



# Quantum Computing Hype or Reality?

**July 2021**



## State of Play

CSIRO's [Growing Australia's Quantum Technology Industry](#) report recently signalled the potential opportunity for 16,000 Australian jobs over the next 20 years in quantum technologies, as well as quantum technologies becoming an integral part of Australia's technology sector. This coupled with an increasing amount of funding from government and private investors, along with the exponential increase in quantum technologies related patents, is a clear indicator that the proverbial lever has been pushed from 'Hype' to 'Reality'.

History can often be our greatest adviser in helping us prepare for the future. To comprehend Quantum Computing, it is worth looking at the beginnings of the classical computer, and appreciate the evolution that has brought it to where it is today. With its origins in the mid-20th century, classical computing has evolved immensely to a state where we now carry incredible computing power in our mobile phones, wearable devices, and leverage advanced classical computing capabilities for prostheses such as bionic eyes.

In comparison, quantum computing today is in its inception, similar to where the classical computer was in the mid-20th century. It is however evolving rapidly, thanks to advanced research and manufacturing capabilities available today. While quantum computing is not set to replace classical computing, it is a powerful complementing technology that technology giants, governments, and private investors are investing billions in to unlock new opportunities.

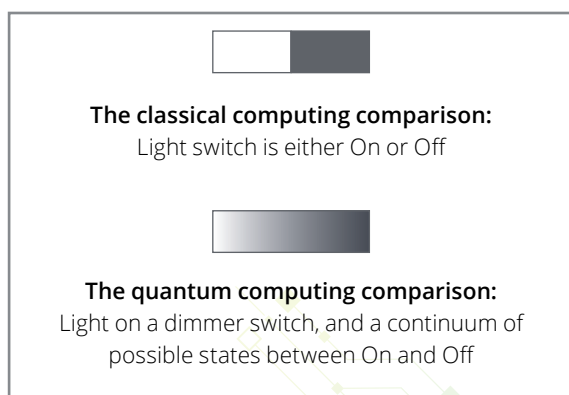
## Inside the quantum computer

Where classical computers used transistors to achieve their binary logic, or bits of 1's and 0's, quantum computers leverage the structure and behaviour of light and matter at their most fundamental level. This can take the form of:

- Superconducting electrical circuits maintained at temperatures close to absolute zero (approximately -273oC), or
- The electronic states of an atom kept trapped in an ultra-high vacuum environment within complex electromagnetic fields.

These are techniques to exploit quantum behaviour. The most important is that quantum particles can exist in combinations of two distinct quantum states, a property known as superposition. Where a classic computer's bits can exist as a 1 or a 0, quantum superposition allows quantum bits (known as qubits) to exist either as a 1 or a 0, or as a combination of the two.

A simple way to imagine the logic differences between a classical computer and a quantum computer is to think of a light switch. Classical computers are a simple light switch – on and off. Quantum computers on the other hand behave like a dimmer switch.



## Entanglement

In addition to superposition, the power of quantum computing is realised through a phenomenon called entanglement; something Albert Einstein referred to as “spooky action at a distance”. Entanglement is a unique property of quantum mechanics where quantum particles are entangled, such that action on one particle affects the other, even when separated by great distance. To put simply, instead of having to compute millions of calculations as we would in a classical computer, a quantum system can potentially infer the logic of the entire system based on just a few calculations.

The ability to combine quantum superposition with entanglement leads to algorithmic solutions for certain problems that are vastly faster than any possible algorithm based on the classical principles of computing.

## Noise and Error Rates

Considering that quantum computing is achieved by manipulating sub-atomic particles, the efficacy in being able to successfully control these particles can be dependent on factors such as the environment (e.g. ability to maintain -273°C without interferences). These interferences result in noise that gives rise to error effects in quantum systems. These error effects are significantly larger than the noise we see in classical semiconductor electronics, and are so large that being able to implement large quantum algorithms is not possible without techniques to mitigate these errors. For large-scale machines, the framework that has been developed for this is known as Quantum Error Correction. Quantum Error Correction requires a large resource overhead in terms of qubits in the quantum chip. In the future this overhead may be made irrelevant through better devices.



## When to use Classical Computing vs. Quantum Computing

### Classical computer

#### Pros:

Faster than quantum computing for structured and ordered computing. Examples include transactional processing, or processing based on structured data sets.

#### Cons:

Slow for complexed data sets, where exhaustive approaches are required. Examples include unstructured data analysis, or big data sets comprised of different types of data such as spatial data.

### Quantum computer

#### Pros:

Faster than classical computing for unstructured or deep analytical problems, such as optimisation problems. Examples include complex problems with vast amounts of scenarios and possibilities that require an optimal path, such as mapping fastest routes, or scheduling flights.


#### Cons:

Slow or not useful for simple computing such as emails, word processing, spreadsheets, or web browsing.

If for example we wanted to solve a problem that required us to count the number of holes on a page, there are two ways to achieve this with classical computing.

1. A sequential count of each hole, or
2. An algorithmic count – if the holes are structured in rows and columns

In quantum computing terms, this would be solved very differently. Rather than counting the holes, imagine flashing a light source through the holes, then using the resultant amount of light transmitted to gauge the number of holes on the page. This way it doesn't matter if the holes are structurally aligned or not – the time to compute the result remains the same – and exponentially faster than sequentially counting.



Quantum computing is not set to replace classical computing – consider them as complimenting technologies.



## Opportunities

Given the potential of quantum computing, what are the opportunities today, and tomorrow?

	Optimisation Algorithms	Data Science/ Quantum Modelling	Quantum Chemistry/ Material Science	Security and Cryptography
Consumer	<ul style="list-style-type: none"> <li>Vehicle Routing</li> <li>Distribution Supply Chain</li> </ul>	<ul style="list-style-type: none"> <li>Freight Forecasting</li> <li>Irregular Behaviors</li> <li>Disruption Management</li> <li>Consumer Offer Recommender</li> </ul>	<ul style="list-style-type: none"> <li>Quantum LIDAR / improved sensors</li> </ul>	<ul style="list-style-type: none"> <li>Secure Communications</li> <li>Quantum-proof encryption</li> </ul>
Energy, Resource & Industrials	<ul style="list-style-type: none"> <li>Oil shipping/trucking</li> <li>Refining processes</li> <li>Feedstock to product</li> <li>Process Planning</li> <li>Supply Chain</li> <li>Fabrication Optimization</li> </ul>	<ul style="list-style-type: none"> <li>Seismic imaging</li> <li>Drilling locations</li> <li>Quality Control</li> <li>Structural Design &amp; Fluid Dynamics</li> </ul>	<ul style="list-style-type: none"> <li>Surfactants, catalysts</li> <li>Chemical product design</li> <li>Materials Discovery</li> </ul>	<ul style="list-style-type: none"> <li>Secure Communications</li> </ul>
Financial Services	<ul style="list-style-type: none"> <li>Transaction Settlement</li> <li>Portfolio Management</li> <li>Financial Modelling</li> <li>Insurance pricing optimisation</li> </ul>	<ul style="list-style-type: none"> <li>Credit/Asset Scoring</li> <li>Derivatives Pricing</li> <li>Irregular Behaviors</li> <li>Investment Risk Analysis</li> <li>Finance Offer Recommender</li> <li>Trading strategies</li> </ul>	?	<ul style="list-style-type: none"> <li>Secure Communications</li> <li>Quantum-proof encryption</li> </ul>
Government & Public Services	<ul style="list-style-type: none"> <li>Vehicle Routing</li> <li>Supply Chain</li> </ul>	<ul style="list-style-type: none"> <li>Irregular Behaviors</li> <li>Disruption Management</li> </ul>	<ul style="list-style-type: none"> <li>Advanced materials research</li> </ul>	<ul style="list-style-type: none"> <li>Secure Communications</li> <li>Quantum-proof encryption</li> </ul>
Life Science & Health Care	<ul style="list-style-type: none"> <li>Medical/Drug Supply Chain</li> </ul>	<ul style="list-style-type: none"> <li>Accelerated Diagnosis</li> <li>Clinical Trial Enhancements</li> <li>Genomic Analysis</li> <li>Disease Risk Predictions</li> </ul>	<ul style="list-style-type: none"> <li>Drug Discovery</li> <li>Protein Structure Prediction</li> </ul>	<ul style="list-style-type: none"> <li>Quantum-proof encryption</li> </ul>
Technology, Media & Telecommunications	<ul style="list-style-type: none"> <li>Network Optimisation</li> </ul>	<ul style="list-style-type: none"> <li>Irregular Behaviors</li> </ul>	<ul style="list-style-type: none"> <li>Semiconductor materials discovery</li> <li>Materials process optimisation</li> </ul>	<ul style="list-style-type: none"> <li>Secure Communications</li> <li>Quantum-proof encryption</li> </ul>

● Near term impact

○ Long term impact

? No known impact at this time

Near term use case

Long term use case



## Opportunities in Financial Services

### Portfolio Management

For asset managers, asset owners, and investment banks who strive to rebalance, construct, and optimise portfolios, the power of quantum computing could potentially allow for on-demand analysis of current and historic data portfolio construction and optimisations in near real-time.

In addition, with a global trend towards private data for asset managers and owners, stock selection, and trading and hedging strategies may potentially be greatly enhanced through quantum computing by providing near real-time analysis of unstructured data to facilitate additional alpha generation or for stock diversification to minimise risk.

### Risk and Scenario Analysis

With the 2008 global financial crisis, many finance institutions are today required to comply with minimal capital requirements under regulations such as Basel 2.5, 3, and FRTB. These regulations require institutions to process vast amounts of historic data, coupled with live banking and trading data to facilitate back testing and 'what-if' scenarios analysis to establish their risk metrics. Quantum computing has the potential to exponentially speed up.



## Opportunities in Compliance and Cryptography

Risk and Fraud Detection for AML (Anti-Money Laundering)/CTF (Counter Terrorism Funding) is another area of great interest where quantum computing has the potential to offer immense benefits, however further analysis is needed.

Quantum Cryptography can enable quantum-secure encryptions, which can be used to protect systems and data from cyber-attacks with a greater level of security than current protocols, and ensuring they are future proofed to tolerate quantum computing attacks.



## Opportunities in Medicine

Bioinformatics is a field that leverages computer algorithms to process big data that can help characterise biological data such as in genomics, proteomics, and epigenomics. Quantum computing could potentially lead to quicker analysis of DNA and RNA sequencing data or facilitate in the design of proteins and their structures. This would massively improve the modelling and effects of particular drugs, and even facilitate personalised medicine.

Pharmaceutical companies would be huge beneficiaries of quantum computing in being able to design and develop targeted drugs for personalised medicine. Quantum computing would allow companies to perform molecular comparison on larger molecules, which could improve early stages of drug design. Particularly as the world races towards COVID-19 vaccines, or cancer therapeutics, imagine the possibilities quantum computing could offer pharmaceutical companies to design targeted therapeutics for the mass population which alleviates some of the current side-effects for a small proportion of the population.

In fact, molecular simulations (which could lead to drug design) and material science is one of the few areas where computational advantage for quantum is proven. Many expect the most profound impact to occur in this space. Further considerations include:

- What kind of modelling do you need in your market? What scale of quantum machine is necessary? Are you modelling small scale catalytic molecules? Or much larger amino acid sequences and protein structures that require many more qubits to model?
- How do you benchmark your specific problem and accurately calculate the physical qubit and time resources needed for your algorithm? How does Quantum Error Correction requirements and current hardware error rates effect the timeline to implementation on actual quantum hardware
- Assuming a quantum solution is appropriate to your simulation problem, what comes next? Does identifying the energy structure of the Nitrogenase compound immediately allow you to replace the Haber-Bosch process for nitrogen fixation and take over a \$1T market? If not, what other steps need to be considered and how does this effect your quantum analysis?

"Quantum computing has the potential to disrupt many industries, with Financial Services, Cryptography, and Medicine being some of the focus areas"



## Threats

As with most new technologies, quantum computing also poses a double-edged sword for the community. There are a number of opportunities as covered thus far, but there are also a number of threats.



## Threats – Bitcoin

Bitcoin is a cryptocurrency. It is a digital currency secured by cryptography and relies on this cryptography to secure the authenticity trust in the currency. With a classical computer (even today's super computers), it is considered impossible to break a Bitcoin account (theoretically, it could take billions of years). Quantum computing on the other hand, poses a very real threat. With the price of Bitcoins surging past \$USD50,000 at the time of this report, our article on [Quantum Computers and the Bitcoin Blockchain](#) contains further details on the risks quantum computers pose to Bitcoin.

"You have already done the things that will get you into trouble"



## Threats – Cyber Security

Information – sensitive or not – may already have been intercepted, and stored by intelligence agencies, or malicious actors. What's preventing access to this information is the encryption protecting it.

Many of today's cybersecurity protocols rely on strong encryption – for both data transmission and data at rest. Computational models based on classical computing methodologies estimate that the time to break an exceptionally strong algorithm (eg RSA-2048) would require 300 trillion years.

However, if the algorithm to crack RSA-2048 were to be run on a quantum computer, the time to break is significantly reduced. It is quite possible that within the next 20 years to have a quantum computer capable of breaking today's RSA-2048 encryption. However, this would require the following developments:

- Increase in absolute number of qubits in quantum processors
- Improvement in the quality of these qubits to reduce the amount of error correction needed

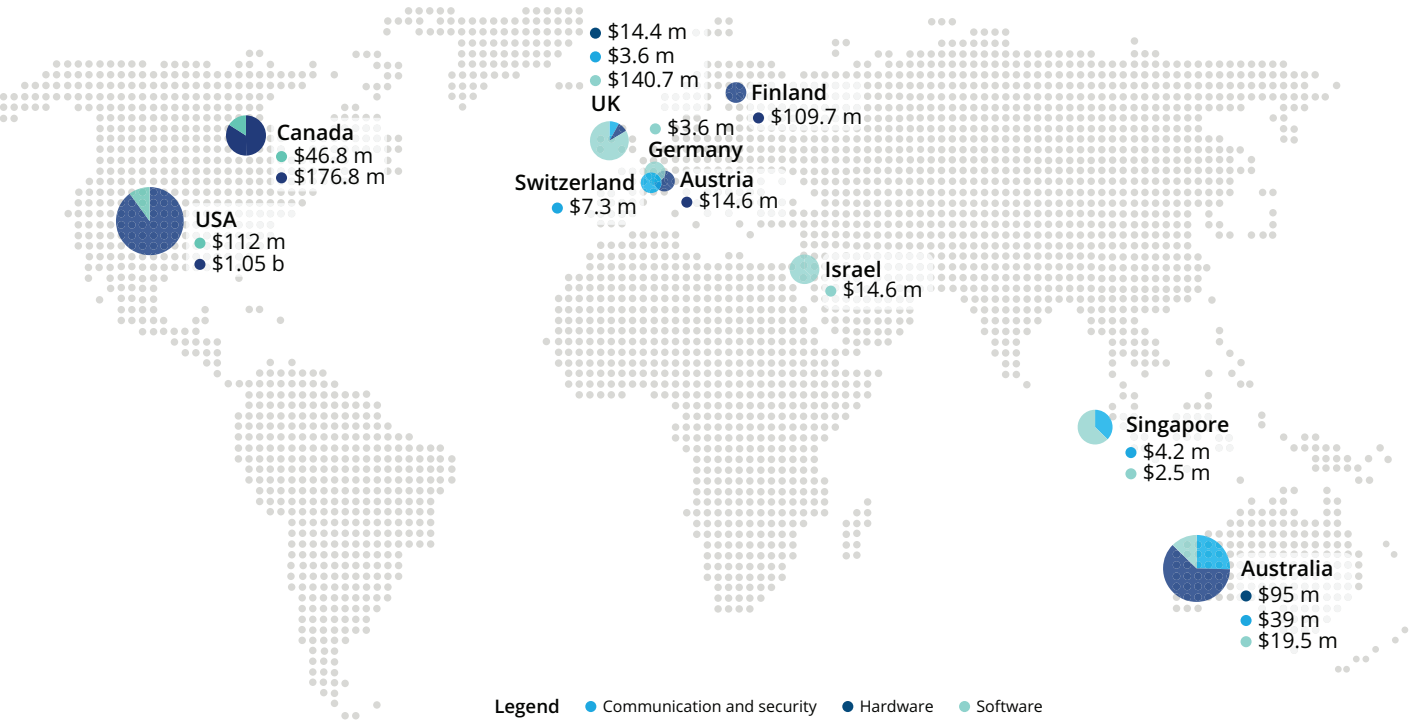
Further considerations for cyber security include:

- How much of a threat is there to your current models for system security? What protocols do you use for public key sessions? Authentication? Symmetric protocols? Storage? And internal data transfers?
- Are you concerned about data retention and the security of transactions transmitted over public networks today but that needs to remain secure 20-30 years from now?
- What is the timeline for quantum threats to cybersecurity and how do you contextualise what the current state of hardware and software development is compared to what is needed to compromise security?
- Is post quantum cryptography a suitable solution for your networks. Given that all post quantum crypto models still rely on unproven computational assumptions, how reliable or cost effective is a switch to a new system when it could be compromised tomorrow?
- Are your security needs so sensitive that a switch to quantum techniques in secure data communications is needed? What is on offer in this space and what could be coming down the pipeline in the next decade or two?
- How does current geopolitics influence choices related to data security? Does the exponential increase in development of quantum secure networks by the CCP indicate a need to find your own solutions to security in an ever increasingly threatening global environment?

# Quantum Investments

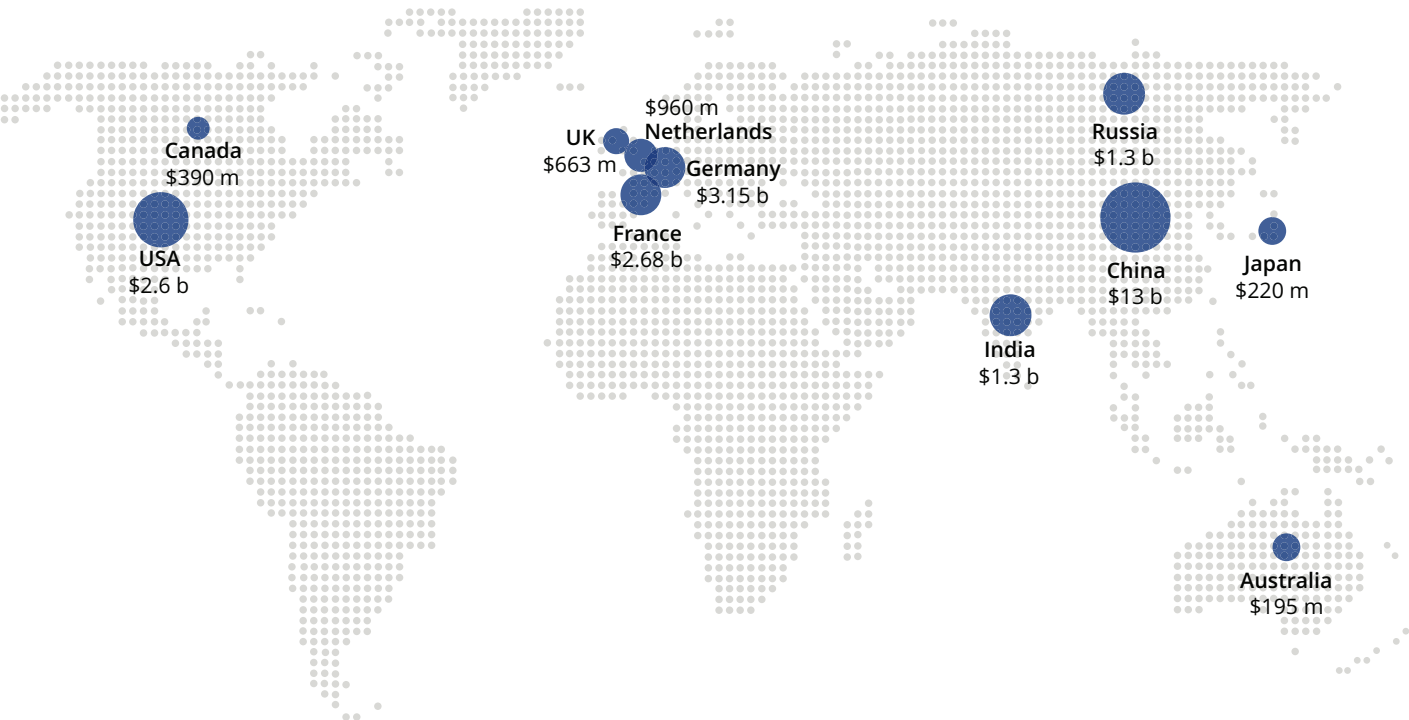
The number of Private firms and Governments investing in quantum technologies has increased substantially over the past few years. USA leads the private investments with two-thirds of the global private sector investments.

Figure 1 – Private Investments in Quantum Technologies as of May 2021 (\$AUD)



The number of Private firms and Governments investing in quantum technologies has increased substantially over the past few years. USA leads the private investments with two-thirds of the global private sector investments.

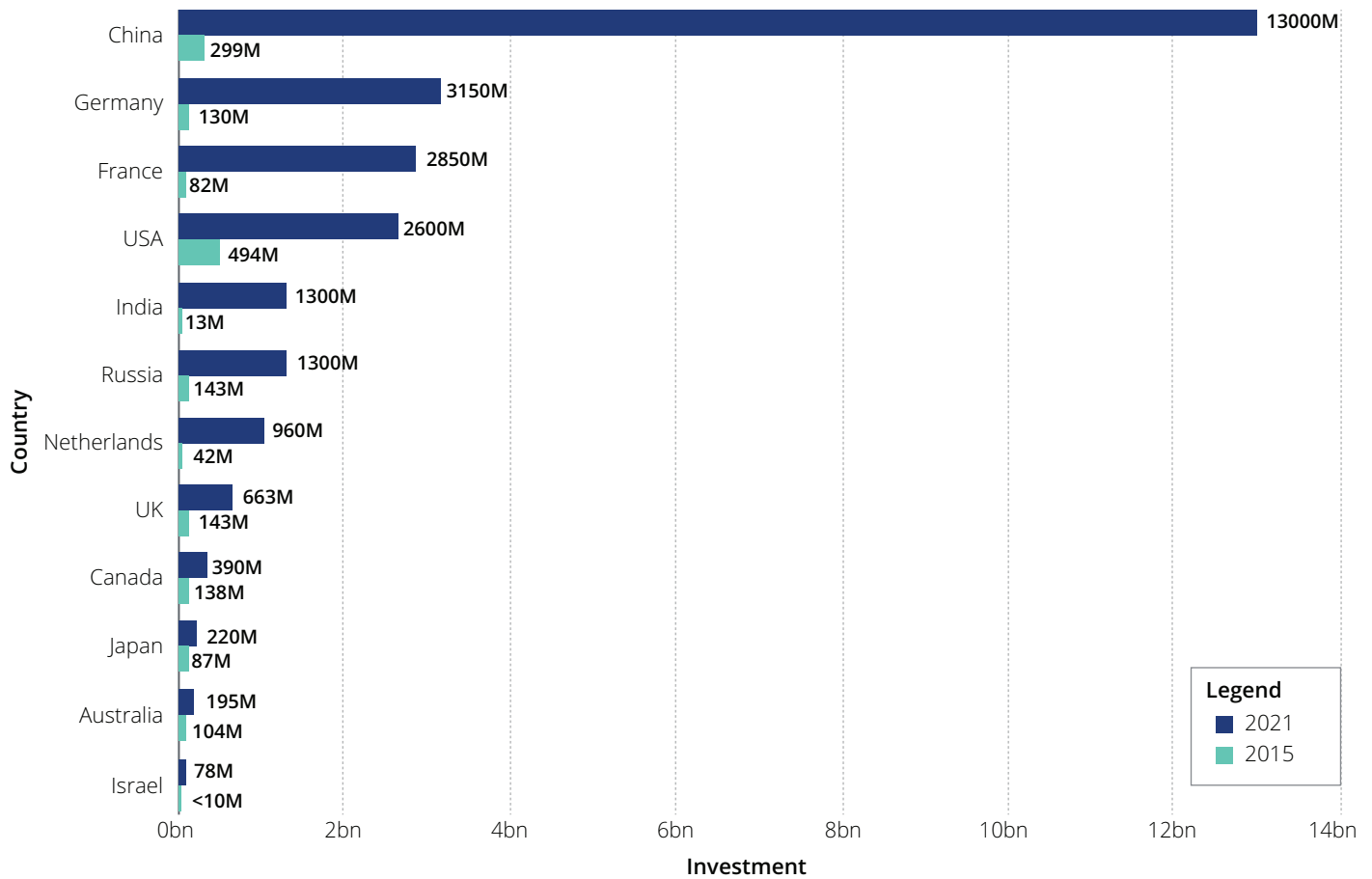
Figure 2 – Sovereign Investments in Quantum Technologies as of May 2021 (\$AUD)





As a comparison of the growing sovereign interest in quantum technologies, the investments over the six years from 2015 to 2021 there has been a step change across all major economies – particularly China with a 4248% increase in sovereign investments.

**Figure 3 – The phenomenal increase in sovereign Investments in Quantum Technologies between 2015 and 2021 (\$AUD)**



## How to assess the need for quantum computing?

As discussed in this paper, quantum computing won't replace classical computing; they are complementing technologies. So how do you assess when you need the quantum advantage, versus when a classical computer will suffice?

### Bottlenecks in current approaches

How are current models simulated and what are the computational bottlenecks in classical approaches. Quantum computers will never replace the entire algorithmic stack in any area of computational finance, so what "line calls" are your most computationally demanding and could quantum computing be used to provide more efficiency in those parts of your modelling algorithm

### Quantum computers are not high data

Quantum computers are not "high data devices". i.e. they cannot work over large data sets. If your solution space requires gigabytes or terabytes of broad data sets, it is unlikely to benefit from quantum computing. This is why identifying optimisation points in complex algorithms is important, as quantum computing can be used as a complementing technology to improve subcomponents of a modelling algorithm.

### Quantify current costs

With terms like quantum advantage, quantum supremacy, quantum impact, and quantum value are buzzwords making waves across tech communities, defining, and analysing the applicability and cost effectiveness of quantum solutions is immensely complicated. A set of guiding principles include:

- Defining very specifically where bottlenecks in your computational task are occurring
- How much do you currently spend in pushing through these bottlenecks?

- How much is it worth to you in pushing through them faster? Or with larger problem instances
- Are they low data problems or can are subroutine choke points low data problems?
- Is there a quantum solution that is demonstrably better than more AWS time?
- What are the quantum resource costs (qubits/time) for that solution?
- Where is the current state of quantum hardware compared to those benchmarks?
- How much will access to hardware of sufficient scale need to be to provide economic benefit?
- When will it be likely that hardware systems will be of sufficient size to meet my needs?
- Will hardware be readily available when it reaches the size I need?
- What is the likelihood that a classical solution will exist when the quantum system finally arrives?

All of these questions are extremely difficult to define and answer, but given enough specificity, they can be quantified.

## How can we help you?

Deloitte is partnered with a number of local leading quantum computing organisations providing a good balance of skills and platforms to allow our clients to explore, understand, and embrace the quantum experience.

There are already a number of demonstrated scenarios where quantum computing has overtaken classical computing. In order to explore opportunities across industries, we would be delighted to have a further conversation with you in our immersion labs, together with some of the leading Quantum Computing organisations in Australia. If you are interested, please get in touch.

### References

- Jeffrey Lim, PW Singer, 'China is opening a new quantum research supercenter', Popular Science, 10 October 2017. <https://www.popsci.com/chinas-launches-new-quantum-research-supercenter/>
- Moonshot Research and Development Program, 'About', Japan Science and Technology Agency, 2020. <https://www.jst.go.jp/moonshot/en/about.html>
- Matt Swayne, 'Qubit allies: Germany invest 2 billion euros in quantum technology, build two quantum computers', Quantum Daily, 15 June 2020. <https://thequantumdaily.com/2020/06/15/qubit-allies-germany-invest-2-billion-euros-in-quantum-technology-build-two-quantum-computers/>
- Matt Swayne, 'La Monde: France pledges 1.8 billion euros for quantum technologies', Quantum Daily, 22 January 2021. <https://thequantumdaily.com/2021/01/22/la-monde-france-pledges-1-8-billion-euros-for-quantum-technologies/>
- Yaacov Benmeleh, 'Israel allocates \$60 million to build first quantum computer', Bloomberg, 3 March 2021, <https://www.bloomberg.com/news/articles/2021-03-03/israel-allocates-60-million-to-build-first-quantum-computer?sref=iTUE3kUq>
- Leiden University, '615 million euros awarded to Quantum Delta NL for Quantum research in the Netherlands', HPC wire, 9 April 2021. <https://www.hpcwire.com/off-the-wire/615-million-euros-awarded-to-quantum-delta-nl-for-quantum-research-in-the-netherlands/>
- T.V. Padma, 'India bets big on quantum technology', Nature, 2020. <https://doi.org/10.1038/d41586-020-00288-x>
- HR 6227—National Quantum Initiative Act. <https://www.congress.gov/bill/115th-congress/house-bill/6227>
- <https://www.hpcwire.com/off-the-wire/canadian-government-commits-360-million-for-quantum-research/>
- <https://uknqt.ukri.org>
- <https://www.hpcwire.com/2020/01/06/russia-invests-790m-into-its-quantum-future/>
- <https://qt.eu>
- <https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own>
- <https://www.bbva.com/en/bbva-and-multiverse-showcase-how-quantum-computing-could-help-optimize-investment-portfolio-management/>

## Authors & Contacts



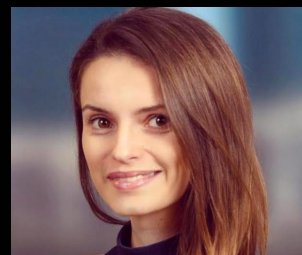
**Karti Mahendran**

Lead Author  
Deloitte  
kmahendran@deloitte.com.au



**Dr Simon Devitt**

QC Researcher  
H-Bar: Quantum Consultants  
devitt@h-bar.com.au



**Rebecca Blackford**

Data Scientist  
Deloitte  
rblackford@deloitte.com.au



**Dr Kellie Nuttall**

Partner AI Strategic Growth  
Deloitte  
knuttall@deloitte.com.au



**Richard Kendall**

Partner Technology Architecture  
Deloitte  
rkendall@deloitte.com.au



**Yousaf Mir**

Partner QC Lead  
Deloitte  
ymir@deloitte.com.au

**With special thanks to Deloitte's Global Quantum Guild**





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

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

#### **About Deloitte**

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

#### **About Deloitte Asia Pacific**

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

#### **About Deloitte Australia**

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at [www.deloitte.com.au](http://www.deloitte.com.au)

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

© 2021 Deloitte Touche Tohmatsu.

Designed by CoRe Creative Services. RITM727292