



Australian Government

Defence



EMERGING DISRUPTIVE TECHNOLOGY
ASSESSMENT SYMPOSIUM

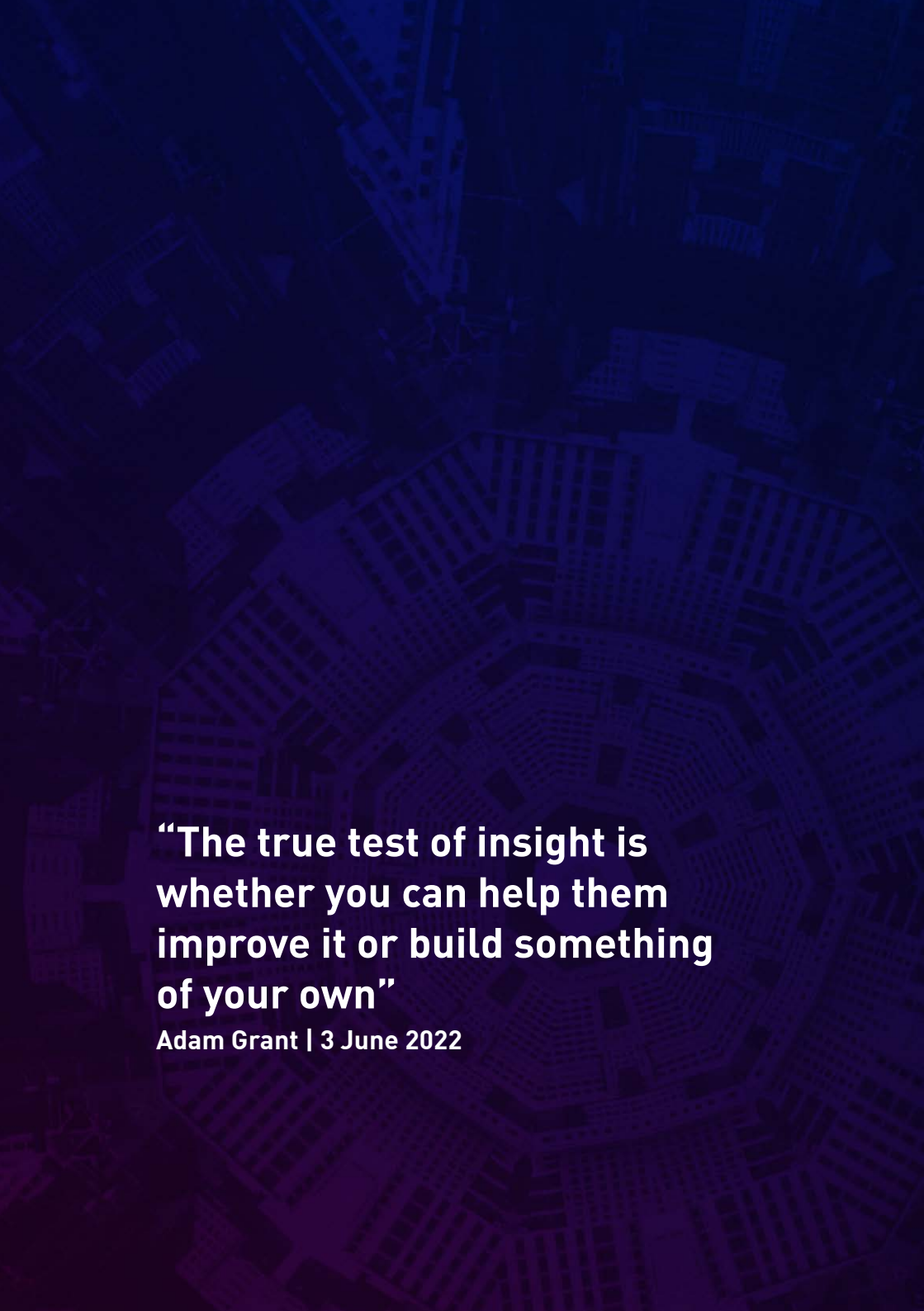
QUANTUM COMPUTING

INSIGHTS PAPER

Noetic

Acknowledgements

The author of this paper is Noetic under contract to the Department of Defence. Noetic would like to acknowledge the insights provided during subject matter expert interviews of a range of people drawn from academia, industry, and Defence, which underpin the development of this paper. This paper also leverages previous work undertaken by Noetic and Defence Science and Technology Group (DSTG) for the 2021 *Quantum Computing: In Focus* event. Noetic also wishes to acknowledge the review and arising comments on the draft paper provided by DSTG and EDTAS Technology Opportunities Event Partners.

An aerial photograph of a city grid, viewed from a high angle. The streets form a complex pattern, with a prominent octagonal shape in the center. The image is overlaid with a dark blue gradient, making the text stand out.

**“The true test of insight is
whether you can help them
improve it or build something
of your own”**

Adam Grant | 3 June 2022

Contents

ACRONYMS AND ABBREVIATIONS	6	Autonomy	27
EXECUTIVE SUMMARY	8	Factoring	27
INTRODUCTION	10	Data Security	27
General	10	Linear Algebra and Artificial Intelligence/ Machine Learning (AI/ML)	27
Background	10	CHALLENGES	29
Aim	10	Technical	30
Scope	11	Regulatory	33
Approach	11	Societal	33
Impact Areas	11	Environmental	35
Quantum Computing	12	Ethical	36
Quantum Computing Future	12	Political	37
Technology Overview	12	Sovereignty	38
Quantum Technologies Ecosystem	13	ENABLERS	41
A Quantum Computing Stack	15	Overview	42
USE CASES	17	Academia	43
Quantum Computing Evolution	18	Industry	44
Quantum Computing in 2040+	21	Commercial	47
Algorithms and Applications	23	Collaboration	49
Chemistry	24	Additional Australian Context	50
Materials	24	CONCLUSION	51
Pharmaceutical	25	Conclusion	52
Optimisation	26	Annexes	53
Finance	26		
Logistics	26		

**ANNEX A USE CASE
(APPLICATION) TO IMPACT AREA
MAPPING 54**

**ANNEX B ADDITIONAL QUANTUM
COMPUTING INFORMATION 57**

Quantum Computing Functionality	57
Quantum Features	60
Key terms	60
Gate-models vs quantum annealing	62
Stack Consideration	64
General	64
Algorithms and Application	64
Software, Compilation, and Control	65
Hardware	67
Selected Hardware Technology Developers	68
Qubits and Materials	75
Qubit Architectures	76
Qubit Housing	78
Networking and Integration	80
Technology Readiness Level (TRL) Across the Stack	82
Quantum Communication	83
Quantum Sensing	84

**ANNEX C ADDITIONAL
AUSTRALIAN CONTEXT 86**

General	86
Australia's Quantum Talent	87
Sydney Quantum Academy (SQA)	88
Australian Quantum Capability	89
Pawsey Supercomputing Centre and Quantum Brilliance Quantum Supercomputing Hub	90
Building Australia's Quantum Ecosystem	91
Technology Pathways	92
Benchmarking and Standards	92

Acronyms and Abbreviations

AC2	Agile Command & Control
AI	Artificial Intelligence
AI/ML	Artificial Intelligence/ Machine Learning
ARC	Australian Research Council
BLOS	Beyond-line-of-sight
CandC	Cyber and Communications
CBRN	Chemical, Biological, Radiological, and Nuclear
CDS	Chief Defence Scientist
QCC2T	ARC Centre of Excellence, Centre for Quantum Computation and Communication Technology
CPU	Central Processing Unit
DARPA	Defense Advanced Research Projects Agency (US)
DSTG	Defence Science & Technology Group
DWE	Disruptive Weapon Effects
EDTAS	Emerging Disruptive Technology Assessment Symposium
EM	Electromagnetic

EQUS	ARC Centre of Excellence, Centre for Engineered Quantum Systems	PC	Personal Computer
FTQC	Fault Tolerant Quantum Computing	PNT	Position Navigation and Timing
GEO	Geostationary Earth Orbit	QAPNT	Quantum Assured Position, Navigation, and Timing
GLOSNASS	Global Navigation Satellite System (Russia)	Q-CTL	Quantum Control
GPS	Global Positioning System (US)	QEC	Quantum Error Control
GPU	Graphics Processing Unit	QKD	Quantum Key Distribution
HAQC	Heuristic and Approximate Quantum Computing	R&D	Research and Development
HPC	High Performance Computing (using classical computers)	RF	Radio Frequency
IDM	Intelligent Decision Making	RMMS	Resilient Multi Mission Space
IOT	Internet of Things	RUS	Remote Undersea Surveillance
IW	Information Warfare	S2M	Sensing and Sense Making
oK	Degrees Kelvin (temperature)	STaR Shots	Science, Technology and Research Shots are challenging, inspirational and aspirational S&T missions that will align strategic research to Defence's force structure priorities
LOQC	Linear Optical Quantum Computing	STEM	Science, Technology, Engineering, and Mathematics
ML	Machine Learning	SWaP	Size, Weight, and Power
NGTF	Next Generation Technologies Fund	TRL	Technology Readiness Level
NISQ	Noisy Intermediate Scale Quantum	UAV	Unmanned Aerial Vehicle
NV	Nitrogen Vacancy	VQE	Variational Quantum Eigen
OQC	Optical Quantum Computing		
P2	People and Platforms		

Executive Summary

The focus of the Emerging and Disruptive Technology Assessment Symposium (EDTAS) on Quantum Computing is to engage the National S&T Enterprise to develop a comprehensive and evidence-based understanding of the technology field. The EDTAS will provide a forum for exploring Australia's strategic needs, future quantum computing R&D directions, and an array of potential use cases. The outcomes of the symposium will be used to inform Defence's framing of relevant challenges and shape future strategy, policy and programs to deliver outcomes for Defence, National Security and the National Interest.

Research drivers, challenges, and opportunities around the following key components of the quantum computer 'stack' will be explored:

- + Hardware and qubits
- + Software, compilation, and control
- + Algorithms and applications
- + Networking and integration
- + Full-stack implementation

The advancement of quantum computing could come through the scaling, or an alternative configuration, of an existing quantum technology, the development of innovative quantum materials, or the discovery of algorithms with new computational benefits. As the quantum computer stack evolves along multiple pathways, it is envisaged that potential new use case will emerge, supported by integration with other technologies and systems. The EDTAS will explore use cases in a future problem space – exploring possibilities beyond what is currently viable today.

Four impact areas will focus the technology opportunities offered by quantum computing at the EDTAS:

- + People and platforms
- + Sensing and sense making
- + Intelligent decision making
- + Cyber and communications

Quantum computing is rapidly evolving and competing technologies will deliver different benefits. Foresight is required to inform strategic choices about the balance of investment across a range of technology options, standards, supply chain arrangements and infrastructure. No matter the future pathway, extensive collaboration across government, academia, and industry will be required to ensure the benefits of quantum computing can be realised for the national interest.

This paper does not intend to be definitive. Rather, the broader themes discussed in this paper will set the scene for EDTAS Quantum Computing. In addition to the anticipated exploration of quantum computing use cases, part of the foresight process requires examining potential second- and third-order effects. The intent is for the Technology Opportunity Symposium to allow participants to do this in an immersive future scenario.

Introduction

General

Background

Defence is seeking to better understand the opportunities, threats and challenges quantum computing presents. 'More, together. Defence Science and Technology Strategy 2030', recognises the criticality of creating scale and partnering with publicly funded research agencies, universities, large companies, and small to medium enterprises to advance Defence's understanding of the impact of quantum computing.

To do this the Defence Science and Technology Group (DSTG), in partnership with Noetic, will hold an Emerging and Disruptive Technology Assessment Symposium (EDTAS) to explore potential quantum computing advances in the 20+ year's timeframe (that is, 2040 and beyond). The Technology Opportunities Symposium engages a broad audience of academia, government and industry from Australia and like-minded international partners. The Technology Opportunities Symposium will feature a diverse range of expert presentations and facilitated immersive workshops to draw key insights on the subject areas. DSTG will capture the output from the workshop to help inform Defence's framing of relevant challenges and shape future strategy, policy and programs to deliver outcomes for Defence, National Security and the National Interest.

Aim

The aim of the Insights Paper is to present key themes relating to recent and projected developments in quantum technologies, with a specific focus on quantum computing, to provide a base level of common awareness to inform EDTAS participants and help engender debate during the symposia. To achieve this aim, the Insights Paper identifies and discusses current thinking related to quantum computing, thereby building a foundation for discussions during the Technology Opportunities Symposium (22-23 June 2022).

Scope

This paper does not intend to be definitive. Rather, the broader themes discussed in this paper will set the scene for EDTAS Quantum Computing to assist discussion during the panel session and syndicate activities. In addition to the exploration of quantum computing use cases, part of the foresight process requires examining potential second- and third-order effects. The intent is for the Technology Opportunity Symposium to allow participants to do this in an immersive future scenario.

Approach

SMEs in academia, industry and Defence were identified and then invited to participate in an explorative, structured interview. The thoughts and insights arising from SME interviews have provided the foundation for the development of this paper. These insights have been supplemented by desktop research. To support the subject matter, additional explanatory and contextual material is provided in annexes at the back of the paper.

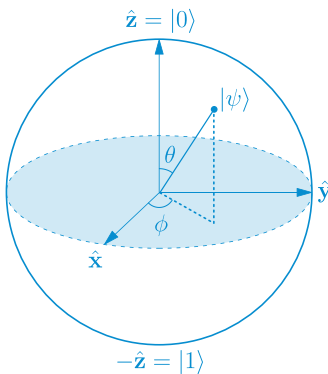
Impact Areas

As quantum computing evolves, it is envisaged that identified use cases and their associated algorithms will broaden to enable other technology areas and opportunities. Four impact areas and their associated use cases will be addressed in the Technology Opportunities Symposium. These impact areas are: people and platforms; sensing and sense making; intelligent decision making; and cyber and communications. An example of potential use cases (algorithms) mapped to impact areas for technology opportunity is provided in Annex A.

Quantum Computing

Quantum Computing Future

Given the current state of technological maturity, most SMEs interviewed were cautious in predicting what the quantum computing environment would look like in five to ten years, and were hesitant to speculate beyond twenty years. However, the conjecture appears to be the range of qubit technology opportunities, their ability to scale, the degree of collaboration for quantum computing to be fully realised as an integrated service, and the degree of collaboration required to realise the capabilities enabled by quantum computing.



Qubit

/'kju:bit/

Basic unit of
quantum information

“The qubits of today will not be in the quantum computers of tomorrow.”

“It’s like asking someone to build a skyscraper when the bricks haven’t been invented.”

Technology Overview

Quantum computing uses quantum phenomena to create a new way of computing. Quantum computers will be able to solve certain types of computational problems that are currently intractable with classical computers. Quantum mechanics also has applications in advanced

communications and sensing. Quantum computing and other quantum technologies are expected to enable a range of future technologies and capabilities. Even now there are a wide range of nascent quantum computing technologies, and other quantum technologies, which have been implemented and are commercially available.

Quantum computing has the potential for significant disruption that whilst not yet realised, is being heavily researched by many nations across the globe. There are already proof-of-concept systems operating, but these are currently limited in scale and real-world application. A fault tolerant computer will only come from ongoing investment.

The consensus is that quantum advantage – i.e. a real-world application where quantum computing outperforms classical computing – whilst still years away, is just a matter of time. Quantum advantage is however application specific, each requiring specific performance characteristics of quantum computers for implementation. This will lead to realisation of applications over a range of timeframes. As such, the key question raised is: When and for what problem might quantum advantage or supremacy be achieved?

Quantum Technologies Ecosystem

Whilst quantum computing has the potential for massive disruption, the quantum technologies ecosystem includes other technologies and uses, such as quantum communication, quantum sensors, quantum materials, quantum simulators, and quantum metrology. These technologies should not be seen as separate pillars but as an ecosystem where each element benefits from advances in others, and integrated with other technologies such as high performance computing and machine learning. Together these technologies have the potential to deliver revolutionary impacts across sectors such as health, automotive, mining, space, defence and finance.

The advancement of quantum computing will come through scaling and there are multiple pathways. It can be formed from existing quantum technologies, through the ongoing development of innovative quantum

materials, or the discovery of algorithms with new computational benefits. As quantum computing technologies evolve along multiple pathways, it is envisaged that potential new use cases will emerge, supported by integration with other technologies and systems.

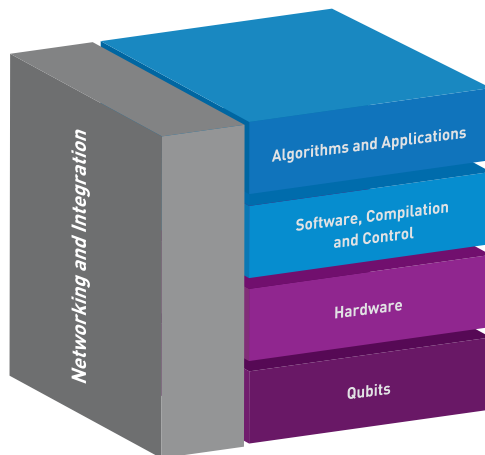
Understanding the impact of quantum computing is complicated due to the different rates of progress, levels of maturity and expected timelines required for development of different quantum technologies. As an example, while gate-based quantum computers are yet to approach a similar number of qubits to quantum annealers, they can solve a wider range of problems efficiently.

In addition to the diversity in performance characteristics, the features and specifications of systems vary across different technologies. Amongst other considerations, this includes scalability; portability; likely interoperability with existing systems and with other quantum systems; reconfigurability; size, weight, and power (SWaP); cooling; maintenance; cost requirements; quality of qubit; and error rates (both in terms of error rate per gate and in preparation and measurement). Ultimately, the future state of quantum computing technology will likely involve several different technologies designed for different applications, accompanied with discrete generations of technologies over time.

A Quantum Computing Stack

The quantum computing stack is largely analogous to the classical computing stack. It provides a conceptual framework to understand the different technologies and how these interact. While the stack provides a simple and useful representation of the technologies, the reality is considerably more complex.

Figure 1. The quantum computing stack.



The composition of the stack varies according to the type of development and Figure 1 illustrates a simplified version of a typical stack¹ with networking and integration added to highlight the integration across the stack, but also connection to other devices in a larger system. As is the case for electronic gates and classical computers, the underlying qubit hardware is only one component of quantum computing systems. They require control systems, software, algorithms, and applications that can harness quantum computing to provide real-world application.

¹ See National Academies of Sciences, Engineering, and Medicine 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. (Page 150) <https://doi.org/10.17226/25196>.

In broad terms the layers indicated in Figure 1 are:

Algorithms and Applications. In this layer, applications are mapped into a set of quantum computer algorithms which together solve a specified problem. However, it needs to be acknowledged that quantum computers are co-processors, and that the vast majority of applications will require orchestration of quantum and classical computers working together.

Software, Compilation, and Control. This layer includes a quantum programming language, which the algorithms required are translated into:

- + A compiler that maps these programs to logical qubit operations
- + A scheduler and optimiser for the logical qubit operations
- + Error correction firmware within which logical qubits are mapped to underlying physical qubits.

Hardware. This layer includes physical level schedulers, optimisers, and device control firmware.

Qubits. In this layer specific pulses are produced which control each qubit. In addition this layer includes readout of qubit values. These values are fed back up to higher layers to implement fault tolerant error correction and calculation output.

Networking and Integration. Communication and quantum state transfer between quantum computers for distributed computation and communication, including integration with hybrid systems and networks.

Further explanatory information regarding quantum computing and 'the stack' is contained in Annex B.

USE CASES

Quantum Computing Evolution

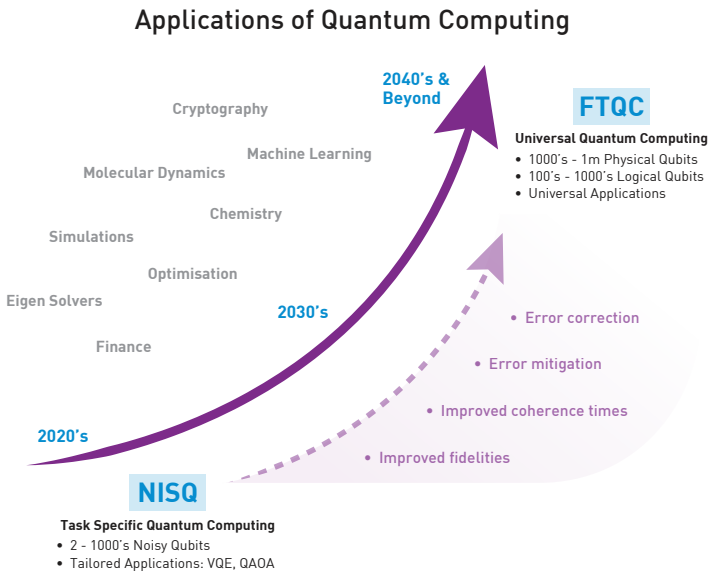
The evolution of quantum computing is likely to mimic the evolution of classical computing, where we evolved from the first transistor back in 1947 to the integrated circuit in 1958, before the first commercial applications in the mid 1960's and first computers available in the 1970s. As such, the computers we currently use have taken over 7 decades of development. It would be expected that quantum computing will follow a similar trajectory of continuous improvement as it scales. A large-scale, universal quantum computer will therefore not suddenly appear without this technological development. And whilst there is no widely agreed upon timeframe for such a large-scale system to be available, it is generally believed to be at least two decades away. The technology is expected to evolve towards a fault tolerant quantum computing (FTQC) solution over time, as shown in Figure 2². However, it is important to realise that as the evolution of quantum computing occurs, through noisy intermediate scale quantum (NISQ) computing towards FTQC, it may lead to a great variety of applications and technologies that are currently unforeseen. As such, FTQC might not be seen as just the end state of quantum computing in and of itself, but a catalyst for the ongoing development of a whole quantum industry.

Progression through the NISQ phase of quantum computing and beyond will potentially lead to a future of quantum computing (2040+) that will be broader than what is able to be predicted now for FTQC. Appreciation of this concept enables quantum applications for use cases that do not rely on fault tolerance to be implemented today, with the likelihood that post 2040 there will be multiple versions of applications that have relied upon evolving hardware from the NISQ phase through to FTQC that have displayed various levels of sophistication and advantage over time. To this end, today's developers are aware of current hardware and are designing applications accordingly. Similarly researchers and developers knowing that hardware will improve are making implementations of current algorithms, plus new novel applications, with an eye for future

² Provided by the RMIT University, La Trobe University, H-Bar Quantum Consultants, Quantum Brilliance, and Pawsey Supercomputing Centre Partnership for the EDTAS Quantum Computing Symposium, 27 May 2022

hardware. Evidence of this point can be seen in the technology roadmaps released by quantum computing companies: DWave, Rigetti, Google, IBM, Quantinuum (formerly Honeywell), IonQ, SQC, Pasqal, Quantum Brilliance and Diraq, which show that they are planning significant activity in the development of useful quantum devices well before FTQC.

Figure 2. Overview of quantum computing evolution.



This simplified view of the potential evolution of quantum computing provides insight into how quantum computing will be used into the future. As quantum computing capability increases, solutions are likely to augment and complement current classical systems. It is not expected that quantum computing will ever replace classical computing; indeed classical computers will have a critical role in control, operation, and co-processing of quantum computers.

The key point is that NISQ scale devices are proving pivotal to explore and develop use cases for future devices now. The possibility of FTQC brought

about by successes in NISQ devices is changing industries today. The fact that researchers have shown that quantum computers will be able to run factoring algorithms, even if it is not at the scale that can beat a classical computer, just the idea that one could exist is forcing industries and governments to take steps now. This is being seen in banking, where public key encryption is widely used and could potentially be a target for quantum computer aided attacks. The likelihood of these events is forcing decisions to be made to change encryption methods now. This change is being prompted just on the idea that FTQCs may exist based on successes of current devices.

As with all technologies, the usability of quantum computing will be critical to its success. The ability to scale qubits in a stable, manufacturable system is critical. Quantum systems will need to be interoperable with classical systems to leverage the strengths of both in hybrid systems. It is important that this is accounted for from the earliest design stages of technologies. Another feature that would support rapid take-up is abstraction of the computation once the core technology is proven. This enables users to interact with different systems through a user interface without needing knowledge, understanding, or awareness of the specific underlying system(s) – potentially even whether calculations are being performed using either classical or quantum computation.

Quantum Computing in 2040+

It is anticipated that quantum computing will harness a new understanding of physics, akin to harnessing electricity in the 19th century, and will contribute to new discoveries that will be applied across society. Full benefit will be realised by the ability for all people to uptake and have access to quantum technology as it evolves. However, quantum computing is an emerging field, which means it is difficult to make predictions as the physics is still being explored, but what we know now should not constrain thinking with regard to technology opportunities.

Until error correction had been demonstrated in the late 1990s, there was scepticism regarding whether quantum computing was possible. However, since quantum error correction (QEC) has been demonstrated³ there has been a steady growth world-wide with many countries and organisations developing quantum computing strategies and plans. This has increased dramatically since the demonstration of quantum advantage by Google in 2019⁴. The importance of QEC is that when the physical error in hardware is low enough, quantum computation may then be extended to arbitrarily long algorithms, allowing the solution to much larger and more important computational problems.



Sourced from: <https://www.businessinsider.com/quantum-computing-investing-computers-enterprise-2021-3>

³ Experimental quantum error correction, Cory DG, Price MD, Maas W, Laflamme, R. et al., Physical Review Letters, Vol. 81, Issue 10, pp 2152-2155, 1998.

⁴ Quantum supremacy using a programmable superconducting processor, F. Arute et al, Nature 574, pages 505-510 (2019), >4000 citations.

Despite being at a relatively early stage of development, some argue that quantum computing has already changed computer science. For example, quantum computing has stimulated debates in computing and information sciences as to whether Alan Turing's (computational) model of what a computer is – which is what we have in the form of classical computers – is the most complete model of what computing could be or should be. With the advent of the quantum computing model it is now apparent that this is not the case, especially if you take efficiencies into account. Quantum computing is a more general model for modelling information and how information sciences work. It is considered more accurate and more tied to the physical world than what has been used before. As such, quantum computing has contested previous thinking regarding information and computing theory.

Many envisage quantum computing as a means to augment classical computers, not to replace them. Indeed, there will be a symbiosis. Development in quantum computing will improve classical computers e.g. classical computer programmers have derived better algorithms for classical computers from quantum algorithms. As such, classical computers will become more powerful alongside quantum computers. In some ways quantum computers are analogous to the turbo in a motor car, where it isn't needed all the time, but operates when it is required to enhance performance. Stand-alone quantum computers will also require classical computers to operate them.

In the coming years impacts from quantum computing may be seen in investment portfolio optimisation from financial institutions and other entities seeking high risk, but high pay off ventures. Similarly, impacts may be seen in encryption for secure transactions, which can potentially be offset by the upgrading to post quantum cryptography, but as quantum computing hardware emerges this will need to be continually monitored. Changes could be seen in the landscape of industry, from advanced manufacturing through to increased simulation capability, the study of new molecules within health sciences, improvements in robotics and autonomous systems, or new, currently unknown industries could emerge.

The 2040 epoch will be based on what we don't know. Predictions for quantum computing in this time and beyond are broad ranging. At the optimistic end, it is envisioned that we may start to see the emergence of full scale quantum computers, bringing transformations similar to classical computers, with quantum computing being pervasive and integrated into everything we have and do. At the other end is scepticism regarding its development and application, with it potentially only being useful for a small number of niche cases, but potentially transformative in certain sectors. However, consideration of how we approach the unknown potential for quantum computing may require consideration of competitive and/or adversarial intent i.e. what are the potential implications of not pursuing quantum computing?

Algorithms and Applications

Quantum algorithms work by exploiting quantum phenomena in clever ways that fit the architecture of a given problem. There are various applications for quantum algorithms. Currently, chemistry simulation algorithms are being developed to support the design of chemicals and the engineering of new materials. Many of these applications are fundamentally quantum mechanical. This is because determining electron energies for different molecules is more efficient using quantum computing. Optimisation is another area where quantum computing is likely to have an impact in problem solving. These types of algorithms support and enable decision-making in problems related to logistic issues, storage and distribution optimisation. Similarly, financial operations and portfolio management benefit from these types of optimisation algorithms. Additionally, there are factoring algorithms that will be used with future cryptographic systems to ensure privacy and security. At the edge, there are linear algebra algorithms used to train models for artificial intelligence/machine learning (AI/ML) applications.

Chemistry

Some of the earliest work on quantum computing has been related to highly complex chemistry modelling. In particular, optimisation of molecules that have applications in materials and pharmaceuticals design. Many portend that this is where the first impacts of quantum computing will be seen.

Materials

Excitement in the materials community stems from the vast potential for the development of advanced materials that could be used across a variety of industries and sectors, including the supporting of quantum computing itself through the development of materials that could enable advances in the operation and size of quantum machines. Other examples from respondents of what quantum computer designed materials may lead to include:

- + Allowing efficient energy transfer over long distances
- + Supporting better energy capture e.g. solar cell and battery efficiency
- + Achieving room temperature nitrogen fixation
- + Supporting high speed rail and enhancing the speed and mobility of other transport platforms in different environments
- + Delivering better protection and survivability to people and platforms in hazardous environments
- + Producing lightweight and more durable equipment and machinery
- + Developing efficiencies in manufacturing
- + Enabling cheaper and more energy efficient housing in terms of both construction and habitation.

Pharmaceutical

Quantum computing in the pharmaceutical sector is also promising. Those considering the application of quantum computing in this domain envisage having the capacity to quickly design bespoke drugs and medicines for specific diseases, for example, the design of catalyst molecules that attack cancerous tumours. However, some of the enthusiasm is tempered by the expectation that early quantum computers will struggle to identify the large molecules for pharmaceutical applications.



Sourced from: <https://1qbit.com/blog/quantum-computing/learn-how-quantum-computing-could-revolutionize-chemistry/>

Optimisation

Quantum computing may be beneficial for a range of complex system optimisation problems. Applications will depend on how problems can be formulated and integrated with classical computers. For instance, quantum algorithms for optimisation may have superior performance for some, but not all, instances of optimisation problems. Hence, hybrid systems would be necessary to provide best performance.

Finance

In the finance sector optimisation algorithms play a role in finding solutions to complex problems quickly in order to speed up financial transactions in shifting markets. However, there is some scepticism regarding applications to finance and trading due to the large amounts of data that need to be processed, and the current limitation of some quantum computing architectures that have relatively small data input and output capability. At this stage, the ability to input large amounts of data into a quantum computer is under development.

Logistics

The 'travelling salesman problem' is an example of an optimisation problem that is straightforward to understand but can be difficult to solve. The travelling salesman problem is a route optimisation problem. Given several locations to visit, the problem is to create a route that minimises the time taken, distance travelled or some other variable. While the optimisation is straightforward to describe, it takes relatively few required destinations (around 20) to make the computational requirements impractical for classical computers in real-world situations. It has similarities to problems faced by supply chain and logistics planning, such as last mile logistics in a complex environment. Furthermore, potential optimised solutions to the 'travelling salesman problem' can be applied to other areas, such as, public transport route optimisations and optimised deployment of first responders to disasters.

Autonomy

Optimisation applications used for logistic operations could be used in combination with sensing technologies to both support logistics tasks and broader activities requiring the use of autonomous mobility platforms in various environments, for example, casualty evacuation from land or sea.

Factoring

Data Security

Encryption, decryption, and encryption breaking is a competitive field in terms of both measures and countermeasures. It is essential to maintaining security and privacy in many aspects of normal cyber activity, from protecting internet banking passwords to securing confidential medical information. Likewise, it is essential to the cyber security of critical infrastructure. Quantum computing has the potential to render cryptography generated by many current standard encryption algorithms redundant. This is because cryptographic problems have a polynomial time quantum algorithm, being Shor's algorithm. As such, new "post-quantum" cryptography schemes will be required to 'resecure' data as quantum computing capacity grows.

Linear Algebra and Artificial Intelligence/ Machine Learning (AI/ML)

AI has evolved in a way in which solutions to problems are not necessarily the best solutions, but they are often quicker, easier, and cheaper, which is attractive to some and drives their continued use. A range of quantum computing equivalents to classical machine learning algorithms have been developed, and provide potential applications for even noisy quantum computing devices. Quantum machine learning algorithms compliment conventional machine learning and provide a new avenue, potentially providing faster and more accurate solutions than using conventional approaches.

The realisation of effective quantum AI/ML algorithms could see them used with other algorithms and applications to both enable autonomy and deliver the potential for quantum computers to support higher order functionality such as pattern recognition and image analysis.

However, there is conjecture regarding quantum AI/ML due to its development being largely experimental. Additionally, there are perceptions that this area is prone to 'quantum hype' and that there is naivety in some industries regarding quantum AI/ML applications, whereby there is an oversimplification that the 'addition of quantum' will improve AI/ML performance compared to classical systems. However, the field is evolving, and recent papers show there may be advantages in quantum AI/ML that were previously unseen.

Due to the complexity of the AI/ML space and the different intersections of quantum computing and AI/ML, four distinct development areas have been identified:

- + Quantum-assisted ML. For example, the use of quantum computers to accelerate training or the development of models for classical ML
- + Quantum-enhanced ML. For example, where quantum computers accelerate a particular computational subroutine in a classical ML application
- + ML-assisted quantum. For example, where classical ML is used to optimise the compilation of quantum algorithms for different hardware platforms
- + Quantum-ML. For example, where the ML is explicitly contained within a quantum context, such as quantum neural networks, quantum support vector machines, etc

Each of these intersections has a very different trajectory in terms of requirements for hardware and application opportunities. Furthermore, there will be emergent opportunities that arise from the confluence of developments in these intersections, i.e. development of one area may change the development of another and vice-versa.

CHALLENGES

Technical

With all technology there are challenges. While quantum computing promises exponential improvement in processing quantum information, there are many paths and differing timeframes for overcoming the technical challenges to produce large-scale quantum computers.

The future will hold a variety of quantum technologies, depending on their ultimate use cases, the different conditions required for operation, and other criteria such as different size, weight, and power (SWaP) characteristics. Technical discoveries, innovation, and challenges will all be part of the journey to realising the future quantum technologies and their differing needs.

There are caveats to quantum computing regarding solving problems with big data. At this stage of evolution quantum computing typically cannot process large amounts of data. Big data is everywhere however and as such, classical computers will be essential to overcoming some of the challenges to enable quantum computing, and there will be a requirement for better interfaces with classical infrastructure to support this symbiotic relationship. To this end, there will need to be greater integration between physicists, mathematicians and computer scientists to solve some of the problems.

While large amounts of data cannot currently be processed in its quantum form, as processors grow in complexity this quantum-classical interface is being continuously expanded and developed. The richness of the quantum information can be lost when processed classically. From a theoretical point of view there may be an advantage to storing it quantumly, but there is a cost overhead, and technical challenges in transferring and storing the data. To solve that problem, quantum memory with associated networking on a large scale would be required. However the concept of quantum sensors, connected to quantum networks and quantum computers through entangled states could be transformative. The technical challenges to achieving quantum advantage for this concept are unlikely to be overcome before 2040.

No matter what happens with the technology, there will always be a very strong need for classical high-performance computers to be working in association with quantum computers. A lot of HPC is done in-situ with the quantum computer so it is likely that we will experience some interesting HPC developments in order for this symbiotic relationship to work in an optimised way

From a production perspective, several technologies developed in Australia will require additional nano fabrication and manufacturing processes for future hardware development with a need for greater industrial scale manufacturing. However some quantum hardware technologies could be realised in Australia with strategic partnerships in the quantum control layers using fabless chip design. In the case of some quantum chips, they will need to be designed from the ground up, possibly from new materials, to support emerging quantum computing architectures. Such architectures are accompanied by the materials science and engineering challenges that will manifest as new materials emerge. It is important to note that materials science challenges for high quality qubits are significantly different from (and more stringent than) most existing computing technologies. Although many of the same materials are being used, large scale quantum computers require low decoherence, high fidelity operations, high fabrication precision, and stability. These requirements are at the limit of what is currently available in existing technologies.

Integration is required at all levels of the stack and will be influenced by the type of quantum computing technology selected i.e. different levels of the stack will not necessarily be 'plug-and-play' as is the case with classical computing. This is particularly so in the case of qubits. Given the relative strengths and weaknesses of different types of qubits, the qubit selected will influence the selected hardware, which in turn will affect the associated software, and so on.

It is likely that there won't be one type of quantum computer that is perfect for all people and/or purposes. To this end, technical challenges along the entire stack will vary with where desired quantum computing outcomes lie. Full stack development and integration from the outset is of paramount importance.

Current technical limitations are likely to result in larger scale quantum computers not being available for approximately a decade. As such, strategies are required which both exploit the advances made in quantum computing in the near term, and leverage the long term development of alternate technologies, architectures and materials. To foster development of larger quantum computing capacity, an illustrative goal may be the demonstration of a set of universal gate operations on two logical qubits within a five-year time frame. Another major achievement would be the demonstration of a quantum advantage using a quantum analogue simulator. Over the past 12 months these systems are looking to provide the first examples of solving problems hitherto impossible with classical computers. Quantum analogue simulators are machines that don't act like a general-purpose computer, but rather are designed to explore specific problems in quantum chemistry such as how room-temperature superconductors work or how a particular protein folds. A classical computer would have to run for thousands of years to compute the quantum equations of motion for just 100 atoms. A quantum simulator could do it in less than a second.

Such systems demonstrate the capabilities of the hardware platforms in a unique way and provide the first applications. It is important to remember that the first applications of classical integrated circuits were in the use of hearing aids and calculators – not full blown computers. It is essential in the quantum computing field to find such equivalents. Such an approach could help drive the effort to pave the way to large scale quantum computing using different architectures and materials. Concurrent to overcoming the technical challenges of quantum computing in and of itself, consideration needs to be given to the potential technical challenges that may be posed by the infrastructure

needed for scaling up quantum computing, particularly if the ultimate goal, which is to network between quantum computers and with the broader quantum technology ecosystem, is to be realised.

Regulatory

Australia has long been a leader in counter-proliferation and arms control, particularly for critical and emerging technologies. Australia also recognises the need to engage with like-minded partners. Initiatives such as the Wassenaar Arrangement, which has components for quantum computing, are under active negotiation between 42 nations. Given the globalised nature of quantum computing development, and the USA's significant investment across sectors, the USA's technology controls are relevant to Australian stakeholders as the USA applies some rules extraterritorially.

Quantum technology is a controlled technology, meaning developments by research or industry may already be subject to export control according to regulatory requirements. However, there is a blanket exemption for the act of publishing any research that is not especially designed or modified for military use. This is only for publishing and does not include the course of research or collaborations. There is also an exemption for basic research, but any applied research is likely to be subject to regulatory controls. The complex interplay of policies, including between nations, is a consideration for the future of quantum computing research and development.

The key challenge for regulators, which is common for emerging technologies, is that without knowing the applications of quantum computers and their requirements for advantage, it is not possible to judge what needs to be protected and what doesn't.

Societal

Most of this paper hails the potential benefits of quantum computing to society, but little is raised regarding societal challenges that may need to be overcome. Indeed most technology papers do not give

significant attention to adequately identify and consider potential societal (environmental and other) challenges to the respective technology's realisation. In fairness, societal consideration is unlikely to be the main aim and/or intent of a technology paper, and they may be too difficult to predict.

While it may be difficult to foresee the societal challenges related to quantum computing, the questions are easier to propose and go both ways i.e. how will society affect the development and deployment of quantum computing? How will the development and deployment of quantum computing affect society?

The potential strategic advantage arising from the realisation of quantum technologies will have international relationship implications. Distinct developments will occur depending on the nature of those relationships, in both competitive and collaborative natures, and some may create societal issues. In particular, what are they likely to be and how can they be addressed?

Additional societal concerns relate to ensuring appropriate constraints for quantum computing to be used properly and appropriately, particularly regarding information privacy and data collection. In addressing such issues, society needs to be captured and engaged in the holistic quantum computing discussion regarding benefits, affordability, access, use, and ethics.

Conversely, perhaps quantum computing is such a complicated, multi layered, and resource intense enterprise, that no entity can fully operate it independently, resulting in the need for multiple parties and/or distributed ownership that results in a socially self-policed environment. Alternatively, but for similar reasons, quantum computing is never realised in the capacity envisioned, and the social status quo remains.

More pragmatically, the cost of development is significant at this stage of the technology. Such investments might be beyond the reach of some countries. The companies that are producing the larger systems are investing billions of dollars and leveraging significant infrastructure. The opportunity cost of quantum computing investments are not insignificant.

Environmental

Environmental aspects require consideration when any new technology is being developed, such as, where from, and how are, the materials required for quantum computing being manufactured and/or acquired. From a quantum computing perspective some thinking is occurring, but more is required, especially in the sphere of materials acquisition. The issue of materials acquisition is far broader than just the quantum computing industry; it is something which the entire technology industry is considering from an environmental perspective.

Realisation of quantum computing is not without climate change concerns. As quantum computing evolves it is expected that, as with classical computing, it might require more and more power. To this end, how do they fit into climate policies and emissions schemes?

In the future different quantum computing architectures may have energy efficiency advantages in comparison to the computing power generated. Just as each generation of current high performance computers achieves greater efficiencies in energy consumption, the processing gains of quantum computers will also need to consider their energy requirements.



Ethical

If you look back in history at the effect of the quite rapid increases in computing power in conventional technology, there are many ethical questions regarding quality of access. Consideration may need to be given to the ethics of “who’s in and who’s out” and the potential for the gap between the ‘haves’ and ‘have nots’ will grow, which in turn may hinder the development of quantum computing in some countries and communities. Ethically, there needs to be fair distribution of the benefits of such devices. Advances and developments in quantum computing should be shared around equally to prevent unfair advantage and sub-optimal outcomes e.g. if a party in the medical field has obtained a quantum-based tool which offers them unique insights into disease diagnosis, but they don’t share it for the good of others, this is not an ideal result from an ethical standpoint. The ethics and values of organisations developing quantum computing will be as important to consider as the capabilities they offer.

Quantum computing power will be a valuable asset similar to data or natural resources. However, currently it is difficult to obtain and there will be smaller quantities due to the challenges of building quantum computers and associated cost constraints that will, in the first instance, only see a small number produced. Hence, owning an advantageous quantum computer will be a strategic asset. Initially, due to complexity and expense, quantum computers will likely be held by large corporations and/or big governments. Cloud based access and differential access to computers of different capacities creates a more open access environment. Hence, ethical questions will surround how these organisations will control, provide access to and use their quantum assets.

There is a rise in quantum ethics, which is good and healthy to be thinking about. A key issue is that it is open-ended, so we are not exactly sure where the technology is going, but that could also imply that we need to have a very strong ethics framework in place. The ethical questions need to be asked all the time, as unfortunately there are likely

to be adverse implications arising from the unknown unknowns. Also, considering that this is a disruptive technology there are likely to be ethical concerns well into the future. As such, ethical considerations should go together with the development process, however they do not necessarily require a different ethical approach to any other tech development.

An alternative perspective using a simplistic binary approach, is that either the technology can be scaled and works, or it can't. In this way, it would mean that if the technology is difficult to build, then perhaps the decision to pursue the technology should be the first deciding factor. If the decision is made in the affirmative, then priority should be to getting the technology working and discovering if it can solve the challenging problems for which it has been developed. Once this has been proven, then consider the longer-term societal, environmental, and ethical (and other) impacts as they are foreseen and develop.

Political

Australia has a huge breadth of technology and experience, combined with early investment over the last 20 years. There are decisions as to where Australia invests to grow the quantum industry to build depth and sovereign capabilities.

Other concerns raised by some respondents in the interviews related to a lack of capacity across government to appreciate the full opportunity to be realised by quantum computing, and a perceived attitude of, "if we (Australia) can't have it, then nobody else will either." As such, there is a perception of a 'fortification' mentality that would rather see domestic quantum endeavours fail than leave Australia, resulting in the potential local industry being crushed.

Respondents also indicated that partnerships and collaboration with like-minded countries requires significant consideration. Leveraging the relative strengths of different national ecosystems could enable the development of quantum computing technology partnerships and establish broader markets for products.

It is suggested by respondents that Government support within the globalised industry will be essential to help cultivate and support networks of trusted partners and collaborators, particularly for high risk ventures. These partners will cover government agencies from other nations as well as companies and other institutions that can work with government and are trusted to deliver important inputs to this capability. Engagement with international partners will also support interoperability of quantum-enabled capabilities to expand opportunities for Australian companies in other markets and to work with prime contractors.

Sovereignty

If Australia does not continue to develop sovereign quantum capability, there is the possibility that threats emerge that we do not understand or cannot counteract. Our national security agencies should be able to continue to develop cutting edge quantum technologies to both understand the credibility of claims made by competitors and be able to implement countermeasures for these threats. Respondents indicated that it may be prudent for Australia to maintain strong quantum capabilities that will be able to develop leading technologies to support quick detection and response to new quantum-enabled threats as they appear. Australia may need to demonstrate to allies our commitment and investment in research and development to share in the benefits of technology advances made by others.

Given the global competitiveness and potentially transformative applications, Australia may need to examine where and how it maintains and develops sovereign quantum capability. Further investment in sovereign capability may be required to, at a minimum, understand the applications of technology as well as potential threats it may enable. Without expertise in Australia, it may not be possible to understand what is credible with quantum-enabled technology, or what could be effective countermeasures. This minimum standard could still require significant investment to achieve. A strong domestic industry could lead to a wide range of quantum-enabled capabilities based on technology produced in Australia and to the significant benefit of Australia's wider economy.

Standards and benchmarking will also be important so that Australia can be an intelligent buyer of quantum technologies and can ensure that what is being developed is suitable for the need.

An Australian quantum capability is expected to require global partnerships with like-minded countries to deliver the full stack of technology. This will require some strategic understanding of the layers of the stack, including where Australian investment will focus and where Australia will seek to collaborate with partners. Consequently, integration of technology and interoperability are necessary from conception.

The applications of quantum computing have the potential to fundamentally change/transform various domestic industries' capability and the national economy. A range of new capabilities could be formed along with quantum-enabled step changes to existing capability and functions. Quantum computing could also enable a range of new opportunities for Australian business and researchers and provide them with an advantage to form new partnerships when competing globally.

Importantly, sovereign quantum capability encompasses more than simply the manufacturing and operation of quantum computing hardware. It also includes considerations for all necessary inputs, integration and interoperability, and the freedom to use quantum devices as Australia sees fit. Having a strong software and development culture domestically will also be important for exploiting increases in hardware development. The concept of securing all inputs to capability is essential to securing sovereign capability. Therefore, the question is, 'How do we secure all the critical inputs to sovereign quantum computing capability of a complexity we desire?' To illustrate the point, with regard to classical supercomputers, Australia did not wait for the capability to build the physical devices domestically before securing a sovereign capability in high performance computing. Similarly, the more tangential capability inputs to supercomputing such as robust highly parallelised algorithms are constantly worked on and developed on shore or obtained through trusted relationships to ensure Australia can use its high performance computers as it sees fit.

As the potential for Australian technologies becomes clearer, it may be necessary for Australia's quantum ecosystem to broaden and deepen connections to the global ecosystem. This will maintain Australia's presence in a future global market and support a unique sovereign capability.

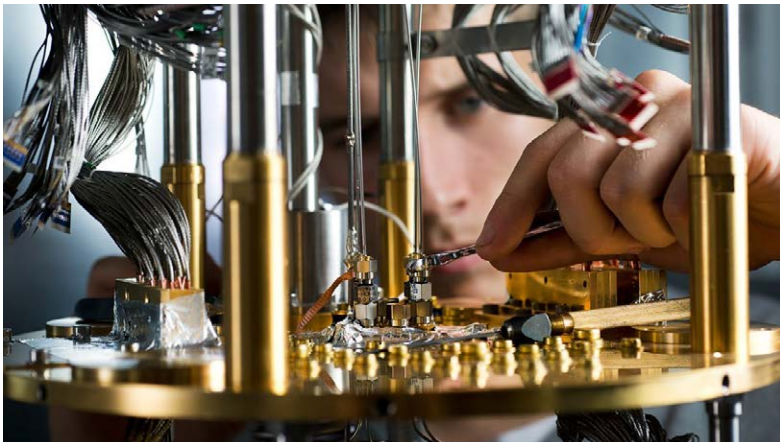
The background features a gradient from dark blue at the bottom to dark purple at the top. It is decorated with several starburst or sunburst patterns, each composed of numerous thin, radiating lines. The colors of these patterns transition from purple at the top to blue at the bottom, matching the overall color scheme.

ENABLERS

Overview

Given the global competitiveness and potentially transformative applications, Australia should examine areas in which we maintain our global leadership and where it is necessary to have sovereign quantum capability. An Australian quantum capability will benefit from global partnerships with like-minded countries to deliver the full stack of quantum computing technology. This will require some strategic understanding of the layers of the stack where Australian investment will focus and the layers of the stack where Australia will seek to collaborate with partners or undertake to access their capabilities.

The international quantum technology workforce is highly sought after, skilled, and mobile. Many jurisdictions are offering significant support packages to individuals and organisations to domicile in their region. A number of respondents have indicated that Australia may need to signal its support and accelerate its investment to support Australian talent if it is to secure its position as part of a rapidly expanding global industry. A growing quantum industry will directly create jobs, but more importantly will underpin a quantum-enabled economy where high-performance computing provides significant advantages and opportunities for growth.



Sourced from: <https://createdigital.org.au/new-research-shows-australian-engineers-at-cutting-edge-of-quantum-computing/>

Academia

Quantum computing has been one of the major drivers for the quantum technology ecosystem over the last 20 years, because it has so many complicated technologies that come together to create it, and its distinct applications and advances in one area are likely to benefit advances in other areas. This further emphasises the importance of cross disciplinary work between quantum physics, computer science, mathematics, engineering, and other supporting academic areas.

The key concerns in academia are the loss of talent and the type of talent being lost i.e. the small and unique group of people who are highly skilled and are essential to grow and lead programs. If this expertise is lost it will take years to re-establish.

Solutions to quantum education and talent flow challenges are not necessarily to train more physicists to be physicists. A lot of engineers and computer science professionals are being trained, but the need is to get them motivated to be quantum aware enough to transition into a quantum workforce and learn more. However, there remains the ongoing competition with other science, technology, engineering, and mathematics (STEM) areas to meet the demands of the respective industries their students are needed for.

Academia has the capacity to work in unique ways with industry and other sectors, both domestically and abroad, in the quantum computing enterprise. Factors, which would assist in this, include reducing risk in joint ventures, allowing people to move back and forth seamlessly between respective organisations, and collaborative knowledge exchanges. Such activities need to be seen as opportunities, not threats. Further work is required to enable this working environment. An example of this was a shift in policy to enable transportable superannuation, which removes a barrier to movement between academic institutions and other organisations.

Respondents have suggested that a long-term investment culture for quantum computing is required from government and business

in a partnership arrangement. The long-term investment should be supported by a culture that nourishes failure. This approach will support the attraction and retention of highly educated talent and continuity of work on quantum computing projects over several years. For the next 5-10 years, dedicated partnerships will be very important to progressing quantum computing work in academia. Furthermore, if all stakeholders are committed, then solid teamwork is enabled, which will increase the chance of success in addressing problems.

Another consideration is finding the balance between imposing necessary security requirements and allowing research to flourish freely in order to ensure that academia remains a quantum computing enabler. Having a more open and collaborative environment prevents barriers and accelerates research. As such, the balance needs to be found that meets security requirements without unnecessarily stifling the sharing of information that will lead to beneficial and timely advances.

Industry

Things will likely need to change over the coming years with regard to the way different industries perceive quantum computing tools. This will continue to evolve along with quantum computing itself and shape things differently. For example, chemistry is moving towards quantum computing just as quantum computing is moving towards chemistry. As such, the way in which chemistry is conducted today is likely to change as quantum discoveries are made. Similarly, continuing to undertake computing in the same way we have for 50 years might not be the way for computing to be conducted in the future.

To quote one respondent, "If we simply swap out the classical computer, replace it with a quantum computer and just do the same things 'quantumly', then why not just find a way to build a better classical computer." In some ways this is analogous to the statement attributed to Henry Ford, "If I'd asked people what they wanted, they would have said faster horses." Just as Ford contributed to revolutionising transport, leaders in the quantum industry are positioned to do the same for computing.

There is a large consensus that Australia has the technical capability for software. However, from a software perspective, greater access to state-of-the-art technology is needed for our researchers and the access needs to remain constant over time.

Large resources and investment will be required to ensure success in the quantum computing industry. Such investment needs to be big enough to be transformational to a business versus “building an armada of canoes” which would see grants that are too small and spread over too many areas to deliver significant outcomes. In particular, depending on the hardware platform quantum computing may require high levels of investment to produce our own homegrown technology. It could be millions to billion-dollars of investment and require a degree of certainty of which platform you are investing in, or if investing in multiple platforms, then understanding of what is achievable for each. Ideally, the investment would be made on the technology results with a reasonable chance at competing with, or complementing, international efforts. Otherwise, there will be a dependence on accessing technology material from overseas.

Australia is a world leader in silicon quantum chips and diamond quantum technology. There is however no commercial semiconductor foundry in Australia working on this. It has been suggested by some respondents that consideration be given to construction of a foundry to leverage the strength Australia has in this area and build a sovereign silicon plant to manufacture qubits (although a key question to be answered is, ‘what type of qubits?’). Other respondents point to the ability to manufacture quantum chips here at much lower cost that does not require foundries.

Interestingly, respondents provided examples within the industry where there are individuals who are satisfied to develop a technology within the lower TRLs and then remain working on the technology at those same levels. There is potentially not the drive, or the right support, to adopt the challenge of trying to develop the technology and raise it to higher TRLs, whereby the technology would become commercially viable.

Further effort needs to be applied to understand the motivation of these people and find ways to lead and/or incentivise them to develop their technologies and progress them to higher TRLs.

Importantly, Australia should consider whether it wants to build across the stack and at scale. This would have to be a national endeavour and industry would need to be provided with the appropriate level of investment. Alternatively, Australia could adopt an approach that entails the establishment of trusted partnerships with global players and attract international investment.

In some areas, Australia already is world-leading in quantum technology. However, keeping this strength and the potential to create a first mover advantage may require supporting the most promising developments in Australia's quantum computing industry across all parts of quantum computer stack in an integrated way. This will also enable the creation of stronger career pathways for young Australians pursuing careers in the quantum computing industry.

Additional considerations for industry to succeed as a quantum enabler are: supporting infrastructure, reducing supply chain length, and identifying synergies that can be achieved both within and external to the quantum computing industry. Similarly, the classical computer industry must continue to be considered in the same discussion with quantum computing as it will be key to the operation of quantum computers and the success of the holistic quantum computing system.

Ultimately, establishing the areas in industry where Australia can be a first mover is critical to developing a sovereign quantum computing capability. This will still require the global collaboration inclusive of international capabilities, but will nonetheless support Australia to develop, produce and market quantum-enabled products and services. It will also have flow on benefits for other Australian industries which can adopt quantum technologies to gain a competitive advantage.

Commercial

From the interviews conducted, there is a perception in some segments of quantum computing that you need a degree of cynicism as 'a lot of people just want to make money'. One answer to this question is by asking a different one, "Why develop quantum computing at all when classical computers have done a great job so far?" A reason is that there is not much 'room left at the bottom' regarding processor miniaturisation. The ability to process using quantum rather than classical states opens a whole new paradigm of computing with enormous potential benefit to humanity. Each time man has figured out how to manufacture at smaller and smaller length scales, whole new industries have emerged. In parallel there will be smaller gains in processing power and at higher costs to improve computing power in classical computers in the next few years. The increased cost of development in improving classical computer processing will become prohibitive. Conversely, quantum computing is one of few technologies with the potential to reduce cost and improve computing/processing power for some major computing problems, thus delivering profits to the eventual provider. There are also other completely different computing paradigms, such as neuromorphic computing, which also offer great potential for certain applications. Regardless of the reason, commercial investment is a major driver, therefore a key enabler of quantum computing.

Quantum computing is likely to be a transformative technology and the returns to be made on it are potentially enormous, but the current state of the hardware is not yet powerful enough to truly know. However, when considering the use cases discussed earlier in the paper, there are many potential commercial applications in the long run.

Commercially, most companies are intrinsically looking at building the machine and are not advanced enough yet to look at networking of multiple machines. Networking will also ultimately be an important component of scaling quantum computing.

There is also major commercial value in application development. The more common questions asked by people from commercial enterprises are, “What are the top 10 applications quantum computing are going to create?” or, “What is the dollar value of this application?”. These questions are valuable. Furthermore, knowing which will be worth a billion-dollar application, or knowing which application is going to raise you ten billion dollars, is valuable information. Appreciating this point is why commercial entities will invest a lot of money into getting that edge and it provides insight into why development of the question, “How we can best use quantum computers?” is incredibly valuable as a research area. This conversation is starting to happen slowly in Australia. Having insight into these questions will be valuable in the long term because this is where people are going to make money, hence where the commercial effort will be allocated. This is something that an industry can be built around, and it is why large technology companies are pursuing it.



Collaboration

Australia has a substantial quantum 'ecosystem' comprising academia, start-ups and large international corporations. Quantum computing and related technologies are highly specialised fields, making this ecosystem diverse in its areas of focus and potential for growth. This provides momentum and an opportunity for a first mover advantage in some areas if Defence and other stakeholders act quickly.

There are concerns whether Australia could capitalise on its current strengths in quantum computing given the rapidly growing industry and the increasing investment in the sector across the world. In September 2021, Defence held the Quantum Computing: In Focus forum, which brought industry, academia, Defence and government together to discuss the current state of play in quantum computing and to investigate the potential impacts the development of quantum computing will have on national security. Some participants thought that there was a risk of Australia losing its talent to overseas competitors and failing to attract international talent. The quantum computing industry is globally dispersed, and individuals can easily move to countries that offer to fund their research or business ventures. Australia lacks the economic scale and mature technology sectors of some of its competitors for international talent. In addition to losing key talent, Australia's manufacturing skills and capacity will need to be able to capitalise on our research success to make products at a scale that is sufficient for global markets.

Another key risk is the need to balance the national interests associated with critical and sensitive technologies with the unique needs of start-ups that drive the quantum sector. Start-ups must often work at rapid pace to demonstrate progress and access capital quickly. Delays caused by investment controls and other regulatory hurdles can be particularly damaging to these businesses and affect their ability to retain talent and compete internationally. Quantum computing relies on highly specialised intellectual capacity and capability, so there is potential for it to provide significant economic value to Australia more broadly.

While it will be necessary to select key areas for focus and commitment, a more strategic and measured approach is needed to assess any risks associated with committing to certain technologies or their applications to ensure they reach their potential. A key challenge will be determining whether some developments are no longer relevant and determining whether the 'hype' of specific technologies or applications are valid.

Ultimately, establishing the areas where Australia is a first mover and can lead may be prudent to developing a sovereign quantum computing capability. This will still require the global collaboration and incorporation of international technology, but will nonetheless support Australia to develop, produce and market quantum-enabled products and services for the nation. It will also have flow on benefits for other Australian industries which can adopt quantum technologies to gain a competitive advantage. However, essential to achieving this, is development of a coherent strategy that ensures all stakeholders across government sectors, industry, academia, and global partners can work together.

Additional Australian Context

Additional context regarding the enablement of quantum computing in Australia is contained in Annex C.



CONCLUSION

Conclusion

Quantum computing technology is a focus of research and investment for many governments, including Australia's partners in the USA, UK and Canada. Each of these governments have invested significantly in quantum technologies and expect these to provide important capabilities to respective nations.

Australia is currently a recognised global leader in quantum computing and sensing research and other areas of quantum-enabled technology. Australia's quantum sector includes academia, Australian start-ups, and the local presence of large multinational companies.

Quantum computing applications have the potential to fundamentally transform national capability and the national economy. Australia has taken steps to leverage the deep technical strengths to create new devices and applications, and demonstrated to partners a commitment to investment in research and development. The EDTAS is an opportunity to explore the future of the technology and the supporting mechanisms that will significantly enhance the commercialisation, research, innovation, adoption, and use of quantum computing to create economic value for Australia and engagement with partners. The international growth of quantum computing and the increasing investment by other nations presents a risk to Australia's relative strength in the industry. Failing to keep pace could see Australia lose talent and no longer attracting international talent to contribute to its domestic quantum ecosystem.

Australia needs to balance the national interests associated with critical and sensitive technologies with the unique needs of academia, multi-nationals and start-ups, that are providing the drive in the Australian quantum sector. Start-ups must often work at rapid pace to demonstrate progress and innovation, which can sometimes conflict with processes and controls necessary for compliance with policy and governance.

Retaining Australia's strength in quantum computing and creating a first mover advantage will require directly supporting the most promising developments in Australia's quantum computing ecosystem across the

stack. If stakeholders can work together to select priority application areas for focussed effort, which are most likely to enhance domestic capability in an informed way, Australia's first mover advantage can be entrenched by establishing and influencing standards and providing scalable technologies.

Annexes

- A. Use Case (Application) to Impact Area Mapping
- B. Additional Quantum Computing Information
- C. Additional Australian Context

Annex A Use Case (Application) to Impact Area Mapping

The table below provides indicative potential use cases (applications) extracted from McKinsey & Company’s 2021 report *Quantum computing use cases – what you need to know*⁵ and maps them to impact areas for technology opportunities.

Use Case (Application)	Algorithm Archetype
Certified randomness	Optimisation
[Job] scheduling optimisation	Optimisation
Route and fleet optimisation	Optimisation
Clinical-trial site-selection optimisation	Optimisation
Synthetic data generation	Simulation
Approximate quantum mechanics simulation	Simulation
Small-scale quantum reinforcement learning	Linear algebra (AI/ML)
Collateral and portfolio optimisation	Optimisation
Robot path optimisation	Optimisation
Production-process optimisation	Optimisation
Light risk simulation	Other
(Approximate) molecular dynamics, molecular mechanics, simulation	Simulation

⁵ <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know?hikid=a774e1a8976d4a078406df70a8406fd5&hctky=3052965&hpid=aca734e5-8f89-49ba-a360-cf60fa973f9a&msclkid=adc763e6c39b11ec88fdd33323a1b11>

Industry	Impact Areas for Technology Opportunities
Finance	Intelligent Decision Making
Automotive	Intelligent Decision Making
Logistics	People and Platforms Intelligent Decision Making
Pharmaceutical	People and Platforms
Pharmaceutical, Chemical	Sensing and Sense Making Intelligent Decision Making Cyber and Communications
Pharmaceutical, Chemical	People and Platforms Sensing and Sense Making Intelligent Decision Making Cyber and Communications
Finance	Sensing and Sense Making Intelligent Decision Making
Finance	Intelligent Decision Making
Automotive	People and Platforms Sensing and Sense Making Intelligent Decision Making
Chemical	Intelligent Decision Making
Finance	Intelligent Decision Making
Pharmaceutical, Chemical, Automotive	People and Platforms Sensing and Sense Making Intelligent Decision Making Cyber and Communications

Use Case (Application)	Algorithm Archetype
Trading strategy optimisation	Optimisation
Protein folding	Optimisation
Breaking RSA cryptography	Factoring
Financial and cyber risk simulation	Other
Large-molecule simulation	Other
Absorption, distribution, metabolism, and excretion (ADME) and toxicity prediction	Simulation
Complex mixture simulation	Simulation
Solid-material simulation	Simulation
Catalysis or synthesis optimisation	Simulation
Finite element method	Linear algebra (AI/ML)
Supply chain optimisation	Optimisation
Supply-chain-disruption modelling	
Self-driving robots	
Credit-risk management	
Financial-crime detection	
Personalised medicine	
Automated drug recommendations	
Multiscale production optimisation	

Industry	Impact Areas for Technology Opportunities
Finance	Intelligent Decision Making
Pharmaceutical, Chemical	People and Platforms
	Cyber and Communications
Finance	Intelligent Decision Making Cyber and Communications
Pharmaceutical, Chemical	People and Platforms Sensing and Sense Making
Pharmaceutical, Chemical	People and Platforms
Pharmaceutical	People and Platforms Sensing and Sense Making
Chemical, Automotive	People and Platforms
Chemical, Automotive	People and Platforms Sensing and Sense Making
Automotive	People and Platforms
Chemical, Automotive	People and Platforms Intelligent Decision Making
Chemical, Automotive	Intelligent Decision Making
Chemical, Automotive	People and Platforms Sensing and Sense Making Intelligent Decision Making
Finance	Intelligent Decision Making
Finance	Intelligent Decision Making Cyber and Communications
Pharmaceutical	People and Platforms
Pharmaceutical	People and Platforms
Chemical	Intelligent Decision Making

Annex B Additional Quantum Computing Information

Quantum Computing Functionality

Our computational ability is fundamentally limited by the laws of nature. Quantum computing, as the name implies, exploits the more fundamental laws of quantum mechanics to gain computational advantage. In our everyday lives the fundamental quantum laws of nature are hidden from us as quantum phenomena usually only occur within very small distances and/or time scales. The main reason for this is that we have not been able to control interaction of quantum systems with their environment up until recently. When quantum systems interact with their environment, a phenomenon of decoherence occurs which washes out uniquely quantum behaviour. We are now able to control interaction of quantum systems with their environment, which has opened the door to full exploitation of quantum mechanical phenomena for computing. This ability is at the heart of the so-called second quantum revolution.

The fundamental logical unit or bit for quantum computing is the quantum bit or qubit. The qubit represents a quantum logical unit using a two-state quantum system. While a classical bit can take on values of 0 or 1, a two-level quantum system can take on a combination, or in the language of quantum mechanics, a superposition of both logical states. The combination or superposition of the two quantum states of a qubit is specified by amplitudes for each of the logical states. When an observation of a qubit is made, we cannot tell which state will be observed, but we can calculate the probability of observing them. The probability of observation of a particular state of the qubit is the square of the magnitude of the amplitude of that logical state.

One way we can represent a qubit in a superposition state is as a point on the surface of a sphere, usually referred to as a Bloch sphere. In this representation, a quantum state equivalent to the logical 0 corresponds to the North Pole, and a quantum state equivalent to the logical 1

corresponds to the South Pole. Unlike a classical computer we can prepare a qubit in a state on the equator of the sphere. In this quantum state, the qubit is for computational purposes in both logical states at the same time with equal probability.

What exactly does this superposition property of a qubit mean in terms of computational power? If we set the qubit state to a point on the equator of the sphere, then any operation carried out on the qubit will be carried out on both logical 0 and logical 1 values simultaneously.

So far, we have only talked about a single qubit. If we have n of these qubits, each in a superposition state and undertaking an operation, then we effectively undertake $2 \times 2 \times \dots \times 2$ (n times), which is 2^n calculations in parallel. This parallelism is central to quantum computational power.

In order to undertake an arbitrary calculation, we need to be able to undertake single qubit operations. That is, be able to change the state of each qubit and move it to an arbitrary position on the surface of the sphere we use to represent its state. In addition we need at least one type of two qubit operation. With these, any quantum computer program can in principle be run. Two qubit operations mix information between qubits and often result in what is referred to as an entangled quantum state. In essence, the two qubits after interaction are no longer independent, hence the name entanglement. As a result, properties observed for one qubit in the pair instantaneously determine what will be measured in the other.

Up to this point we have outlined a process which provides exponential parallelism. However in quantum mechanics we can only ever observe one of the possible final states in a computation. That is, although we have undertaken 2^n calculations, we can only observe one of the possible outcomes. To make matters worse, we don't know which answer we will observe. Fortunately, we usually only want one of these answers. As an example, we might want to find the entry in a data base which is the closest fit to a particular input. This is where another property of the quantum superposition states comes into play, interference. Specifically, as quantum states can have amplitudes with different signs, when quantum operations are carried out the amplitudes can reinforce each

other or cancel each other out. Quantum algorithms are designed in such a way that the probability of observing the answer we are seeking is magnified by constructive interference, and the probability of observing answers which we are not interested in is reduced.

In the description above we discussed the fact that we have 2^n different calculations being undertaken simultaneously, each with its own amplitude. This means that any unintentional changes (through uncontrolled interaction with the environment) to 2^n different amplitudes can cause the computation to fail. That is, the larger the scale of a quantum computation, the more susceptible they become to errors. These challenges can be overcome by improving the engineering of quantum computer hardware and implementing algorithms for error correction in a fault tolerant manner. These are the key focus areas of research to date across industry and academia.

Quantum Features

Superposition describes how a quantum system can be in more than one state at a time. Mathematically speaking, the quantum system in a superposition state is expressed as the sum of the contributing states, each weighted by a complex coefficient. In layman's terms, this means that qubits can sometimes be 0 and a hint of 1, at other times possibly 0 but more likely 1, and so forth.

Entanglement is the property where two or more quantum objects in a system are correlated, or intrinsically linked, regardless of how far apart they are. For entangled objects, measurement of one qubit changes the possible measurement outcomes for the remainder of the system.

Coherence describes the quality of a quantum system which enables quantum phenomena such as interference, superposition, and entanglement to occur. A quantum system is coherent when the coefficients of the contributing quantum states are clearly defined in relation to each other, and the system can be expressed in terms of a single wave function.

Decoherence is the process in which a quantum system exchanges some information with the broader environment over time. In severe cases this quantum information cannot be recovered once lost, but in less severe cases specialised quantum error correction can be used to reduce its impact. Decoherence is one of the sources of error in qubit systems which has no classical analogue.

Key terms

Quantum error correction (QEC) is a process used to protect quantum information from errors that arise due to decoherence or other quantum noise. The fundamental ideas behind error correction for classical computers can be used to describe quantum computers to some degree. By employing redundancy (multiple repetitions of the same information), if copies are later found to disagree, a majority vote is taken as true. However, due to superposition, it is more complex than classical error correction. QEC is intricate at higher numbers of logical qubits, which poses a problem to resource usage and scalability.

A **logical qubit** is an abstract concept used to describe a collection of physical qubits implementing quantum error correction that can carry out a single fault-tolerant qubit operation. One logical qubit is made up of multiple physical qubits to correct for noise or errors. For example, if 10 physical qubits were needed to form one logical qubit, a quantum computer with 100 physical qubits would provide 10 logical qubits for operations. In general the number of ancillary qubits required for fault tolerant computation depends on the likelihood of error in the system.

Quantum volume is a metric of the overall capability and error rate of a quantum computer. It is a single number designed to compare the performance of quantum computers. The larger the volume, the more complex the problems a quantum computer can solve. This recognises the need to account for many factors that influence the performance of quantum computers, such as error rates and coherence times, in performance and capacity benchmarks.

Measuring progress in quantum computing technology in comparison to classical computers is often considered in terms of **quantum advantage** or **quantum supremacy**. However, the terms are often used interchangeably and there are elements within the quantum community that only ever use one term or the other. In simple terms, both terms relate to the demonstrated and measured ability to process problems faster than on a classical computer.⁶ However, some may argue that quantum advantage relates specifically to the solving of ‘real world problems’. Regardless, quantum computers are expected to achieve quantum advantage/supremacy, because quantum computing resources double for each additional qubit added. This means that a quantum computer with n qubits can process 2^n possible solutions in parallel. The art of quantum computing is to make optimal use of this exponential resource. For some problems this exponential increase in computational resources directly translates to an exponential increase in computational power when compared with classical computers. For other problems, the improvement is more modest or there is no advantage at all.

⁶ Brown, Rebel. Why Quantum Advantage & Supremacy Aren't That Complex. quantum computing: Ready-to-run Quantum Software. Viewed 10 September 2021 <<https://www.quantumcomputinginc.com/blog/quantum-advantage/>>

Universal quantum computation refers to a quantum computer which is able to execute any algorithm developed for a quantum computer, typically using a circuit-based approach. The circuit-based approach uses a set of quantum computer logic gates, the analogue of classical computer gates. As with a classical computer the quantum computer gates are connected in a circuit to undertake computations.

Quantum annealing refers to a quantum computer typically used to find solutions to problems via optimisation. To implement this, qubits in the computer are coupled together with different weights which represent the optimisation landscape. In this mode of operation the final quantum state of the system, which has the lowest energy, represents the solution to the optimisation problem. Quantum annealing finds an approximation of this state. When a calculation is initialised all the qubits are in an equal superposition of all quantum states and coupling between qubits are also equal at this initial stage. Over time, the coupling between the qubits is changed to that representing the optimisation problem. The quantum system then evolves staying close to the ground state of the system. If there were no noise, then the final quantum state would represent the solution to the optimisation problem. Given environmental noise, quantum annealing can produce a range of solutions which are close to the global optimum.



Gate-models vs quantum annealing

Most quantum computers, such as those developed by Google and IBM, operate using a so-called gate model analogous to classical computers. These are universal quantum computers in the sense that they can execute any quantum computer algorithm. Quantum logic gates are similar in concept to logical gates in classical computing, although they function differently to utilise quantum system properties. By applying logic gates, these computers can provide a wide range of computing solutions and produce logic similar to classical computers. However, these systems are currently limited by the reliability of current qubits and scaling these devices presents significant challenges to achieving fault tolerance. They must operate at extremely low temperatures, creating a significant energy requirement.

Quantum annealing technology is fundamentally different to gate model technology because it uses quantum fluctuation effects to find the global minimum of an objective function. This method translates a function into biases and couplers to change the energy states of qubits and create entanglement.⁷ The qubits will then return to their minimum energy state, or one close to it, to represent the solution (the global minimum) to the optimisation problem. Problems framed as energy minimisation can be solved using quantum annealing with a high probability.

Quantum annealing is more error tolerant than gate models and can extract results even with significant quantum noise. The cost of using quantum annealing architecture is that the results derived may only approximate the answer required. The system's error tolerance means the qubit architecture can be much simpler than that of gate models. Currently developed annealers have over 5000 qubits; in comparison, one of the most recent gate-based quantum computer has 65-qubits. However, the applications of quantum annealing are limited in comparison to gate models, which have wider use beyond global minimisation problems.

⁷ D-Wave. What is Quantum Annealing? Viewed 10 September 2021 <https://docs.dwavesys.com/docs/latest/c_gs_2.html>

Stack Consideration

General

Substantial resources are being invested globally across the full stack. It is worth considering that most of the devices have arrived to where they are today through significant effort, so further levels of effort are required to keep improving the remarkable work that has gone before. The important point is that work has to be done for every layer of the stack and in the vertical integration along the stack. Key to this will be giving serious thought to identifying which technologies are believed to be the best to scale up and progress.

Algorithms and Application

Algorithms define the steps by which quantum computers solve problems. Quantum algorithms take advantage of quantum mechanics to perform calculations. Australian and international researchers are developing algorithms to make more efficient use of systems and open new applications for quantum computing. Worldwide approximately 70 different algorithms have been developed to date for application on quantum system.

Current research on quantum algorithms is primarily theoretical. For some established algorithms, such as Shor's and Grover's algorithms, it is straightforward to establish benefits of their application. However, experimentation on true quantum computers is generally required to understand the potential benefits of algorithms designed for near-term computers with noisy qubits (such as the Variational Quantum Eigen (VQE) solver algorithm⁸ used for optimisation problems). Ideally, these algorithms could solve useful problems that would otherwise take classical computers an impractical amount of time. Practically, it is difficult to ascertain their potential real-world applications and benefits when compared with high performance classical computers.

Breakthroughs are required in algorithms, applications, and computer science more broadly. In the algorithm space many breakthroughs

8 Invented and first demonstrated by Alberto Peruzzo (first author) and colleagues.

are required. At the moment quantum computers have a small generic asymptotic advantage for many of the hard problems being investigated, but the question is how big is that advantage? For example, with 'factoring problems', the advantage of a quantum computer is exponential, where every qubit added to the size of that integer achieves exponential improvement, whereas it gets more difficult classically. However, for other generic optimisation problems quantum computing will have a square root advantage, whereby instead of having exponential improvement, the improvement is flatter. Hence, most work is being done in the large and difficult problem space.

An example of a difficult problem that highlights the need for advances in algorithms is in a graph (complex network) learning problem. Consideration is required with regard to what the graph needs to look like, and questions will be posed about the various properties of the graph e.g. which nodes are connected, the properties of those nodes that are connected, etc. Greater advantage can be achieved using quantum computing by more closely leveraging the structures that emerge in the graphs. As a result this is where a lot of algorithm development is occurring and where progress needs to be made, but the number of people working in this field is low. This is because of the requirement for people with both mathematic capability and quantum capability. As such, when considering the development of quantum algorithms and applications, there is a demanding education component as it requires double (or more) degrees.

Software, Compilation, and Control

Control and software technology advances seek to improve error suppression and hardware stability by providing more efficient and robust control software, and the development of quantum firmware.

A key technology area in Australian research is in error-correcting software that addresses errors caused by decoherence and other quantum noise. These errors may mean that the system may not produce logical results as a classical computer would. Quantum error-correcting software encodes a logical qubit amongst many physical qubits to provide

fault tolerance. This software requires measurements to be carried out to diagnose the error and make the necessary correction. However, the operations to detect and correct errors can introduce additional noise and decoherence. For a system to be considered fault tolerant it must account for all these factors. Fault tolerant systems require significant resources to produce logical qubits (defined below) and perform logic gates. In addition, the computational overheads required for their implementation can significantly reduce their prospective benefit.

There are many issues around quantum software development and compiling, such as, which processor does what, when and how? How is that achieved in an optimal way? and, how does it work without balking your computer? Key to answering these questions and developing solutions is by having a robust quantum operating system, which is not quite a reality. This is exacerbated by the current need to use compilers which the classical computing industry stopped doing in the 60's. There are only one or two start-ups looking at this, but more attention is needed. However, as quantum computing develops there will be a need to compile quickly and this will likely garner the attention required. The next difficult issue is how to compile quickly in a near optimal way. Whilst achievable 'in principle', it becomes incredibly processor dependent and requires significant overarching error correction architecture/processing within the whole software stack. Furthermore, the question of interplay between the evolving processor design and which error correction is being used is awkward, and then how that changes the way compilation is undertaken becomes more complicated. Hence, it is likely that it will be years before there is a standardised way of accomplishing this task.

All of this has deep relationships with how software and applications will be developed. Currently, the calculation work people are doing to determine the number of qubits that are required to solve a particular problem are using a heavily optimised sub-routine to get a good accurate number out of it, but it is artisanal compiling, almost hand crafted. The fact that it is hand crafted is probably not sustainable and it has to assume that everything works. This final point further emphasises the need for vertical integration along the stack.

Hardware

Current understanding is that quantum computers are bulky and heavy. Quantum effects are also very fragile, so if the quantum computer is small enough to be portable then it is unlikely the quantum effects are well controlled. Quantum computers are very sensitive and require use of expensive, rare materials for superconductors that need to operate at extremely low temperatures. Furthermore, they are currently very expensive, in the order of hundreds of millions of dollars. As such, whilst many teams across the globe are racing to build a practical system, until it is built there remains a degree of scepticism that such a large-scale system would emerge within the next 20 years.

To take advantage of qubit architecture for computing, other hardware developments will be required, particularly technologies that enable classical control and the development of quantum networks. Quantum networking technology research seeks to create networks to transport information in the quantum state. This is predicted to have significant benefits for efficiency, information security and scalability of quantum computers. Networking is challenging because quantum state information cannot be repeated, as it would be for a classical repeater since qubits cannot be copied. Any attempts to observe or measure qubit will alter their quantum state.

Current research is focused on developing quantum interconnecting technologies that can enable quantum networks to reproduce the functionality of repeaters and nodes in classical networks. There is Australian research focussed on developing quantum processors to create quantum memories. Using rare earth crystals, memory-based quantum processors aim to provide long storage time (up to hours) and high storage capacity that will be essential for quantum networks. Research is also focussed on how this hardware can be used in space to create quantum-enabled satellites.

Other hardware developments seek to produce computing units that can be operated on site – i.e. not contained to a mainframe – to provide accelerated computing power. Quantum Brilliance, an Australian start-up, is aiming to develop a prototype of a functional quantum accelerator within the next five years using NV diamond qubits.

Selected Hardware Technology Developers

Centre of Excellence for Quantum Computation and Communication

(CQC2T). The ARC CQC2T is focused on delivering world-leading quantum computing and communications research to develop full-scale quantum computing systems. Its research focusses on silicon and optical quantum computing and covers quantum hardware, architecture, software and algorithms research across the quantum computing stack. The Centre also investigates secure quantum communication and distributed quantum information processing. CQC2T investigators have spun out 4 quantum technology companies, including QuintessenceLab, Silicon Quantum Computing, Aqacia and Diraq. As well as its world leading research in atom based and quantum dot qubits in silicon, the Centre also host research into the development of integrated optics technology to produce low loss, telecommunication-compatible, and compact circuitry. The Centre was established in 2011 and funded by the Australian Research Council as well as the US Army Research Office (ARO), Semiconductor Research Corporation, Department of Defence, NSW Government and participating universities. It houses major research infrastructure such as cryogenic facilities to limit quantum noise and highly specialised facilities capable of functions such as nanofabrication and single ion implantation.

- + **QuintessenceLabs** is a spin-off company founded in 2007 from the ANU Quantum Optics Group. It is currently headquartered in Canberra, Australia and has offices in San Jose, California USA. QuintessenceLabs produces encryption key and policy management products that conform to the Key Management Interoperability Protocol (KMIP), as well as a hardware quantum random number generator, and develops a quantum key distribution (QKD) system and other encryption solutions that include automatic key zeroization. The company is exporting these information security products to companies in Australia and the USA. Some of its commercial partners include PKWare, NetDocuments, VMware, Penten and Westpac. QuintessenceLabs was selected by the World Economic Forum as a Technology Pioneer in 2018 and a Global Innovator in 2020.

- + **Silicon Quantum Computing (SQC)** was launched in May 2017 with over A\$83 million of capital funding from the Australian Commonwealth Government, UNSW Sydney, the Commonwealth Bank of Australia, Telstra Corporation and the State Government of NSW. SQC's foundation intellectual property was developed by the CQC2T. It uses atom-based qubits in silicon and is a full stack company aiming to demonstrate a quantum integrated circuit by 2023, a 100-qubit processor by 2028, and employ error correction by the mid-2030s, enabling access to useful quantum computing solutions for a broad range of users and multiple uses.
- + **Aqacia** is a machine learning start-up that builds on machine learning technology originally designed to optimise magneto-optical traps. Here in a feedback loop setting, this neural network based technology is capable of simultaneously optimising up to thousands of parameters in complex processes. It can also be configured for deep learning for pattern recognition. Aqacia is utilising this technology in the renewable sector with applications in predictive modelling of chaotic wind patterns for wind energy generation and optical recognition of defects in solar panels. Aqacia plans to harness powerful deep learning approaches to enable and accelerate technologies in quantum computation and quantum communication.
- + **Diraq** was launched in May 2022 as an end-to-end quantum computing provider – providing quantum hardware and software as a full stack, cloud accessible service. Their proprietary technology is backed by 20 years of research and over \$100m in funding across 9 patent families, allowing scaling using existing silicon CMOS manufacturing and existing foundries.

The **University of Technology Sydney’s (UTS)** Centre for Quantum Software and Information (QSI) researches and develops software for quantum computers and seeks to discover new information processing applications and hardware infrastructure for future quantum technologies. UTS works with researchers in Australia and around the world on both the foundational understanding of quantum information science and developing the software, information processing and hardware infrastructure required for future quantum technologies. UTS’s theoretical research spans the development of “full stack” quantum computing and communication, while its hardware team focusses on developing tools and techniques critical for superconducting circuit-based quantum information science, which appears to be one of the most promising hardware platforms for quantum computing.



Sourced from: <https://www.uts.edu.au/research-and-teaching/our-research/centre-quantum-software-and-information/qsi-research/qsi-research-programs>

Q-CTRL uses quantum control to solve problems, improve hardware performance and pave the way to more efficient and useful quantum computers. Q-CTRL specialises in quantum firmware, making advancements in reducing error rates, increasing hardware stability and uptime, and maximising device performance homogeneity. Quantum firmware reduces the need for extra error-correcting qubits and stabilises qubits against noise and decoherence. Q-CTRL believes that quantum advantage will be reached faster by focusing on quantum firmware rather than on quantum error-control. In 2021, Q-CTRL received \$4.5 million from the Australian Government's Modern Manufacturing Initiative and is funded by a range of venture capital firms from the USA and Australia.

Quantum Brilliance. Founded in Canberra in 2019, Quantum Brilliance aims to be a world leader in quantum accelerators, providing at 50+ qubits of quantum utility that end users can deploy where required to provide accelerated computing power. By focusing on size and mobility, Quantum Brilliance aims to push towards a mass market technology and broaden perspectives on the potential use cases for quantum technology. In 2020, the **Pawsey Supercomputing Centre** announced a partnership with Quantum Brilliance to collaborate on a quantum supercomputing hub. In 2021, Quantum Brilliance received \$13 million in seed investment to advance development of their quantum accelerator technology.

IBM Quantum is dedicated to building universal quantum computers for business, engineering and science. This effort includes advancing the entire quantum computing technology stack and exploring applications to make quantum broadly usable and accessible. IBM's roadmap leads from noisy, small-scale devices to million-plus qubit devices of the future. Their larger mission is to design a full-stack quantum computer deployed via the cloud that anyone around the world can program. IBM developed a 127-qubit system in 2021 (IBM Quantum Eagle) and are planning to advance to a 1,000-plus qubit device (IBM Quantum Condor) in Q2, 2023. They are also developing a suite of scalable devices. IBM is partnering with industries and fostering a growing ecosystem through their IBM Q Network. This includes collaboration with The University of Melbourne

as an IBM Quantum Hub, partnering with organisations such as Daimler-Benz, ExxonMobil and CERN, and enabling start-ups such as Q-CTRL.

Google Quantum AI is building a quantum computer using superconducting integrated circuits in conjunction with the associated software and algorithms required to deliver useful quantum computing. Google are aiming to build a “useful, error-corrected quantum computer” by the end of the decade.

Rigetti Computing is a full-stack quantum computing company. It designs and fabricates quantum chips, integrates them with a controlling architecture, and develops software for programmers to use to build algorithms for the chips. The company hosts a cloud computing platform called Forest, which gives developers access to quantum processors so they can write quantum algorithms for testing purposes. In October of 2021, it was announced that Rigetti planned to go public with an estimated valuation around \$1.5 billion. This will allow the company to raise an additional \$458 million in funding. With this funding, Rigetti plans to scale its systems from 80 qubits to 1,000 qubits by 2024, and to 4,000 by 2026.

Microsoft are engaging in quantum computer development. They also claim to have provided the world’s first full-stack, open cloud quantum computing system. In terms of quantum computer hardware development Microsoft have focused on a unique topological qubit, specifically a so-called Majorana qubit, which if realisable will significantly reduce quantum computer vulnerability to decoherence and would pave the way to realising stable quantum computing. Microsoft have also developed the Azure Quantum open cloud system with an interface which allows quantum computer programs to be run on quantum computers from IonQ, Toshiba, qci, 1Qbit, Honeywell and Microsoft. Microsoft also have a presence in Sydney where they have established a node of Microsoft Quantum, directed by Prof. David Reilly. Research in Sydney focuses on bridging the gap between fundamental quantum physics and the engineering approaches needed to scale quantum devices into quantum machines.

D-Wave and NEC. D-Wave Systems is a Canadian company that is seeking to provide the fastest path to practical quantum applications that have real-world value to users. D-Wave has focused on quantum annealing to aim for a quantum advantage as early as possible. They develop hardware as well as important user services such as cloud access and application development. In 2019, D-Wave entered into a partnership with NEC, a Japanese ICT solution and services company, to accelerate the development and application of quantum computing to customer problems. In Australia, D-Wave and NEC participated in the Army Quantum Technology Challenge to demonstrate the potential use of quantum computing to optimise how autonomous vehicles might resupply army forces from a central base.

Qubits and Materials

Quantum bits (qubits) underpin quantum computing. Qubits are quantum objects in a two-state quantum mechanical system. These are directly analogous to the two states of classic binary bits. Quantum computing is well suited to solving certain algorithms because qubits can be in these two states simultaneously (superposition). Additionally, qubits can be entangled, meaning their system's states are correlated with each other, significantly increasing potential computational power. These features give quantum computers an advantage for specific types of computational problems.

Quantum computing takes advantage of either static or flying qubits, and these have applications in technology that are easily represented in the stack. Flying qubits are required for quantum communication, which facilitates information transmission in the form of qubits for both computation and encryption. Another application of quantum technology is quantum sensing, which relies on quantum scale objects that are extraordinarily sensitive to their environment to create advanced probes and measuring devices. Quantum sensors, producing information in the quantum state, can be combined with quantum computers, processing information that would otherwise be lost on classical computers. This kind of measurement and processing capability could provide new

information and capability to scan environments, detect underground structures and detect patterns.

Quantum Error Correction (QEC). Due to the sensitive nature of qubits, QEC is essential to protecting quantum information in quantum computers. Furthermore, QEC will need to be imported back into other quantum technologies as it is enhanced. Many advancements in QEC can have benefits in sensing e.g. sending entangled states across large distances will require heavy error correction to support the protection of quantum information. What is learnt from quantum computing about generating and verifying quantum entanglement is likely to feed back into quantum communication and quantum sensing.



Sourced from: <https://www.abc.net.au/news/science/2021-02-02/quantum-computing-heat-qubits-control-chip-microsoft-sydney/13109148>

Qubit Architectures

Several qubit architectures using different materials are being actively researched. These architectures provide different advantages and disadvantages based on the underlying physics of the systems. Furthermore, there are likely to be qubits made of different and new materials as quantum computing progresses. Importantly, due to the strengths and weaknesses of different types of qubits, qubit selection will fundamentally affect the selection of all other stack components of the quantum computer being built. Hence, stack components within a quantum computer cannot be constructed independently of each other. Furthermore, until devices get above 1,000 qubits, it is unlikely that quantum computers will achieve the levels of fidelity and accuracy currently being achieved with classical computers. However, what quantum computers lack in fidelity and accuracy, they make up for in speed. As such, sub-optimal quantum solutions can be achieved far more quickly than optimal classical solutions. The following provide examples of qubit types.

Superconducting qubits are the focus of IBM and Google's research, using phenomena found in superconducting circuits to create a quantum two-state system. The main advantages of superconducting qubits are their fast gate times (essentially faster computation) and the technology they're based on (they have benefited from technology such as printable circuits). They also come with disadvantages, such as their large physical size, the more rigorous calibration and their expensive temperature requirement (necessarily significantly below 0.1K).

Ion trap qubits utilise magnetic and electric fields to trap ions and hold them in place. The outermost electrons are used as qubits by putting them in different energy states. They are much more stable than a superconducting qubit (lower decoherence) and can effectively work at much higher temperatures (\rightarrow 4 K). However, they are slower than superconducting qubits and there are challenges in scaling up ion traps to accommodate more than a few dozen qubits. Nevertheless, ion trap qubits are very well understood given the research effort which has gone into ion trap-based clocks (which rely on qubits coupled together using

vibrational modes of chains of ions in traps). There is current research focussing on scaling up ion traps to accommodate more than a few dozen ion/qubits. However scaling requires different technologies to be developed. A very similar technology is **neutral atom quantum computing**, which uses arrays of ultra-cold neutral atoms in an optical lattice. Qubits are encoded on electronic or nuclear spin states of the neutral atoms. This approach builds on technology used to implement neutral atom clocks. Using this technology, single qubit operations can be carried out with great precision. Two qubit operations can be carried out by exciting neighbouring atoms in the lattice to so-called Rydberg states where their wave functions interact strongly. Two-qubit interaction can then be implemented using so-called Rydberg blockade. Although not without scaling challenges for error correction, such a device has the potential to be scaled up to many thousands of qubits.

Nitrogen vacancy (NV) diamond qubits are formed from special defects in diamond lattices. NV centres are formed when a single carbon atom in a diamond's atomic lattice is replaced by a nitrogen atom adjacent to a vacancy in the lattice, where a carbon atom is missing. The NV centre's electronic spins react with the nuclear spin of some of the carbon atoms nearby, thus resulting in the NV centre and the adjacent carbon atoms functioning as qubits. They may be limited in their scalability; however, they can operate at room temperature.

Silicon qubits seek to use either the electron or nuclear spin states of donor atoms in silicon or electron spins in quantum dots to form qubits. Using electron or nuclear spins in silicon may have significant advantages in reducing errors in quantum computers as their spin state can be controlled for relatively long periods of time in comparison to other qubit architectures (up to a few minutes for nuclear spins). This technology requires isotopically pure silicon (sourced globally and now manufactured in Australia with an Australian manufacturer, Silex). The main challenge is to manufacture at the nano to atomic length scales, an area where Australia has global leadership.

Optical Quantum Computing (OQC) relies on photons as the main information carrier and uses optical elements to process quantum information, and photon detection and quantum memories to detect and store quantum information. A major advantage of OQC is its ability to link quantum computation and quantum communication in the same system. Other advantages include room temperature gate operations and the potential for ultra-fast gate operation. The most developed versions of OQC are linear optical quantum computation (LOQC) systems which use linear optical elements to process the quantum information. Superpositions of quantum states can be easily represented, encrypted, transmitted, and detected using photons. Although single qubit operations are straightforward to perform, two qubit interactions are more difficult to implement. Two qubit interactions in many instantiations of photonic quantum computing are not deterministic, which requires techniques to manage the inherent latency this causes. State-of-the-art LOQC systems have a scale of the order of 60 qubits, but currently suffer from low re-configurability and are typically built to specialise at one or a few types of problem.

Bosonic Codes encode discrete quantum information within bosonic systems such as modes of light, superconducting microwave cavities, or the collective motion of material systems. Bosonic codes can use single photons as the quantum information carrier, but also other sophisticated encodings exist, such as cat codes, binomial codes, and grid codes (also known as GKP codes). These new codes provide robustness to noise within the qubit itself, and grid codes in particular also allow for deterministic single- and two-qubit gates. They are compatible with demonstrations of scalable OQC architectures using time-bin encoded modes. The challenge in optics lies in producing the code states themselves. Bosonic codes offer advantages in superconducting systems: using this code reverses the usual roles of the hardware components, allowing the longer-lifetime microwave cavities to carry the quantum information, while the superconducting qubits play a supporting role.

Rare Earth Quantum Memory and Computing are technologies in which rare earth ions are embedded in a crystal lattice. Nuclear and electronic spin states of rare earths are particularly stable and make excellent qubits. One of the reasons for the stability of rare earth qubits is that the electronic spin states of electrons used as qubits are inside closed shells. The closed shells act like a Faraday cage, shielding inner qubit electrons from their environment. Qubit lifetimes of 6 hours have been demonstrated, making rare earth systems excellent quantum memories. Two qubit operations can also be implemented in a few ways. There have been proposals to use the long lifetime of rare earths to reduce the number of qubits required for large-scale quantum computing, although at the cost of some reduction in speed.



Qubit Housing

Qubit housing refers to the physical materials that allow controllable qubits. For almost every approach to quantum computing there is a requirement to start with highly specialised materials which need to undergo precise fabrication to build the 'homes' for the qubits. Indeed, Australia's leading quantum computing hardware manufactures: Silicon Quantum Computing, and now Diraq, require semiconductor grade base materials with isotopic purity. These materials must then be processed by high precision steps to yield devices suitable for high fidelity 'quantum chips'. Increasing the quality of these material and processes leads to improvements in the overall quality and is very important when considering quantum computers in terms of both the full quantum computing stack and sovereign quantum capability. The talent and facilities required to produce high quality devices is non-trivial and serious thought needs to be applied with regard to how this fits into the broader quantum ecosystem.

Networking and Integration

Quantum networking, cloud-based quantum computing and other developments will rely heavily on technology developments occurring in parallel to deliver the potential value promised by various quantum technologies. In one sense all quantum technologies are linked; nodes in the network are quantum computers, or the network as a whole is a quantum computer. With this type of large convergence, it can be simple to not distinguish between the two. Similarly, anything that is relevant for sensing is relevant for quantum computers, and perhaps vice versa. Therefore, is quantum computing something that will underpin the quantum technology ecosystem, is it the umbrella, or is it interwoven into everything?

What is meant by a network? Would it mean physically connecting quantum computers to one another with a coax cable, or would it mean connecting the computers in a quantum manner? Physical connection (via wire) could result in a linear increase in power. On the other hand, to get an increase in power from quantum effects by networking computers,

they would need to be connected in a quantum mechanical way. Which invites the question, is it just one connector coming out of the quantum computer, or is it from all of the qubits on the edge, or is it from all of the qubits? It is difficult to know what the outcome will be as the network would have to be very carefully defined.

The nature of qubits is such that it may be that the more qubits are connected, the more computing power is achieved, so the network will be greater than the sum of the parts (in this respect a quantum computer is a network in and of itself). As such, the idea of having repeater networks to allow secure communication systems will create a larger network and exponentially more powerful quantum computing. However, from a practical perspective, one assertion is that focus should be applied to developing one quantum computer first, in order to prove that it works before applying effort to developing a network. Following on from this, is there a compelling argument for a 'quantum internet'?

As with classical computing, quantum computers will ultimately be networked. This will enable greater computational power to be harnessed; collection of information from quantum sensors for processing; secure communication; and secure and anonymous information processing using techniques such as blind computation and homomorphic cryptography. To achieve this, quantum channels are required. These channels will need not only to bridge large distances, but also convert between different physical types of qubits. For example, if we have two silicon-based quantum computers which we wish to connect via an optical fibre, we need a mechanism which enables transfer of quantum information encoded on nuclear spin of phosphorus atoms to photon polarisation and back again.

Hybrid quantum-classical systems are one of the key directions of development. These systems are well-suited for many use cases (such as quantum-assisted ML mentioned in Section 2 of the main body) where quantum computers work in a hybrid computing system, co-existing with CPUs or GPUs and cross interacting with each while being best in their own domains. Examinations of algorithms and applications need to

include the development of software that will allow these hybrid handoffs and networking to occur. This includes integration with current and future classical systems, networking, protocols, and industry standards. It is anticipated that when considering integration and networking the majority of problems will rest on the classical side of computing.

One of the challenges of the transfer of quantum information is that quantum states are fragile and regular communication techniques cannot be used to make them more robust. Currently, long-distance quantum communications systems require transmission over the free space channel to minimise loss. However, for many future applications this may not be feasible or desirable. The most likely way this limitation will be overcome is to use specialised quantum repeaters, which are in effect small-scale quantum computers. These repeaters make a resilient quantum channel by applying techniques to continuously create and distribute quantum entanglement. This entanglement resource can then be used to teleport quantum information around a network. One can think of quantum entanglement as a fuel for communication, which is used as quantum information is teleported around a network. A second option is to create systems which are able to store entangled quantum states for long periods of time. The stored quantum entanglement can then be used to teleport quantum information with the aid of classical communication. These quantum memories would need to be refuelled by replenishing the entanglement as it is used to transport quantum information.

Technology Readiness Level (TRL) Across the Stack

Progression of technology across the stack is interdependent. For example, developments in control software or error correction can reduce the number of physical qubits required to produce computations. Equally, development of hardware that has a higher number of logical qubits, or produces qubits with higher fidelity, will reduce the need for further error correction. As a result, research and industry development across the stack is reliant on the progression and architecture of other components. Some researchers and organisations focus on one or two layers of the stack, while others look at the full stack.

When we assess the TRL of quantum computing, the maturity of each of the elements of the quantum computer stack needs to be considered. It is instructive to consider the TRL of each element of the quantum computer stack to determine the most useful focus of resources to realise quantum computation.

There is a complex relationship between the various elements of the stack and the tasks each layer needs to perform will depend on:

- + the type of qubits used
- + error rates and types of errors
- + the number of qubits required to run an application
- + the amount of time a calculation required for a particular application.

As the TRL of the qubits evolve the supporting levels in the stack have evolved with them to extract as much processing power as possible. In this sense, currently, the limiting levels in the stack are the qubit and hardware levels.

Given the requirement for full stack integration, all stack components will need to be at a level of TRL maturity to enable integration and subsequent generation of a level of quantum computing that can be applied to use cases i.e. allow the associated algorithm to be run. Currently, qubits and hardware are stack components considered to be on the critical path for achieving desirable overall system maturity for a functioning quantum computer. However, this may or may not be the situation for all use cases and their associated algorithms and software could be the constraint.

Quantum Communication

Quantum communication networks and cybersecurity technologies may provide more security for communication channels and enable networking of quantum computers. Quantum networks could enable distributed quantum computing and rapid problem solving, which will have implications for infrastructure, telecommunications, and space sectors.

As quantum systems cannot be observed or measured without changing their properties, information encoded in quantum objects will be affected by attempts to read it. Quantum key distribution is the most mature application exploiting this property. It involves sharing cryptographic keys using quantum states so that attempts at intercept can be detected. However, this only applies to information in a quantum state, because as soon as the information is transferred to a classical system, it becomes vulnerable. Quantum key distribution is significantly more technically complex and sensitive to disruption than classical communications, which may limit its application to niche areas.

Quantum communications could offer more secure communications systems, especially as the development of quantum computing provides a greater threat to some forms of conventional encryption standards, which could be broken by a sufficiently large quantum computer. Quantum communications may be relevant to Defence and other industries to protect sensitive data and critical infrastructure.

Quantum Sensing

Quantum sensing technology has the potential to enable a range of new or improved capabilities. Position, navigation, and timing systems can use quantum-enhanced sensing to provide location and environmental information without requiring GPS systems. Quantum-enabled PNT will utilise advanced sensors for magnetic and electric field, gravity, and chemical detection. Quantum sensing may also provide faster and cheaper geophysical surveying and imaging technology at the nanoscale.

It is important that investment decisions look to where real value can be added, of which, quantum computing is one aspect. While commercial investors do not tend to be interested in quantum sensing, it is suggested that a broader investment approach should consider quantum sensors as a complementary activity in the development of quantum computing. The pathway to useful quantum computing is potentially longer than anyone recognises, as the difficulties are not fully appreciated. However, there is a shorter-term play in quantum sensing, as most quantum sensors behave like a one qubit quantum computer. As such, lessons from

sensors can drive quantum computing advancement. Using a quantum sensing business play could be a way to bridge the gap to long-term quantum computing development. Examples include:

- + The ability to detect and discover ground water and mineral deposits that will unlock needed resources, including in Australia where we are water quality constrained.
- + Bio imaging and bio sensing areas that could result in the development of quantum microscopes and quantum diagnostic technologies that can detect illness at a molecular level and make early diagnoses before signs and symptoms develop.
- + Quantum astronomy and Earth observation to provide enhanced space exploration, astronomical sensing, space-based imagery, and gravimetry and magnetometry measurements.

As quantum sensors and other quantum technologies are developed, they will continue to collect quantum information, which if kept at the quantum level can then be processed with a quantum computer. On one level the entire system could be considered a single quantum sensor. Consideration of such a holistic approach at the system level, and at the ecosystem level, may lead to a significant change in the approach to quantum computing.

Annex C Additional Australian Context

General

Australia's particular expertise includes quantum information processing, quantum computing technology in silicon and optics, and quantum error correction and control. Australia has significant bilateral and multilateral agreements and is involved with international partners through activities such as The Technical Cooperation Program. The Australia–US Multidisciplinary University Research Initiative Program (AUSMURI) is a great example of Australian and US international collaboration.

AUSMURI is part of the Next Generation Technologies Fund (NGTF) where an Australian university selected to be part of an Australia-US collaborative research project in the US Multidisciplinary University Research Initiative (MURI) program may be eligible for Defence funding up to a maximum of AUD\$1 million a year over three years, with a possible extension for a further two years.⁹

The 'Quantum Control Based on Real-time Environment Analysis' project was selected for funding in 2018, with an extension of funding announced in 2021. This project is a partnership between Griffith University, the University of Technology Sydney, and the University of NSW in collaboration with the US team, led by Duke University.¹⁰

The USA's National Quantum Initiative, signed into law in 2018, has led to much greater investment and coordination across government bodies. The USA has historically committed to basic research and has funded Australian quantum research over the long term. There are various avenues for information sharing and agreements between the USA and Australia, which should ensure that this relationship continues.

⁹ Defence Science and Technology Group. AUSMURI 2021 round 5 announced. Accessed 10 September 2021. <<https://www.dst.defence.gov.au/partner-with-us/opportunities/ausmuri-2021-round-5-announced>>

¹⁰ IQT News. Funding Extended for Two Years for Griffith University's 'Quantum Control Based on Real-Time Environment Analysis By Spectator Qubits' Project. 28 June 2021. <<https://www.insidequantumtechnology.com/news-archive/funding-extended-for-two-years-for-griffith-universitys-quantum-control-based-on-real-time-environment-analysis-by-spectator-qubits-project/>>

Australia's Quantum Talent

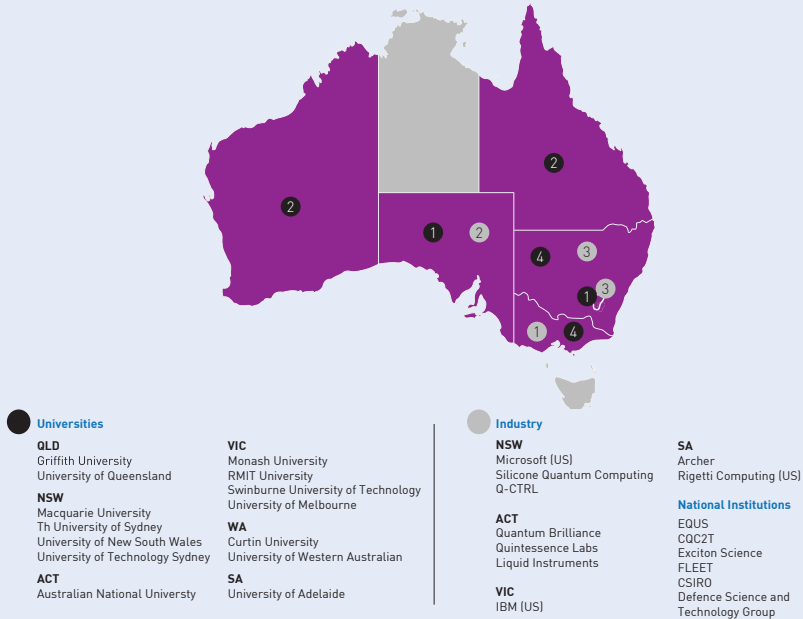
Australia is currently a recognised global leader in quantum computing and areas of quantum-enabled technology. The international quantum technology workforce is highly sought after, skilled, and mobile. Many jurisdictions are offering significant support packages to individuals and organisations to domicile in their region. Australia has been both a producer of quantum computing talent that have studied and researched with Australian institutions, and a destination for individuals seeking support for their fields of research or commercial application. It needs to be acknowledged that Australia's quantum computer technology lead has been developed through the consistent support of the Australian Research Council (ARC).

Australia has produced and attracted important leaders in the quantum computing sector. Outside of Australia, Canadian start-up Xanadu was founded by an Australian, and the UK-based PsiQuantum was cofounded by Australians and has an Australian CEO.

Many Australian-based start-ups now have a global presence and attract international funding. QuintessenceLabs is headquartered in Canberra but also has offices in Silicon Valley in the USA. Australian start-up Q-CTRL has a presence in the USA and investment from Silicon Valley venture capital funds. Quantum Brilliance, also headquartered in Canberra, has a presence in Germany.

Participants at the 2021 *Quantum Computing: In Focus* event suggested that government stakeholders can support Australia's quantum talent by demonstrating commitment to the quantum sector and setting a clear agenda for growth. This will provide confidence to the sector and will encourage young scientists and engineers to pursue study and careers in quantum.

Key stakeholders in the Australian quantum computing ecosystem (Adapted from CSIRO Futures, 2020).



Academic and research institutions play a critical role in developing Australian quantum workforce. Australia’s growing quantum industry can take advantage of the benefits this talent pool brings, with the support of Defence as a collaborator and end user for its technologies. Industry will also provide career opportunities for these skilled professionals.

Sydney Quantum Academy (SQA)

Sydney Quantum Academy’s stated vision is to build Australia’s quantum economy. By collaborating with academia, industry, and government, SQA will harness Sydney’s collective quantum expertise to develop diverse talent and a globally recognised quantum ecosystem. SQA is a joint venture between Macquarie University, UNSW Sydney, the University of

Sydney, and the University of Technology Sydney. They have received a total of almost \$35 million in funding, including \$15.4 million in funding by the NSW government in 2019.

“At Microsoft Quantum in Sydney we have dozens of people employed in new, high-tech jobs. But we will need hundreds, if not thousands, of trained quantum engineers to make the promise of quantum technology a reality. The Sydney Quantum Academy will help us achieve this vision.”

Professor David Reilly (Chief Investigator, EQUS & Director, Microsoft Quantum Laboratory)

Australian Quantum Capability

Australia has world class quantum technology research and development capabilities. In some areas, Australia’s academic and research institutions are globally renowned because of sustained investment since the 1990s. This investment has been sourced from Australian Research Council (ARC) programs, Defence, and industry grants as well as start-ups in the sector attracting venture capital funding. Australian research has also attracted long-term investment from the US Department of Defense.

There is, however, a growing consensus that Australia must accelerate its investment to secure its position as part of a rapidly expanding global industry. Many countries have expanded their investment in quantum capabilities and increased the competition for talent and domestic strength in key areas of the quantum technology stack.¹¹ Countries that have provided significant public funding for quantum technology in recent years include the United States, United Kingdom, Germany, Netherlands, India and Russia.¹² This increase in investment internationally has been noted in calls from industry (such as by the Australian Information Industry Association¹³ and the Australian Strategic Policy Institute) for Australia to more deliberately plan for and invest in its quantum industry.¹⁴

11 Brennen, G., Devitt, S., Roberson, T. and Rohde, P. (2021) Policy Brief: An Australian strategy for the quantum revolution. Australian Strategic Policy Institute, Australia. Viewed 7 September 2021, <<https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-05/Quantum%20revolution-v2.pdf>>

12 CSIRO Futures (2020) Growing Australia’s Quantum Technology Industry. CSIRO, Australia. Viewed 7 September 2021, <https://www.csiro.au/-/media/Do-Business/Files/Futures/Quantum/20-00095_SER-FUT_REPORT_QuantumTechnologyRoadmap_WEB_200518.pdf>

13 AIIA (2021) Growing globally competitive industries: Powered by Australia’s innovation technology. Australian Information Industry Association. Viewed 7 September <<https://aiia.com.au/wp-content/uploads/2021/08/AIIA-Growing-Globally-Competitive-Industries.pdf>>

14 Brennen, G., Devitt, S., Roberson, T. and Rohde, P. (2021) Policy Brief: An Australian strategy for the quantum revolution. Australian Strategic Policy Institute, Australia. Viewed 7 September 2021, <<https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-05/Quantum%20revolution-v2.pdf>>

This perspective is summarised in the CSIRO Futures' report on Growing Australia's Quantum Technology Industry released in 2020.¹⁵ CSIRO Futures recommends a range of coordinated actions to enable the growth of Australia's quantum technology industry, to be led by a national quantum technology strategy. Growing Australia's quantum computing industry will have direct and indirect advantages. A growing quantum industry will directly create jobs, but more importantly, will underpin a quantum-enabled economy where high-performance computing provides significant advantages and opportunities for growth.

Australia has an opportunity to benefit from the 'first mover advantage' as we are a world-leader in some aspects of the quantum sector. However, continuing this leadership and securing an advantage will require commitment to our domestic ecosystem and incentives for talent to contribute to Australia's quantum capability.

Pawsey Supercomputing Centre and Quantum Brilliance Quantum Supercomputing Hub

The Pawsey Supercomputing Centre and Quantum Brilliance collaboration is a direct initiative to implement the recommendations from CSIRO's "Growing Australia's Quantum Technology Industry". Quantum Brilliance will install a diamond quantum accelerator to the Pawsey Supercomputing Centre in Perth. The Pawsey facility is one of two Tier-1 high-performance computing and data research facilities in Australia. It is an unincorporated joint venture between CSIRO and Western Australia's four public universities, supported by the State and Federal governments. Pawsey is managed by CSIRO as a national facility available to the broader science community.¹⁶ The collaboration will enhance domestic quantum expertise and provide researchers access to a quantum emulator.

¹⁵ CSIRO Futures (2020) Growing Australia's Quantum Technology Industry. CSIRO, Australia. Viewed 7 September 2021, <https://www.csiro.au/-/media/Do-Business/Files/Futures/Quantum/20-00095_SER-FUT_REPORT_QuantumTechnologyRoadmap_WEB_200518.pdf>

¹⁶ <https://www.csiro.au/en/News/News-releases/2020/Pawsey-and-Quantum-Brilliance-join-forces>

Building Australia's Quantum Ecosystem

Australia has a substantial quantum ecosystem comprising academia, start-ups, and large international corporations. Quantum computing and related technologies are highly specialised fields, making this ecosystem diverse in its areas of focus and potential for growth. This provides momentum and an opportunity for a first mover advantage in some areas if Defence and other stakeholders act quickly.

The major risks identified at the 2021 *Quantum Computing: In Focus* event hosted by DSTG concerned whether Australia could capitalise on its current strengths in quantum computing given the rapidly growing industry and the increasing investment in the sector across the world. Participants thought that there was a risk of Australia losing its talent to overseas competitors and failing to attract international talent. The quantum computing industry is globally dispersed, and individuals can easily move to countries that offer to fund their research or business ventures. Australia lacks the economic scale and mature technology sectors of some of its competitors for international talent. In addition to losing key talent, Australia's manufacturing skills and capacity will need to be able to capitalise on our research success to make products at a scale that is sufficient for global markets.

Another key risk is the need to balance the national interests associated with critical and sensitive technologies with the unique needs of start-ups that drive the quantum sector. Start-ups must often work at rapid pace to demonstrate progress and access capital quickly. Delays caused by investment controls and other regulatory hurdles can be particularly damaging to these businesses and affect their ability to retain talent and compete internationally. Quantum computing relies on highly specialised intellectual capacity and capability so there is potential for it to provide significant economic value to Australia more broadly.

Technology Pathways

Australia should be engaging internationally to participate in and shape conversations on frameworks, benchmarking, and standards at this early stage of the quantum computing development. Doing so will help understand the progress of Australia's technologies, as well as support their integration into global conversations and markets. Australia is well-placed to participate in this space because of its global leadership position. It is challenging for small organisations such as early start-ups to invest in activity to support global coordination and governance. Setting international benchmarks and standards is time-consuming and the benefits will only be realised in the longer-term. It is worth exploring whether Defence or the government should directly support or fund these global endeavours.

While it will be necessary to select key areas for focus and commitment, a more strategic and measured approach is needed to assess any risks associated with committing to certain technologies or their applications to ensure they reach their potential. A key challenge will be determining whether some developments are no longer relevant and determining whether the 'hype' of specific technologies or applications is valid.

Benchmarking and Standards

The need for benchmarking and quantum computing metrics will be essential as quantum computing continues to develop. Standardised benchmarking of systems will enable the performance characteristics of different systems to be understood and compared. This should provide a consistent and objective measurement of the quantum computing advantage that is based on specific applications, rather than a simplified theoretical model of potential applications. Benchmarking will help overcome the challenge of comparing the diversity of technologies under active research, as well as comparing quantum solutions to classical solutions to determine whether quantum advantage has been achieved. Currently, one concept for benchmarking is quantum volume, but there are many others. This considers the whole technology stack, although it cannot be applied to individual layers of the stack. Tailored benchmarking

will be required for different applications of the technology, as well as for quantum communications and sensing applications.

Developing and applying quantum computing standards is an important step in supporting global and domestic interoperability and coordination of quantum computing technologies across different layers of the stack. Setting standards can play a significant role in gaining a first or early mover advantage.

