Quantum Technologies Insights Paper

June 2023

Digital Regulation Cooperation Forum

CMA Competition & Markets Authority · Ofcom making communications work for everyone · ico. Information Commissioner's Office · FCA Financial Conduct Authority

This Insights Paper aims to foster debate and discussion among our stakeholders. It should not be taken as an indication of current or future policy by any of the member regulators of the Digital Regulation Cooperation Forum (DRCF).

We appreciate the input and contribution from colleagues at the National Quantum Computing Centre.

Content

4 Executive Summary
9 Introduction
10 Overview: Quantum Technologies
11 Quantum Computing
20 Quantum Communications
26 Regulatory Considerations
34 Looking Ahead: Addressing Potential Future Regulatory Concerns
41 Conclusion and Next Steps
42 Glossary

Executive Summary

Quantum technologies have the potential to enable breakthroughs in how people can process, transmit and secure information, thereby opening new frontiers in innovation across the economy.

Many quantum technologies are still at an early stage of development, and there are significant technical and engineering barriers to overcome. However, given the potential step change in technological capabilities, and the national and global interest in these developing industries, it is crucial for the DRCF member regulators - the CMA, Ofcom, the ICO and the FCA - to be aware of how these technologies may evolve, and to consider the potential regulatory implications of such advances. Through our horizon scanning programme,[1] the DRCF takes a proactive approach in understanding the potential benefits, risks, and regulatory implications of emerging technologies, including quantum.

This Insights Paper, which builds on our learnings from the DRCF Quantum Symposium,[2] held in February 2023, aims to contribute to the global conversation. We discuss examples of where our existing regulatory remits are already relevant, and where the voice of DRCF regulators may be important as quantum technologies, and the UK's quantum industry, develop and mature.

What could a potentially quantum-enabled world look like?

There are several categories of quantum technologies, each at different stages of development, but each with the potential for transformative technological impacts. This paper focusses on two technologies of interest to DRCF member regulators: quantum computing and quantum communications.[3]

Quantum computing is a promising and diverse technology. Conventional computers perform calculations by encoding information as digital bits ('0s and 1s'). While the output of quantum computers is also presented in digital bits, they work internally by using quantum bits, or qubits. Qubits can, unlike digital bits, hold two states at the same time, that is, simultaneously be in a position of 0 and 1. For some important tasks (but not universally so), this ability would allow future quantum computers to find a solution to a problem using far fewer steps and calculations than a conventional computer would need, thus solving certain classes of problems at much greater speeds than 'classical' computers, and perhaps tackle previously unsolvable problems too.

---

1 DRCF, Joining up on Future Technologies, DRCF, 2021, https://www.gov.uk/government/publications/joining-up-on-future-technologies digital-regulation-cooperation-forum-technology-horizon-scanning-programme/joining-up-on-future-technologies

2 DRCF, The Metaverse and immersive technologies - A regulatory perspective, DRCF, 2022, https://competitionandmarkets.blog.gov.uk/2022/06/22/the-metaverse-and-immersive-technologies-a-regulatory-perspective/

3 Additional categories include quantum-enhanced imaging and quantum sensing and timing, the latter being the most developed subset of quantum technologies. They could reach unprecedented measurement precision. Sensors could be deployed for non-invasive brain imaging, advanced positioning, navigation and timing solutions, new techniques to inform climate modelling and forecast natural disasters. They could find applications in civil engineering and infrastructure projects also, to develop much more accurate pictures of pipes, cabling and underground obstructions. See further: UK Quantum Technology Hub Sensors and Timing, UK Quantum Technology Hub Sensors and Timing (quantumsensors.org) The ICO are looking to explore quantum sensing and timing technologies in their further futures work on quantum.

This innovation could provide significant advances in a range of industries and fields, from advancing materials science and physics research, to accelerating machine learning. In the healthcare and pharmaceuticals industry, for example, using a quantum computer could significantly accelerate the development of new medicines[4] or enable more personalised healthcare.[5]

In financial services, quantum computers could simulate and optimise investment trading portfolios, taking into account a much wider range of real-life factors and market conditions to generate value for consumers.[6] Quantum computers could also make artificial intelligence (AI) more powerful as machine-learning algorithms could learn complex tasks using fewer than the millions of examples typically used to train AI systems today.[7] However, they also have the potential to undermine standard encryption techniques used to protect communications, personal and financial information, requiring a major transition to secure them in future.

Quantum computers are not the only quantum technology on the horizon. Quantum communication provides new ways of transmitting information securely. This could help harness the full power of quantum cloud computing to provide novel quantum compute resources at scale over distributed systems. Quantum-assisted communication, a hybrid of quantum and classical technologies, could potentially improve the speed and reliability of 'classical' digital communication.[8] Additionally, Quantum Key Distribution (QKD) offers a new way of securely sharing cryptographic keys to protect the security of communications against the processing power of future quantum computers.

Obstacles to realising quantum technologies

However, despite their potential, quantum computers and quantum communications are currently in a stage of nascency, with much attention being directed towards academic research, industry research and development (R&D) and testing. As such, there are numerous technical and engineering challenges that must be overcome to realise the potential of these quantum technologies.

From a technological perspective, the nature of quantum information poses considerable challenges. Qubits, the fundamental unit of quantum information, are extremely delicate, requiring extensive protection from external interference and in some setups near absolute-zero temperatures for efficacy. Currently, qubits have a limited lifespan of a few microseconds only[9], and the difficulty of maintaining these quantum states leads to errors.

---

4 McKinsey & Company, Recalculating the future of drug development with quantum computing, 2020, https://www.mckinsey.com/industries/life-sciences/our-insights/recalculating-the-future-of-drug-development-with-quantum-computing

5 European Parliament, What if quantum technologies were to revolutionise healthcare?, 2020, https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/737121/EPRS_ATAG(2022)737121_EN.pdf

6 IBM, Exploring quantum computing use cases for financial services, 2020, https://www.ibm.com/downloads/cas/2YPRZPB3

7 Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe & Seth Lloyd, Quantum Machine Learning, Nature, 2017, https://www.nature.com/articles/nature23474

8 Ofcom, Quantum Communications: new potential for the future of communications, 2021, https://www.ofcom.org.uk/__data/assets/pdf_file/0013/222601/Executive-Summary.pdf

9 Chenlu Wang, Xuegang Li, Huikai Xu, et al., Towards practical quantum computers: transmon qubit with a lifetime approaching 0.5 milliseconds, 2022, https://www.nature.com/articles/s41534-021-00510-2

To address the technical difficulties inherent in quantum technologies, significant progress in engineering is required. This includes the development of advanced systems capable of dealing with the fragility of qubits and expanding quantum computers to fulfil real-world computational requirements. It should be noted, however, that there is not yet a unified agreement on the precise timelines for the development of quantum technologies for practical applications. According to estimates from the DRCF Quantum Symposium, the period where quantum computers may begin to demonstrate 'quantum advantage'- or superiority over classical computing in many advanced applications - is estimated to be within the next 5 to 10 years.[10] Further, broader integration of quantum computing into commercial applications is predicted to occur within a 10 - 20 year timeframe.[10] As such, today's quantum computers are considered to be prototypes, and overcoming these technical and engineering barriers will be essential to realise the potential promised by quantum technologies.

The national and global race for quantum advantage

Beyond these opportunities and barriers, stakeholders have also highlighted concerns that countries that are slow to harness the capabilities of quantum could be left behind in global science and technology innovation.[11] In light of the potential increase in technological capabilities promised by quantum technologies, quantum has attracted substantial interest and investment from governments worldwide.[12]

In 2014, the UK Government launched its National Quantum Technologies Programme with some initial funding of £214M.[13] In 2020, the National Quantum Computing Centre (NQCC) launched. Funded through UK Research and Innovation (UKRI), the new Centre receives nearly £100M over a five-year period. The UK enjoys a particularly vibrant quantum ecosystem of nearly 50 startups and considerable venture capital investment. The NQCC finds that the UK comes second only after the US in terms of corporate engagement, number of startups, startup capital raises and supply chain maturity. Building on these foundations, in March 2023, the UK government published its National Quantum Strategy to provide a ten-year vision for a quantum-enabled economy in the UK.[14] The strategy points to the opportunities for the UK to be at the forefront of quantum regulation that supports innovation and the ethical use of quantum technologies across the economy.[15]

---

10 DRCF Quantum Symposium - Panel.
11 DRCF Quantum Symposium.
12 McKinsey & Company, Quantum Technology monitor, 2023, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf
13 UK National Quantum Technologies Programme, About Us, 2023, https://uknqt.ukri.org/about-us/
14 Department for Science, Innovation & Technology (DIST), 'National Quantum Strategy', 2023, National quantum strategy - GOV.UK (www.gov.uk)
15 Department for Science, Innovation & Technology (DIST), 'National Quantum Strategy', 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1142942/national_quantum_strategy.pdf

Quantum technologies: Initial considerations for DRCF member regulators and stakeholders

As quantum technologies and industries develop and use cases evolve, existing regulation will continue to apply. But not all future use cases or aspects of quantum technologies will be within the remits of DRCF member regulators. We will need to remain aware of emerging use cases.

At this stage, building on learnings from the DRCF Quantum Symposium, we have identified several initial themes of interest. In this paper, we consider:

- **The role of the regulator in emerging technologies:** Our individual and collective approach to regulation and innovation seeks to enable emerging technologies to evolve and develop responsibly. For this reason, we are technology neutral. As such, we do not approach quantum technologies any differently to other emerging fields.

- **Information and data security, privacy and the transition to quantum secure technologies:** The impact of future quantum computers on the security of communications, personal and financial information is a key issue for several DRCF members who have information and data security-related responsibilities.

- **Transition to quantum-safe technologies:** The risks to data security and privacy will require a major transition to secure information in future. The DRCF regulators are considering how we might best support the ongoing and well-established initiatives from bodies such as the National Institute of Standards and Technology (NIST) and the National Cyber Security Centre (NCSC) in respect to the transition to quantum-safe technologies.[16]

- **Competition in quantum-enabled markets:** As with any emerging technology, quantum innovations could allow new firms to challenge existing firms and business models, and/or increase barriers to entry for new competitors by reinforcing existing market power. As the ecosystem develops, the DRCF regulators seek to ensure that quantum technologies develop in ways that promote open, competitive markets and provide effective consumer protection.

- **The role of quantum standards and specifications in complementing regulation:** There are extensive efforts to scope and develop standards and specifications in emerging quantum technologies, to facilitate collaboration, develop best practices, mitigate risks and accelerate innovation. The DRCF member regulators recognise their potential to complement regulation, and we seek to collaborate internally to coordinate our contributions to standards initiatives.

16 NIST, 'Post-Quantum Cryptography', https://csrc.nist.gov/projects/post-quantum-cryptography; NCSC, 'Preparing for Quantum-Safe Cryptography', 2020, https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography; NCSC, ' Quantum Security technologies', 2020, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

- **Explainability of future quantum machine learning, including hybrid applications:** The DRCF regulators have active AI workstreams, which consider issues such as the explainability of AI decisions and other areas of AI.[17] Historically, explainability issues have been considered in the later stages of development and deployment. However, it is important, at an early stage, to explore how this quantum step change might exacerbate the opacity of decision-making or the efficacy of current explainability models.

As quantum technologies evolve, the DRCF member regulators will seek to ensure that the technology develops in ways that promote open, competitive markets, as well as protect consumers and their information rights. Ongoing dialogue with industry, government and academia, and other interested stakeholders, will enhance our mutual understanding of the intersections of quantum technologies and existing regulation, shape responsible innovation, and help the UK harness the potential of a quantum future.

17 For example, under UK GDPR, where personal data is processed, organisations deploying AI systems are expected to explain the outputs to data subjects. ICO, Explaining decisions made with AI: Part 1 Legal Framework, 2019, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/part-1-the-basics-of-explaining-ai/legal-framework/#legal_framework_3

Introduction

Quantum technologies such as quantum computing and quantum communications have the potential to unlock exciting new technological capabilities. While many of these technologies are still at an early stage of development and timeframes are difficult to predict, they promise to enable breakthroughs in how we can process, transmit and secure information, opening new frontiers in innovation across the economy.

Through our horizon scanning work programme, the Digital Regulation Cooperation Forum's (DRCF) member regulators–the CMA, Ofcom, ICO and the FCA–seek to identify these new frontiers and develop a coherent view of emerging technologies and markets. The DRFC is exploring what are quantum technologies exactly, how are they different from their 'classical' counterparts and what could they potentially achieve? What issues should the DRCF regulators be thinking about now to prepare for a quantum enabled world?

This Insights Paper considers these questions, building on contributions and learnings from the DRCF Quantum Symposium held in February 2023.[18] We aim to contribute to the global conversation by discussing examples of where our existing regulatory remits are already relevant to the nascent world of quantum, and where the voice of DRCF regulators may be important as these technologies develop and mature. Ultimately, we want to ensure that the UK can harness the benefits of quantum innovation while protecting consumer and citizen interests.

Building on the contributions from panellists and attendees at the DRCF Quantum Symposium, this Insights Paper:

- Provides an overview of two quantum technology areas of collective interest to the DRCF (quantum computing and quantum communications) including the current and anticipated capabilities and the current state of development ('Overview: Quantum Technologies');
- Explores some of our current thinking on the cross-cutting regulatory considerations relevant to our remits ('Regulatory Considerations');
- Sets out the DRCF's next steps in this space ('Conclusions and Next Steps').

The paper also draws on desk-based research and our findings from our ongoing engagement with stakeholders. We are grateful to all who have inputted into and reviewed the paper. We appreciate the input and contribution from colleagues at the National Quantum Computing Centre.

This paper is a futures-focussed piece intended to provide initial insights into our thinking on how quantum technologies may develop, and how the DRCF remits may intersect with them. It should not be read as regulatory guidance or taken as an indication of current or future policy by any of the DRCF member regulators. We welcome any comments or suggestions in relation to this topic. Please contact us at JoiningUpOnFutureTech@ofcom.org.uk.

---

18 DRCF, The Metaverse and immersive technologies - A regulatory perspective, DRCF, 2022, https://competitionandmarkets.blog.gov.uk/2022/06/22/the-metaverse-and-immersive-technologies-a-regulatory-perspective/

Overview: Quantum Technologies

Of various types of quantum technologies, quantum computing and quantum communications are of collective interest to the DRCF regulators. On the following pages, we provide greater detail on each of these technologies, their potential applications and the likely risks and benefits associated with them.

Quantum Computing

The potential of quantum computing is considerable. While a reliable quantum computer that would be powerful enough and sufficiently resilient to errors is still many years away, proponents of this fundamentally different approach to computing, point to significant potential benefits, such as a vast scaleup of processing power. For instance, current encryption protocols that would typically take a standard desktop computer billions of years to crack could, in principle, be decrypted by a future quantum machine in a couple of seconds.[19] [20] [21]

Quantum computing also promises an enormous speedup for tasks in some well-defined domains, such as number crunching[22] and optimisation[23], which will be discussed in more detail below. Further, quantum computing is hoped to also tackle new classes of mathematical problems that are intractable to our computer systems as they exist today, and which may have real-world applications in analysing huge chunks of data.[24]

The concept of a quantum computer was first introduced 40 years ago when the renowned physicist Richard Feynman suggested that quantum systems would be easier to model with a computer that is also quantum. However, it was not until a decade ago that efforts greatly accelerated, mainly thanks to significant progress in assembling the very machinery that is required to build quantum computers, such as large-scale cooling devices and appliances to manipulate subatomic particles. Today, the global competition to construct reliable and useful quantum computers is well underway.[25]

On 15 March 2023, the UK Government announced its National Quantum Strategy.[26] It aims to increase Britain's share of global private equity investment into quantum technology companies and its share of the global quantum technologies market to 15 percent each (currently at 12 and 9 percent, respectively), backed by a planned £2.5B in public funding over the next ten years. The US Government's National Quantum Initiative[27] is set to invest $850M in 2023.

19 John Preskill, Introduction and Overview, California Institute of Technology, 1997, http://theory.caltech.edu/~preskill/ph229/notes/chap1.pdf
20 Davide Castelvecchi, Are Quantum Computers about to Break Online Privacy?, Nature Magazine, 2023 https://www.scientificamerican.com/article/are-quantum-computers-about-to-break-online-privacy/
21 Alex Wilkins, Quantum computers proved to have 'quantum advantage' on some tasks, New Scientist, 2022, https://www.newscientist.com/article/2323540-quantum-computers-proved-to-have-quantum-advantage-on-some-tasks/
22 Martine Giles, Explainer: What is a quantum computer?, MIT Technology Review, 2019, https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/
23 Robert Davis, Cutting Through the Hype of Quantum Optimization, Qiskit, 2021 https://medium.com/qiskit/cutting-through-the-hype-of-quantum-optimization-6d4b5c95e377
24 Mordechai Rorvig, Quantum Algorithms Conquer a New Kind of Problem, Quanta Magazine, 2022, https://www.quantamagazine.org/quantum-algorithms-conquer-a-new-kind-of-problem-20220711/
25 Oxford Analytica, Global quantum technology competition will heat up, Emerald, 2022, https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB266828/full/html
26 Department for Science, Innovation and Technology (DSIT), National Quantum Strategy, 2023, https://www.gov.uk/government/publications/national-quantum-strategy
27 National Quantum Initiative, Quantum Gov, 2018, https://www.quantum.gov/wp-content/uploads/2022/04/NQI-Factsheet.pdf

In Europe, the EU's Quantum Technologies Flagship has a budget of around €1B.[28] At present, most major technology businesses as well as international banks invest in setting up quantum computing capabilities. Global start-up funding in 2021 was more than $4B and has been growing continuously over recent years.[29]

The UKRI's National Quantum Computing Centre (NQCC) summarises current efforts and investment levels in the following infographic:

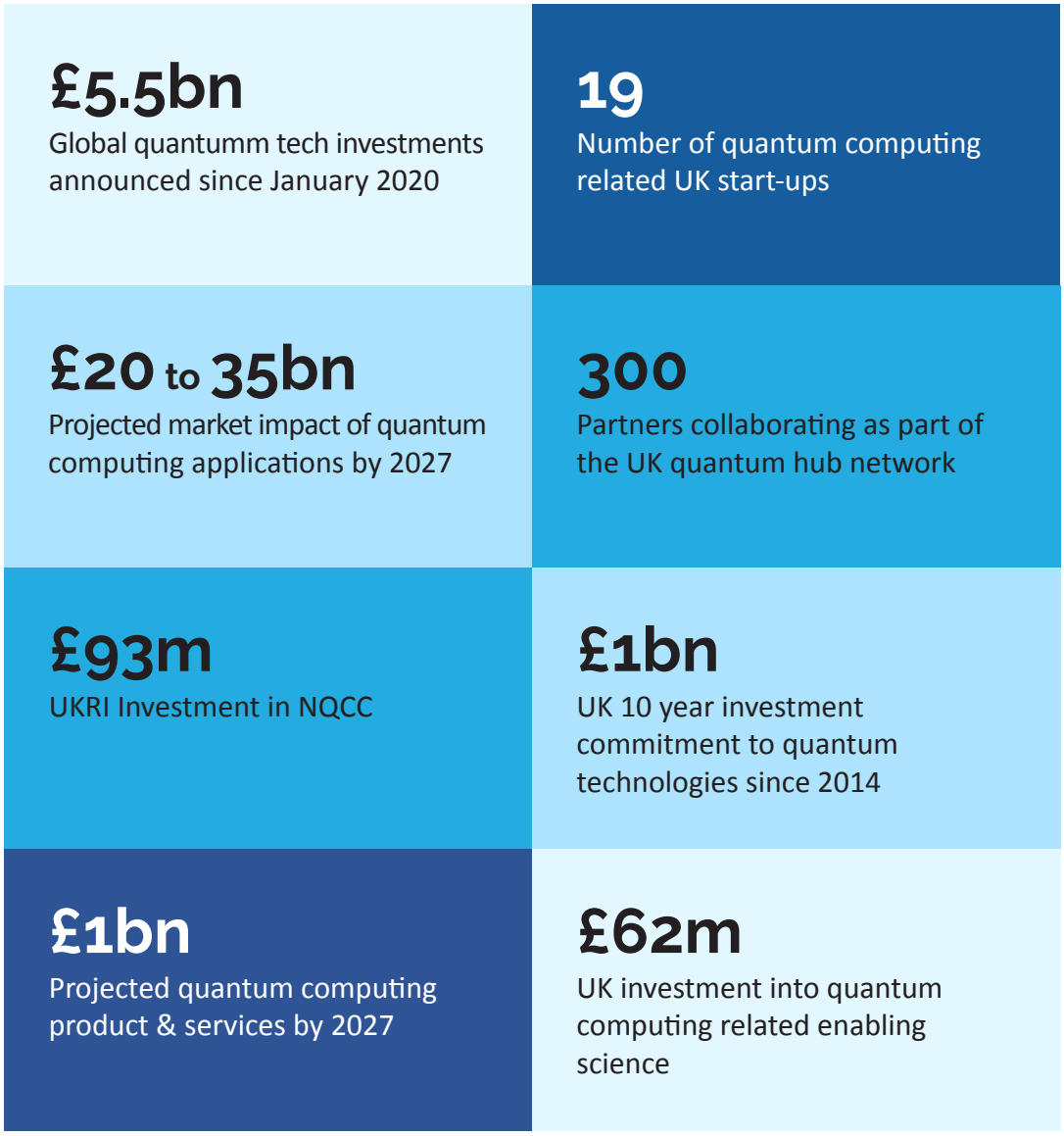

Figure 1: UK investment in quantum technologies. Source: NQCC.

28 Quantum Flagship, The future is Quantum, 2018, https://qt.eu/
29 Thomas Alsop, Quantum technology startup funding worldwide 2001 – 2021, Statista, 2022, https://www.statista.com/statistics/1317776/global-quantum-technology-startup-funding-segment/

How does quantum computing work?

The computers we use today are built on transistor technology - there are billions of transistors in an average laptop. Whichever device we use, from tablet to laptop, PC or supercomputer, computation is achieved by amplifying electrical signals, which are represented as 0 and 1 when the transistor flips between voltage levels. This is the 'bit' (binary digit), which is the fundamental unit in 'classical' computing. Transistors can be linked together for the purpose of representing more complex operations. This binary representation of voltage levels is the language the computer understands; various programming languages translate between user input and binary sequences.

The bit itself can only ever be in one of its two distinct states, 0 and 1. Yet things are very different in the world of quantum. The basic unit in quantum computing is the quantum bit, or qubit. Unlike the 'classical' bit, a qubit can hold two states at the same time.

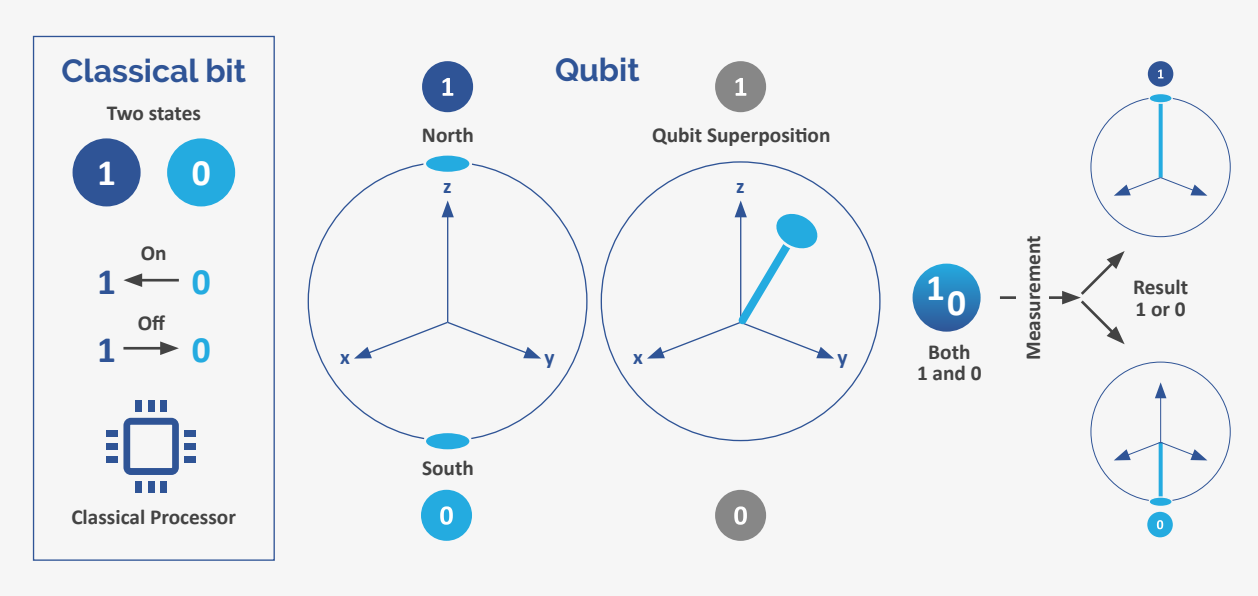

Figure 2. Image source: https://www.shutterstock.com/search/qubit

The potential of quantum computing becomes more obvious in the interaction of these qubits. Two qubits can be made to enter a special kind of bond so they form a new computational unit, and as such can hold four states at the same time. Three qubits in this relationship, which is called entanglement, can hold eight states and so forth: the number of possible states rises exponentially with the number of qubits added. The important point is that each of these states can represent information.

While the compute power of a traditional, digital laptop rises as a linear function of the number of bits, the rise is exponential in the quantum world for each additional qubit. As a result, quantum compute resources could in principle quickly reach colossal levels. In practice, a quantum computer will require large numbers of additional 'replacement' qubits to sustain computations as qubits are fragile and quickly disintegrate (they 'decohere').

Classical bits 2xn			Qubits 2^n	
(2x2)	**4**	**n=2**	(2^2)	**4**
(2x3)	**6**	**n=3**	(2^3)	**8**
(2x4)	**8**	**n=4**	(2^4)	**16**
(2x5)	**10**	**n=5**	(2^5)	**32**
…	**…**	**…**	…	**…**
(2x100)	**200**	**n=100**	(2^{100})	**1267650600228229401496703205376**

Figure 3: the exponential growth of compute power of qubits vs 'classical' bits. Source: TU Delft.

With qubits having the potential to be so powerful, the question arises how they can be realised in practice. In 'classical' computing, bits are the representation of processes on a machine level, which are physically realised using silicon wafers that are implanted on a chip.[30] The research field of superconducting circuits attempts to leverage existing silicon wafer manufacturing principles for building qubit technologies. However, there are many other experimental approaches that try to establish which physical object would make for a good qubit in a quantum computer. Further examples are photons, trapped ions or nitrogen vacancies in diamonds. At present, it is not clear which type of particle exactly is best suited to make a 'good' qubit that can perform effectively and reliably in a future quantum computer. The question of physically realising the (theoretical) advantages of qubits is one example of the fundamental challenges that quantum computing is facing, which sets it apart from 'classical' computing where basic engineering principles were settled many decades ago.

30 Imin Kao and Chuhui Chung, Wafer Manufacturing: Shaping of Crystal Silicon Wafers, Wiley Online Library, 2021, https://onlinelibrary.wiley.com/doi/book/10.1002/9781118696224

How is quantum computing different to 'classical' computing?

It is important to note that quantum computing is a very different approach to computing. A 'classical' computer is binary as outlined above, with its fundamental unit being in one of two discrete states ('0' or '1'). The outcome is deterministic in that, assuming the system is free of errors, logic demands the result of the computation. In contrast, the quantum computer arrives at a result that is probabilistic. Run multiple times, the probabilistic result reaches such high levels of confidence that it can be accepted as true. John Preskill from the California Institute of Technology likens the difference to the way in which we typically read, say, a 100-page book: line by line, paragraph by paragraph, page by page. The quantum computer however "reads" the entire 100 pages at once with a bird's eye view and finds the result of a computation in the correlation between the pages, not in a single specific paragraph.[31]

Using a quantum computer for complex modelling

There is huge potential for quantum computers to undertake complex modelling that a 'classical' computer would struggle with. A prime example is assessing how a drug molecule will react in different environmental conditions. The computers that exist today find it hard to model how molecules form and behave due to the sheer number and speed of possible formations that need to be considered. In theory, quantum computers will have the capacity to match this complexity. If realised, such modelling could have a number of potential future applications e.g. in pharmaceutical research, drug discovery or research in materials science.

Beyond this example, quantum computing is also hoped to support the modelling of complex systems more generally across a wide range of different sectors and research interests. For instance, economic behaviour at systems level, how social networks evolve, ways to optimise transport routes or how distant galaxies form. Again, each of these problems involves such a vast number of variables that interact with each other so that it becomes very difficult for 'classical' computers to solve these problems.

Improving our ability to tackle optimisation problems is of huge importance in sectors such as logistics, transport and warehousing–indeed any field that requires optimal routing or finding the shortest path. Similarly, it is assumed that quantum computing will greatly support asset pricing and portfolio optimisation.[32] Researchers also hope that quantum computing can increase the speed of learning from training data and add capabilities to neural networks.[33] This topic will be discussed in more depth and with a view to regulatory considerations in later sections of this paper.

---

31 John Preskill, Quantum Computing & the Entanglement, Institute for Quantum Computing, Youtube, 2014, https://www.youtube.com/watch?v=3XbQpUtqgnU

32 Dylan Herman et al., A Survey of Quantum Computing for Finance, Arxiv, 2022, https://arxiv.org/pdf/2201.02773.pdf

33 Biamonte, J., Wittek, P., Pancotti, N. et al. Quantum machine learning. Nature 549, 195–202, https://www.nature.com/articles/nature23474

Potential risks to encryption

A well-established area of risk arising from the development of quantum computing is their anticipated future ability to break most standard encryption systems. At present, digital computers can easily calculate the product of two large prime numbers, but the reverse is much more difficult. For sufficiently large integers, even the best digital computers require, on average, an impossible amount of time to find the two prime numbers it is composed of. As a result, factorisation of large integers forms the basis of most encryption systems.

In 1994, Peter Shor from the Massachusetts Institute of Technology demonstrated that unlike digital computers, quantum computers would be very effective at factorising large integers (with the procedure by which this advantage can be realised has come to be known as Shor's Algorithm).[34] This will have serious implications for encryption protocols as they exist today. In particular, the widely deployed Rivest-Shamir-Adleman (RSA)[35] encryption method is feared to be an easy target for a quantum computer, even one of modest scale.

This risk has implications both now and in the future. One key challenge is the possibility of 'Harvest Now, Decrypt Later' practices by which an adversary may already be targeting and storing sensitive communications, whether it be government data, intelligence signals, private sector business secrets or indeed personal data of individuals.[36] While adversaries are unable to decrypt and exploit this information today, a future quantum computer may deliver on the brief, sometimes referred to as a Cryptographically Relevant Quantum Computer (CRQC).[37] In light of the intensifying global competition over emerging technologies in general and quantum computing in particular, efforts are well underway to find new encryption protocols that even quantum computers will be unable to crack. This nascent research field is commonly referred to as postquantum cryptography.[38]

34 Peter Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, IEEE, 1994, https://ieeexplore.ieee.org/document/365700
35 Daniel Kleitman, Undergraduate Seminar in Discrete Mathematics, Spring 2006, DSpace@MIT, https://dspace.mit.edu/handle/1721.1/100853
36 Paul German, Data and encryption strategies in post-quantum world: Harvest now decrypt later, Open Access Government, 2022, https://www.openaccessgovernment.org/data-and-encryption-strategies-in-a-post-quantum-world-harvest-now-decrypt-later/146562
37 John Mattsson, Migration to quantum-resistant algorithms in mobile networks, Ericsson, 2023, https://www.ericsson.com/en/blog/2023/2/quantum-resistant-algorithms-mobile-networks
38 National Institute of Standards and Technology (NIST), Post-Quantum Cryptography, NIST Computer Security Resource Centre, 2022, https://csrc.nist.gov/projects/post-quantum-cryptography

Emerging technical responses to the quantum risk to encryption: Quantum Random Number Generation (QRNG)

In addition to the development of new quantum resistant encryption protocols, researchers and industry are exploring the potential of using quantum technology to generate 'truly random' numbers. This technique, called quantum random number generation (QRNGs), could potentially be used to support quantum secure systems.

Truly random numbers (i.e. arrays of numbers that have no discernible pattern to them) are required in a wide range of applications, including cryptography. While sufficiently approximated, mathematically true randomness, however, is widely assumed "impossible with only classical means."[39]

Different ways to generate random numbers (random number generators or RNGs) without quantum require such a high degree of complexity that they are considered practically impossible to work out. Nonetheless, their security is premised on the computational power of the would-be attacker and the knowledge they might be able to gain about the system.

QRNGs make use of the inherent randomness of quantum particles, rather than 'randomness' due to the high complexity of the way a classical (pseudo) random number generator operates, although it is important to note that "in many classical RNGs, the dominant hardware noise is also a consequence of quantum processes"[40], as the National Cyber Security Centre (NCSC) explains in its white papers on quantum key distribution and quantum random number generation.

39 Xiongfeng Ma, Et al., Quantum random number generation, NPJ, 2-16, https://www.nature.com/articles/npjqi201621#citeas
40 National Cyber Security Centre (NCSC), Quantum security technologies, 2020, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

Obstacles to realising quantum computing

While the promise of quantum computing is huge, there are considerable obstacles towards its realisation. The first of these is that there are many competing and different approaches to the basic engineering principles behind quantum computing, let alone ideas to design entire quantum computer systems. Finding the winning qubit modality (the "type" of qubit) that could realise the technology physically on a chip is also still very much an open race. This is because different methods of generating a qubit make different demands on the supporting technologies and computing hardware. The type of qubit used changes how the quantum computer needs to be designed.

A further challenge is that superconducting circuits, a qubit modality pursued by Alphabet[41] and IBM[42], among many others, all require large cooling devices. This creates significant challenges to scalability and raises questions about energy use and sustainability. That said, if successful, the ability to use existing superconducting circuits for quantum computing has an advantage, in that unlike other competing qubit modalities, superconducting qubits may be able to utilise existing silicone chip manufacturing systems.[43]

Finally, approaches to generating a qubit suffer from low fidelity and high error rates. Quantum compute resources scale exponentially with each additional qubit embedded in the system, which is their chief advantage over binary computing, but unfortunately so do errors. At the subatomic level, where particles move at high speed and are easily disturbed, noise and interference can quickly ruin computations. Moreover, qubits quickly fade away ('decohere') and therefore lose the information they hold. Correcting errors of this kind is one of the biggest challenges to making quantum computing a reality.

Potential timelines for realising quantum computing

Quantum computing is said to be approaching the so-called NISQ (Noisy Intermediate-Scale Quantum) era where first-generation machines of several hundreds of qubits can be expected. These machines are noisy, somewhat error prone and best considered prototypes. Scaling remains a significant challenge. A concept advocated by John Preskill in 2018, NISQ era computers will be useful to some degree but lack the universal features that will ultimately make quantum computers superior.[44]

---

41 Google Quantum AI, Explore the possibilities of quantum, https://quantumai.google/
42 Ryan Gordon, Quantum Computing with Superconducting Circuits, IBM, 2020, https://research.ibm.com/publications/quantum-computing-with-superconducting-circuits
43 University College London (UCL), Study shows promise of quantum computing using factory-made silicon chips, Phys Org, 2021, https://phys.org/news/2021-03-quantum-factory-made-silicon-chips.html
44 John Preskill, Quantum Computing in the NISQ era and beyond, Arxiv, 2018, https://arxiv.org/abs/1801.00862

Many companies have published different indicators or have made competing claims to 'quantum supremacy', a term that has recently been softened to the more appropriately phrased 'quantum advantage'. In 2019, Alphabet made headline news when the company claimed to have reached quantum supremacy following the implementation of a task on their quantum computer that quickly solved a problem the magnitude of which would take a digital supercomputer many thousand years to complete.[45] However, IBM vocally disputed this claim.[46]

If they mature, quantum computers are likely to be integrated with existing digital infrastructure so that they can excel at tasks for which they are superior while supporting digital computing in other domains where established computing is more sensible and practicable. Quantum computing will not be universally faster in all domains, and for a great number of problems digital computers will remain the technology of choice. As discussed below, this may have regulatory implications for managing the transition period towards the quantum era. The NQCCs estimates the era of genuine quantum advantage to be within the next 5-10 years, with the arrival of universal fault-tolerant quantum computers predicted to be within a 10-20 year timeframe. Once basic features and components such as qubit modalities have been universally agreed upon and persistent issues in error correction resolved, algorithms can be implemented and architectures for quantum computing be designed. At that point, scaling up will become a genuine opportunity.

45 Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510, 2019, https://www.nature.com/articles/s41586-019-1666-5#citeas

46 Adrian Cho, IBM casts doubt on Google's claims of quantum supremacy, Science.org, 2019 https://www.science.org/content/article/ibm-casts-doubt-googles-claims-quantum-supremacy

Quantum Communications

The society we live in today is made possible by communications technology. To enable people to connect with friends and family, and to power a modern economy, communications technologies make use of electromagnetic waves and electrical signals. Through ongoing research and development, communications are continually getting faster and more capable. Advancing knowledge of phenomena at the quantum level is enabling potential breakthroughs in how we can transmit and secure information, opening a new frontier in communications innovation.

How do quantum communications work?

Current communications technologies, such as ultrafast broadband or 5G, make use of electrical signals and electromagnetic waves such as radio waves, to transmit information. For fibre optic links, information is encoded into the amplitudes or pulses of electromagnetic waves. Quantum communication, in contrast, makes use the properties of quantum particles, such as the polarisation of single light photons, to transmit information between different parties. Quantum communication is a new approach to communications and will require new hardware and software to make it possible; systems that may require costly future updates to both hardware and software elements.

It is important to note that the term 'quantum communications' has been closely connected with Quantum Key Distribution (QKD), with some even using the term as shorthand for QKD. However, the topic area is broader than that and the section below explores some of these other areas of research and development.

How is quantum communications technology different from existing technology?

Quantum communications may achieve technological breakthroughs in three main ways:

- Using quantum communications to provide security to communications.
- Using quantum communications to enable the full potential of quantum computing, ultimately moving towards a 'quantum internet'. Given how quantum computing will develop is uncertain, the potential implications from this are yet to be seen. It is important to note that a future quantum Internet is not expected to supplant or replace the existing internet, but rather run parallel to it, whilst providing certain improvements (such as in security) or new quantum functionalities.[47] Essentially, a quantum internet is likely to connect quantum computers over secure quantum communications channels alongside digital infrastructure.

47 Andrew Nellis, The quantum internet, explain, University of Chicago, 2022, https://news.uchicago.edu/explainer/quantum-internet-explained

- Using quantum to improve classical (i.e. non-quantum) communications. This area is still undergoing research, and potential capabilities are even more uncertain than the two areas noted above.

Using quantum communications to provide security

The previous section of this Overview section discussed the risks to the security of information, personal data and communications posed by advances in quantum computing. One of the key areas of quantum communications research is the use of quantum phenomena to secure communications. The techniques under development, such as Quantum Key Distribution (QKD), have the potential to provide an additional layer of security capable of resisting advanced quantum computers.

At present, online communication typically makes use of cryptographic key exchange protocols. In this, each participant holds a cryptographic key that can be used to encrypt or decrypt information. However, the ongoing security of the information is based on the computational difficulty of brute forcing an attack and the computational power of a potential eavesdropper. A would-be eavesdropper with sufficient computing power could potentially discover the key needed to decrypt information, and then decrypt it using that key. Whilst the difficulty of attempting a brute force attack can be increased by using longer keychains, quantum computers may reduce the difficulties and time involved in a brute-force attack. This is essentially what the aforementioned Shor's algorithm achieves, and why quantum-safe, or postquantum, cryptographic approaches will be needed.

Quantum engineers have created a hybrid classical/quantum approach called Quantum Key Distribution (QKD) that uses quantum phenomena to develop a protocol that does not depend on the potential hacker having sufficient computational power. In this, encryption keys can be agreed between two parties, utilising the 'no cloning' theorem of quantum mechanics that ensures that the key cannot be tampered with by potential eavesdroppers without it being evident that they have attempted to read off the message.[48] It should be noted however that with QKD, only the exchange of key pairs is quantum-encoded; the actual message to be exchanged still requires 'classical' communication channels.

QKD is now being explored as an option to provide security for data which might otherwise be at risk from 'Harvest Now Decrypt Later' attacks.

48 Quantum Flagship, Quantum Key Distribution (QKD), https://qt.eu/quantum-principles/communication/quantum-key-distribution-qkd

Given the specialised hardware requirements of QKD, and that physical human-in the-middle attacks could still occur (e.g. an attacker could agree keys with two parties who think they are actually communicating with each other), NCSC does not endorse QKD for any government or military applications and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors. NCSC advises that any organisations considering the use of QKD ensure that robust quantum-safe cryptographic mechanisms for authentication are implemented alongside them.[49]

While the terms 'quantum communications' and 'QKD' are often used interchangeably, QKD is only one way to make use of quantum phenomena for securing information. There are other ways of sending 'private information' through encoding information into quantum states, and so making that information fundamentally inaccessible to others.[50]

Using quantum communications to connect quantum computers

As described in the above section, quantum computing holds great promise in a number of areas. In particular, it is anticipated that quantum communications will be needed to fully realise the potential of quantum computing, particularly over the NISQ era.[51]

For example, it could enable distributed quantum computing where quantum states are involved in computations. Distributed quantum computing is where quantum computers are connected over secure quantum channels to then run computations together, enabling smaller quantum computers to benefit from the computational resources of larger ones. Distributed systems of this kind would use quantum compute resources in a more effective way and help scale up the numbers of qubits that can be used in computation, thereby enabling the creation of virtual qubit machines of higher compute power. A quantum internet would be a network of these machines. The principles of quantum mechanics might also be used to enhance 'classical' distributed computing.[52]

In similar fashion, quantum communications could benefit quantum cloud computing. Given the cost and complexity of quantum computers, it is likely that most users will only access them from third-party providers remotely. If a user wanted to use a quantum device, such as a quantum sensor, and then send information from that, for example to a cloud quantum computer to run calculations on it, then quantum communications would be required if a quantum state were part of such a calculation.

---

49 National Cyber Security Centre (NCSC), Quantum security technologies, 2020, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
50 Hlér Kristjánsson, Robert Gardner and Giulio Chiribella, Quantum Communications Report for Ofcom, Ofcom, 2021, https://www.ofcom.org.uk/__data/assets/pdf_file/0012/222600/Quantum-Communications-report-for-Ofcom.pdf
51 Davide Castelvecchi, The quantum internet has arrived (and it hasn't), Nature, 2018, https://www.nature.com/articles/d41586-018-01835-3
52 Daniele Cuomo, Marcello Caleffi, and Angela Sara Cacciapuoti, Towards a distributed quantum computing ecosystem, The Institute of Engineering and Technology, 2020, https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-qtc.2020.0002

Quantum communications could further enhance the privacy of computation. For example, it could enable multi-party quantum computation, which is where parties do not need to reveal information about their input data in order to run computations together. The calculations in question might not be difficult to do, but the benefit of quantum communications would be that the secrecy of the input data could be maintained. Quantum communications could also enable blind or private quantum computing, which is where a client can carry out a quantum computation on a third-party quantum computer without revealing the information, algorithm, or output to the third party.[53]

In addition to the above, ultraprecise quantum clocks and Positioning, Navigation and Timing solutions (PNS) are expected to benefit from quantum communications. In this context, entangled quantum states and quantum communications between atomic clocks could provide additional security. The precision of this synchronised clock time would be close to the fundamental limits of what is possible, providing benefits where such synchronised time is likely to be important, such as in a future quantum internet. QKD could also be added as a security layer for this purpose.

Using quantum to improve communication characteristics

The use of quantum phenomena may improve communications characteristics. This is being explored down multiple avenues, depending on whether the information being transmitted is 'classical' or quantum information (bits or qubits, or both), and whether the transmission channel is a 'classical' channel or a quantum channel:

Benefits from the use of a quantum channel when transmitting classical information

'Classical' information could be sent using a quantum transmission channel, potentially leading to improvements in communication rates. One current area of research is looking at how using entanglement between successive qubits when sending information through a quantum channel could speed-up the rate of transmission. This is known as superadditivity.[54]

Secondly, 'classical' information (bits) could be sent down a quantum channel, where the sending and receiving parties share entangled quantum states, in an approach known as 'superdense coding'.[55] Through the use of entanglement, superdense coding enables the number of bits to be transmitted to be doubled, as a single qubit can be used to transmit two classical bits of information.

---

53 Joseph Fitzsimons and Elham Kashefi, Unconditionally verifiable blind quantum computation, Physics Review A 96, 2017, https://journals.aps.org/pra/abstract/10.1103/PhysRevA.96.012303

54 Mohamed Nawareg, Sadiq Muhammad, Pawel Horodecki, and Mohamed Bourennane, Superadditivity of quantum information resources, Since Advances, Vol 3 Issue 9, 2017, https://www.science.org/doi/10.1126/sciadv.1602485

55 Qiskit, Superdense Coding, https://learn.qiskit.org/course/ch-algorithms/superdense-coding

It is important to note that both superadditivity and superdense coding are still in the theoretical research phase. There are challenges to overcome, such as communication parties need to share entangled qubits and currently error rates remain high.

Moreover, it is unclear in what contexts these types of functionalities might be significantly more useful than simply employing 'classical' communications systems–for example, using 'classical' communication links and taking more time to transmit the information, or upgrading a 'classical' communications channel to have greater bandwidth. Specialist equipment would be needed, alongside overcoming the challenges of integrating such into existing communications systems.

In summary, the quantum technology involved in the above areas needs to undergo more research and development before their potential becomes obvious. Based on current knowledge, it is possible that 'classical' communications using bits will largely continue to perform the same functions as they do now and not be replaced by quantum communications. However, technological advances might change this outlook.[56] Quantum communications are expected to be used in new use cases, such as providing assured security or to enable the full potential of quantum computing and other quantum technologies. 'Classical' and quantum communications should therefore not be simply compared to each other, as they will likely fulfil different use cases.

Obstacles to realising quantum communications

There are a number of challenges that need to be overcome in the development of quantum communications.

The most significant one is that of enabling long-distance communications due to the error rates involved in transmission, which grow with distance. Error rates in transmission that grow with distance also happen with existing communications, and to address it modern day communication networks have nodes that can detect incoming signals and either amplify them or retransmit them. However, for quantum communications, a quantum state cannot be viewed, read or observed without collapsing its quantum state, nor can it be copied (due to the no-cloning theorem). Therefore, for quantum communication to work over larger distances a new approach needs to be taken, namely through the use of quantum repeaters.

Quantum repeaters would make use of entanglement between nodes, and then use the principle of quantum teleportation to transmit information. Quantum teleportation allows qubits to be 'transmitted' without the physical transfer of the particle storing the qubit.[57] By having repeater nodes sufficiently close to each other, entanglement can be used to join together multiple nodes into a single entangled state, known as entanglement swapping.

---

56 Hlér Kristjánsson, Robert Gardner and Giulio Chiribella, Quantum Communications Report for Ofcom, Ofcom, 2021, https://www.ofcom.org.uk/__data/assets/pdf_file/0012/222600/Quantum-Communications-report-for-Ofcom.pdf

57 Angela Sara Cacciapuoti, Marcello Caleffi, Rodney Van Meter, Lajos Hanzo, When Entanglement meets Classical Communications: Quantum Teleportation for the Quantum Internet, Arxiv, 2019, https://arxiv.org/abs/1907.06197

There are however significant practical challenges to achieving this. Firstly, the quantum repeaters would need to be time synchronised, given the operations on the entangled states need to be synchronised perfectly. This means 'quantum memories' will need to be developed that can store quantum states and then allow them to be used when needed. In this example, the quantum information would be transferred from the photon that carried it between nodes, and then stored in a memory system. Given the information itself would be transferred, rather than copied, this would not violate the no-cloning theorem. However, currently these memory systems only last very short periods of time, which poses limitations for quantum communications networks unless new breakthroughs occur to lengthen the amount of time information can be stored.

Another way to improve the distances over which quantum communication networks can function is through the use of satellites. Breakthroughs are also occurring in this area. In 2020, the Micius satellite, which is exclusively designed for quantum communications, acted as a communications relay that simultaneously transmitted a pair of secret keys (entangled photon pairs) to two ground stations more than 1,000km apart, which is a significant improvement given that it is multiples of what can be achieved using ground links.[58] However, satellite links also pose challenges. Coverage is low given the small number of satellites with this capability, and it also requires relatively good weather to enable it to work, which is a significant limitation. Also, satellites cannot provide indoor coverage, especially if the satellite is sending photons. As such, researchers have suggested that perhaps a hybrid of terrestrial and satellite communication links might be the way forward.[59]

Potential timelines for realising quantum communications

QKD networks are currently being developed. For example, BT and Toshiba have launched a quantum-secured metro network to connect customers across London.[60] The UK Quantum Communications Hub is developing a large-scale testbed, with networks in Cambridge and Bristol, and connections between Cambridge, London and Bristol. In 2022, the Tiangong-2 space lab in China received quantum encryption keys from the Micius satellite, as an example of a space-borne quantum network.

The Internet Research Task Force has published architectural principles for a quantum internet which discusses the goals of such a network, the state of development in these areas, and includes a discussion of the challenges needing to be overcome for this to be built.[61]

---

58 Karen Kwon, China Reaches New Milestone in Space-Based Quantum Communications, Scientific American, 2020, https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/

59 de Forges de Parny, L., Alibart, O., Debaud, J. et al., Satellite-based quantum information networks: use cases, architecture, and roadmap, Commun Phys Vol 6, Issue 12, 2023, https://www.nature.com/articles/s42005-022-01123-7

60 EY, BT and Toshiba launch first commercial trial of quantum secured communication services – EY becomes first commercial customer, EY Press Releases, 2022, https://www.ey.com/en_uk/news/2022/04/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services

61 Wojciech Kozlowski, et al., RFC 9340: Architectural Principles for a Quantum Internet, The Internent Engineers Taskforce (IEFT), 2023, https://datatracker.ietf.org/doc/rfc9340/

Regulatory Considerations

This section draws from ideas and themes raised at the DRCF Quantum Symposium, informed further by our ongoing stakeholder engagement, to set out how regulation may apply to quantum technologies. First, we set out the role of the regulator in emerging technologies; then we discuss how current regulations may apply before turning to some potential future areas of interest for the DRCF member regulators in quantum technologies.

The role of the regulator in emerging technologies

Each DRCF member regulator is committed to fostering safe and responsible innovation within their regulatory remits.[62] DRCF member regulators aim to engage with innovators in order to understand the implications and impacts of emerging technologies, identify potential harms, and develop early regulatory thinking. Our engagement informs how individual regulators may use the wide range of policy, guidance and supervisory tools in our regulatory toolkit.

Throughout 2022 and 2023, the DRCF's Joining up on Future Technologies workstream organised a number of symposiums, convening stakeholders to improve the regulators' understanding of emerging technologies and promote knowledge sharing throughout their respective ecosystems.[63] [64]

In addition to these events, the DRCF member regulators have undertaken various initiatives to enhance their knowledge of quantum technologies, such as:

- Ofcom's Emerging Technology Programme published a report on Quantum Communications, exploring the implications of quantum systems on the transmission of information.[65]
- The FCA has hosted workshops with stakeholders from academia and the quantum research community to identify the core opportunities and challenges that quantum technologies may present in financial services. The FCA published its findings in a research article, 'A Quantum Leap for Financial Services'.[66]
- The ICO's Emerging Technology team are engaging further to build on insights from the DRCF Quantum Symposium and have started to prepare additional futures thinking on quantum technologies and their intersection with information rights legislation.

62 DRCF, Joining Up on Future Technologies, DRCF, 2021, https://www.gov.uk/government/publications/joining-up-on-future-technologies-digital-regulation-cooperation-forum-technology-horizon-scanning-programme/joining-up-on-future-technologies
63 DRCF, The Metaverse and immersive technologies - A regulatory perspective, DRCF, 2022 https://competitionandmarkets.blog.gov.uk/2022/06/22/the-metaverse-and-immersive-technologies-a-regulatory-perspective/
64 DRCF, Insights Paper on Web 3, DRCF, 2023, https://www.gov.uk/government/publications/insight-paper-on-web3
65 Ofcom, Quantum Communications: a new potential for the future of communications, Ofcom, 2021, https://www.ofcom.org.uk/research-and-data/technology/general/quantum-communications
66 Pavle Avramovic, Sam Qayyum, Dr Rupesh Srivastava, and Evert Geurtsen, A Quantum Leap for Financial Services, FCA, 2021, https://www.fca.org.uk/insight/quantum-leap-financial-services

Quantum 'Technology Neutrality'

The DRCF members take a technology neutral approach to regulation. This means that the regulators do not regulate a technology as such but instead the products and services built on the technology. This ensures that regulation provides a level playing field for emerging technologies, focusing on the potential outcomes of innovation and not the technology itself.

With technology neutrality as a guiding principle, quantum technologies will not differ from other technologies in terms of the DRCF members' regulatory approaches. DRCF member regulators will continue to focus on the products and services of a technology and the subsequent outcomes for consumers, markets, and society.

The DRCF members utilise this approach to explore and understand developing use cases to ensure we are well placed to consider how existing and prospective regulatory frameworks may apply to outcomes. Technology neutrality enables the regulators to ensure consumers are adequately protected whilst allowing them to benefit from novel products and services.

How do our current regulations apply?

Although quantum technologies could have many regulatory implications, two key areas of collective interest to the DRCF emerged from the DRCF Quantum Symposium and subsequent research: information and data security and competition.

Quantum technologies and security

Quantum technologies present new opportunities to develop innovative processes such as quantum computing, quantum communication, and quantum sensing.[67] However, if quantum computers become increasingly powerful, this technology has the potential to break many of the encryption standards that are widely used today, prompting regulatory consideration from a security perspective.

As explained in the Quantum Computing section of this paper, the most well-known example of these security threats arises from the practical application of Shor's algorithm.[68] [69] [70] This future security threat has been drawn into the present, due to the risk that a malicious actor could acquire encrypted data today, to decrypt using a quantum computer at a later date (a 'Harvest Now, Decrypt Later' attack).[71]

Furthermore, encryption is not the only security consideration arising from the development of sufficiently advanced quantum computers and quantum algorithms. Authentication concerns also surface, particularly in the area of digital signatures, with implications for digital communications.

Currently, digital signatures rely on asymmetric cryptography to authenticate the identity of the sender, confirm the integrity of the message content, and provide non-repudiation.[72] Quantum algorithms such as Shor's algorithm significantly reduce the security margin of these schemes by providing a significant speed increase in calculating integer factorisation used for asymmetric keys.[73] As such, in a world where quantum computers are sufficiently advanced, digital signatures based on these schemes would provide fewer guarantees of the integrity and authenticity of digital signatures. This could potentially undermine trust in digital communications.

---

67 Department for Science, Innovation & Technology (DIST), 'National Quantum Strategy', 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1142942/national_quantum_strategy.pdf
68 Jeremy Wohlwend, 'Elliptic curve cryptography: pre and post quantum, Massachusetts Institute of Technology, 2016, https://math.mit.edu/~apost/courses/18.204-2016/18.204_Jeremy_Wohlwend_final_paper.pdf
69 IBM Quantum, 'Shor's Algorithm', 2021, https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm
70 World Economic Forum, 'Transitioning to a Quantum Secure Economy', 2022, https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf
71 EY, 'Are you ready for the "Exponential Quantum Cyber Threats?", 2023 https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/noindex/ey-quantum-approach-to-cybersecurity-v2.pdf
72 NIST, Special Publication 800-63-3 Digital Identity Guidelines, 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
73 Martina Rossi, et al., Using Shor's algorithm on near term Quantum Computers: a reduced version, Arxiv, 2021, https://arxiv.org/pdf/2112.12647.pdf

Some sectors and organisations may be at greater risk than others to the cyber security threats presented by quantum algorithms and advanced quantum computers. For example, financial services firms may be particularly vulnerable to potential quantum computing attacks due to the inherent sensitivity of financial data and the sector's reliance on cryptography to secure communications and transaction activity.[74] Similarly, organisations providing critical national infrastructure such as power grids, transportation systems, and communications networks may face greater risks and cyber security threats due to the sensitivity of the systems they protect, and the potential for widespread disruption.[75]

All businesses that utilise current encryption methods to protect sensitive information and authenticate communications will face further security risks once quantum computers are sufficiently capable. This includes risks to personal data, intellectual property, the integrity of communications or confidential business information. The National Institute for Standards and Technology (NIST) in the US have recognised the scale of the challenge and established a long-standing work programme to develop new cryptographic algorithms to protect against the potential cyber threat of quantum computers. They also recognise the challenges in adapting to this risk which we discuss in a later section of this paper.[76]

With these security considerations in mind, below are some examples of the security-focused regulations of the relevant DRCF member regulators. These security regulations help to ensure that organisations maintain robust cyber resilience, protect personal data, ensure that consumers are protected from harm, and that firms can continue to provide consumers with essential products and services. As quantum technologies continue to develop, organisations are expected to maintain their compliance with all applicable regulations.

74 World Economic Forum, 'Transitioning to a Quantum Secure Economy', 2022, https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf

75 HM Government, National Cyber Strategy 2022', 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

76 William Barker, W. Polk, Murugiah Souppaya, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, NIST CSRC, 2021, https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final

Examples of DRCF Member Regulators' Security-focused Regulation:

Three of the four DRCF member regulators (Ofcom, the ICO, and the FCA) apply security-related requirements as part of their broader regulatory remits. These include the following:

- **Ofcom** is responsible for ensuring telecoms providers comply with the Telecoms Security Act and Network and Information Systems Regulations (NIS).[77] [78] These regulations require providers to identify and reduce security risks and comply with security duties to ensure the integrity of essential services and network information systems.[79]

- **The ICO**, under the UK Data Protection Act (UK DPA) and the UK General Data Protection Regulation (UK GDPR), regulates the processing of personal data across the economy. Organisations must take appropriate security measures to protect personal data.[80] The ICO also oversees additional security regulations under Privacy and Electronic Communications Regulations (PECR), applicable to communications and internet service providers, and NIS (where an organisation is a relevant digital service provider, such as a cloud service).[81]

- **The FCA** imposes a range of obligations that are relevant to operational resilience. These include detailed specifications for certain firms, who are required to identify and address vulnerabilities through mapping exercises, conduct scenario testing exercises to ensure their operational resilience plans are robust, and to learn the lessons for their operational resilience plans in place.[82]

77 UK Public General Acts, Telecommunications (Security) Act 2021, 2021, https://www.legislation.gov.uk/ukpga/2021/31/enacted
78 UK Public General Acts, 'The Network and Information Systems Regulations 2018, 2018, https://www.legislation.gov.uk/uksi/2018/506
79 Ibid.
80 UK Public General Acts, 'Data Protection Act 2018', 2018, https://www.legislation.gov.uk/ukpga/2018/12/enacted
81 ICO, 'NIS and the UK GDPR', https://ico.org.uk/for-organisations/the-guide-to-nis/nis-and-the-uk-gdpr/
82 FCA, 'PS21/3 Building operational resilience', 2021 https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf

Competition in quantum-enabled markets

Quantum technologies may have the potential to disrupt markets and impact competition across multiple sectors. In some instances, technological innovation might lead to stronger competition, for example, where it enables new firms to challenge established incumbents and business models. However, there could also be risks to competition, for example, if new technologies reinforce the market power of existing firms and increase barriers to entry for potential competitors.

As quantum technologies mature, the DRCF member regulators will seek to ensure that the technology develops in ways that promote open, competitive markets and provide effective consumer protection. Success in this approach will require the DRCF member regulators to take a proactive approach to identifying the emerging competition risks associated with the adoption of quantum technologies in their respective remits. For example, in the wholesale financial services markets, early adopters of quantum computers may gain advantages by performing quicker, more accurate predictions and transactions.[83] [84] These conditions could potentially lead to barriers to effective competition in these markets if other competitors are unable to access these technologies.

The CMA and other concurrent sector regulators will continue to monitor emergent markets for competition issues arising and can use existing competition powers to act where necessary. The Digital Markets, Competition and Consumer Bill also proposes giving the CMA additional powers to regulate firms that enjoy substantial, entrenched market power ('Strategic Market Status') in digital activities.

It is important to acknowledge that quantum-enabled services may not always fall within existing remits, depending on the specific issues and contexts involved. The DRCF member regulators will continue to collaborate to understand how to effectively approach any challenges that may arise in competition due to the wider adoption of quantum technologies once they mature.

The breakout box on the next page provides an overview of some of the relevant competition regulation from the DRCF member regulators.

83 Jean-François Bobier, Jean-Michel Binefa, Matt Langione, and Amit Kumar, It's tTime for Financial Institutions to Place Their Quantum Bets, Boston Consulting Group (BCG), 2020, https://www.bcg.com/publications/2020/how-financial-institutions-can-utilize-quantum-computing

84 McKinsey & Company, Quantum Technology Monitor, 2023, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20technology%20sees%20record%20investments%20progress%20on%20talent%20gap/quantum-technology-monitor-april-2023.pdf

Examples of DRCF Member Regulators' Competition-focused Regulation:

Three of the four DRCF member regulators (the CMA, the FCA, and Ofcom) exercise competition-related regulation as part of their broader regulatory remits, for example:

- **The CMA**, as the UK's principal competition and consumer protection authority, promotes competitive markets and tackles unfair behaviour by investigating mergers and enforcing consumer protection legislation.[85] The Digital Markets Unit (DMU) within the CMA has started work on operationalising a statutory pro-competition regime for digital markets, as announced in the 2022 Autumn Statement. The Digital Markets, Competition and Consumers Bill was introduced on 25 April 2023.[86]

- **Ofcom** is responsible for promoting competition in communications markets and ensuring beneficial outcomes for consumers. Under the 2003 Communications Act,[87] Ofcom has powers to regulate communications markets, investigate breaches of competition law in the sector (including anti-competitive behaviour), and impose remedies to address competition concerns.

- **The FCA**, as the UK's financial services regulator, promotes competition and ensures that financial markets work for consumers. The FCA's competition powers,[88] set out in the 2000 Financial Services and Markets Act and the 1998 Competition Act,[89] allow it to investigate suspected breaches of competition law, conduct market studies, and address competition concerns by imposing behavioural or structural changes.

85 Competition and Markets Authority (CMA), New CMA strategy prioritises outcomes for people, businesses, and economy, UK Government, 2023, https://www.gov.uk/government/news/new-cma-strategy-prioritises-outcomes-for-people-businesses-and-economy
86 UK Parliament, Digital Markets, Competition and Consumers Bill, 2023, https://publications.parliament.uk/pa/bills/cbill/58-03/0294/220294.pdf
87 UK Parliament, Communications Act 2003, 2003, https://www.legislation.gov.uk/ukpga/2003/21/contents
88 Financial Conduct Authority (FCA), Competition Law, 2016, https://www.fca.org.uk/about/what-we-do/promoting-competition/powers
89 Financial Conduct Authority (FCA), FG15/8 – FCA's powers and procedures under the Competition Act 1998, 2022, https://www.fca.org.uk/publications/finalised-guidance/fg15-8-fcas-powers-and-procedures-under-competition-act-1998

Looking Ahead: Addressing Potential Future Regulatory Concerns

Whilst the existing regulations noted in the previous section will continue to apply to organisations, the development and adoption of quantum technologies presents some potential future implications that may require further regulatory consideration.

Transitioning to quantum-safe systems

As noted previously in the quantum technologies, the development of quantum computers presents a significant potential risk to organisations' cyber and information security. To mitigate these threats, NIST has taken the lead on facilitating the development of quantum-resistant public-key cryptographic algorithms. The aim of this programme is to develop protocols that are secure against quantum-enabled cyber security threats.[90] Although the DRCF member regulators recognise the potential role they might also play in the transition to postquantum cryptography, we are yet to develop and set out our approach in more detail. The transition to quantum-safe systems is likely to bring adoption challenges that go beyond the development of quantum-safe approaches to cryptography. While groundwork in a software environment may enable an easier transition, 'legacy' hardware-based systems may require a physical hardware swap. The World Economic Forum's Global Future Council on Quantum Computing estimates that 20B digital devices will need to be upgraded or replaced with post-quantum cryptography in the next 20 years, and this challenge is further complicated by the requirement for interoperability in telecoms and other digital communication systems.[91]

Given the scale and complexity of this transition, the NCSC recommends that large businesses factor this into their long-term planning.[92] In doing so, organisations could benefit from conducting an inventory of their digital infrastructure, gaining a deep understanding of the cryptographic protocols they deploy, and a mapping of the personal data they hold.[93] Such actions may help organisations to adopt a crypto-agile approach to facilitate their transition to other quantum-secure systems.[94]

Throughout this period of uncertainty surrounding the pace and timing of the transition to quantum, the DRCF member regulators will continue to monitor the development of quantum technologies, the potential security risks they present to the current digital systems and collaborate with a wide range of stakeholders to develop our regulatory approaches accordingly. Fostering an innovative, pro-competitive environment that also protects individuals will be at the heart of these concerns.

90 National Institute of Science and Technology (NIST), 'Post-Quantum Cryptography', https://csrc.nist.gov/projects/post-quantum-cryptography
91 The World Economic Forum (WEF), Global Future Council on Quantum Computing, 2020, https://www3.weforum.org/docs/WEF_Global_Future_Council_on_Quantum_Computing.pdf
92 National Cyber Security Centre (NCSC), 'Preparing for Quantum-Safe Cryptography', 2020, https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
93 Ibid.
94 World Economic Forum, 'Transitioning to a Quantum Secure Economy', 2022, https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf

Standards and specifications to complement regulation

The DRCF member regulators recognise the potential of standards and specifications to facilitate stakeholder collaboration, accelerate innovation, and mitigate risks in these emerging technologies.

Through the provision of shared frameworks and established best practices, standards and specifications can help ensure reliability, interoperability, and security for quantum technologies. In the process, standards and specifications could help to address barriers in the design and development of quantum technologies whilst also easing the deployment of quantum technologies across industries and facilitate their integration into the existing digital infrastructure.

There are a number of national and international bodies working towards establishing standards and specifications in quantum technologies. For example:

- The National Institute of Standards and Technology (NIST) are leading in the efforts to develop standards and specifications for quantum-safe cryptography and quantum key distribution.[95] This work programme is seeking to test and develop cryptographic algorithms that are resilient to quantum computers and potential, future cyber-attacks. In November 2022, the National Physical Laboratory (NPL) and NIST signed a Memorandum of Understanding to strengthen UK and US collaboration on future standards for quantum technologies.[96]

- The National Cyber Security Centre (NCSC), part of GCHQ, has active work programmes on the development of guidance in both quantum-safe cryptography and Quantum Key Distribution.[97] In 2020, they published a white paper on preparing for quantum-safe cryptography, and a whitepaper on QKD and QRNG.[98]

- The British Standards Institution (BSI), the UK's national standards body, launched the ICT/1/1/2 Quantum Technologies Panel which has close to 60 members representing industry, academia, government and more jointly form national positions and prioritisations. The panel in BSI is tasked with representing UK interests and leading on international standards development efforts on quantum technologies.[99]

95 NIST, 'Post-Quantum Cryptography', https://csrc.nist.gov/projects/post-quantum-cryptography
96 National Physical Laboratory, 'NPL and NIST sign Memorandum of Understanding', 2022, https://www.npl.co.uk/news/npl-and-nist-sign-mou
97 NCSC, 'Preparing for Quantum-Safe Cryptography', 2020, https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
98 NCSC, ' Quantum Security technologies', 2020, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
99 British Standards Institution, ICT/1/1/2 - Quantum technologies, 2022, https://standardsdevelopment.bsigroup.com/committees/50299888

- The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) jointly host ISO/IEC/JTC 1/WG 14 quantum information technologies, a working group under an international joint technical committee on information technologies. Its scope is directly in correlation to the approved work programme. There is development of a vocabulary document on quantum computing and an informative overview of quantum computing to date with other proposals currently under review.[100]

- International Electrotechnical Commission (IEC) IEC/SEG 14 is an open-to-public international Standardization Evaluation Group that sets out to formulate strategic standards roadmaps and to make recommendations for the next stages of international development activities. This could see the establishment of a new international standards committee to deliver on new work programmes to support the quantum industry.[101]

- The International Telecommunication Union's (ITU) Study Group 13 is working on developing standards for QKD. In this programme the ITU have also worked to identify technical specifications for elements of QKD networks, although much of this work will ultimately be delivered through the industry-led standardisation activities above.[102] The ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N) was established to provide a collaborative platform for pre-standardization aspects of QIT for networks.[103]

The DRCF member regulators are aware of the ongoing work on standards and specifications by these organisations and plan to continue engagement as their work progresses. At this stage, each regulator has identified standards bodies most relevant to their current efforts and regulatory remits, for example:

- The ICO will engage with the NCSC and explore how they can contribute to the conversation with other relevant stakeholders on the development of standards for quantum-secure systems to prevent risks to personal data,

- Ofcom is engaging with ETSI and NIST, and follows the ITU on the development of standards for quantum technologies in the communications sector, and

- The FCA is exploring further engagement with standards bodies as it expands its work on quantum computing and financial services.

As these work programmes mature, ongoing collaboration between DRCF regulators will be increasingly important to identify gaps, share findings, and ensure ongoing alignment and coordination.

---

100 JTC 1, Quantum Information Technology, 2020, https://jtc1info.org/technology/working-groups/quantum-computing/
101 Interntional Electrotechnical Commision (IEC), SEG 14: Quantum Technologies, 2022, https://www.iec.ch/ords/f?p=103:186:400692540391534::::FSP_ORG_ID,FSP_LANG_ID:28910,25
102 ITU, Joint Coordination Activity on Quantum Key Distribution Network, https://www.itu.int/en/ITU-T/jca/qkdn/Pages/ToR.aspx
103 International Telecommunications Union (ITU), ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N), 2019, https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx

Explainability, quantum computing, and artificial intelligence

Given that innovation does not occur in a vacuum, there is a possibility that advancements in quantum technologies may intersect with or influence the development of other existing technologies. The intersection between these technologies may have implications under existing regulation, for example the convergence of quantum technologies and machine learning (quantum machine learning).

Quantum machine learning is the field of study to develop algorithms for machine learning that can run on quantum computers. Essentially, quantum machine learning aims to integrate advanced quantum algorithms in 'classical' machine learning environments in order for these systems to run more efficiently, build bigger neural networks, find new patterns, and attempt computations that are unavailable by 'classical' means alone.[104] This nascent field will require significant advancement in quantum computing and supporting infrastructure.

AI and machine learning play an ever more important role in the provision of services and products across the economy. Many existing machine learning and AI models draw connections between a vast amount of different data points to identify patterns, derive inferences, and support decision -making processes.[105]

The growing integration of these systems into the economy means that the outputs can under certain circumstances have materially significant implications for individuals, firms, and markets. As such, it is important, and in many circumstances a legal requirement, that these outputs and the systems by which they come to conclusions are explainable.[106] Explainability enables human evaluation and meaningful challenge to outcomes, and helps protect against bias, which are fundamental to building trust in the application of this technology.[107]

This topic of AI explainability is an active and ongoing area of interest for the DRCF member regulators. For example, the ICO has released guidance on AI explainability in partnership with the Alan Turing Institute[108] whilst the FCA has explored this topic through a joint Discussion Paper with the Bank of England and the Prudential Regulatory Authority.[109] The DRCF have also considered explainability and algorithmic transparency issues in a 2022 paper, as part of the wider algorithms work programme.[110]

---

104 Biamonte et. al, 'Quantum Machine Learning', 2018, https://arxiv.org/pdf/1611.09347.pdf
105 David Leslie, Project ExplAIn, Alan Turing Institute, 2019, https://www.turing.ac.uk/news/project-explain
106 For example, under UK GDPR, where personal data is processed, organisations deploying AI systems are expected to explain the outputs to data subjects. ICO, Explaining decisions made with AI: Part 1 Legal Framework, 2019, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/part-1-the-basics-of-explaining-ai/legal-framework/#legal_framework_3
107 ICO, Explaining decisions made with AI, 2019, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/ (pp 7, 13, 17 -20), see also David Leslie, Project ExplAIn, Alan Turing Institute, 2019, https://www.turing.ac.uk/news/project-explain
108 ICO, Explaining decisions made with AI, 2019, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/
109 BoE and FCA, 'DP5/22- Artificial Intelligence and Machine Learning', 2022, https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence
110 DRCF, The benefits and harms of algorithms: a shared perspective from the four digital regulators, 2022, https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/the-benefits-and-harms-of-algorithms-a-shared-perspective-from-the-four-digital-regulators

AI explainability is an important issue within broader AI work programmes that include ensuring fairness, transparency, governance and accountability in algorithmic decision-making, as well as creating better outcomes for consumer, markets, and firms.

While the convergence between quantum technologies and AI presents potential opportunities to enhance insights and shorten the time to derive outputs, it also has potential implications for explainability.[111] In the long-term, advances in quantum machine learning may be able to identify previously invisible patterns and generate insights beyond the capability of current machine learning models.[112] However, the fragility of current qubit modalities could also affect the operation of existing explainability models,[113] whilst quantum-enabled machine learning could increase the complexity and opacity of AI models.[114] These challenges may require a significant increase in both technical skills and knowledge to develop frameworks for explainability in a quantum-enabled age.

Many of these challenges are not new, and there are lessons to be learned from previous experiences. Historically, explainability issues have been considered in the later stages of development and deployment. Important steps can be taken to ensure that explainability is considered at the early stages of technological development, particularly as new hybrid quantum-classical use cases are explored.

Given the uncertainty surrounding the development timeline of quantum technologies and the nature of the integration between quantum technologies and AI, quantum machine learning use cases are still speculative. However, DRCF research and insights from the DRCF Quantum Symposium suggest there could be future use cases relevant to our remits, including in high-risk areas such as finance and medicine, where explaining the reasoning behind a decision could be particularly important, and/or required by law.

For example:

- **Fraud detection:** Researchers have begun exploring the use of hybrid quantum-classical machine learning for fraud detection, using highly complex and unpredictable credit card transaction and bank loan datasets. This study highlighted the possibility of near real-time fraud detection, with improved accuracy for particular types of complex datasets compared with standard machine learning approaches.[115]

---

111 Deloitte, Quantum Computing may create ethical risks for businesses. It's time to prepare, 2022, https://www2.deloitte.com/uk/en/insights/topics/cyber-risk/quantum-computing-ethics-risks.html

112 See, eg, Biamonte et. al, 'Quantum Machine Learning', 2018, https://arxiv.org/pdf/1611.09347.pdf; IBM, Expert Insights: Exploring quantum computing use cases for financial services', 2019, https://www.ibm.com/downloads/cas/2YPRZPB3

113 Steinmüller et al, Explainable AI for Quantum Machine Learning, Arxiv, 2022, https://arxiv.org/abs/2211.01441; Moreno et al.,Noise in quantum computing, AWS Technologies Blog, 2022, https://aws.amazon.com/blogs/quantum-computing/noise-in-quantum-computing/; ICO, Explaining decisions made with AI: Task 3: Build your system to ensure you are able to extract relevant information for a range of explanation types, 2019, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/part-2-explaining-ai-in-practice/task-3-build/

114 See, e.g., Deloitte, Quantum Computing may create ethical risks for businesses. It's time to prepare, 2022, https://www2.deloitte.com/uk/en/insights/topics/cyber-risk/quantum-computing-ethics-risks.html

115 Alessandra Di Pierro and Massimiliano Incudini, Quantum Machine Learning and Fraud Detection, Spring, 2021, https://link.springer.com/chapter/10.1007/978-3-030-91631-2_8

- Personalised medicine: Machine learning powered by the additional processing power of quantum computing could be capable of delivering real time insights into clinical datasets, and more advanced predictive capabilities that can take into account a wide variety of individual patient characteristics.[116]

- Quantum machine learning and hybrid applications could also have applications in customer targeting and prediction modelling.[117]

As these technologies evolve, the DRCF member regulators will continue to develop their approaches to AI explainability within broader AI work programmes, remain alert to ongoing developments, and further consider emerging quantum use cases relevant to our remits. In the process, the DRCF member regulators will continue to engage with national and international stakeholders from industry, academia, government, and civil society. In the meantime, the ICO, FCA, and DRCF's existing explainability resources provide further insight into our current approach.[118]

116 Virginia Mahieu, What if quantum technologies were to revolutionise healthcare?, European Parliamentary Research Service, 2022, https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/737121/EPRS_ATAG(2022)737121_EN.pdf; IBM, Expert Insights: Exploring quantum computing use cases for healthcare, 2020 https://www.ibm.com/downloads/cas/8QDGKDZJ; Solenov et al, The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine, Missouri Medicine, 2018, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6205278/

117 IBM, Expert Insights: Exploring quantum computing use cases for financial services', 2019, https://www.ibm.com/downloads/cas/2YPRZPB3

118 ICO, Explaining decisions made with AI, 2019, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/ (pp 7, 13, 17 -20), see also David Leslie, Project ExplAIn, Alan Turing Institute, 2019, https://www.turing.ac.uk/news/project-explain; Financial Conduct Authority, Bank of England, and Prudential Regulation Authority, DP22/4: Artificial Intelligence, 2022, https://www.fca.org.uk/publications/discussion-papers/dp22-4-artificial-intelligence; DRCF, The benefits and harms of algorithms: a shared perspective from the four digital regulators, 2022, https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/the-benefits-and-harms-of-algorithms-a-shared-perspective-from-the-four-digital-regulators

Conclusion and Next Steps

As with any technological advance, it is anticipated that, as quantum technologies develop, they will enable novel solutions and present new challenges. The DRCF Quantum Symposium, related engagement and subsequent research have been invaluable in informing our understanding of what this new technological frontier could look like, as well as the ongoing technical and engineering challenges that need to be overcome. The DRCF member regulators are alert to concerns highlighted at the DRCF Quantum Symposium, that regulating "too early" could limit innovation in this nascent industry, as well as the risks of engaging or intervening too late. Our individual and collective approach to regulation and innovation seeks to enable emerging technologies such as quantum to evolve and develop responsibly. We seek to engage early with the emerging technology ecosystem and build our understanding of the potential future impacts to shape how we may use the wide range of policy, guidance and supervisory tools in our regulatory toolkit.

Existing regulation will continue to apply as quantum technologies develop and use cases evolve, including, for example, in the areas of competition, security and data protection relevant to the DRCF. The symposium, our engagement and our research also emphasised that national and international standards for quantum technologies will have an important, complementary role to play. As this paper highlights, there are still further questions for DRCF regulators to explore, in consultation with all relevant stakeholders. This includes, for example, our individual and collective approach to the transition to quantum-secure technologies.

Equally, not all use cases or aspects of quantum will fall within the remits of DRCF member regulators. Understanding potential future applications of quantum, as they continue to develop, will therefore be important.

The DRCF horizon scanning team will share their insights internally and externally to enable member regulators to determine their next steps on quantum in the context of their wider work plans. Building on the findings from the DRCF horizon scanning workstream, the FCA, for example, continues to explore the implications of quantum computing in financial services.[119] The ICO intends to publish further futures thinking on quantum and information rights in the coming months. The horizon scanning workstream also aims to keep abreast of major developments in quantum and will review whether to include further work on quantum technologies in the 2024-2025 DRCF workplan.

Above all, as these complex technologies continue to develop, the DRCF member regulators look forward to continuing the conversation with industry, government and academia, and other relevant and interested stakeholders. Ongoing dialogue will enhance our mutual understanding of the intersections of quantum technologies and existing regulation, shape responsible innovation, and help the UK harness the potential of a quantum future.

119 Financial Conduct Authority, Emerging Technology Research Hub, 2023, https://www.fca.org.uk/firms/emerging-technology-research-hub

Glossary

Complex systems: large-scale systems that are inherently difficult to model due to the vast number of variables and the intricate ways in which they interact.

Decoherence: the process by which qubits lose the information they carry due to their intrinsically fragile and ephemeral nature.

Entanglement: a special kind of bond that two or more qubits can form the effect of which is that properties measured on one qubit reveal the measurement results of the other qubit so entangled, even if they are separated over a vast distance.

Entanglement swapping: the process by which the state of a qubit can be transferred onto another.

Fault-tolerant quantum computer: quantum computers that have sufficient processing power and compute resources to perform computations, have a good protocol for dealing with errors and are therefore reliable and durable enough so that they are commercially viable.

Gate: a gate combines several transistors into a unit so that logical operations can be performed, such as AND, OR or NOT.

High / Low fidelity: fidelity is a measure of goodness in terms of accuracy, quality and reliability.

No cloning theorem: the quantum states of qubits cannot be copied, which requires novel approaches to building quantum repeaters as established protocols to amplify signals do not apply.

Postquantum cryptography: cryptography protocols and systems that even a quantum computer will find difficult if not impossible to break.

Public key cryptography: a cryptographic system that uses key pairs, one of which is public (common knowledge) and the other is nonidentical and private to encrypt, then decrypt information.

Quantum memory: the quantum equivalent to Memory on a 'classical' computer, e.g. for storing the quantum state of a qubit.

Quantum state: a probability distribution that spans the possible outcomes if the quantum system is measured.

Qubit: the logical unit in quantum computing and communications, which can be physically realised in many different ways.

Logical qubit: an abstraction to express how many more qubits are needed to secure computation given that they decohere so quickly. If, much simplified for the purpose of illustration, only one out of 10 qubits survives computation, the system only contains one logical qubit.