian institutions, especially when accounting for 2023 data[295] (Figure 16). Not surprisingly, continued strong performance can be seen at Caltech and MIT, but importantly growth in output can be seen at key institutions worldwide that have received increased government support as the activities in the sector have grown. However, the Australian institutions have remained stagnant, or even declined in the last few years as the rest of the world is ramping up activity.

The US universities such as the University of California, Berkeley,[296] the University of Chicago[297] and the University of Maryland[298] are the epicentres of new initiatives that have come about through the US national quantum initiative. Importantly, the US initiative has built on existing capabilities, without cutting existing strengths, such as the longstanding effort at Caltech.[299] Likewise, it can be seen that QuSoft, in the Netherlands, has increased capacity because of strategic research initiatives by the Dutch Government.[300]

National strategic initiatives in the US, Europe and China, combined with the scale-up of the quantum industry and the relative lack of funding, have made it increasingly difficult for Australian universities to retain[301] and attract highly trained QAST researchers, especially those working at the cutting edge of quantum algorithms and complexity theory research. This provides appreciable risk to the generation of the QAST pipeline and quantum application development IP in Australia.

[295] Note that 2022 data was unavailable for comparison at the time of compilation of the report.
[296] https://ciqc.berkeley.edu/.
[297] https://chicagoquantum.org/.
[298] https://mqa.umd.edu/.
[299] https://iqim.caltech.edu/.
[300] https://qusoft.org/.
[301] https://twitter.com/hbar_consultant/status/1411247731067133952.

8. Commercial opportunities in quantum algorithms and software

Arguably, use case development for quantum algorithms has been the main driver of commercial activity in the quantum software space. In 2021, McKinsey estimated that up to US$700 billion of value could potentially be impacted by quantum algorithm use cases in the automotive, pharmaceutical, chemical and finance sectors.[302] A service industry in helping existing companies determine whether quantum algorithms are a solution to existing or potential future computational bottlenecks in their businesses is emerging. Use case development is being offered as a service by major consultancies[303,304] and startups alike. Large technology companies in quantum computing are also working closely with partners to understand the potential industrial landscape and market size. Significant government programs such as the DARPA Quantum Benchmarking program[305] are working to concretely quantify the improvements that can be yielded from quantum algorithms and to deliver industry benchmarks that can be tied to the utility gains from quantum computers.

There are three pillars to use case analysis and quantum application development:

1. close collaboration between quantum algorithms experts and subject matter experts SMEs from industry to determine where there exist key computational bottlenecks and whether existing quantum algorithms could be used to address them
2. resource estimation to predict the scale, time frame and cost of deployment of a quantum application, often relative to existing classical costs
3. new research by quantum and subject matter experts SMEs into new algorithms, methods of error correction and other intellectual property relevant to a potential use case.

In many cases, these studies are based on the known quantum algorithms for quantum simulation, optimisation and equation solving, and involve determining how they can be optimised or varied to adapt to a commercially relevant scenario.

Thorough use case analysis can typically take months to perform, usually involving a range of quantum and SMEs working together to determine where quantum computing may play a role in an industrial problem. Given that much of the technology stack for quantum computing is not mature, significant theoretical expertise is currently required for this analysis.

Given the scale of the market for developing quantum applications, many companies are developing software tools to accelerate use case analysis. Importantly, this is also being done to take the first steps towards developing the essential components of a more mature quantum 'software stack'. Like classical computers, quantum applications are built on a stack of interdependent technologies that manage and optimise the task of performing a computation.

There are many commercialisation opportunities for business, both in the creation of new use cases for quantum computing and in the development of tools associated with the quantum software stack. While there is no definitive version of a quantum software stack yet, presented in the following section is a version of this intended to capture the key elements of these technologies and some of the key companies working on them.

[302] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know.
[303] https://kpmg.com/xx/en/home/services/advisory/management-consulting/technology-consulting/quantum-technologies.html.
[304] https://www.bcg.com/capabilities/digital-technology-data/emerging-technologies/quantum-computing.
[305] https://www.darpa.mil/program/quantum-benchmarking.

	Quantum algorithms and complexity	Quantum programming theory	Fault-tolerant architecture design	Quantum control and charactersation	Quantum hardware and device physics
Applications	●				
Programming language/software verification	●	●			
Performance analysis/ benchmarking	●	●			
Quantum algorithms	●	●			
Logical quantum compiler/resource estimation	●	●	●		
Error correction compiler/resource estimation	●	●	●	●	
Processor/network architecture			●	●	●
Control software and hardware verification			●	●	●
Hardware			●	●	●

Figure 17. Elements of the quantum software stack and how they intersect with sectors of the QAST community.

8.1 Programming language and software verification

Current programming and data structures for quantum information technologies are built for NISQ hardware, not quantum computers that can solve large-scale problems. To recognise the utility of quantum computers and networks, data structures and programming languages need to be developed to allow for efficient integration with classical programming languages and computing systems. In addition, quantum programming languages will also need diagnostics and software verification tools. Classical model checking and verification tools will need to be incorporated into the software systems that drive quantum devices to enable debugging tools comparable to the standards expected in today's classical computing systems.

Industry examples: While there has been some significant academic work in this area, few companies are developing programming tools beyond what is required for the NISQ era. Some exceptions include software developed by Horizon computing[306] and the Microsoft Q#[307] programming language.

8.2 Performance analysis/benchmarking

Analysing the performance of quantum algorithms in a sophisticated application requires the development of benchmarks and tools to test their integration with other software. Key to this is the creation of algorithm benchmarks that integrate with quantum technologies, and analyse best-practice in classical complexity theory, operations theory and algorithms research.

Industry examples: Industry-accepted benchmarks for optimisation and AI are now commonplace. Quantum-specific tools for these purposes are under development in the DARPA Quantum Benchmarking Program by companies such as HRL Laboratories, L3Harris, Zapata and Riverlane. Recently, Google Qualtran[308] was released which has functionality in this direction.

8.3 Quantum algorithms

The continued development of quantum algorithms is a high value activity within the field that will continue to evolve as quantum computers become more sophisticated. The adaptation of new quantum algorithms to use cases is a commercial activity that a number of quantum corporations perform as a service.

Industry examples: There are many companies working on the development of new quantum algorithms. Google, IBM, Microsoft and AWS all have significant efforts in quantum algorithm research. There are also some very notable startups including HQS Quantum Simulations,[309] Phasecraft[310] and QCWare.[311]

8.4 Logical quantum compiler/Resource estimation

Programming languages and software tools that enable high-level programming languages to deploy subroutines on classical and quantum information processing hardware will be essential for developing and assessing high-impact quantum technologies. Today's computers utilise sophisticated virtual layers that transition code from a compiler to an optimised intermediate representation, suitable for deployment to an instruction set to a processor. In the future, quantum devices will be made more complicated due to the interplay between quantum and classical processor characteristics.

Industry examples: High-level logical compiling of this type is very much still a research question. Some work in this direction has been undertaken by Horizon computing[312] and IBM Qiskit Runtime,[313] however, there is much more work to be done over the coming decade.

[306] https://www.horizonquantum.com/.
[307] https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk.
[308] https://github.com/quantumlib/Qualtran.
[309] https://quantumsimulations.de/.
[310] https://phasecraft.io/.
[311] https://www.qcware.com/.
[312] https://www.horizonquantum.com/.
[313] https://www.ibm.com/quantum/qiskit-runtime.

8.5 Error correction compiler/Resource estimation

Optimising the logical instructions relative to the error correcting codes supported by an architecture is essential for minimising the resource cost of quantum applications. This task involves taking in the logical level instructions and identifying the appropriate code and how it should be implemented relative to the processor architecture of the computer.

Industry examples: The optimisation of error-corrected circuits is becoming increasingly sophisticated. Significant work in this direction has been done in industry by Riverlane,[314] PsiQuantum,[315] Google Quantum AI, AWS and IBM, for example. Automated resource estimation tools are emerging to help with application development, for example the Microsoft Azure Quantum Resource Estimator[316] and the BenchQ platform being co-developed by Zapata, Rigetti and UTS.[317]

8.6 Processor/Network architecture

Future large-scale quantum processors are likely to consist of a sophisticated processor architecture including elements of quantum and classical computing resources. Error correction and quantum control systems will be very dependent on how the processor architecture is designed, and how information can be transported around the processor.

Industry examples: Quantum processors are still in a relatively early phase of development, and development of large-scale architectures is still underway. IBM and Google indicate on their roadmaps that this is work under development.

8.7 Control software and hardware verification

As quantum devices become more sophisticated, the problem of certifying their quality, verifying that they are working as planned, and varying the way in which they are controlled becomes extremely difficult. The same features that make quantum computers powerful, also make them difficult to characterise and certify. New software-based methods to allow for the certification, verification, calibration and control of devices at both the quantum level and via their integration with classical systems will need to be deployed.

Industry examples: There are many companies deploying a range of techniques integrating control theory and AI to improve the control and verification of quantum hardware. A key activity is working out how to deploy such techniques leveraging classical hardware at cold temperatures. Examples include Q-CTRL,[318] Microsoft, Keysight,[319] Google and IBM.

[314] https://www.riverlane.com/.
[315] https://www.psiquantum.com/.
[316] https://learn.microsoft.com/en-us/azure/quantum/intro-to-resource-estimation.
[317] https://github.com/zapatacomputing/benchq.
[318] https://q-ctrl.com/.
[319] https://www.keysight.com/us/en/solutions/emerging-technologies/quantum-solutions.html.

9. Recommendations

The development of quantum applications is the commercial driver of quantum computing and the ultimate reason for investment in quantum computing hardware. A strong and vibrant development ecosystem is vital for discovering and capturing the benefits of quantum computing. While there is significant commercial potential, fundamental research is still required to understand how best to utilise the advantages of quantum processors. Quantum application development has entered a new phase, where industry-based subject matter experts SMEs are regularly working with QAST researchers to flesh out the details of potential quantum computing applications to determine if and when they might be deployed. However, these activities are currently limited by the availability of highly educated specialists in quantum algorithms.[320,321] For these reasons, in the near future, securing QAST talent is essential for value capture in quantum computing.

The development of strong research, training and commercialisation pipeline in QAST is an opportunity for Australia that has yet to be fully exploited. Contrasted with hardware development, QAST is critical for realising the potential of quantum technology, an area that Australia historically and currently excels in, and is comparatively inexpensive. NSW should endeavour to foster an expansion of QAST, to invest and expand QAST-related activities, become a recognised leader internationally and solidify expertise for education and training. This will allow Australia to provide needed technical infrastructure to incentivise further startup creation focused around QAST activities. The establishment of an institute, taking the best practises from world-leading institutes in the US,[322] Canada[323] and Japan,[324] but focused exclusively on QAST research, will allow NSW to gain a foothold in this critical aspect of the quantum ecosystem.

Provided below are potential action items within the scope of QAST that could significantly strengthen NSW's place within the global quantum ecosystem and solidify an international reputation as a global quantum hub.

[320] https://foreignpolicy.com/2023/07/31/us-quantum-technology-china-competition-security/.
[321] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/five-lessons-from-ai-on-closing-quantums-talent-gap-before-its-too-late.
[322] https://www.kitp.ucsb.edu/.
[323] https://perimeterinstitute.ca/.
[324] https://www.oist.jp/.

9.1 ACTION ITEM 1 A world-class research institute for QAST research

The establishment of a flagship, world-leading institute that is focused on QAST research would be a drawcard for internationally renowned talent in the space. This would provide a vital pipeline of IP and know-how into the local commercial ecosystem, providing a competitive advantage to local industry. Given a sufficient concentration of talent, a QAST-dedicated research institute could be a catalyst for continued growth of the local quantum industry.

The ongoing development of quantum technologies requires a strong R&D effort into QAST. Determining what can be done with quantum computing, sensing or communications as the technology becomes ubiquitous will be critical in realising commercial outcomes from intellectual property over the coming decades.

In contrast to the development of quantum hardware, R&D in the QAST space is inexpensive. The ability of a nation or a geographic region to have a significant advantage in this part of the quantum ecosystem is effectively a question of hiring people. While Australia already has a notable pool of research expertise in the QAST space, it is not sufficient for the nation to maintain ongoing leadership in an increasingly competitive international ecosystem.

9.2 ACTION ITEM 2 Government support to increase teaching and skills capacity

Government programs that provide additional funding for research and research training will continue to be important over the next decade. The SQA and ARC CoE programs have been essential for the development of the existing quantum ecosystem, providing both direct funds for research and training but also providing motivation for universities to expand their faculty. However, as the industry grows, so will the demand for talent and enhanced research and training programs will continue to be necessary.

The existence of an exceptionally strong QAST research base in Australia also contributes to the growth of the local talent pipeline in quantum. As has been detailed, both in CSIRO's assessment of the Australian quantum landscape to 2045[325] and in the National Quantum Strategy,[326] it is anticipated that for Australia to take full advantage of the opportunities available from the global quantum ecosystem, a quantum workforce of 16,000 would be needed by 2040 (with over 10,000 working in quantum computing).

Reports indicate that industry has a significant need for higher degree research training in quantum technology roles,[327] with many companies indicating that PhD level experience is required for a significant fraction of roles. While these numbers are preliminary, and expected to change with time, it is clear that there is strong demand internationally for specialist training in quantum technologies, and especially in QAST as these skills are essential for quantum application development. If Australia is to achieve the proposed workforce targets, training capacity must be increased. Specifically, this means that Australian universities need to retain PhD-qualified academics that are ideally internationally competitive.

[325] https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/csiro-futures/future-industries/quantum.

[326] https://www.industry.gov.au/publications/national-quantum-strategy.

[327] Greinert F et al. (2023) 'Future quantum workforce: Competences, requirements, and forecasts', *Physical Review Physics Education Research,* 19:010137.

9.3 ACTION ITEM 3
A research skunkworks for new NSW spinouts

The idea of a quantum skunkworks for the QAST community is somewhat akin to the types of infrastructure support the experimental community has built up in other areas. There is an entire profession within the experimental and hardware side of quantum information science, dedicated to the technical tools and services a researcher would need to start a world-class effort in quantum hardware. This takes many forms in Australia, from the Australian National Fabrication Facility[328] to the Semiconductor Sector Service Bureau[329] to the infrastructure and lab technicians employed by larger institutions such as the University of Sydney or UNSW Sydney. All of this exists to support the extremely complex and capital-intensive tasks of materials fabrication, testing and packaging needed to take the ideas of a university research team and produce the first working demos. This can then be used to solicit the funding to establish prototypes at a sufficiently high readiness level to gain entry into an accelerator program or to attract funding to further progress the project.

In the QAST space, an entity that enables researchers to progress theoretical ideas to a higher technology readiness level, or to take the first concrete steps towards commercialisation, would be highly valuable. Access to technical capability to translate a research paper into something more tangible is essential, giving researchers additional capability to solicit the first stage of funding from a government grant, angel investor or company. Such an entity could work in concert with bodies such as the announced federally funded quantum growth centre[330], or other programs such as the CSIRO On program[331], the Blackbird Giants Program[332], Cicada Innovations[333] or other accelerator programs.

The QAST community does not have its equivalent. Once an academic paper is written and submitted, that is usually where the process ends and researchers move onto the next project. Occasionally, researchers will find a collaboration with an experimental group or company and take the next steps, but this is almost always financed by the external partner in exchange for the IP rights underlying the theoretical idea. There is very little support for QAST researchers to independently develop an idea as a software platform or protocol stack to drive their own spinout that can sell for additional capital rather than trade the underlying IP simply to get it one step further than an academic paper.

As with anything QAST-related, the concept of a type of skunkworks for the software and theory community would be significantly cheaper than the type of infrastructure necessary for quantum hardware. Elements of the skunkworks could be, for example:

- dedicated coders and software development teams that can take high level and often dirty academic code bases and turn them into stable, production level libraries
- front- and back-end developers that can help build cloud services for a research idea that can be delivered to customers over the internet
- electronics and device engineers that can help prototype a physical product (for example, a new microwave control system for superconducting or solid-state qubits) that has arisen from research into quantum control theory
- security engineers that have the expertise to implement a prototype of a new post-quantum cryptographic scheme.

These types of resources would be invaluable to QAST researchers, and they are critical in turning what is usually pen and paper into something that can be demonstrated to non-experts or investors.

[328] https://anff.org.au/.
[329] https://s3b.au/.
[330] https://www.industry.gov.au/news/help-create-australias-centre-quantum-growth.
[331] https://www.csiro.au/en/work-with-us/funding-programs/Innovation-programs.
[332] https://www.blackbird.vc/programs/giants
[333] https://www.cicadainnovations.com/.

Published by the Office of the NSW Chief Scientist & Engineer

chiefscientist.nsw.gov.au

Title: Quantum Algorithms and Applications
First published: March 2024

Office of the NSW Chief Scientist & Engineer

NSW
GOVERNMENT