ascent
atos thought leadership

White Paper

Quantum finance opportunities: security and computation

Trusted partner for your **Digital Journey**

Atos

About Ascent
Thought Leadership Program from Atos

Atos does more than accompany its clients on their digital journey, the Group actively helps them to stay one step ahead. Through its Ascent initiatives, Atos shares its vision and innovative thinking on the emerging trends and technologies that will shape business in the future.

For further information on Ascent vision, download Ascent publications, and read, share or comment the latest Ascent blog stories, please go to **ascent.atos.net**

About Atos
Quantum

Atos recently launched "Atos Quantum", the first quantum computing industry program in Europe. "Atos Quantum" is an ambitious program to develop quantum computing solutions that offer unprecedented computing power, while enhancing its cyber security products to face with these new technologies.

For more information, please go to **atos.net/atosquantum**

Authors

Matthew Bingley
Client Innovation, Atos
@matthewbingley

Karsten Bronnert
IPR Management, Atos
@BronnertKarsten

Vincent Couteau
Head of Legal IPR, Atos
@VincentCouteau

Frederik Kerling
Business Consultant – Quantum Specialist, Atos
@QuKerling

John Hall
Head of Strategy and Portfolio, Atos
@John4Hall

Thomas Walker
Physics Undergraduate, University of Sussex
@twalker_

Paritosh Wechalekar
Senior Technical Architect, Atos
@pawechalekar

Contents

Executive summary

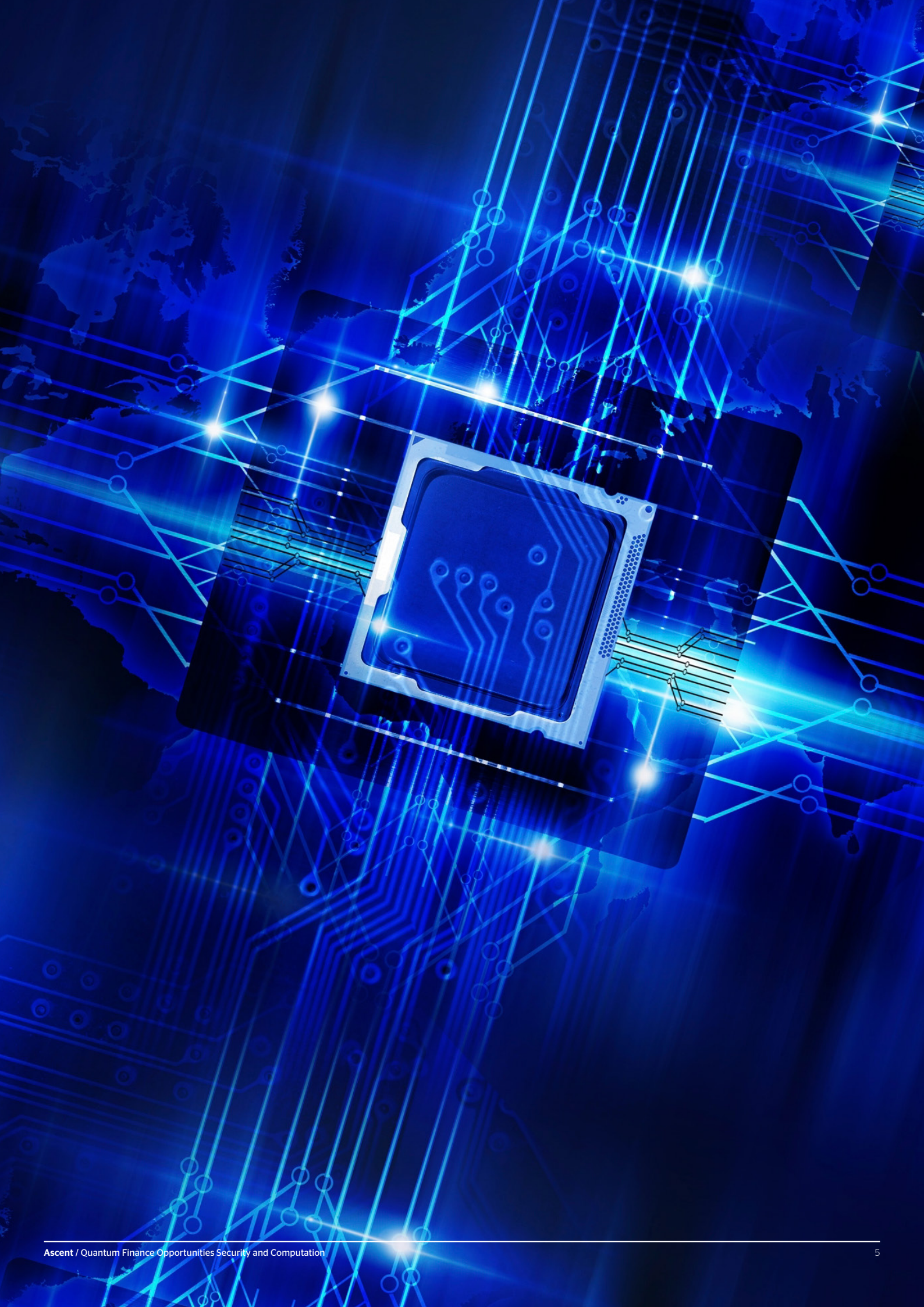
Quantum computers, unlike today's classical computers, make use of a quantum-mechanical phenomenon that allows data to be represented as 'Qubits' — these are not constrained to conventional 0 or 1 binary values, but instead can be a combination (or superposition) of 0 and 1 at the same time. A set of Qubits is able to represent exponentially more values than their 'Bit' counterparts — allowing them to interact and deliver computation and algorithm solving rates several orders of magnitude faster than with more conventional technology.

Quantum related technologies have the potential to massively disrupt a number of areas of IT. In particular, there will be a significant impact on the Financial Services industry, in terms of the opportunities that such computing power will enable. However, with these opportunities also come threats to some conventional security techniques and even business models, as current encryption methods become trivial to break and are therefore rendered useless.

Whilst quantum computers are not anticipated to become mainstream until around 2025, there is much that businesses can and should do to prepare for this next digital revolution. A proper awareness of the threats posed can allow businesses to deploy Quantum Safe Security right now; and some of the mathematical algorithms that will enable the full power of quantum computing to be exploited can also be deployed on conventional computer architectures for immediate and significant business benefit.

This paper will consider the current and emerging trends within the field of quantum computing and will look specifically at how this technology will influence future business in the Financial Services sector.

Quantum Computers will present significant opportunities AND risks to a number of areas of conventional IT.



Sector focus: Financial Services
(UK as reference geography)

Financial Services is one of the most Globalized markets there is and it is also one of the most dependent on IT. Its high dependence on security and regulation of processes and the relentless need to deliver differentiated services, means that disruption brings both risk and opportunity. To help explain the importance of understanding the impact of Quantum Computing on the Financial Services industry, we will use the UK market as an example, although similar argumentation can be applied to most geographies that have a strong FS market.

The UK economy is heavily dependent on the services sector which accounts for 78% of GDP, with 8% of the total coming from Financial Services alone. Additionally, 3.4 % of the UK workforce (1.1 million people) is employed by Financial Services organizations, making it one of the most productive sectors by size — more than double the overall UK average.[1] The UK is a world leader in finance, and is currently home to the world's second largest stock exchange, making finance a significant part of the UK's position on the global stage. In addition, two thirds of all foreign investment in the UK comes through the finance sector.

Technology in finance, or 'Fintech', is a vital part of the UK maintaining its position internationally and securing continued growth. The UK Chief Scientific Advisor has identified four key areas of Fintech Innovation: Machine Learning, Big Data Analytics, Digital Currencies, and Mobile Payment systems[2].In an age where algorithmic trading makes up more than 95% of all executed trades[3] and where companies are collecting more and more data, efficacious computers and algorithms are a key to gaining an edge over the competition. At the same time, new ways of communicating and interacting with Financial Services digitally (e.g. online and mobile banking, peer-to-peer payment platforms and digital currencies), as well as the continuing improvements in computing power and the development of distributed computing methods, have led to increased concerns over cyber security. It is an ongoing challenge for encryption methods to keep pace with the sophistication and processing power of technology that is capable of compromising the protection they offer. Quantum computers promise such a leap forward in compute speed, that they could open up wide-scale and systemic breaches of existing security and governance mechanisms – such developments would be disastrous to the Financial Services market if they are not properly anticipated and managed. Hence much of Fintech today is focused on the areas of computing and security.

Successful cooperation between business and research bodies to innovate in these areas will have a significant impact on the stability and growth of the financial sector, and therefore the UK economy as a whole.

Current data encryption techniques could be rendered obsolete by the promised capabilities of Quantum Computing.

[1] Key Facts about UK Financial 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/
"Financial Services: contribution to the UK economy", parliamentary briefing, Gloria Tyler, February 2015

[2] FinTech Futures: The UK as a World Leader in Financial Technologies", Sir Mark Walport, 2014

[3] http://www.forbes.com/sites/richardfinger/2013/09/30/high-frequency-trading-is-it-a-dark-force-against-ordinary-human-traders-and-investors/#afaed7d51a68

Quantum technologies — an overview

Quantum technology is fundamentally different from today's classical technologies; it uses certain properties of quantum mechanics to approach computing problems in an entirely new way. Data values are expressed by quantum spin states using "qubits" that interact in ways that allow them to carry out certain computational tasks exponentially faster than a classical computer is able to — even doing things that would be impossible with classical technology. Whereas conventional bits can hold the values 0 and 1, Qubits can represent 0, 1 and a probabilistic range of values in between.

Quantum technology brings fundamentally different concepts to the computing arena and opens up new possibilities across a range of application areas.

Applications of quantum technology include four key areas: imaging, sensing, computing, and communications. Computing and communication includes potential applications in algorithmic trading, fraud detection, and encryption and transaction security: All of which have a significant impact on the financial sector and will therefore be the focus of this paper.

These applications can be grouped into either quantum hardware or quantum software categories. Quantum hardware is technology that utilizes quantum effects in its primary functionality; for instance for computing, sensors or key distribution. Quantum software is coding either designed to counter quantum IT effects, like quantum cryptography, or to run on quantum hardware like quantum algorithms.

One of the things that quantum computers will be able to do is break, or significantly weaken many of the encryption methods used today. It is expected that this will be achievable within the next 5-10 years. Therefore, there is a pressing need to develop information exchange strategies that are capable of resisting such quantum attacks. Failure to address this threat could result in widespread security breaches that would put the entire banking system at risk.

Possible elements of a solution to this threat include the development/implementation of new encryption algorithms and methods that are resistant to attacks from quantum computers ('post-quantum cryptography'); and the potential use of quantum key distribution (QKD: a technique that uses quantum technology as a defense to ensure privacy in data exchange — Quantum states are affected by the very act of measuring them, so it is relatively easy to detect if Quantum Keys have been intercepted and read by 3rd parties during the process of exchange). The adoption of at least one of these techniques will be vital in coming years to anyone who wishes to transmit sensitive or confidential data securely. There are already QKD solutions available commercially and it is an active research area for many academic institutions and government organizations, including GCHQ and the NSA.[4]

Quantum technology is a field which is increasingly referred to in the media and many governments and large companies are now investing in it. In 2013, the UK government announced the "National Quantum Technology Programme", which includes £270m in funding for research and outreach, and a commitment to position the UK as a world leader in quantum technology by building a coherent community and supply chain including stakeholders from government, academia and industry.[5] £120m of the fund was put into the creation of four "Quantum Hubs" for each of the four areas of quantum technology, including the National Quantum Information Technologies (NQIT) computing hub, headed by the University of Oxford, and the Quantum Communications Hub, headed by the University of York.

Governments, agencies, academia and industry are investing heavily and collaborating on the development of Quantum Technologies.

A number of US agencies are looking into quantum computing, including NASA and the NSA. The Netherlands has also committed €135m [6] to quantum computing research through QuTech, [7] a collaboration between the Delft University of Technology and the Netherlands Organization for Applied Research (TNO). In Asia, the Chinese Academy of Sciences has teamed up with Alibaba to further research the field. Australia has also announced a $36m project, about a third of which is financed by the Commonwealth Bank of Australia[8]. In addition there are investments being made in the private sector by large corporations such as Google, Microsoft, Lockheed Martin, IBM, and Intel. [9]

[4] https://www.nsa.gov/ia/programs/suiteb_cryptography/ https://www.gchq.gov.uk/news-article/gchq-funds-academic-research-quantum-technology
[5] https://www.epsrc.ac.uk/newsevents/news/quantumtechhubs/
[6] http://qutech.nl/project/investment-quantum-technology/
[7] http://qutech.nl/
[8] http://www.afr.com/technology/innovation-statement-cba-increases-investment-in-unsw-quantum-computing-20151208-gli1h0
[9] http://www.businesswire.com/news/home/20150903005352/en/Intel-Invests-US50-Million-Advance-Quantum-Computing

What are the opportunities?

Security

On-line fraud linked to financial transactions costs the global economy hundreds of billions of Pounds each year according to Eugene Kaspersky, co-founder of Kaspersky Lab. In the UK alone, the cost of on-line banking fraud for 2013 to 2014 is reported by the ONS to be £60.4m and is increasing at the alarming rate of 48% per year.[10] In addition there is the 2014 estimated loss of £217m from e-commerce transactions. Much of the fraud results from scams, phishing attacks and ransomware. Incredibly, every day, an estimated 80,000 users unwittingly compromise their security.[11]

The promised power of Quantum Computers could result in a systemic failure of the current Financial Services approach to security and privacy.

Putting these numbers in perspective with the 27 million UK adults using online banking and with a total e-commerce spend of £148Bn, the losses due to fraud reflect ~£2 per customer per annum and 0.15% of total e-commerce spend. These seem small, but one should keep in mind that this happens in spite of efforts to secure transactions and their related systems. Given the massive increase in compute capability of Quantum computers, their ability to break conventional encryption keys through brute force attack will open the flood gates, promoting the problem of fraud from a manageable nuisance to a systemic breach of security and privacy.

Atos believes that across all markets, but especially within Financial Services, "Trust and Compliance" is one of the major transformation challenges faced by organizations as they undertake their Digital Transformation Journey. The other three being: Customer Experience; Business Reinvention and Operational Excellence). Businesses and Governments. Digital Technologies must do so in a way that fosters confidence amongst all parties engaged in transactions and collaboration: *"Am I who I say I am?", "Can I guarantee the integrity and security of transactions?", "Will my privacy be appropriately protected?"* Failure to consistently address these questions will quickly lead to a loss of trust and presents a significant risk to the business.

On December 19th 2013, Target announced to the world that, due to lapses in cyber security, it had been the victim of a malicious data breach that compromised a large proportion of its customers' data. Hackers stole over 70 million customer records including 40 million Credit and Debit card details. Almost 3 million of these card details were resold on the black market for an average of almost $25 each.

The recent spate of security breaches and data leaks emphasize just how vulnerable business are if they are unable to maintain the trust of their customers and the market.

Target suffered a profit reduction of nearly 50% and has now committed $100 million to securing its payment infrastructure.

Whilst the Target breach was not directly encryption related and was more down to poor security procedures, it nonetheless shows the cost impact of failing to take security seriously.

Quantum cryptography offers the potential to address these challenges with a consistency and level of protection that was previously impossible. Implementing QKD and post-quantum cryptography is not a trivial process and requires specialized (possibly national) infrastructure, processes, and people. The quantum computing related risks in a big data context are generally those associated with supporting technologies such as; data/cloud storage and data transmission. Quantum solutions in this domain will form the future paradigm in handling, securing and gaining greater business benefits.

Algorithm Design

One of the most overlooked aspects concerning quantum computers is the design, use and implementation of quantum algorithms. People 'know' that quantum computers can do wonderful things, but they can forget that it is not the computers, but the algorithms that they execute which do the useful and interesting work. Neglecting algorithms in your quantum business strategy is a risky mistake. Likewise anticipating and working in the algorithm market today can give businesses a clear head start in the exploitation of Quantum Computing potential.

The known, the unknown and the possible

Current Quantum Computing techniques are particularly good at solving certain types of mathematical problems – these typically involve searching for prime factors and unstructured data searching. It may be some time before Quantum Computing can be applied to more general problems and so it is important to focus on areas where it is likely to demonstrate material benefit compared to classical computing techniques. There are three areas to be recognized; the Known algorithms, the Unknown algorithms, and the Possible algorithms.

Known algorithms are those with proven application and benefit, they include:

- Factoring algorithms (breaking factoring cryptography), Discrete-log algorithms (Breaking elliptic curve cryptography)
- Pell's equation algorithms, Principal ideal, Gauss Sum, and other classically impossible algorithms.
- Ordered and unordered searching algorithms (Quadratic speed up), Fourier transform algorithms, large logistical tree computations, minimization and learning algorithms, pattern matching algorithms, statistical difference algorithm.

[10] http://www.financialfraudaction.org.uk/cms/assets/1/2014%20annual%20fraud%20figures%20release%20-%20final.pdf

[11] statistics from Financial Fraud Action UK 2015

Others include; decoding, formula evaluation, hidden shifts, linear differential equations, matrix operations, counterfeit coins, etc [12] These known algorithms can in some cases effectively break mainstream security, solve previously unsolvable (and hence unusable) algorithms, and exponentially increase today's computational pace. There is already a vast catalogue of algorithms that have been produced by mathematicians over the past 3 decades that are publically available. They work extremely well in the fields of cyber-security, big-data, neural networks, stock prediction, and even bitcoin generation. Any organization that relies heavily on complex and repetitive calculations, should research the benefits of the known algorithms.

The nature of Quantum Computing makes it particularly powerful for solving complex mathematical algorithms with real world applications. Known quantum algorithms can break encryption, speed-up database queries, improve pattern recognition and offer a variety of analytical speed-ups.

Then there are also unknown algorithms. These are the algorithms that are already found, but it is in the best interests of the developer not to disclose them publically. Any organization that has an interest in breaking mainstream encryption has no interest in publically divulging how this is done by brute force with a quantum computer. The "unknowns" represent a huge risk particularly to systems that are only protected with more classical approaches to computation, security and encryption. As an example an algorithm to determine winning strategies in High Frequency Trading could offer a huge advantage to a group of Stock traders, who are able to influence and manipulate global markets as a result.

Finally there are the possible quantum algorithms. These are the means of unlocking future additional value in the quantum IT world. There is no limit to the number of possible quantum algorithms, but due to the immense complexity of multi-valued logic behind quantum algorithms, the number of present day mathematicians that can develop them successfully is very small. The journey to more ubiquitous adoption of useful quantum algorithms is, as a result, at its very start Nevertheless, selling quantum algorithms, using them privately (for market predictions for instance), or even using them as computational options in a datacenter, are three potential markets that will open up. In the future, the best choice for a Datacenter Company may no longer just be based upon price, but could be aligned to the ones that can most effectively perform your applications tasks. Choosing between conventional suppliers and a supplier that offers ten times the speed of operation for mission critical tasks is a no-brainer.

Benefits for the financial sector

For the finance sector this opens up a whole range of compliance, improvements, savings and new markets. Besides compliance (e.g. security and cryptocurrency markets) there is most to be gained in pattern recognition, real-time risk analysis and financial forecasting. Also for banks with large client databases, overheads can be reduced through the use of improved searching algorithms.

Alongside security compliance, quantum computing can offer reduction in database query times, real-time risk analysis and financial forecasting.

[12] http://math.nist.gov/quantum/zoo/

Current Research and Development Activity

Technology developments

Patent searches worldwide provide a good indicator of technology advancement in quantum technologies. There is a clear divide between the two categories of quantum technologies; quantum hardware and the software centric quantum cryptography solutions.

Current trends identified in the quantum technologies landscape are as follows:

- A number of "genuine quantum patents" can be identified. There is a 3:1 ratio in numbers of hardware-related quantum patents vs. software-related quantum patents. This can be partly explained due to the general difficulties associated with obtaining software-related patents. In addition, the power of algorithms often resides in their secrecy — Patent applications would make the algorithms public and provide sufficient levels of detail so as to enable an appropriately skilled person to replicate the invention without too much additional effort.
- Patenting rates in the over-all quantum domain has been steady ever since the 90s, with a peak in 2014 and a slight decline after that.
- Next to "genuine quantum patents", numerous patents exist (and are still being filed) which qualify as "hidden quantum patents". Basically, these are traditional device (hardware) patents containing some secondary claims relating to applying the invention to quantum use cases.
- Applicants in the quantum hardware domain are traditional hardware vendors. The most active ones are D-Wave, IBM, Toshiba, HP, Fujitsu, Hitachi, etc. Among this group, top applicants are D-Wave and Toshiba. A majority of the quantum embodiments are tied to quantum devices or components thereof and methods to enhance their scalability or modularity for industrial application or to correct errors in their processing: e.g. semi-conductors (with a purpose of becoming superconducting), processors, memory units, etc. A smaller number of patents address methods to use qubits in innovative ways or architectures involving various quantum devices or networks. Examples are: adiabatic computing annealing, 3D or other types of representation and processing of qubits, acceptor-based qubits, Ising model, integer quantum computing, collision detection methods using Bloch spherical coordinates, single photon emission, passive optical networks, dynamic routing, etc. Recent filings address the introduction of real-time quantum computing into mobile communication. This trend is also noticeable for quantum crypto (software) applications which follow the main trend of mobile adoption by end-users.

2015 VALID QUANTUM COMPUTING IMPORTANT APPLICANTS

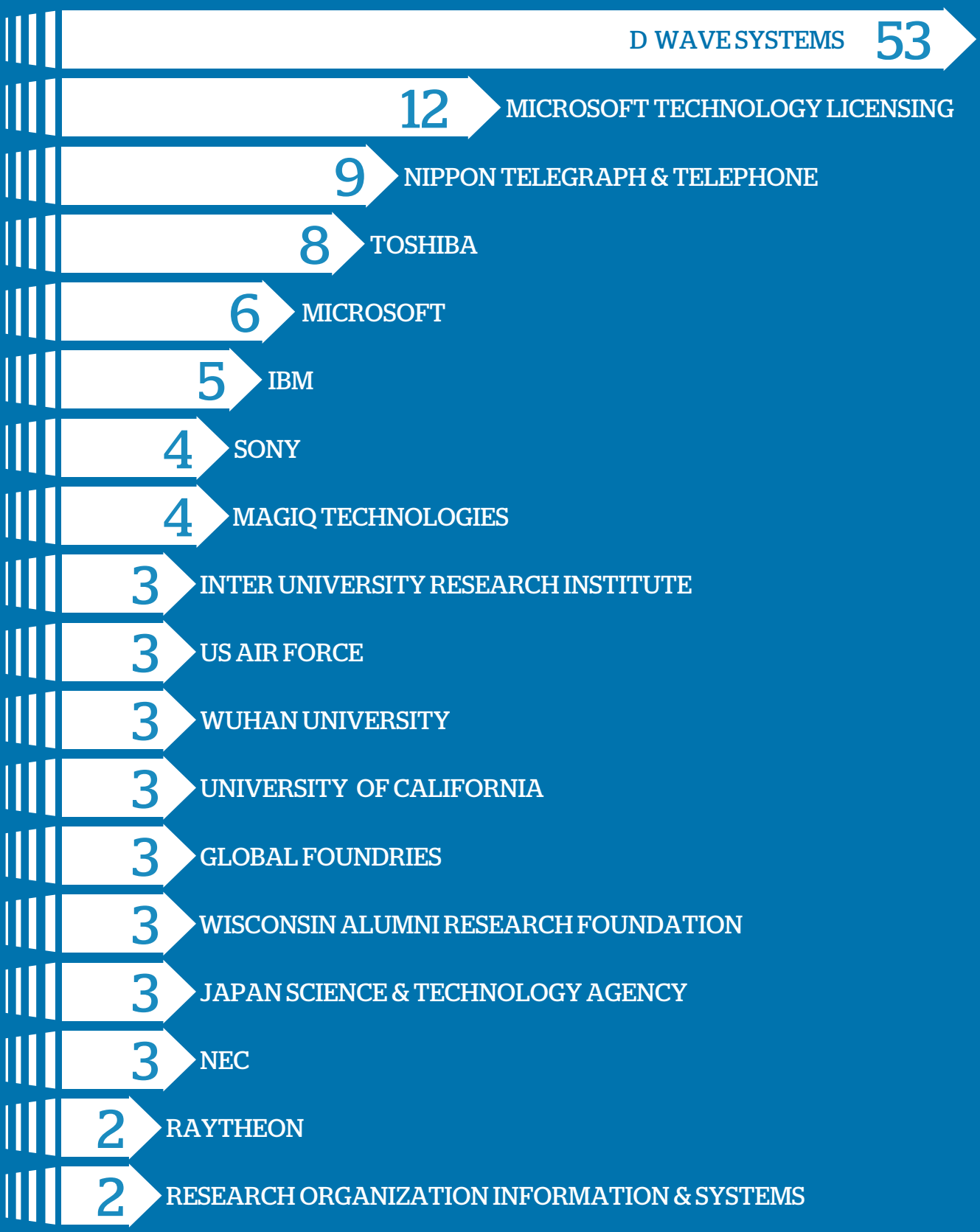


Figure 1. Patent applications concerning Quantum Computing

- In the **quantum software domain**, the filing landscape in quantum cryptography is more diverse and is scattered over a larger number of applicants. The chart below provides an overview.

- Recent applications in cryptography address various systems and methods for quantum-safe communication methods. Usually algorithms used are just mentioned as potential embodiments, meaning that patents can be implemented using different types of algorithms. This is logical, since applicants don't want to be tied to existing algorithms.

- Most strikingly; high-level trends show a very intense filing activity by Chinese (semi-) public R&D organizations for quantum hardware and software technologies.

Obviously, the patent landscape which is publically visible only shows what has been published. Much of the current research is embodied in patent filings which are still in the pre-publication phase. Also, not all research is subject to patent filings for purposes of confidentiality. A large part of knowledge on quantum technologies is suspected to be guarded and protected by various secretive public and private players. It would be naïve to think that crime syndicates or terrorist organizations worldwide are unable to fund and grow their own quantum computing knowledge and competences, internally or externally.

One thing is certain; academics aside, most engineers active in the quantum crypto-domain will keep their knowledge secret and only share it for their own benefit with others. As commercial adoption of the technology comes closer, new partnerships between technology providers, academics and governments will arise. The advent of quantum computers and ways to leverage opportunities and handle risks associated therewith shall be addressed through these partnerships. In order to start to raise awareness of quantum risk at board levels, To raise awareness of quantum risk at board levels, Atos offers quantum assessments to its customers, which could support the IT or CxO representatives in bringing the topic on their company's radar.

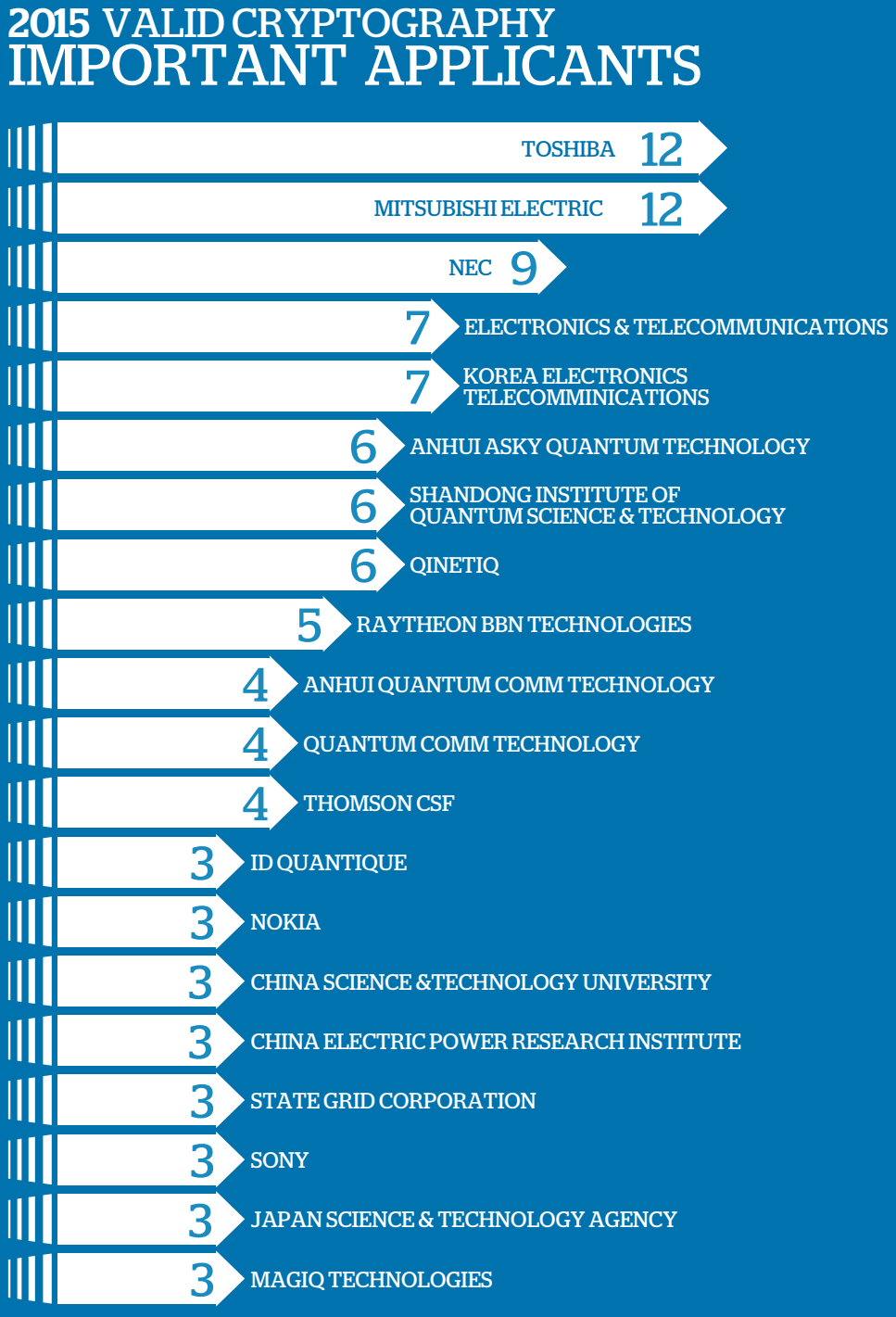
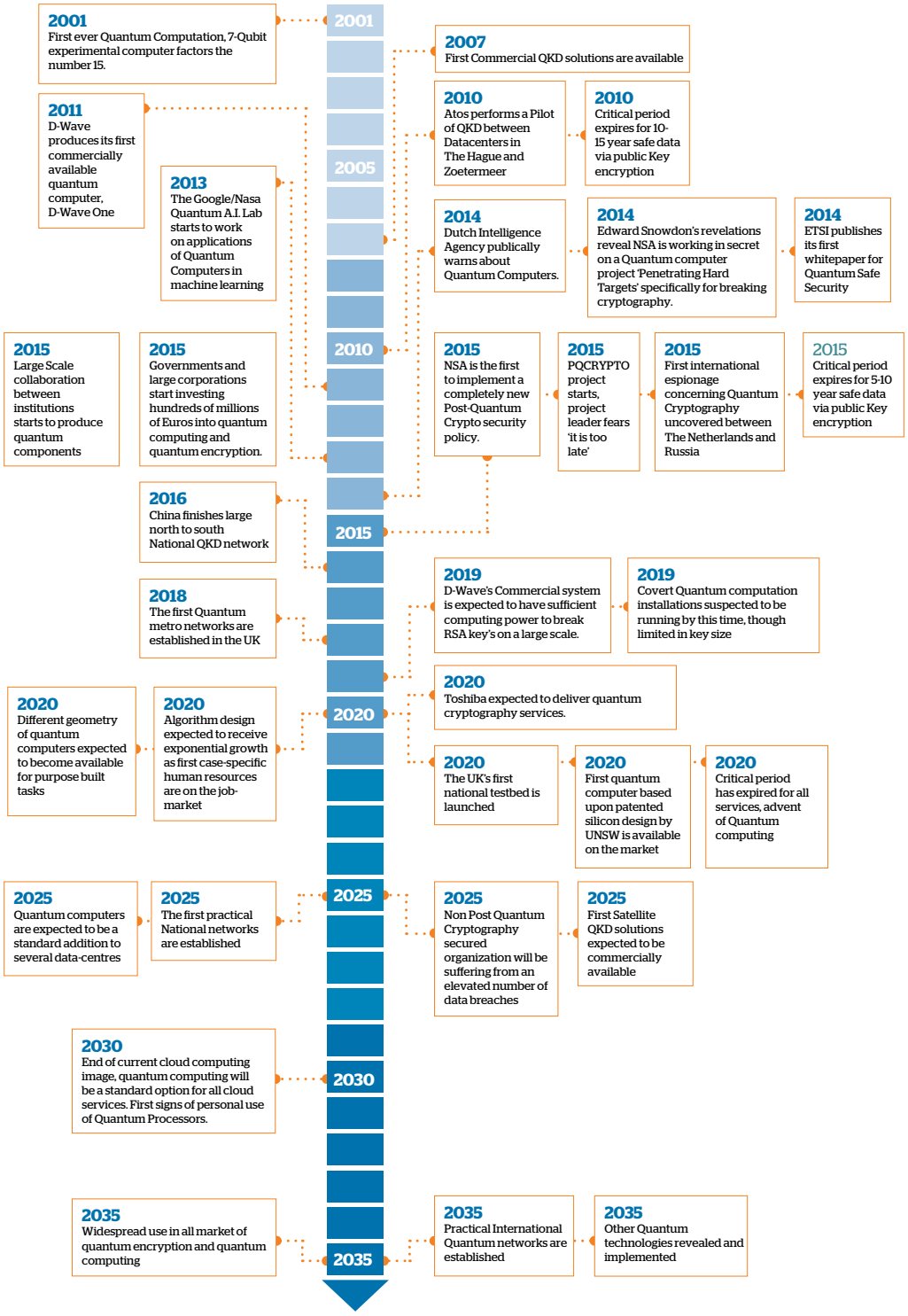


Figure 2. Patent applications concerning Quantum Cryptography

Quantum Computing Timeline

In the timeline of events, there is a so called 'critical period'. This is the moment where a company's data is exposed to interception and depends on the period it needs to remain safe.

The Critical period is defined as the time of implementation + minimal duration of data secrecy. Once passed you are at risk.



Practical applications

Quantum Computation

Quantum Computation is a field of science which only recently entered the commercial arena. In 2008 D-wave was the first company to claim to have a quantum computer for purchase. Though the applicability of the label 'true' quantum computer is still under debate, it was at the start of a rapidly developing and heavily invested field of development.

Quantum Computers are still very much under development but technical advancements in the past decade have lowered the barrier to engagement in this field.

Whilst classical silicon based computing architectures can be subdivided into CPU's and GPU's, no such paradigm exists yet in the field of quantum computing. There are several architectural approaches that can be taken, each with their pro's and con's, and no consensus has been reached upon which is the best material or architecture to use. Nevertheless the first general purpose quantum computers are expected to arrive within 5 years, at least one of these will be silicon based.

The true power of quantum computers lies with the algorithms they are capable of running.

Whatever the future of quantum computers may be, the power of change will not be derived from the hardware itself, but on the algorithms that can be executed. Whilst there are huge opportunities to utilize these algorithms for functions similar to those executed in the present day IT landscape, there are also great opportunities to develop a new breed of algorithms for completely new use cases.

Benefits for the financial sector

High frequency trading

Out of the many hundreds of algorithms that exist, there are a few that are specifically and maybe even exclusively relevant for the financial services sector, since they address operations related to core business processes of financial institutions.

Some algorithms are able to solve large systems of coupled linear equations much faster than when using classical techniques. Generally if a classical computer requires N calculations to arrive at a solution, quantum algorithms would require logarithmically fewer calculations to achieve the same result. This makes them particularly useful for image processing, video processing, signal processing, robot control, weather modelling, genetic analysis, and population analysis.

One particularly interesting application for banking is algorithmic trading. This uses algorithms to automatically initiate stock trades according to pre-defined strategies. Becoming proficient in running these algorithms for high-frequency trading can offer a significant advantage over those without such a capability.

Fraud Detection

Fraud detection is most often reliant on pattern recognition — this is done expertly via neural networks and machine learning. Machine learning is a discipline that is rapidly developing and is being invested in heavily by Google and Microsoft. The goal of machine learning algorithms is to dramatically accelerate the learning rate of artificial neural networks — using classical techniques it is very difficult to train a neural network in big-data applications.

Particularly in the complicated mathematical world of the banking and insurance sectors, having fast learning neural networks will provide levels of insight and understanding which were previously inconceivable. Pattern recognition algorithms can be effectively used to spot fraudulent activities, automated attacks on clients and reduce data breaches. Additionally, patterns in other complicated forms of attacks can be more effectively detected than is humanly possible.

Development of Algorithms for the financial institutions

Because fully functional quantum computers are not yet available in the coming 5 years, the development of algorithms is often overlooked. This is actually rather strange since even without quantum computing capability, algorithms can offer significant advantages for many IT processes. Hiring a few mathematicians and letting them work on algorithm development is a relatively cheap investment that can have very significant business benefit.

However, good mathematicians with the necessary skills and backgrounds are generally hard to come by, leading forward thinking companies to hire teams of general mathematicians in order to train them on the job.

Threats for the financial sector

Crypto Currency threats

The Elliptic Curve Digital Signature Algorithm (ECDSA), which is the basis for the public-key/private-key of Block chains, is not quantum safe. This puts the development of crypto-currency markets at risk, since currently their keys are sent via the internet. In theory, having acquired a quantum computer, it will be possible to take any number of public keys and rapidly de-crypt them to determine their private key counterparts. The first person to perform this feat could use such knowledge to execute the largest bank robbery in the history of mankind.

Security algorithm threats

In a similar way, Shor's algorithm can decrypt RSA keys, rendering them practically useless. In fact there are many cryptography standards in use today that are not quantum safe. It is advisable for any institution to perform a Quantum Risk Assessment to determine the risks associated with their current encryption infrastructure. It should be noted that if the outcome of such an assessment shows serious gaps in security, the institutions' core business will be rendered extremely vulnerable with the advent of Quantum computers.

Security

Encryption

If data is to be transmitted securely between two or more parties, it must be encrypted. This is achieved using an encryption algorithm that makes use of a specific key to render the original data unreadable to anyone who does not possess the corresponding decryption key.

For asymmetric systems, different Public and Secret "paired" keys are used – the public key is used to encrypt the data in a format that can only be decrypted by the holder of the secret key pair. The public half of the key can be freely distributed since it is only used for encryption and not decryption.

Asymmetric encryption is typically used for applications like secure e-mail and on-line banking where a message is encrypted (e.g. by a customer) using the recipients publicly available key. The message can only be decrypted by the intended recipient (e.g. by a bank), using their paired secret key that is held only by themselves.

In the case of symmetric encryption, the same key is used in both the encryption and decryption process - An appropriate key distribution system must be used to securely exchange keys with intended recipient(s). This can be done physically, face-to-face, or may be carried out using public key distribution process. A symmetric key distribution system is truly only ever as secure as the method of key exchange.

Both of these systems rely on the computational complexity of cracking the key, which often requires carrying out very difficult computations involving the factorization of large numbers. It would take even the most powerful "conventional" supercomputers an impractical amount of time, years or even decades, to break modern keys. However, computers are becoming ever more powerful, and any encryption method that uses a particular computational difficulty (key length) to provide its security inevitably has a time-limit on its usefulness.

Quantum computers will provide a step-change in computational speed and should easily be able to break many of the encryption methods used in public key encryption today — significantly weakening symmetric key methods. Therefore, methods for encryption and key distribution that are 'quantum-safe' will need to be developed.

QKD

Quantum key distribution (QKD) seeks to provide a method to generate and exchange a key while communicating over a public channel. Rather than relying on computational difficulty, QKD uses the properties of quantum physics to ensure its security. Specifically, it takes advantage of the fact that the very act of measuring a quantum system changes it and so any interception of the transmission can be detected. QKD distribution is particularly useful for securing a specific communication channel for a specific session. If interception is detected or suspected at any time, the encryption key can be changed ensuring that secure data transmission is restored.

Typically, the encryption key is encoded in the polarization and axis of measurement of photons prior to them being sent to the receiving party. The sending and receiving parties can publically compare part of their keys, and if they differ they know that someone was eavesdropping. QKD signals may be transmitted over fibre optical cable or wirelessly (provided there is direct line-of-sight). This leads to two primary ways of implementing QKD: closed QKD-secured networks for businesses, and mobile solutions via special satellites.

Various commercial QKD solutions for businesses are already available through suppliers such as ID Quantique and Toshiba, but a lack of standards and infrastructure has limited their proliferation. Working with ID Quantique, non-profit R&D organization Battelle built the US' first commercial purpose QKD network in 2013. Many QKD networks currently in existence serve as testbeds for research. Such networks have been set up in Tokyo, Vienna, and Geneva, to name a few. The UK Quantum Communications Hub is currently building a national QKD network, starting with metro networks in Bristol and Cambridge, which will then be connected via London to form a long distance network. This will be used as a testbed for research and demonstration purposes and the network is set to be completed in the next five years. China is also active with QKD; in 2016 they plan to have constructed both a fibre QKD network connecting Beijing to Shanghai, and a "quantum satellite" that will secure its communications using QKD— both highly ambitious projects.

PQ-Crypto

Quantum safe encryption can be achieved using classical algorithms and technology; this is known as post-quantum cryptography. Such solutions range from the use of encryption algorithms where increasing complexity drives an exponential increase in solution runtime even for quantum computers; through to the creation of all new encryption methods that would be problematic for a quantum computer. Some such methods already exist, though they cannot truly be tested until a practical quantum computer also exists. Government bodies are now recognizing the need to establish quantum safe communications. GCHQ is researching post-quantum cryptographic methods and the NSA has announced plans to transition towards quantum safe encryption standards for the US.

Pros & Cons

The development and application of quantum safe encryption methods may be seen as applying a bandage to a broken system rather than fixing it and, with any maths-based security system, it is only ever a matter of time before a computer, whether classical or quantum, is powerful enough to break it.

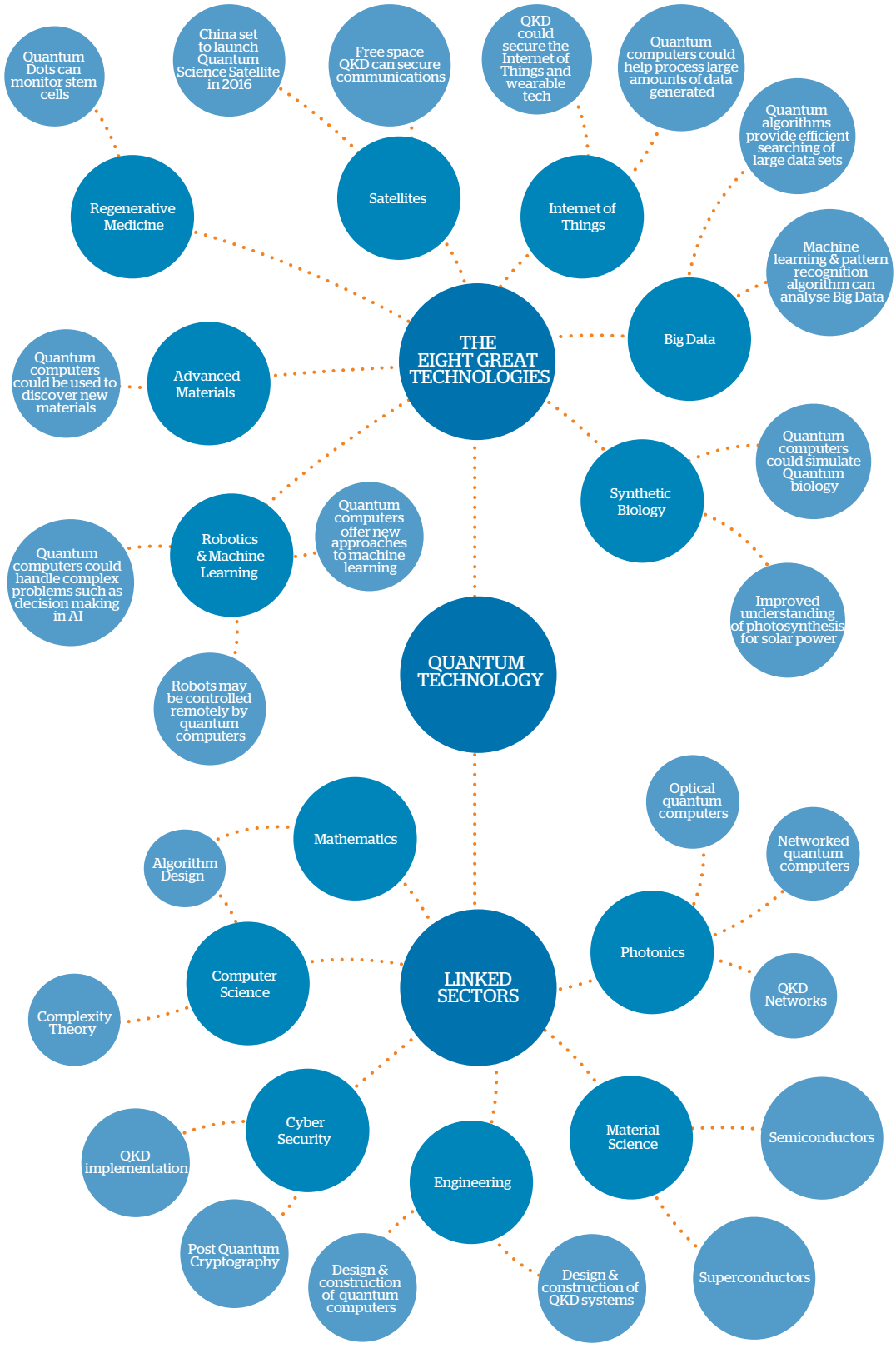
Whilst QKD is most likely to be the safer option in the long run, when compared to post- quantum cryptography, it comes at the cost of needing to install optical fibre networks, which can be expensive, or using current dark fibre networks — where possible. It may be more cost effective for businesses to move to quantum-safe encryption standards rather than invest in QKD infrastructure. Such considerations should be assessed separately in each case, for instance through a quantum assessment.

"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

Other developments

While this paper focuses on the benefits that quantum technology could bring to the finance sector, the potential applications are very much broader. Many of the "Eight Great Technologies" (big data, satellites, robotics & machine learning, agri-science, advanced materials, synthetic biology, regenerative medicine, and energy storage) which were outlined by the UK government as areas in which the UK could be a world leader, may be directly impacted by the emergence of quantum technology.



Conclusion

While it is likely to be a decade before quantum technology starts to significantly impact the world of financial services, the potential implications of the technology mean that financial institutions must begin to prepare for its arrival now. In terms of security, this should be done through quantum risk assessments and investment in quantum safe cryptography, such as quantum safe encryption algorithms and QKD networks. There are already commercial entities ready to provide these services, with more companies gearing up to do the same.

The critical period for this will be the next five years; beyond that point, the safety of encrypted data transfer cannot be guaranteed, as the advent of quantum computing will be imminent at this point. In ten years, practical national QKD networks will be ready and international networks will follow ten years after that. Such networks will be important for secure communication between companies or different headquarters within companies, as many companies will not be able to construct these networks themselves.

Progress in the design and build of quantum computers will continue through academic research collaborations such as the UK Quantum Computing Hub and QuTech in the Netherlands, and technology companies such as Google and Lockheed Martin. However, it can only be through engagement with academia, or in-house research, that effective quantum algorithms with direct financial applications will be produced.

The ability to produce and patent quantum algorithms prior to the advent of quantum computing in finance will provide a large head-start for businesses when they become more commonplace. In the early stages of the implementation of quantum computers in finance, the hard limit on computing ability will be in the hardware available; the edge a company can gain over rivals will come through software development.

About Atos

Atos SE (Societas Europaea) is a leader in digital services with pro forma annual revenue of circa € 12 billion and circa 100,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.

For more information, visit: atos.net

Interested in our Ascent - Thought Leadership publications?

Stay connected with the latest forward-looking and inspirational publications on business & technology
ascent.atos.net

atos.net

All trademarks are the property of their respective owners. Atos, the Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Worldline, BlueKiwi, Bull, Canopy the Open Cloud Company, Unify, Yunano, Zero Email, Zero Email Certified and The Zero Email Company are registered trademarks of the Atos group. Atos reserves the right to modify this document at any time without notice. Some offerings or parts of offerings described in this document may not be available locally. Please contact your local Atos office for information regarding the offerings available in your country. This document does not represent a contractual commitment. © 2016 Atos