Australian Government
Office of the Chief Scientist

Quantum Meets Finance Workshop Summary

A workshop led by the CSIRO
and the Sydney Quantum Academy

CSIRO

SYDNEY QUANTUM ACADEMY

Acknowledgement of Country

The Office of the Chief Scientist acknowledges the traditional owners of the country throughout Australia and their continuing connection to land, sea and community. We pay our respect to them and their cultures and to their elders past and present.

Artwork: Connection to Country, 2021 by Shaenice Allan

Meeting Place icon by DISR employee Amy Huggins

Copyright

Disclaimer

The purpose of this publication is to summarise the events and outcomes of the Quantum Meets Finance event which occurred in Sydney on 23 August 2024.

The Commonwealth as represented by the Department of Industry, Science and Resources has exercised due care and skill in the preparation and compilation of the information in this publication.

The Commonwealth does not guarantee the accuracy, reliability or completeness of the information contained in this publication. Interested parties should make their own independent inquiries and obtain their own independent professional advice prior to relying on, or making any decisions in relation to, the information provided in this publication.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this publication. This publication does not indicate commitment by the Commonwealth to a particular course of action.

Microsoft Co-Pilot was used in developing this summary.

Workshop Overview

Quantum Meets Finance was presented by the Office of the Chief Scientist, in partnership with the CSIRO and the Sydney Quantum Academy. The workshop was held at the Sydney Quantum Terminal on Friday 23 August 2024. More than 100 people attended, including representatives from the finance sector, quantum businesses, academia and government.

The finance sector includes a wide range of services including banking, superannuation, investment, insurance and real estate. It plays a crucial role in the economy by managing money, facilitating transactions, and providing financial products and services to individuals, businesses and governments.

Quantum technology holds immense promise for the future of banking and financial services. Quantum computers have the potential to do complex calculations at unprecedented speeds, which could improve things like risk assessment, securities pricing, fraud detection, improved banking sector resilience and investment portfolio optimisation. They could be used to analyse large amounts of data almost instantly, which could help financial services make more accurate assessments on real-time information, making it easier to spot fraud. However, these capabilities could also lead to quantum computers breaking the encryption used to protect data, so new types of cryptographic algorithms will need to be developed.

Other future uses of quantum technology in the finance sector include secure data transmission and storage using quantum key distribution. Additionally, quantum-enhanced machine learning could improve the client experience by making better predictive models and personalising services.

Scene setting

Australia's Chief Scientist, Dr Cathy Foley described the status of the Australian quantum industry, the implementation of Australia's National Quantum Strategy[1] and the "Quantum Meets" program events. She introduced a range of quantum technologies including sensing, communications and computing, noting that sensing was of less relevance for the financial industry.

Dr Foley explained that there is a global race to build a useful fault-tolerant quantum computer such as those being developed by PsiQuantum, Diraq and Silicon Quantum Computing (SQC). There are several different quantum computers currently available: Quantum Annealers, Noisy Intermediate Scale Quantum Computers (NISQ), quantum accelerators that are hybrids with high performance computers such as those developed by Quantum Brilliance and, quantum simulations operating on classical computers and the development of a useful fault tolerant quantum computer such as those being developed by PsiQuantum, Diraq and SQC. Many of these capabilities are available on the cloud now. She pointed out that Australia has the largest pool of quantum software research talent in the world with more than 110 individuals in Australia.

Dr Foley reported that by 2035, quantum computing use cases in the financial industry could create $622B in value, assuming a 50% take up. This includes corporate banking, risk and cybersecurity, retail banking, payments, asset and wealth management, investment banking and operations and finance. Overall, quantum technology can support optimisation problems, secure communications, fraud detection, simulating complex phenomena, predictive analysis, and credit rating modelling. Some examples of applications are:

- risk – broader set of variables, cyber security, collateral optimisation – securities lending
- liquidity simulation – handle vast array of boundary conditions
- random number generators
- boost accuracy and speed of classical Monte Carlo simulations – quadratic increase in speed
- payments – properties of quantum states address money laundering
- quantum money – transform banking with non-falsifiable security
- wealth management – portfolio optimisation and quantum-encode contracts – encoded in quantum states – faster, secure, more sustainable compared to block chain.

Dr Foley referred to research on using quantum computers for forecasting financial crashes, option portfolio analysis, and made attendees aware of the more than 500 research publications that consider the use of quantum technologies for the financial industry.

Dr Foley concluded by indicating that early-stage quantum computing is here now, post quantum cryptography planning is essential and referred to the Australian Signal Directorate (ASD) who are leading the Australian charge on Australia's preparedness for quantum security.

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

Image 1. Australia's Chief Scientist, Dr Cathy Foley addresses the 100+ audience at 'Quantum Meets Finance'. Credit: Sydney Quantum Academy.

Ms Anna Bligh, CEO of the Australian Banking Association, talked about how people across the globe are relying on digital money more and cash less – 99.9% of all transactions are online. Today banks have changed from big buildings to something invisible. Banks now hold a lot of data and offer a range of services. There are also more competitors to banks, like big tech companies such as Apple and Google. These companies don't have banking licenses and are not subject to banking rules, but they offer similar services like loans and savings. Ms Bligh highlighted some future trends for people to think about such as central bank digital currency, cryptocurrency, the rise in online scams and customers demanding convenience. One example of an app that could automatically move money around to get better interest rates without customers having to do the research themselves. Potentially quantum technology could be used in the future to avoid industrialised size scams and build greater trust in the banking industry by protecting customers as best as possible.

Ms Anna Bligh AC, CEO Australian Banking Association:
"Customers are shifting online at speed with over 99.9% of transactions now taking place online. This brings efficiency and convenience but also presents security challenges."

Image 2. Ms Anna Bligh, CEO of the Australian Banking Association, addresses the 100+ audience at 'Quantum Meets Finance'. Credit: Sydney Quantum Academy

Areas of industry impact

Fraud detection

Quantum computing may become a powerful new tool in the continuous fight against hacking, scams and fraud.

Risk assessment

Quantum computing's increased processing power could allow for more thorough risk assessments of complex or high dimensionality data.

Breaking cybersecurity

In the future, general-purpose quantum computers might break the encryption that keeps data safe. This is because quantum computers can solve certain complex math problems faster than regular computers, which are the basis of current encryption methods.

Providing cybersecurity

Quantum cryptography, like quantum key distribution, could offer secure data transmission in the future. It uses the principles of quantum mechanics to send private information in a way that makes it impossible for eavesdroppers to go undetected.

Efficiency and productivity enhancements

Quantum computers are anticipated to be particularly good at solving certain types of optimisation problems and simulating complex financial models.

Program schedule

Setting the scene

Dr Cathy Foley, Australia’s Chief Scientist

Ms Anna Bligh AC, CEO of the Australian Banking Association

Keynote 1 – Critical challenges for the finance sector

Dr David Garvin, Head of Applications in Quantum Finance at Rigetti
Ms Michelle Bower GAICD, CEO of Gateway Network Governance Body

Keynote 2 – Meeting the challenge with quantum technologies

Dr Andre Saraiva, Head of Solid-State Theory at Diraq
Professor Gavin Brennen, Director of the Centre for Quantum Engineering at Macquarie University

Panel 1 – Efficiency and productivity enhancements from quantum computation and algorithms

Chair: Associate Professor Simon Devitt, Research Director at the Centre for Quantum Software at the University of Technology Sydney

- Dr Hakop Pashayan, Postdoctoral Research Fellow at the Free University of Berlin
- Ms Mary Delahunty, CEO at Association of Superfunds Australia
- Mr Rehan D’Almeida, CEO at FinTech Australia

Panel 2 – Quantum communication technology and cybersecurity – new opportunities

Chair: Associate Professor Chris Ferrie, Associate Professor at the University of Technology Sydney

- Mr Alexey Bocharnikov, APAC Quantum Technology Lead at Accenture
- Ms Camilla Bullock, CEO & Co-Founder at Emerging Payments Association Asia
- Professor Gavin Brennen, Director Centre for Quantum Engineering at Macquarie University
- Professor Stephen Bartlett, Director of the Sydney Nano Institute and Professor in the School of Physics at the University of Sydney

Panel 3 – Preparing for the cryptography breaking threat from quantum computers

Chair: Mr Andreas Baumhof, Vice President of Quantum Technologies at Quintessence Labs

- Mr Andy White, Chief Executive Officer at Australian Payments Network
- Professor Nalini Joshi AO, Chair of Applied Mathematics at the University of Sydney
- Dr David Liebowitz, Principal Technologist at Penten

Panel 4 – Integrating quantum in commercial and strategic planning

Chair: Dr Dimitrios Salampasis, Frontier Technologies and FinTech Capability Lead and Senior Lecturer in Emerging Technologies and FinTech at Swinburne University

- Professor Peter Turner, CEO at Sydney Quantum Academy
- Mr Dilan Rajasingham, Australia & New Zealand – Head of Customer Strategy and Business Development (Greenfields) at Amazon Web Services
- Mr Robert Wilson, Chief Technology Officer at the Bank of Queensland
- Mr Nicholas Giurietto, Head of Future Policy at the Australian Banking Association

Breakout sessions

- Five breakout sessions focused on finance sector issues where there could be applications of quantum technology.

Overview of Government funding opportunities

Michele Graham, General Manager of the Quantum Branch, Department of Industry, Science and Resources

Next steps and closing statement

Dr Cathy Foley, Australia’s Chief Scientist

Keynotes

Critical challenges for the finance sector

Dr David Garvin, Head of Applications in Quantum Finance at Rigetti, emphasised that early-stage quantum computers are available and usable now. There are potential applications in finance that could improve revenues, reduce costs, minimise risk and enhance customer experiences. Examples include identified value creation, asset pricing, trading strategies and fraud detection**.** Referring to the findings of McKinsey, Dr Garvin suggested that by 2035, quantum computing use cases in the finance industry could create USD $622 billion in value[2]. In particular, quantum computing could be pivotal in fraud detection given its potential capacity to process larger data sets than classical computing. He encouraged attendees to get involved and learn more about quantum computing.

Ms. Michelle Bowers, CEO of the Gateway Network Governance Body, talked about the challenges in the superannuation sector. In this sector data security is very important, and identifying cybersecurity threats is a key challenge. Fraud is a big risk to customers, especially with new AI technology that can simulate voices. Cyberattacks commonly occur with verified information obtained through stolen or lost credentials. Ms. Bowers asked the quantum community if quantum computing could predict customer needs, could it also predict threats such as modelling the tactic of threat actors? Any protection that quantum computers could offer would be valuable as threats evolve quickly and the size and scale of data exposure increases.

Financial Usecases
Potential applications across the financial organisation
Opportunity to improve revenues, reduce costs, minimize risk and enhance customer experiences
Small improvements can lead to large value capture
rigetti
Australian Government

Image 3. Keynote speaker Dr David Garvin,
Head of Applications in Quantum Finance at Rigetti

Meeting the challenge with quantum

Dr Andre Saravia, Head of Solid-State Theory at Diraq, talked about how quantum computers will need to be fault-tolerant for financial use cases. The cost of computation should not be more than the profit or savings it will generate. Fault-tolerant computers will need many more qubits than current quantum computers have, and they will cost a lot more. To achieve their potential, we need more cost-effective ways to manufacture quantum computers on a large scale. Dr Saravia also described the type of quantum computer being developed by Diraq which is more compact than other quantum computers.

Professor Gavin Brennen, Director of the Centre for Quantum Engineering at Macquarie University, talked about how quantum technology could be used with blockchain technology. Blockchain validates transactions by solving a difficult computational problem called “proof of work”. However, this process is slow and uses a lot of energy. Professor Brennen explained how quantum technology could offer an alternative to this work using quantum stages of light. One-shot signatures are another example of unexpected applications of quantum technology that could be possible for **the** finance **sector**.

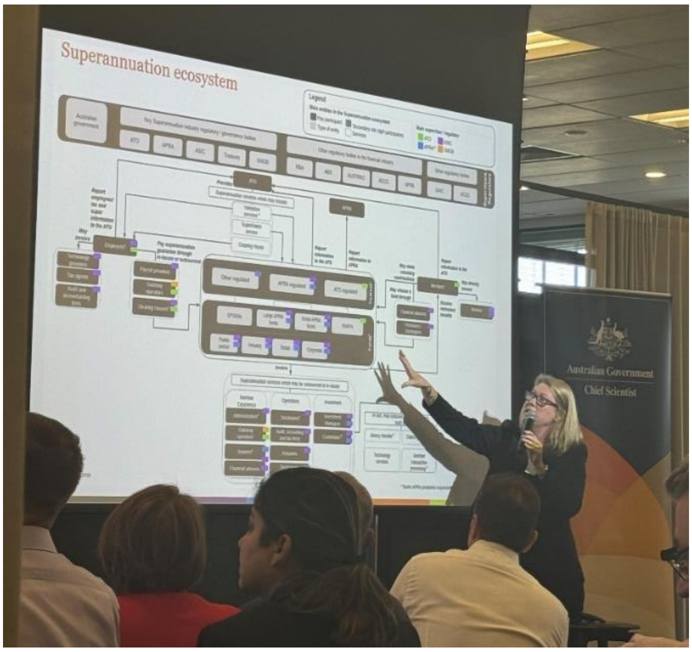

Image 4. Keynote speaker Ms Michelle Bower GAICD, CEO of Gateway Network Governance Body

[2] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/quantum-technology-use-cases-as-fuel-for-value-in-finance

Panel composition and discussions

Panel 1 – Efficiency and productivity enhancements from quantum computation and algorithms

Chair: Associate Professor Simon Devitt, Research Director at the Centre for Quantum Software, University of Technology Sydney

- Dr Hakop Pashayan, Postdoctoral Research Fellow at the Free University of Berlin
- Ms Mary Delahunty, CEO at Association of Superfunds Australia
- Mr Rehan D’Almeida, CEO at FinTech Australia

The panel talked about the computing needs of the finance sector and the difference between classical and quantum computing. Quantum computing is expected to achieve higher processing speeds and solve more complex problems than classical computers, such as factorisation problems. In superannuation, this can help calculate the right risk assessments on unlisted assets. In the much longer term it could also be useful in processing the vast amount of data used in fintech applications, though the panel acknowledged that there are some significant technical developments still required to make this possible.

Quantum computers could also be used in risk assessment at an economy level, such as considering the risk of climate change. Today, institutional investors, like superannuation funds, hold large, diversified portfolios that represent a large slice of the entire market. Before being able to perform these applications, the issue of how to get data into a quantum computer needs to be solved.

and Algorithms
...nts from Quantum Computation ...Productivity
Chair: Associate Professor Simon Devitt, UTS
Panellists:
• Dr Hakop Pashayan, Free University of Berlin
• Ms Mary Delahunty, Association of Superfunds Australia
• Mr Rehan D'Almeida, FinTech Australia
Australian Government
Office of the Chief Scientist
Australian Government
Chief Scientist
Building the next-generation of quantum technologies

Image 5. Panel 1 discussion

Panel 2 – Quantum communication technology and cybersecurity – new opportunities

Chair: Associate Professor Chris Ferrie, Associate Professor at University of Technology Sydney

- Mr Alexey Bocharnikov, APAC Quantum Technology Lead at Accenture
- Ms Camilla Bullock, CEO & Co-Founder at Emerging Payments Association Asia
- Professor Gavin Brennen, Director Centre for Quantum Engineering at Macquarie University
- Professor Stephen Bartlett, Director of the Sydney Nano Institute and Professor in the School of Physics at University of Sydney

The panel explored the importance of payments in trade, emphasising that payments are essentially now just the movement of data across borders. They discussed the different types of payments in Australia and highlighted the challenges of real time payment transactions. These types of transactions have more data, making reconciliation more challenging, and must be resilient with no downtime which is costly and has higher risks. There is also the issue of organised cyberattacks. Most attacks aim to steal money through deception or by encrypting data and asking for a ransom.

The panel also discussed the threat of quantum computing breaking current cybersecurity encryption methods. One panelist suggested that hiring researchers to attempt quantum attacks could help identify risks and improve security. Another panelist emphasised the need for raising awareness and conducting research on quantum technology now, even before it becomes widely used. Businesses don't necessarily know where or what encryption they use, nor the weaknesses of these encryptions. They must research the specific cryptographic solutions that suit their needs. There is potential for quantum cryptography to offer secure transmission of data protected by the laws of physics however, this technology is not yet compatible with classical computing.

Panel 2: Quantum Communication Technology and Cybersecurity – New Opportunities
Chair: Associate Professor Chris Ferrie, UTS
Panellists:
Mr Alexey Bocharnikov, Accenture
Ms Camilla Bullock, Emerging Payments Association Asia (EPAA)
Professor Gavin Brennen, Macquarie University
Stephen Bartlett, University of Sydney
Australian Government Office of the Chief Scientist
Australian Government Chief Scientist
Quantum Meets Finance

Image 6. Panel 2 discussion

Panel 3 – Preparing for the cryptography breaking threat from quantum computers

Chair: Mr Andreas Baumhof, Vice President of Quantum Technologies at Quintessence Labs

- Mr Andy White, Chief Executive Officer at Australian Payments Network
- Professor Nalini Joshi AO, Chair of Applied Mathematics at University of Sydney
- Dr David Liebowitz, Principal Technologist at Penten

The panel talked about the challenges of changing cryptographic algorithms for secure data transmission. It is important to continue developing advanced software, noting that replacing codes requires accreditation, and there is a need for mathematically proven algorithms for national security. There is growing awareness of cybersecurity threats from quantum computing but an uncertainty of when these threats will materialise. This situation could be compared to the Y2K problem, noting the difficulty in predicting the exact timing and impact of quantum computing threats. Businesses need to start preparing for the transition to post quantum cryptography now as it will take 7 to 8 years to implement.

Next, the panel discussed the need for regulation and standards to ensure the use of post-quantum encryption. Interdisciplinary collaboration will be important in addressing these challenges. The panel also highlighted the importance of ensuring Australia has the necessary mathematics skills to respond to quantum threats.

Image 7. Panel 3 discussion

Panel 4 – Integrating quantum in commercial and strategic planning

Chair: Dr Dimitrios Salampasis, Frontier Technologies and FinTech Capability Lead and Senior Lecturer in Emerging Technologies and FinTech at Swinburne University

- Professor Peter Turner, CEO at Sydney Quantum Academy
- Mr Dilan Rajasingham, Australia & New Zealand – Head of Customer Strategy and Business Development (Greenfields) at Amazon Web Services
- Mr Robert Wilson, Chief Technology Officer at Bank of Queensland
- Mr Nicholas Giurietto, Head of Future Policy at Australian Banking Association

The panel explored the importance of talent and human skills in the quantum field, noting the current challenges in training and security clearance requirements. There is a need for strong regulatory processes to protect banking systems and the slow pace and requirements for regulatory change, such as ensuring resilience and redundancy. Currently there is significant investment in AI compared to quantum computing. Banks would need to invest in quantum technologies to stay ahead. Clear quantum use cases could help to get the attention of the financial sector for this purpose.

The panel also discussed the potential interplay of quantum computers and privacy. Banks are expected to predict and prevent fraud. With increasing information available from individual day-to-day transactions, banks might also have a social duty of care on issues such as financial abuse.

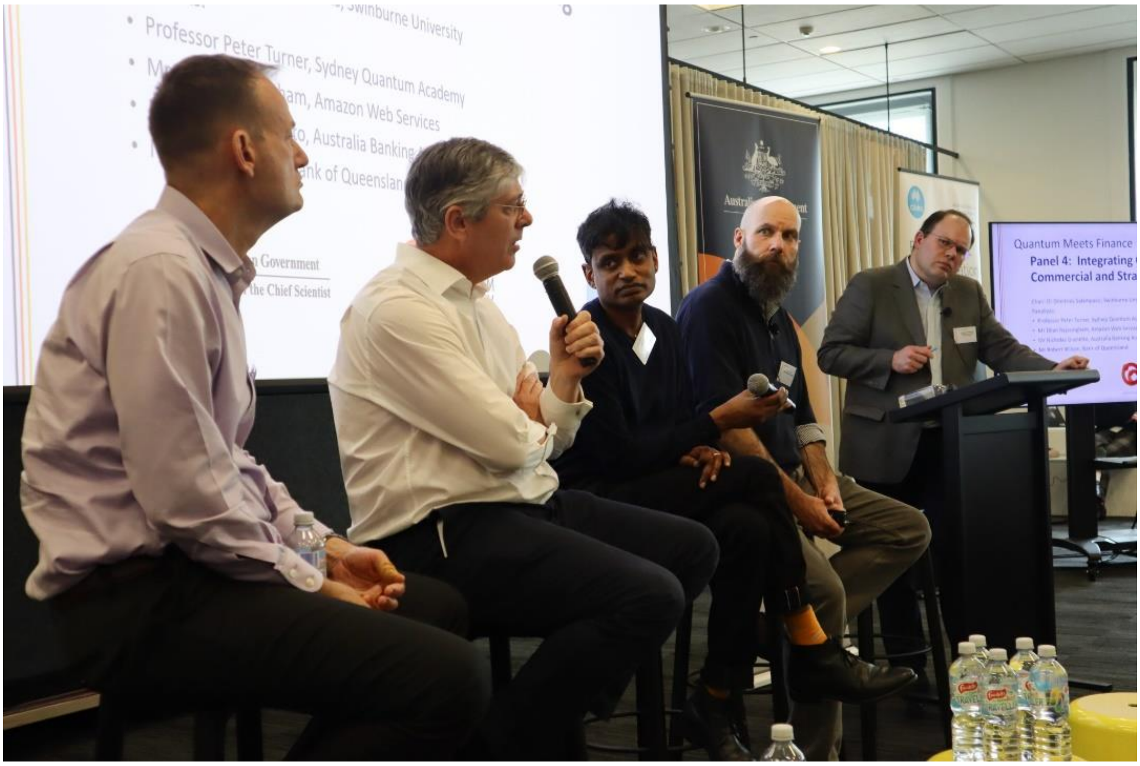

Image 8. Panel 4 discussion

Breakout sessions

Five breakout sessions focused on finance sector issues where there could be applications of quantum technology. In small group discussions, attendees broke down the problem and discussed where quantum technology developments could be used and what developments were needed.

The breakout sessions were:

- Applications of quantum technology in insurance
- Implementation of post-quantum cryptography for finance organisations
- Future skills needed around quantum technology
- Quantum enhancement to real-time payment systems
- How quantum computers could be used to optimise portfolios.

Some of the problems identified included:

- Challenges in accurately pricing and managing risk, such as setting assumptions for Monte Carlo models and monitoring the costs of products offered
- The risk of encryption being broken, the scale of this problem and the challenges around legacy systems and maintaining consumer trust
- The burden of proof and the speed of transactions in real-time payment systems
- The lack of understanding of quantum technology within the industry and the need to develop a quantum-literate workforce.

The interest and discussions on these topics were used to construct the case studies in the appendix.

Image 9. Breakout sessions

Next steps and closing

The workshop identified opportunities for where quantum computing and communications could add benefit to the financial services industry sector. Cyber security is the main issue in the near term. However, using quantum capabilities to reduce risk, support better decision making, and provide improvements in optimisation across many financial services activities were priority possibilities. Resilience and redundancy are needed for the day when full error corrected quantum computers are available.

Using a quantum computer to predict situations such as the 2007 financial crisis is a dream that the finance and technology sectors would like to realise. The financial services sector has already experienced massive change and disruption over the COVID period and expects to continue to see changes. These changes make the landscape more complex and difficult to manage. Quantum capabilities offer a pathway to address these issues, but the sector needs to start planning for adoption now.

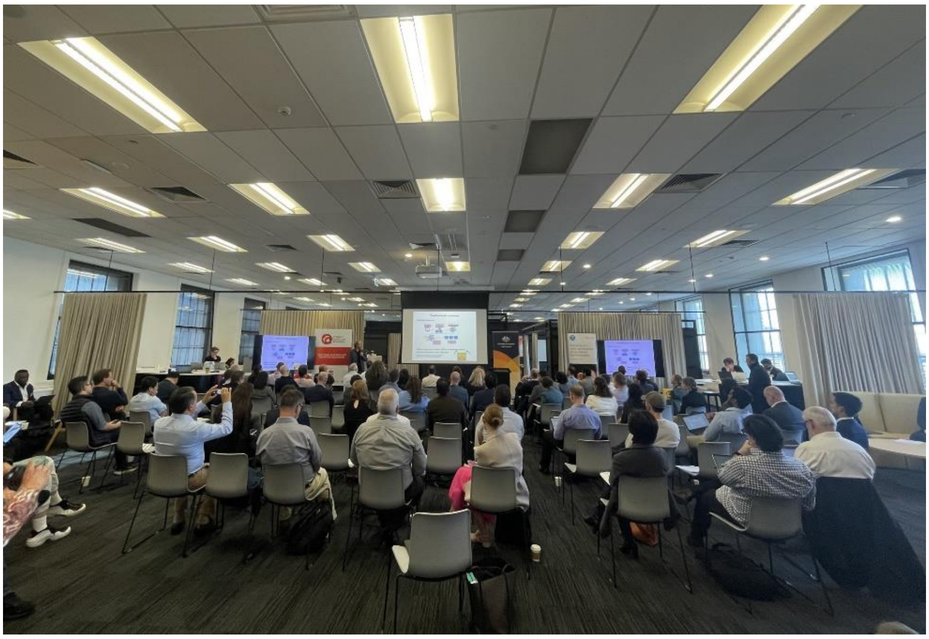

Image 10. Quantum Meets Finance workshop

Case study 1: Preparing for post-quantum cryptography

Big picture problem

In the finance sector, maintaining secure communications is crucial. Currently, we rely on public key cryptography to protect online banking and financial transactions. However, the advent of a general-purpose quantum computer poses a significant threat to this technology, rendering it insecure and inadequate for safeguarding sensitive information.

Current operational quantum computers only have a couple of hundred of qubits, the quantum equivalent of a bit in classical computers. These are termed ‘noisy intermediate-scale quantum computing’. A general-purpose quantum computer is anticipated to need around 20 million qubits. These general-purpose quantum computers are anticipated to be able to solve the particular complex mathematical problems that underpin cybersecurity encryption methods much faster than classical computers.

While a general-purpose quantum computer is still a way off, financial organisations must proactively anticipate future requirements and dependencies of vulnerable systems. This involves transitioning to post-quantum cryptography (PQC) standards, which are encryption algorithms designed to withstand the capabilities of quantum computers. Companies need to prepare now by researching and implementing these quantum-resistant cryptographic solutions, a transition that could take several years. Further adding to the urgency of this problem is the risk that encrypted data stolen now could be stored to be decrypted later once general-purpose quantum computers are available.

Breaking the problem down

The discussion highlighted several key aspects of the problem:

- The challenge of transferring data securely, especially with legacy systems and businesses unfamiliar with their encryption requirements.
- The need for stronger encryption methods to protect data at rest and in transit.
- The scale of the problem, with a vast number of digital certificates and keys that need to be managed.
- The importance of understanding which algorithms are being used for encryption and their vulnerabilities.
- The necessity for crypto agility to adapt to new threats and maintain security. Crypto agility is the ability of a security system to rapidly switch between encryption mechanisms.
- The significant loss of trust amongst users should encryption be broken, and the consequences for financial services in society.

How could quantum technology help?

Some ways that quantum technology could assist in addressing this challenge include:

- Quantum computers could be used to test post-quantum encryption algorithms.
- Quantum-generated random numbers could enhance the entropy and security of encryption methods.
- Quantum cryptography could provide more robust encryption techniques that are resistant to quantum attacks.
- Optimisation calculations through quantum computers could help manage the computational expense of securing data and improve the efficiency of encryption processes.

Next steps

The group identified several next steps to address the challenges discussed:

- Begin the transition to post-quantum cryptography immediately, despite the uncertainty of when quantum computers will become a significant threat.
- Increase awareness and understanding of quantum technology within industry.
- Encourage businesses to secure the necessary budget and organisational support to implement quantum solutions.
- Develop regulations and industry-wide standards to ensure a coordinated response to the quantum threat.
- Encourage businesses to improve their cryptographic hygiene by knowing what encryption methods are being used, what they are protecting, and their vulnerabilities.

These steps will help prepare for a post-quantum environment and ensure the continued security and trust in digital systems used in financial services.

Case study 2: Quantum enhancement to real-time payment systems

Big picture problem

The primary problem identified was the challenge of instant payment leading to instant fraud. This issue arises because the rapid speed of transactions makes it difficult to detect and prevent fraudulent activities in real-time.

However, customers increasingly want the convenience that real-time payment systems offer. These transactions are expected to become increasingly popular, with a corresponding rise in fraud. Financial organisations must constantly evolve how they combat fraudulent activity in real-time payment systems.

Breaking the problem down

Several challenges were identified:

- The rapid speed of transactions makes it difficult to detect and prevent fraud in real-time. Monitoring behaviour and spotting unusual transactions is complicated, especially as attackers tend to move around and are quick to adapt their methods making them hard to track.
- Determining who owns and is responsible for proof in fraud cases remains a significant challenge. In some regions, accountability is shared between the bank and the customer.
- Stolen authentication is how a lot of fraud occurs so ensuring the identity of both the sender and receiver is crucial. The emergence of AI that can simulate voices is a further challenge to this. There is a need for a more sophisticated form of identification that can prevent authentication theft.
- The use of quantum technology in fraud detection applications raises concerns about privacy and the ethical implications of data access.
- There is a need for more awareness about quantum technology as it is still abstract and not well understood by the public.

How could quantum technology help?

Quantum technology presents two main opportunities to address these challenges:

- **Potential ability to process huge amounts of data quickly:** Quantum computing has the potential to encode and analyse huge amounts of data very quickly and accurately. This could be used for pattern recognition in real-time to monitor and spot unusual transactions that indicate fraud. Classical computers need considerable time and computation power for data analysis, making them less capable of real-time fraud detection.
- **Ability to handle complex data:** Quantum computers can model simulations such as complex financial models that use transaction data with high dimensionality (data which possesses many features that make it complex to analyse). This would be particularly useful to combat the constant evolution of fraudulent behaviour.
- **Quantum-generated data:** Data generated by quantum computer simulations could be used to train machine learning models. This data could be used to train and assist classical computers, enhancing their capabilities for fraud detection or identity verification without the need to replace existing real-time payment systems.

Next steps

To realise the potential of quantum technology to enhance real-time payment systems, the following steps are suggested:

- **Research and investment:** A quantum computer capable of outperforming classical computers for complex financial calculations does not yet exist. However, there are quantum computers available that could be used to start identifying the problems and approaches where quantum computing has an advantage. Many finance organisations are focused on the near-term benefits offered by AI and should also consider research into quantum enhancement of machine learning.
- **Reframing the problems to be solved:** Quantum computers explore all possible solutions to a problem at the same time unlike classical computers which check possibilities one at a time. This makes quantum computers very good at solving problems with a small amount of output and input data. Where this is not the case, the problem needs to be framed in a particular way to be solvable.
- **Education:** Increasing education and awareness about quantum technology in schools and the public is necessary to build trust in the technology. It is also necessary to build quantum tech expertise within the finance sector to enable finance experts to identify and collaborate on issues solvable by quantum technology.

In conclusion, the discussion highlighted the potential of quantum technology to revolutionise real-time payment systems by enhancing fraud detection and identity verification. However, significant challenges related to proof of responsibility, speed of transactions, privacy, and the need for education and investment, must be addressed to realise these opportunities.

Case study 3: Optimisation applications

Big picture problem

The finance sector faces significant challenges in optimising complex financial processes, such as portfolio optimisation and risk management. Traditional computational methods, like Monte Carlo simulations, are computationally expensive and time-consuming to solve using classical computers. The unique aspects of quantum computing however make them particularly good at solving optimisation problems.

Breaking the problem down

The discussion highlighted several aspects of the problem:

- Portfolio optimisation involves handling NP (nondeterministic polynomial time) - hard computation problems which are difficult to solve efficiently with classical computers.
- Monte Carlo simulations rely on taking many random samples to calculate the range and likelihood of possible outcomes. This kind of computation is essential for various financial calculations but is also computationally expensive and require significant resources.
- Accurately pricing and managing risk is challenging, especially when setting assumptions for Monte Carlo models and monitoring the costs of products offered.

How could quantum technology help?

Quantum computing offers several potential solutions to these challenges:

- Quantum computers can handle complex optimisation problems more efficiently, leading to better asset allocation and improved returns for investors.
- Quantum algorithms can run Monte Carlo simulations faster and with more accuracy, providing better quality solutions with constraints.
- Quantum-enhanced machine learning can improve predictive models, helping banks to better understand customer behaviour and personalise their services.

Next steps

The group identified several next steps to address the challenges discussed:

- **Transition to quantum solutions**: Begin integrating quantum computing into financial processes to leverage its optimisation capabilities.
- **Increase awareness and understanding**: Educate industry professionals about quantum technology and its potential applications in finance.
- **Secure budget and support**: Obtain the necessary budget and organisational support to implement quantum solutions.
- **Develop industry standards**: Establish regulations and industry-wide standards to ensure a coordinated response to the quantum threat.
- **Improve cryptographic hygiene**: Focus on better understanding and managing of current encryption methods and their vulnerabilities.

These steps will help prepare the finance sector for a post-quantum environment and ensure the continued efficiency and security of financial processes.