KTN
the
Knowledge Transfer
Network

Quantum Technology in Finance

Introduction

In 2013, the UK unveiled the National Quantum Technologies Programme[1], a £270m investment to build a coherent quantum technology community including government, research and industry. The aim was to position the UK as a world leader in quantum technology and to ensure that society receives the best possible benefits from the technology.

As a part of this program, £120m was invested in a network of four 'Quantum Hubs'[2]. These are collaborations between research and industry looking into different areas of quantum technology, each headed by a leading university in the field. They are: the Quantum Communications Hub; the Quantum Computing and Simulation Hub, Networked Quantum Information Technologies (NQIT); the Quantum Sensing and Metrology hub; and the Quantum Imaging Hub, QuantIC.

The finance industry is incredibly important for the UK's economy, contributing £129 billion, or 8%, of the country's GVA, and providing 1.1 million jobs, representing 3.4% of the total workforce[3]. The UK is a world leader in finance. If the UK wishes to retain this place on the global stage, it must encourage technological innovation and give businesses the tools to utilise this innovation.

The UK Chief Scientific Advisor identified four key areas of technological development for UK financial technology (fintech) in the FinTech Futures report[4]:

- Machine learning and cognitive computing
- Digital currencies and blockchain
- Big data analytics, optimisation and fusion
- Distributed systems, mobile payments and peer-to-peer applications

---

[1] Quantum Technologies, EPSRC, https://www.epsrc.ac.uk/research/ourportfolio/themes/quantumtech/

[2] Quantum Leap as Clark unveils UK's network of Quantum Technology Hubs, EPSRC, 2014, https://www.epsrc.ac.uk/newsevents/news/quantumtechhubs/

[3] Key Facts about UK Finaicial and Related Goods and Services, TheCityUK, January 2014, http://www.thecityuk.com/research/our-work/reports-list/key-facts-about-uk-financial-and-related-professional-services/

[4] FinTech Futures: The UK as a World Leader in Financial Technologies, Mark Walport, 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf

This report explains how quantum technology, through computing and communications security, has the potential to have a large impact on the finance industry.

Quantum Computing

Quantum Computing is the use of quantum mechanical principles to perform computation. Quantum computers are often referred to in the media as being "super-fast" computers; this is, however, only partially true. They are expected to be able to perform *certain tasks* incredibly quickly compared to classical computers, often by many orders of magnitude. The exact extent of these tasks, and the level of "quantum speedup" attainable, is still a matter open to debate.

> *"Quantum technologies for finance would enable new 'disruptive markets'. They would permit computing and simulation models with (many) orders of magnitude increase in fidelity and sophistication, compared with today's conventional computing approaches. Rather than providing abstractions of key financial models, direct interactions between low-level transactional data would permit models that deliver improved prediction and forecasting of major financial events (e.g. stock markets collapses, regulatory fraud, money laundering). These could help support response and recovery to major global financial events, or identify new financial mechanisms for improving global financial stability."*
>
> *-Dr Roberto Desimone, Manager, Strategic Innovation, BAE Systems Applied Intelligence.*

Applications to the Finance Industry

There are several key areas in which quantum computers are expected to outperform classical computers: factorisation, simulation of quantum systems, optimisation problems, big data analysis, and machine learning[5]. It is the latter three that will be most useful to the finance industry.

Quantum computers could eventually be used for algorithmic trading: the use of algorithms to perform trades on capital markets. These can be seen as optimisation problems with a large number of interacting variables; the goal is to feed information about the market into the algorithm, and have it return the set of trading decisions that would lead to an optimal portfolio. In the same vein, quantum computers could also be used for problems such as risk management. It is not yet known what level of speedup, if any, a quantum computer would be able to provide in this area, and would likely vary depending on the specific nature of the problem presented. The value of this speedup will not come from being able to perform the same computations

[5] Read the Fine Print, Aaronson, S., 2015, *Nature*, http://www.nature.com/articles/nphys3272.epdf (alternative link via open sharing initiative)

faster, but rather from being able to perform far more complex computations in the same amount of time.

Machine learning is a concept in computing related to artificial intelligence and pattern recognition. One practical application of it is in analysing large sets of data, such as that which is collected by financial institutions. In many cases this data cannot be effectively used due to limitations in computational power. A survey[6] of 333 executives from US and Canadian companies conducted by Oracle found that "93% of executives believe their organization is losing revenue – on average, 14% annually – as a result of not being able to fully leverage the information they collect". Quantum computers could offer a new, efficient way to analyse and find patterns in this data, and quantum algorithms that could act as a basis for this task have already been developed.[7]

Description

Unlike classical bits, which encode binary states ('0' and '1'), quantum bits (or 'qubits') encode quantum superpositions of these states. These qubits have a finite probability to return either result when measured, but occupy neither state until measurement takes place. Qubits can be encoded in a variety of ways, including in trapped ions, photons, and solid state materials. This leads to a number of different ways of building a quantum computer. Some types of quantum computers may be better at specific applications than others. Those allocating funding and deciding on research focus have to carry out a fine balancing act between making sure all avenues are properly explored and avoiding spreading themselves too thin by taking too broad an approach. Beyond the hardware, quantum computers will need new quantum algorithms designed to take advantage of the speedup available, and a new generation of programmers to design them. Many quantum algorithms already exist, the most famous of which are Grover's search algorithm and Shor's factoring algorithm, which offer quadratic and exponential speedups, respectively.

The engineering side of quantum computing is still very much in the research stage. Qubits are extremely fragile, and lose their quantum state if exposed to interference (decoherence), making it an engineering challenge to keep qubits stable sufficiently long enough to correct for errors and to be able to carry out a calculation. Most researchers right now are working on making a small number of stable, useful qubits. For example, the UK Quantum Computing Hub is working

[6] From Overload to Impact: An Industry Scorecard on Big Data Business Challenges, Oracle, 2012 http://www.oracle.com/us/industries/industry-scorecard-1683398.html

[7] Quantum algorithm for linear systems of equations, Harrow, Aram W, Avinatan Hassidim, and Seth Lloyd.*Physical review letters* 103.15 (2009): 150502.

on a quantum computing device, the Q20:20, which will consist of 20 cells of 20 qubits, each cell being a single processor. The device itself, due to be completed in 2020, will have very limited capability, but should be able to demonstrate quantum speedup on specific problems, and could later be used as part of a larger, more practical quantum computer.

Canadian company D-Wave Systems has produced what they call the world's only "commercial quantum computer", the current iteration of which is called the D-wave II. It is the size of a small room; to keep the qubits from decohering, the processor must be kept to almost absolute zero temperature and shielded from external interference. It is a specific type of quantum computer which can only perform optimisation tasks. The machine has sparked huge amounts of controversy within the academic community[8]. D-Wave's approach is different to that of most researchers; they put together as many qubits as they believe is feasible and see what they can do with them. Their latest processor has 1000 qubits, and after initial testing appears to be on par with, or very slightly better than, an ordinary PC[9]. The problem is that no true quantum speedup has been demonstrated. Google and Lockheed Martin each own a D-Wave machine, the only two to be sold. The machines are interesting for research, and great feats of engineering, but not even D-Wave is claiming that they are currently practical.

Barriers

It is likely to be 15-20 years before a practical, general-purpose quantum computer is available. However, purpose-build quantum computers could be available much sooner than that, in the next 5-10 years, that could effectively solve specific tasks with a quantum speedup. These could either be built by companies for their own use, or by quantum computing companies to be rented out or accessed remotely. Achieving this will require cooperation between industry and research. It is important to identify which problems the industry has that need to be solved, so that researchers can look into creating quantum algorithms to solve them, and see what kind of speedup may be achieved. The question then becomes a matter of cost-benefit comparison: are the costs of building or renting a quantum computer greater than the money that could be made or saved by its use? The answer will vary from problem to problem and company to company, which is why cooperation between research and industry is so vital at this stage. Useful quantum algorithms need to be ready when quantum computers arrive, otherwise we will be left with powerful computers with no useful function, a list of algorithms with no commercial use, and an industry with problems that don't have a known solution.

---

[8] Defining and detecting quantum speedup, Rønnow, Troels F, Zhihui Wang, Joshua Job, et al. 2014. *Science* 345, no. 6195: 420-424.

[9] Quantum Computer Firm D-Wave Claim Massive performance Boost, , Aron, J, 2015, *New Scientist*, https://www.newscientist.com/article/dn28078-quantum-computer-firm-d-wave-claims-massive-performance-boost/

Roadmap

Q20:20: 5 years
Purpose-build quantum computers: 5-10 years
General purpose quantum computer: 15-20 years

Quantum Communications

Applications to the Finance Industry

Security is a huge concern across the finance industry, impacting to some extent almost every facet. Banks have to secure transactions, ATMs need to be safe from attack, online services must protect connection between themselves and their users. Almost all of the financial services industry handles user data in some way, and people are aware now more than ever of the security concerns involved with the storage of such personal data. Current cryptography is based on the computational difficulty in cracking encryption methods. Even today, encrypted data that cannot be cracked now is being intercepted and stored by hackers, in the hope that will be able to access it when the technology becomes available. One of the most commonly referred-to uses of quantum computers is their ability to crack many modern encryption methods, such as the widely-used RSA algorithm. As practical quantum computers becomes less of an 'if' and more of a 'when', steps will need to be taken to make our technology and communications 'quantum-safe'; that is, immune to attack from them.

As the security of quantum communication is independant of computing power, it is a quantum-safe. There are two key ways of using quantum communications which may be employed in finance: optical fibre networks to facilitate key distribution for point-to-point security, and a portable, short-range, wireless system that is being called 'consumer QKD' by some researchers[10].

> *"The Quantum Communications Hub aims to advance proven concepts in QKD through to commercial-ready technologies, delivering low-cost, short-range QKD for consumers, chip-based devices with mass manufacture potential and a fibre-based UK Quantum Network for user engagement and demonstration purposes. In the finance sector, all three of our QKD developments could contribute, from high value fibre solutions through to widespread consumer applications"*
>
> *-Prof. Tim Spiller, Director of the UK Quantum Communications Hub*

[10] Quantum Communications hub launch presention, https://connect.innovateuk.org/documents/11487824/22230824/York+QC+Hub.pdf/7d5f1cb5-e14d-4559-bd84-5fba7a7fdb75

Description

Quantum communication is the transfer of quantum information. One of the main practical focuses of quantum communication research is quantum key distribution (QKD). QKD is not in itself a method of transmitting data; it is a method of producing and sharing encryption keys so that information may be securely exchanged. Classical encryption methods rely on the computational difficulty of cracking an encryption key for their security. QKD, on the other hand, prevents an attacker from obtaining the key in the first place.

QKD involves the creation of keys encoded as quantum information which may be exchanged securely. This relies on two key principles of quantum mechanics: that quantum information cannot be perfectly copied, and that the information in a quantum system is changed when measured. This means that if a hacker gains access to a quantum channel and attempts to read a key, the act of reading will change the key. Once the keys are distributed over a quantum communications channel, encrypted information can safely be transmitted over classical channels. No assumptions need to be made regarding a hacker's access to the data channel, or their computational power, to ensure security. The system is not immune to attack, but attempts to steal the encryption keys will be detected and communications halted until a secure channel is established.

Networks

Electronic data interchange (EDI) is the transfer of data between computer systems using a standardised format. EDI is sometimes carried out over the internet, but often uses point-to-point connections and private networks within and between businesses. As QKD networks are closed, this is an ideal use case. The information sent over such connections are often sensitive or high-value, meaning security is incredibly important. An example is CHAPS, which facilitates bank transfers within the UK and is often used for important and high-value transactions. In the first half of 2014, the average value of a CHAPS transfer was £2 million[11]. Securing such high-value transactions may be deemed to be worth the cost of implementing a QKD network. Using QKD for financial transactions has already been demonstrated: in 2004, a €3,000 donation from the Mayor of Vienna to the University of Vienna was secured using entangled photons. The use of QKD networks for EDI is not limited to banks and financial transactions; it may also secure the transfer of user data, and corporate and trade secrets, alleviating the need for trusted couriers.

Consumer QKD

QKD may be used to securely transfer secrets in authentication systems. A two-factor authentication system, such as Chip & PIN, requires a user to provide both something they know

[11] "CHAPS Factsheet", CHAPS Clearing Co. Ldt., 2014m
http://www.chapsco.co.uk/files/chaps/about_chaps/chaps_factsheet_06012015.pdf

and something they have in order to verify their identity. In the case of Chip & PIN, the smartcard is something they have, and the PIN is something they know.

One key vulnerability of Chip & PIN is that the PIN is static; if it is attained by a malicious party, they can use it make purchases. An alternative to Chip & PIN, currently used in Germany, is the Transaction Authentication Number (TAN) system. A TAN is a single-use password. Users are provided with a list of TAN numbers by their bank, either physically, or electronically via mobile phone. Once exhausted, a user must visit or contact their bank to replenish their TAN list.

While this means that the theft of *any one password* doesn't matter, there is still the risk of a man-in-the-middle attack intercepting a TAN list and using the passwords that are still valid. However, a QKD system could be used to secure the transfer of TANs. This is usually envisioned as a 'quantum ATM' that can dispense TANs to a user's quantum token. This quantum token would be some sort of mobile device, either stand-alone, or integrated into a mobile phone. This quantum TAN system may be used to verify in-person transactions, or online transactions using a quantum-enabled chip authentication program, much like the current PIN system. This technology is expected to be ready for commercialisation in the next 5 years, but would take time to be implemented on a large scale.

Public Image Benefits

A report from Royal Holloway[12] makes note of the potential intangible benefits of QKD. They say that "implementing the newest, coolest technology makes a company seem cutting-edge". It is possible that a company may wish to implement quantum communications technology in some inexpensive way so that they can attach the word 'quantum' to their brand, or boast of their new, state-of-the-art security system. Such intangible benefits should rarely be the focus of research, but cannot be ignored as a use-case for many new technologies.

Barriers

Some QKD systems are already commercially available, but their usefulness is limited by a lack of standardisation and infrastructure, and are therefore primarily targeted at R&D[13][14]. Quantum networks use optical fibre to transmit data, so new fibre must be laid down where none is already available - a slow and expensive task.

Financial institutions, particularly banks, allow for a certain amount of financial loss due to fraud and security breaches. They tend to look for a "good enough" solution The benefits of any

[12] Quantum Key Distribution: Awesome or Pointless, Carlos, Cm Cobourne, S, 2011, http://media.techtarget.com/rms/pdf/RHUL_Cobourne_Final.pdf
[13] http://www.idquantique.com/
[14] http://www.magiqtech.com/Products.html

proposed new security system must outweigh the cost of their implementation. As it stands, it is very difficult to perform a cost-benefit or risk-reward analysis for QKD, because many of the threats it protects against do not yet exist and are not yet fully understood. The finance sector is particularly risk averse, and implementing an expensive new security system such as QKD without a full understanding of the protection it can offer is a risky move. This risk will be reduced by reducing the cost of QKD technology and gaining a better understanding of quantum computers and how they will affect modern cryptographic systems.

In terms of consumer QKD, it is not just the financial institutions who need to accept the technology, but the general public as well. Chip & PIN required the public to be informed and prepared on a large scale[15]; this would need to be done again if a TAN-like system were to be introduced. The British public has become accustomed to Chip and PIN, and may be resistant to the added inconvenience that comes with a TAN-like system. Public surveys and trials would be required to gauge how acceptable this new technology would be to the public. The system is also still vulnerable to identity theft or theft of the consumer's quantum token, but banks already have measures in place to deal with these with the Chip & PIN system.

Roadmap

Commercial QKD solutions: Now
Metro networks in the UK: 2-3 years
National UK testbed network: 5 years
Practical national networks: 5-10 years
International networks: 10-20 years
Consumer devices ready for commercialisation: 5 years
Need for quantum-safe security: 10 years

Post-Quantum Cryptography

An alternative solution solution to using quantum secured communications is post-quantum cryptography: that is, the creation of cryptographic methods that are secure against a quantum attack. Many post-quantum cryptography methods have been developed, and some are already available to consumers[16]. The issue, however, is that the efficacy of such methods cannot be tested until practical a quantum computer is produced, and it is difficult to predict exactly what such a computer would be able to do. An example of this comes from CESG's *SOLILOQUY: A Cautionary Tale.* SOLILOQUY was a cryptographic algorithm designed to be safe from both

[15] Exafor example: http://www.chipandpin.co.uk/reflib/Consumer_digi-guide_Post_14_Feb_FINAL.PDF http://www.chipandpin.co.uk/reflib/retailers_implementation_guide.pdf
[16] Notably the UK-based PQ Solutions, who received funding from the Barclays Accelerator programme

classical and quantum attacks. However, it was abandoned due to the discovery of a "reasonably efficient quantum attack"[17]. A paper on quantum security by the European Telecommunications Standards Institute (ETSI) said:

"Quantum Safe Security is a concept that is less about moving from an old technology to something that is new. It is more about promoting the idea that communication standards... make a naive assumption that current ciphers will remain good enough until replaced by something superior."[18] Many see post-quantum cryptography as an extension of this assumption, meaning that quantum secured communications are something that organisations must seriously consider if they wish to ensure the security of their data going forward. However, the relatively cost-effectiveness of adoption quantum safe encryption standards will make this much more attractive to businesses than QKD, and so action must be taken to make industry aware of the benefits that QKD can have so that they can make the correct decision when adopting quantum safe communication practices.

Conclusion

It is clear that quantum technology will have an impact on the finance industry, but questions still remain regarding how large this impact will be and how receptive the industry and its consumers will be to the new technology. The only way to answer these questions is engagement along the entirety of the supply chain, from academia to industry.

For quantum communication, industry must be aware of of the coming threats to their security systems and the ways in which quantum technology can protect against them, so that organisations can make informed decisions on how best to secure their data. QKD may not be entirely practical or even necessary for another decade, but it can take a decade for a large organisation from making a decision on a new security system to the actual implementation of it.

It will be at least five to ten years before industry can begin to make use of quantum computing, and even then the impact will only be small. Once quantum computers are practical and widely available, the edge a company can gain over its competitors will not come from having a faster quantum computer, but a faster and smarter algorithm to run on it. It is a company's interest to work with those involved in research to ensure they understand exactly how they will be able to take advantage of quantum computing when it becomes a viable option to them; meanwhile, academia must engage with industry to ensure that the work they are doing will be useful.

[17] "Soliloquy: A Cautionary Tale", Peter Campbell, Michael Groves and Dan Shepherd, CESG, 2014, http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf

[18] https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf

KTN
the
Knowledge Transfer
Network

About the Author

Thomas Walker

Thomas is a physics student at the University of Sussex. He currently studying for a Masters (MPhys) specialising in quantum technology. This work was completed as part of a SEPNet Summer Placement with the KTN.

Email: taw27@sussex.ac.uk