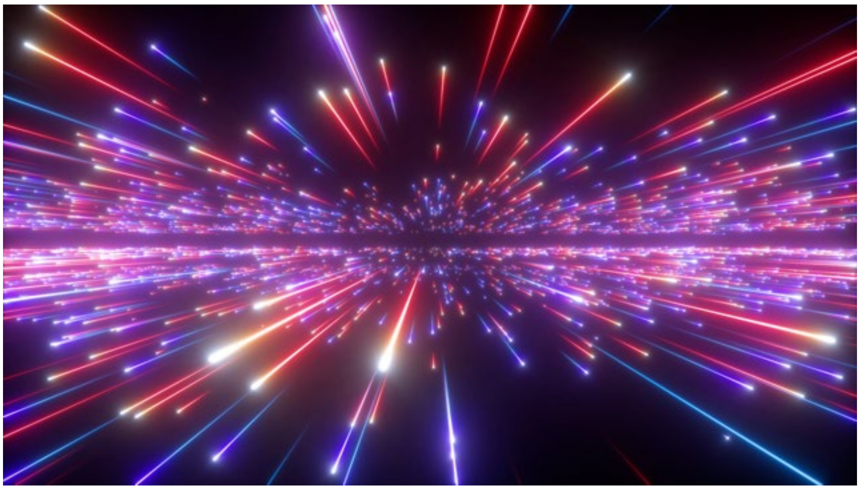
INTERNATIONAL INSURANCE SOCIETY

Affiliated with THE INSTITUTES



Quantum Technologies, Cybersecurity and the Change Ahead

In the 1980s, one of the pioneers of quantum computing, Nobel physicist Richard Feynman[i] observed that "Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical"[ii].

According to a study by Precedence Research[iii] "The global quantum computing market size is projected to hit around USD $125B by 2030 and poised to reach a CAGR of 36.98%."

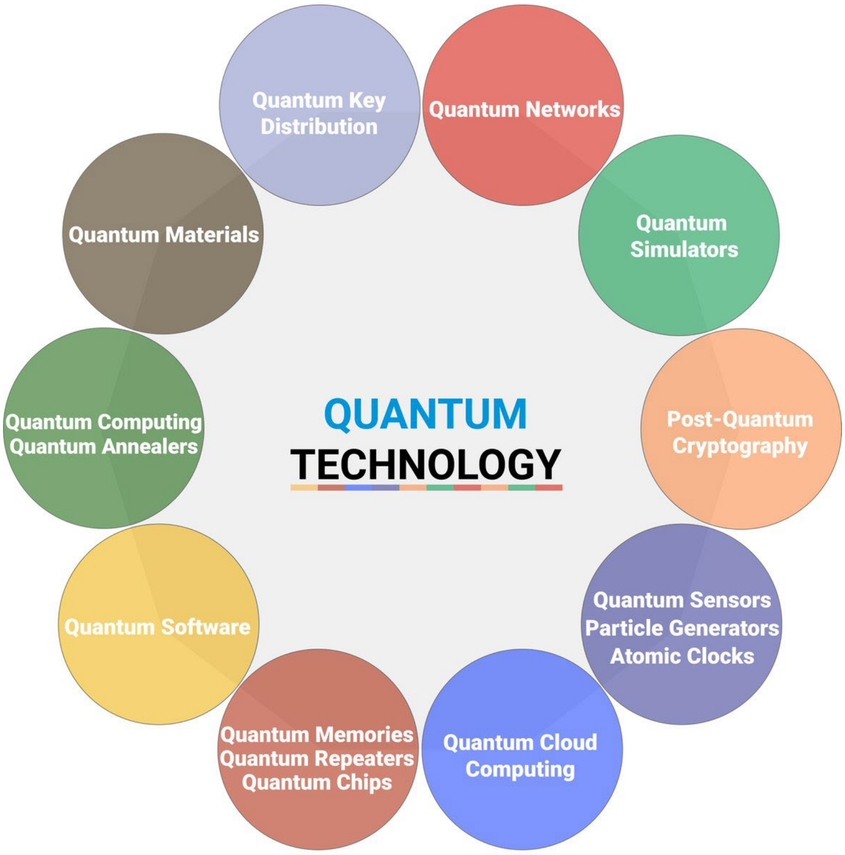
What if you could envisage a world where millions of entangled energised atoms are connected across the planet and into space all working in parallel at the speed of light to compute a specific solution for say cancer cure, a new battery or carbon emission reduction.

This paper is a primer for quantum computing[iv] that experts say is 10 years away but there is need to understand and act now because of –

- Recent adoption of generative AI[v] has greatly sped the race to quantum computing.
- Cybersecurity outcomes of quantum computing need to be addressed today.
- Hybrid computers interfacing classical computers with quantum computers are now available and can address some key world issues.
- Climate change urgency requires faster development of quantum computing.
- Error correction that challenges quantum computing today is fast being addressed.

Quantum technologies have existed for some time. The transformational spotlight of this paper is the shift from classical to quantum computing. This aligns computing with physics, chemistry, biology and laws of nature, moving from a binary transistor state to a world as envisaged by Richard Feynman. Explosion of data and smart devices pushes classical computing to the limit hence the evolution of quantum computers. This evolves data mining which collects data and extracts patterns, to data farming which grows and cultivates data for user designed computational experiments to analyse using quantum computing for forecasting and modelling to obtain insight into complex problems. ***It is likely that only quantum computing technology can address and solve the climate change crisis***.

Quantum computing combines computer science, physics, and mathematics utilizing quantum mechanics to solve complex problems faster than on classical computers. Applications where quantum computers can provide such a catalyst now include machine learning, optimization, and simulation of physical systems. The following diagram shows the diversity of quantum technologies. In physics, the term "quantum" also refers to the smallest possible unit of a physical object at atomic level.



Source: https://www.insidequantumtechnology.com/home/

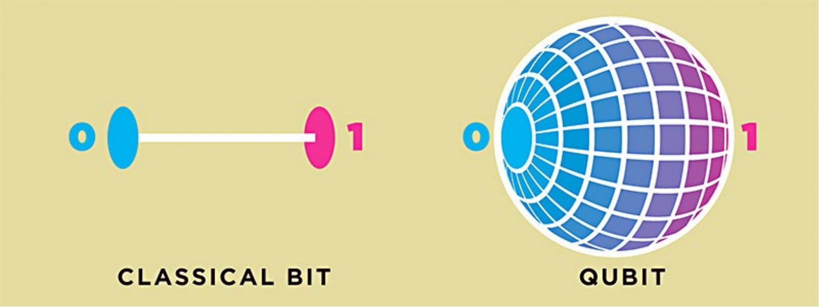
Countries and corporates set ambitious targets for reducing emissions at the 2021 United Nations Climate Change Conference (COP26)[vi]. A pledge of $4 Trillion annual investment by 2030 for measures reducing warming to between 1.7°C and 1.8°C by 2050 falling short of the 1.5°C level logged to avoid catastrophic climate change. To meet the net-zero emissions goal, advances in climate technology are required that powerful supercomputers cannot do today. Quantum computing is the one technology that could develop climate solutions capable of abating carbon emissions by 7 gigatons a year of additional carbon dioxide by 2035, with the potential to align the world with the 1.5°C target [vii].

At the atomic level different rules of physics apply and quantum rules determine how atoms interact and entangle together. This understanding enables advanced and rapid calculations. Quantum computers form an exponential increase in processing capacity by considering all possible outcomes to a problem simultaneously rather than sequentially. The result is a computer that delivers atomic-level speed, millions of times faster than anything today.

Explanation of the Quantum Ecosystem

Quantum mechanics is the area of physics that studies the behaviour of atomic and subatomic particles. **Quantum computers** take advantage of these behaviours to perform computations. **Quantum phenomenon** is not new and is the basis of the development of lasers and semi-conductors since the 1950s. Emerging **quantum technologies** support development of quantum computers. Foundationally the technologies use the quantum mechanics principles of **entanglement**[viii] and **superposition**[ix] **(**how atoms work together when energised**)** to share information. This is not possible with **classical computers** which work on binary bits where a **bit** is an electronic signal that is either off or on (0,1). The value of this switch makes computers follow specific logic making them reliable for mathematical calculations but unsuitable for intangible problems such as climate change and medical breakthroughs where situational awareness of all data is required.

The best analogy to describe quantum computing is a coin toss. For classical computers it is binary, either a heads or tails state. Quantum can be envisaged as a spinning coin where heads and tails states are both active while it is spinning. When the coin stops spinning it falls either heads or tails reverting the state to binary, losing the quantum state. At this point the result is measured as it has gone through every possibility while the coin was spinning and stores results back in the binary state. **Superposition** is akin to the spinning coin, giving quantum computers inherent parallelism, allowing millions of operations simultaneously.



Source: https://www.austinchronicle.com/screens/2019-04-19/quantum-computing-101-a-beginners-guide-to-the-mind-bending-new-technology/

Quantum computers substitute bits with quantum bits known as **qubits** representing quantum particles at atomic and subatomic levels. Superposition can be achieved using photons[x] (packets of light) creating an interference pattern where the photon is travelling every path at once causing multiple states to occur allowing complex calculations at scale and in parallel.

Superposition shows why solutions going through trial and error in laboratories take years but with quantum technology can take hours. This can also be illustrated with programming a mouse out of maze. Classical computers program all possibilities to find the quickest route out by trial and error, but quantum computers simultaneously plot all routes, stop and measure to find the quickest route. When a quantum state is measured, atomic wavefunction collapses and you measure the state as either a zero or a one known as the **deterministic state,** where the qubit acts as a classical bit and reveals the best path out of the maze.

Because of entanglement, where qubits can connect anywhere, multiple qubits are pushed into the same state that can connect over large distances. Quantum processors can draw conclusions about one particle by measuring another one to solve complex problems faster. Superposition and entanglement work in parallel. This phenomenon is exponential as the more qubits the more possibilities of storage capability. The optimization of this process is known as **Quantum Annealing**[xi] and is the most promising quantum technology for shorter term delivery as easy to build stable processors and qubits. When the number of qubits increases, the possibility of noise[xii] or heat generation occurs and needs to be addressed by **quantum error correction** (QEC). Noise in the quantum state is known as **decoherence** where the system degrades, losing entanglement and data, so needs to be fault tolerant.

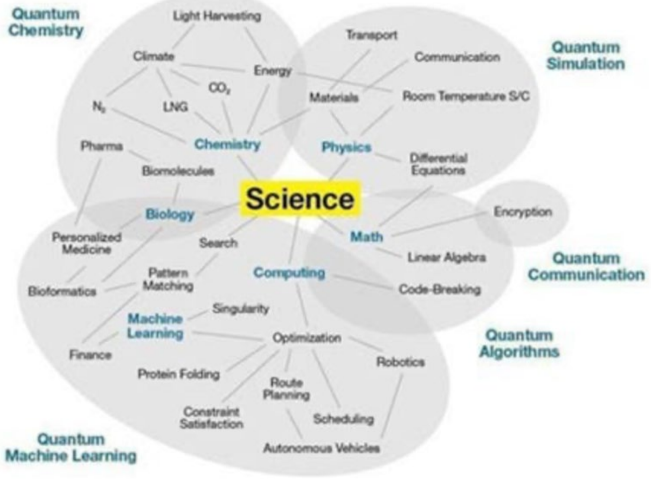
To reinforce this explanation Scientific American has a good video, noted in the reference section.[xiii]

High level Applications of Quantum Computing

Computational capabilities via quantum technologies allow supply chain optimizations, molecule/vaccine discovery, discovery of mineral deposits, climate change solutions, cures for cancer and more. Governments know this, hence the large national investments.

There is no need to wait for mainstream adoption to start addressing these issues as small error tolerance is acceptable as quantum computers deal with probability theory. Even though **error correction** is required to correct decoherence, techniques exist now to correct by using **logical qubits** (cluster of physical qubits to do error adjustment), building Noisy Intermediate Scale Quantum computers (NISQ)[xiv] and finding qubits not sensitive to noise.

This spawns **hybrid quantum computing**[xv], available now for commercial applications use including investment predictions, logistic route optimization, smart city planning and energy distribution. Hybridization provides access to quantum computing for business problems in partnership with classical computers (GPU/CPU) and Web3 technology.



Source: gartner.com/SmarterWithGartner

In order to assess quantum commercialisation, it behoves to look at **quantum advantage,** the threshold where a quantum system can perform operations that any classical computer cannot simulate in reasonable time. Currently, no quantum computer can perform a meaningful task, faster, cheaper, or more efficiently but that will soon change. Quantum sensors will be commercialised before quantum computers providing a catalyst.

There are 4 important areas below where classical computers will fail and, using superposition, all viable options can be generated, bypassing non scalable long trial and error experiments in labs. Emission of carbon dioxide into the atmosphere and reversal through clean fuels and energy storage are functions of nature, battery improvement aligned through chemistry and healthcare through biology, all which can be seen through a quantum lens and encapsulated by the laws of quantum mechanics.

- Climate Change – carbon capture, nuclear fusion, renewable sources, decarbonize ammonia process, remove methane from agriculture, make cement production emissions free, lower cost of hydrogen to replace fossil fuels and energy grid analysis.
- New Battery Development – align quantum chemistry to battery chemistry, create longer life faster charging batteries, halve the cost of grid scale storage.
- Healthcare – precise medical imaging, new drug discovery, early disease detection, cell level intervention with nano quantum sensors and combining healthcare life sciences with quantum technologies aligned with biology.
- Space Exploration – more precise navigation systems, communication networks, quantum clocks and putting energy collectors in space.

Cybersecurity Issues

Quantum technologies promise much but could disrupt a country's national security. They are complex and diverse technologies with varying levels of technical readiness, so mitigation is required to avoid any quantum cyber surprises. Cryptography experts say that a classical computer will take millions of years to find the prime number of two factor combinations used in encryption today, but quantum computers can crack that in less than an hour, putting data security and privacy at risk with the advancement of quantum computing. This needs to be on all risk radars. Bad actors can harvest data now and once quantum advances will decrypt the data. **Quantum-safe cryptography**[xvi] is the process of securing and transmitting data in a way that cannot be hacked by quantum or classical computers. Safe transition is achieved through technology lifecycle management. The urgency to initiate and complete the transition to quantum safe cryptography is bespoke for individual organizations. EvolutionQ's "Quantum Threat Timeline 2022"[xvii] explains how three simple parameters can evaluate this:

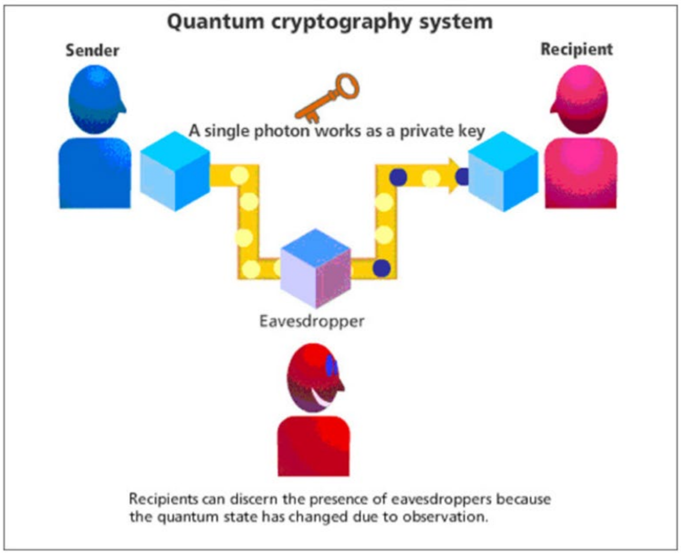
- shelf-life time: the number of years data should be protected.
- migration time: the number of years needed to safely migrate the systems protecting that data.
- threat timeline: the number of years before relevant threat actors can potentially access cryptographically relevant quantum computers.

Organizations will not protect their assets from quantum attacks if the quantum threat timeline is shorter than the sum of the shelf-life and migration times. The quantum threat to cybersecurity could become apparent sooner than many expect.

Quantum Computing improves modelling and predictive analysis by the use of AI, simulation and optimisation. The pace of data explosion has increased the need to process and store data far broader than computer capabilities can today, increasing cybersecurity risk. Data scientists say that public key cryptography systems in use today such as RSA[xviii] can be broken by quantum computing. The world has entered a post quantum phase where strategies are being developed to protect the encryption and confidentiality of data. The United States is pioneering this phase by releasing post quantum standards in 2024 backed by government investments. This assumes mainstream adoption of quantum computing within a 5-10 Year timeframe now accelerated by third wave AI and increasing natural catastrophes.

Given quantum-enabled cyberattacks, no public-key encryption today is safe. Quantum Key Distribution (QKD)[xix] is available but not at smartphone level yet. Computers can use prime factors to a large number to act as an encrypted key: the receiver must know the prime factorization to decrypt the information, a secret between sender and receiver. With QKD, an eavesdropper can only see the composite number and a feature of quantum mechanics means that any interloper would need to measure so interception is easily detected, and hackers cannot cover their tracks. By partnering with organizations that can provide resources and training on quantum computing while also notifying when new standards are released, companies can update their technology with patches to keep their data secure.

Quantum cryptography

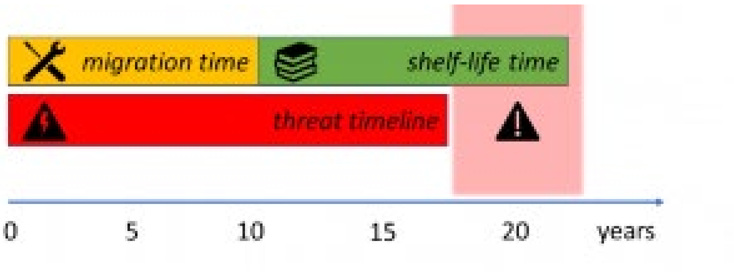


Quantum cryptography system

Recipients can discern the presence of eavesdroppers because the quantum state has changed due to observation.

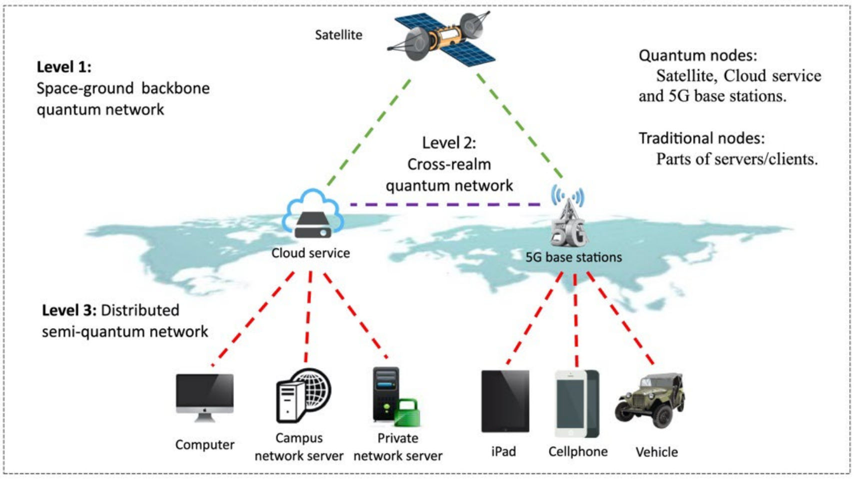
Source: BBVA open mind

Quantum Threat Timeline can be mitigated by deploying new cryptographic tools that are resistant to quantum attacks. Transition to quantum-safe cryptography requires the development/deployment of hardware/software, quantum immune solutions, establishing standards and legacy migration. A milestone will be to demonstrate “**quantum supremacy”** where a quantum computer outperforms the most powerful supercomputer. This will signify having achieved control on a large number of physical qubits, necessary for quantum computing. That quantum supremacy milestone could easily be passed in the next couple of years, so these cybersecurity mitigation preparations need to start. From the threat timeline to the migration timeline, assessing the overall risk see below. (Mosca & Mulholland, 2017).



Source: https://globalriskinstitute.org/publication/quantum-threat-timeline/

Enterprise level risk assessments all need revision. The ecosystem shows the quantum technologies interoperating together and how quantum communication networks link to space technology. QKD is physically realized using photon quantum computing and that requires fiber optics so wireless connectivity is needed to connect to smartphone. The Post Quantum phase will exist until wireless connectivity can transmit qubits. When QEC ends decoherence that will be a tipping point for quantum computers. Distance problems are addressed by connecting ground stations with satellites enacting QKD by transferring a group of keys to a satellite and then using those keys to secure communication. The ability to distribute entanglement across oceans from space makes the quantum internet real, securing data between countries cell phones from space and beyond as in the diagram below.[xx]



Source:https://onlinelibrary.wiley.com/doi/abs/10.1002/sat.1392

Today the largest quantum computer has 1000 qubits[xxi] but this is exponential so when you get to 1 million qubits this is a powerful machine capable of breaking the current encryption systems. A quantum computer was built based on an algorithm by Peter Shor[xxii] to prove that current encryption can be broken so it has to be taken seriously but not as to cause a Y2k like panic.

Standards

In 2016, the National Institute of Standards and Technology (NIST)[xxiii] requested submissions for algorithms that could replace public key encryption. NIST has been working on post quantum cryptology for five years and it will take the same amount of time to get critical mass to adopt the standard. NIST announced the current secure Advanced Encryption Standard (AES)[xxiv]. While NIST released one quantum-resistant signature standard it announced the final algorithm choices and draft standards early in 2022 with final standards to be announced in 2024[xxv]. These techniques are more resilient against advances in classical computing than the current public-key algorithms and offer more overall security. Organizations must be crypto-agile, and AES is a safe default standard for today. Cloud companies such as Microsoft, Google and Amazon are all developing quantum-safe encryption algorithms and software.

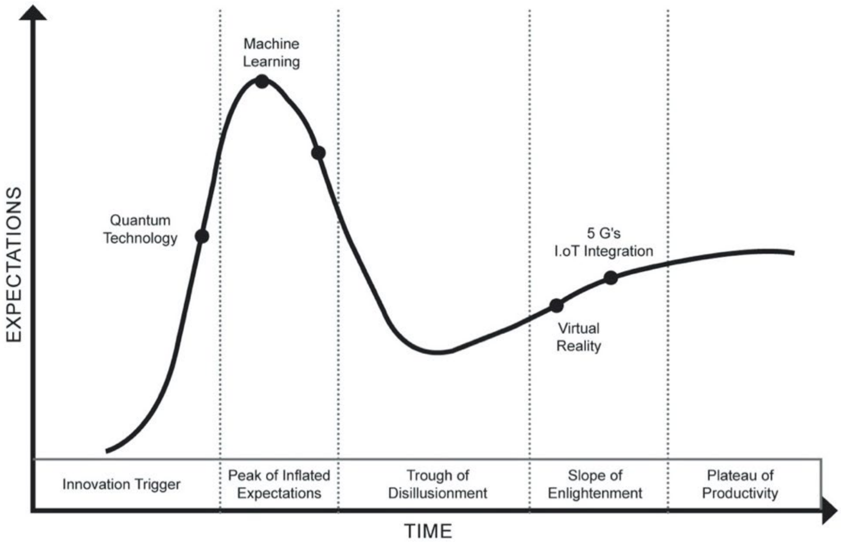
Transition to post-quantum algorithms via standards is priority to protect critical digital and hardware assets from future cyber threats. Cyber security risks posed by cryptographically relevant quantum computers is a systemic risk. The algorithms that support encryption today are still considered safe for e-commerce because while quantum computing is real, the technology is at an early stage and will not be a threat until computers have 1 million qubits, hence the need for the time threat timeline hand in hand with the standards.

Preparation means security certificates and current **trust anchors**[xxvi] must be updated and the key sizes for public-key algorithms will change. Organizations need a transition plan and need to decide whether to migrate to post quantum via hybrid certificates or create two parallel environments with single certificates. Institutions must use standards to become "quantum resilient or immune" using security by design. Manufacturers must include hybrid certificates into devices at production time, which is a digital certificate that features a classical crypto algorithm, like RSA, alongside a post-quantum crypto algorithm. A single certificate allows communicating securely with algorithms that NIST has listed. A hybrid digital certificate provides customers a preview on how a post-quantum crypto algorithm can work without infrastructure change. Quantum resilience mitigates effects of cyber vulnerabilities ensuring that sensitive data is broken into smaller, encrypted pieces and stored in different places.

Regulation

The development of quantum technologies raises questions for policy makers and regulators in the same vein as AI, to ensure that it is being used in a responsible manner as well as assessing the societal and ethical implications. With such a transformational technology regulators should be inside the quantum ecosystem as a node on the network in real time to promote their understanding of the wider market innovation, competition and national developments. The cybersecurity challenges are clear, the development of standards is underway and changes in policy need to be reflected in cybersecurity laws. Anticipatory governance should be aimed at responsible quantum technology to achieve socially desirable outcomes. Quantum technologies serve as a broader reference to quantum computing. There have been many hype cycles in AI which has led to moratoriums, fear and confusion. Cybersecurity, societal or privacy risks posed by quantum enabled technologies on assumption of decrypting currently used encryption systems must be addressed even with penalties if deadlines are not met. To maximize the opportunities for quantum we must also push for greater inclusion and diversity to avoid accidental bias within AI training and the unintended consequences if not regulated.

Regulatory bodies want to enforce quantum compliance over sensitive parts of the infrastructure including the supercomputer and cloud. Encryption affects everyone so an increase in computational powers does mean that some people can exploit security more than others. Access to quantum technology today is not about community so it is important to move this to the community level early. Governments must protect their citizens on how to regulate a new **quantum internet** and recognize secrets that are valuable for more than say 10 years (such as child healthcare records). There is a long gap between lab to production to early adopters to mass market adoption. Quantum technologies are sovereignty technologies where countries are developing their own with significant funding so there is a need to try and avoid a scientific and technological gap between countries causing a quantum divide. Sovereignty technologies have strategic interests and already export controls of quantum processes exist even though these machines are at the early stage of growth with limited qubit capacity. Regulators must deal with hype and while the hype cycle is still there the reality cycle is starting to grow as shown by Gartner.



Quantum Technology: Gartner's Hype Cycle and its Implications for National Security Policy

Generative AI

Generative AI[xxvii] (such as ChatGPT) is at an early stage of development with a challenge being the amount of data to train the models. Generative AI produces content similar to the work of human intelligence where the human is the curator and the machine the creator. Quantum computing as established can process vast amounts of data at lightning speed and therefore will be a serious contributor for Generative AI by producing more accurate and complex outputs through **quantum machine learning**. The integration of these two fast moving technologies over time will transform computing and AI. The Consumer-Packaged Goods business sector is a key recipient of AI and quantum to unlock deeper insights into the consumer to see relationships and information to protect brands. AI research intersects with quantum research to become a new computing concept for the sector. This is where hybrid quantum computers can solve contingency problems using heuristics as no exact answer is required, just requiring approximations based on probability theory. The key question being asked is if Generative AI can scrape the internet quickly for information on quantum, is it possible that quantum algorithm code could be generated? If the answer is yes, then this has big implications. At this transitory stage it is probable that Generative AI is not ready to generate quantum algorithms that solve worldwide problems as confidentiality and cybersecurity is paramount and more training is required. However, as these technologies mature and **quantum AI** emerges, the fusion of these technologies will be highly significant as long as they remain within the caveat of responsible and ethical usage.

Technology Considerations

Classical computers are approaching a technology barrier. According to Moore's Law[xxviii], the number of transistors doubles approximately every two years in an integrated circuit. Today's computers are rapidly approaching the size of atoms hence the quantum shift.

It is important to discuss **quantum clocks** as they complement atomic clocks which are needed for precise position measurement of GPS (Global Positioning System[xxix]), and time critical Internet applications and are the most accurate time standards known. Based on atomic physics these clocks exist at absolute zero temperatures where atoms slow down. Every GPS satellite carries atomic clocks and are used in mobile phones, space navigation, aviation programs and digital television. Banks guarantee the time and date stamps of high-frequency transactions. Reducing these clocks in size on chips is key for applications with no GPS signal. Quantum clocks are part of the quantum technology sensor toolkit.

Quantum computer node networks all have super cooling to slow down the atoms (qubits) to do calculations using superposition and entanglement. **Quantum repeaters** keep the superposition, entanglement and measurement going to share sensitive data across large distances. For cost reasons these networks will initially be accessed through the cloud as a distributed quantum computer network and eventually bring to the smartphone level where low orbit satellites with wireless are used for last mile connectivity.

Deployment of IoT[xxx] (Internet of Things) is greatly enhanced by quantum devices and sensors leading to massive increases in data volumes which is ingested by quantum computing and improves risk management. Quantum Computing will enable a change in the security, protection and transfer of data within IoT ecosystem by use of QKD. The quantum network layer is responsible to channel and monitor data transfers through quantum and classical systems within local networks and the internet. IoT systems require rapid results as they generate heavy volumes of data. Therefore, Quantum Computing processes complex data faster within the IoT system. Optimum complex computation capabilities integrate quantum technologies in digital twin simulations. Quantum simulation and quantum machine learning can be used to build a Quantum (Digital) Twin[xxxi]. Digital twins are used in critical infrastructure and autonomous transport to do industrial simulations. In the manufacturing sector when quantum algorithms are integrated into digital twin simulation across manufacturing plants, connecting multiple machines with multiple devices, the impact will be exponential. The Internet is enhanced and not replaced by entry of the **Quantum Internet** which transfers encoded qubit information through optical fiber networks and satellites.

Thermodynamics of Quantum Computing and Energy Consumption.

When computers overheat, they underperform or crash. For quantum computers heat is a crucial interference factor and must be measured at speed as changes to a quantum state take only a millionth of a second. **Fault tolerant quantum computers**[xxxii] are being built with QEC to fend against noise and heat. This comes with an energy trade off.

The qubit environment needs to be close to absolute zero (-273°C) to ensure no interference. QEC preserves quantum information but incurs a high energy cost by adding qubits for error detection. There is correlation between “error rate” and “energy” in quantum computing that will allow the design of energy efficient computers to calculate the minimal energy cost. Even if a quantum logic operation consumes more energy than a classical logic operation, the smaller number of quantum logic operations mean that the quantum computer will ultimately be more energy efficient. Quantum computers should consume less energy as they solve problems quickly that would take supercomputers eons to solve. Recent experiments in comparing bitcoin mining[xxxiii] using level entry hybrid quantum computers showed strong energy efficiency gains, proving less powerful quantum computers are capable of solving computations comparable to supercomputers with less energy.

Insurance implications

Quantum computing is considered a long-tail risk (an unknown) implying claims may not be settled until a relatively long time after a policy period expires and even require commutation. The potential of quantum computing is not obvious to many in the insurance industry though there are several early adopters. New entrants are likely with foundations in the technology. Financial craft brothers such as securities and banking applications utilise quantum algorithms and software are gaining traction in risk analysis, portfolio optimization and credit risk. Early adopters for quantum computing for risk analysis will have the vision to future-proof the insurance industry. Monte Carlo simulation speedups can use random sampling to estimate numerical quantities difficult to calculate outright via classical methods.

Emphasis should be on sharing data and improving risk modelling. Insurers cannot be complacent on the systemic threat of emerging risks such as cyber or climate change. Frequent catastrophic events, combined with meeting evolving regulatory requirements, challenge company business models and can make risk unaffordable. Quantum technologies offer exponential increase in computing power, precise measurements (quantum sensing), high-performance computing (quantum computing) and tamper-proof communications (quantum communication) to assess and quantify environmental risk, acting as an early warning signal for insurers. Quantum computers can handle precisely those computational tasks that form the basis for solving actuarial problems. Risks could be identified at an early stage by calculation and losses avoided. Analytics required for the development of products and services could be calculated faster and more accurately than was previously possible.

When taken in context with AI, quantum computing will show improved pricing and risk models within the underwriting process using benchmarking and baselining using Causal or Explanatory AI[xxxiv] leading to exposure management, reserve adequacy, reinsurance risk transfer, better fraud detection, claims management and better explanations with regulators. The ability to accurately simulate climate systems delivers significant improvements to catastrophe modelling and property insurance, benefiting the process of pricing, reserving and setting policy limits. The modelling of other aggregate risks such as supply chain interruption, liability risks or cyber, also benefit from quantum computing capabilities.

The insurance industry has many legacy systems holding data as they implement all the security measures needed to protect against quantum threats while maintaining data integrity. Data hygiene is the mitigator of certain cyber-attacks such as using data exchange platforms as back up. The cloud is the foundation for the successful application of quantum computing. Insurers need to strengthen cloud adoption and optimize the way they leverage the cloud to collect data in preparation for using quantum computing. The more cloud adoption, the more opportunities to collect data produced by workflows happening across the digital world.

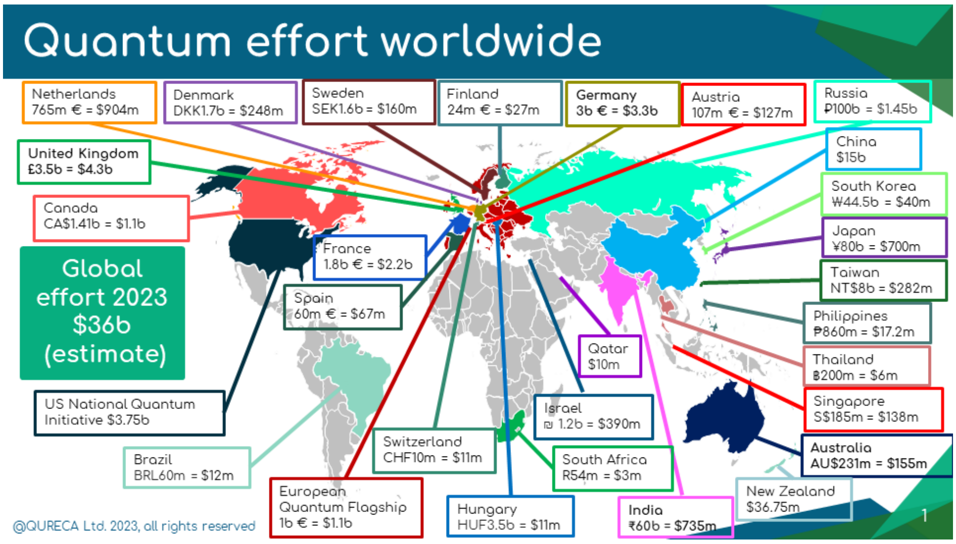
A lack of experts applying quantum mechanics and quantum computing in actuarial mathematics settings is a barrier to entry as using principles of quantum mechanics in insurance research is very recent, however most hurdles will be overcome in 10 years and education now is paramount in universities and internal company education.

Global progress

The quest for a quantum computer is a ‘quantum race’ with competition at the nation level as well as global companies. This has increased intensity in recent years, with new private player entrants, grants from governments, and the emergence of start-ups backed by venture capital. As scientists, engineers and PhD’s race to access the calculating power of quantum computers, cryptographers in parallel are developing new encryption standards to prevent quantum computers falling in the hands of bad actors for malware purposes. The history of quantum computing has an embryonic cord to quantum physics. Physicists 40 years ago were finding that simulations calculated on classical computers were ineffective leading to the conclusion that an accurate simulation of quantum mechanics would require a processor that could work on the basis of quantum physics and closer to the laws of nature.

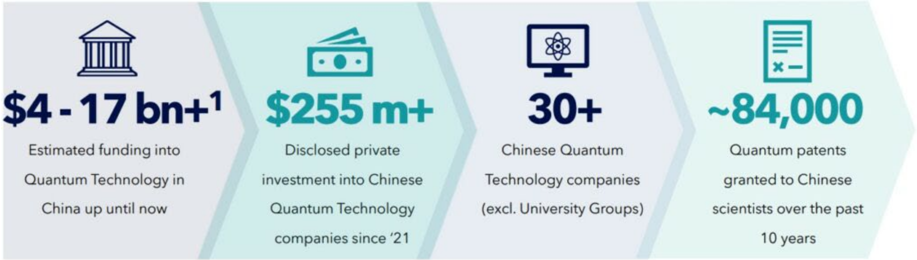
Since the 1990s, scientists globally have been working on quantum computing development. Germany has their own Quantum Alliance[xxxv] and in mid-June 2021, the first German quantum computer went into operation[xxxvi]. German multinational reinsurance company, Munich RE, is one of the founding members of the country’s Quantum Technology & Application Consortium. [xxxvii]

The US and China dominate government spending and private investments in quantum technologies followed by Germany, France, UK, Canada, India, Israel but the Netherlands are a leading investor in quantum as a percentage of gross domestic product. Total global government investments are estimated at the equivalent of 36 billion U.S. dollars for 2023 compared to 1.6 billion U.S. dollars in 2015[xxxviii]. NATO has developed the Niels Bohr Institute[xxxix] in Copenhagen as an incubator accelerator for use of quantum in defense. The US launched the Quantum Alliance Initiative in 2018[xl] to establish clear thought leadership in quantum computing as a crucial area of information technology for mankind. QURECA[xli] has an excellent map to show the quantum effort worldwide.



Source: https://qureca.com/

A 21st-century technology race has evolved between the West and China on emerging technologies. Geopolitical risks straining global supply chains have prompted China to seek technological sovereignty in semiconductors, quantum technology, AI, and blockchain. Chinese state funding in quantum doubles the EU commitment and four times that of the US.



$4 - 17 bn+[1]
Estimated funding into Quantum Technology in China up until now

$255 m+
Disclosed private investment into Chinese Quantum Technology companies since '21

30+
Chinese Quantum Technology companies (excl. University Groups)

~84,000
Quantum patents granted to Chinese scientists over the past 10 years

Source: Quantum Technology in China

Different economic models underpin China, and the US as China has significantly higher public spending beyond research and development compared to the US where private investments in quantum technologies, research, and start-ups are much higher. China's public spending on quantum exceeds the US fourfold. China accounts for over 50% of the estimated global public investment in quantum allocated to research with quantum companies. Because of the rising geopolitics in the technology war, nations are turning protectionist in national strategy including the US, as the race to quantum supremacy commences. This dashes ambitions about collaboration to speed up quantum research and to address the talent shortage in the field.

The UK has a national quantum technologies program with a National Quantum Computing Center[xlii] plus a Regulatory Horizons Council[xliii] to set standards and be quantum ready. Work is in progress to develop a quantum clock at the size and scale required for a net zero smart grid and the first scalable noise adjusted quantum computer using private public partnerships with a government contribution of 2.5 billion pounds sterling.

The Australian government released a national quantum strategy to fund the build of quantum technologies. The Centre for Quantum Software and Information[xliv] at the University of Technology Sydney is working with DARPA[xlv] in the US on its quantum benchmarking program which assesses the performance of quantum computing algorithms. Australia is a founding partner of the Entanglement Exchange[xlvi].

Canada launched a National Quantum Strategy in January 2023 [xlvii]. As a large country with low population densities where the distance between cities can exceed 300 kilometers (outside QKD limits), they need trusted network nodes using satellite technology and the use of quantum repeaters to ensure entanglement, measurement and data integrity.

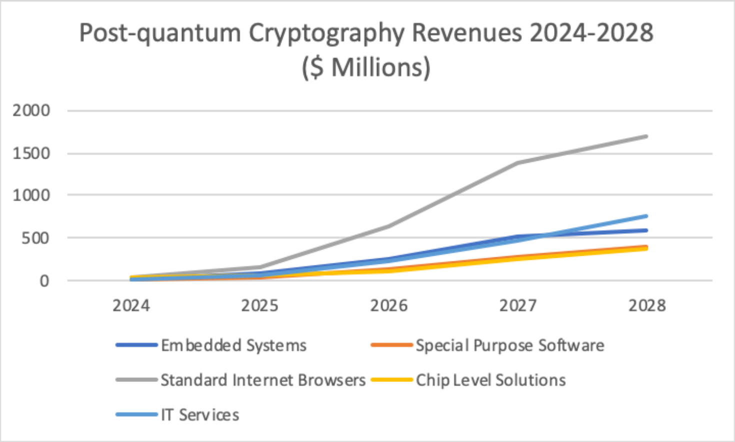
Quantum Internet Alliance[xlviii] is a European consortium formed to build a clock synchronized Quantum Internet in the cloud to enable quantum communication between any two points on earth based on QKD where sensitive information is protected from eavesdropping even if the eavesdropper has a quantum server in the cloud.

A year after Google AI Quantum announced Sycamore Quantum[xlix] achieving 53 Qubits with a declaration of quantum supremacy which was hotly debated, China announced they overtook Google with two quantum computers named Zuchongzhi[l] (66 qubits superconductor quantum computer) and Jiuzhang[li] 2.0 (photonic quantum computer). An important sidenote is Google's Sycamore consumes 26 kilowatts of electrical power, less than a supercomputer and runs a quantum algorithm in seconds. Although good progress it will be several decades before quantum computers are available to everyone. However, prototypes are running in research facilities, proving that the theory of quantum computers works in practice such as quantum pioneer D-Wave Systems[lii], IBM, Google, Microsoft, Honeywell and Alibaba. Different manufacturers of quantum computers work with different technical approaches. Performance is looked at by the number of qubits, the error rate and the extent of entanglement. All processors are error-prone and work in isolation from any environmental interference, however quantum computing power is available in the cloud via the Internet.

Conclusions

Quantum computing is a moving target. Success may hinge on collaboration to create awareness of what quantum technologies can achieve. Quantum computers capable of solving complex problems far beyond the capacity of classical computers are conservatively 10-15 years away but this timeframe will surely shrink. Post-quantum-cryptography triggered a race to revamp classical encryption in preparation for quantum computers. Our digital societies must be able to withstand a quantum computer threat. Algorithms must be available that make classical computers resistant to quantum hacking without requiring enterprises to replace their classical encryption infrastructure. One recent report[liii] estimates that the market for post quantum security technology will rise from around $200 million today to $3.8 Billion as the quantum threat develops as shown below.

.



The claim that quantum computing is years away from being useful is not factual. Although most quantum hardware is still in the labs, hybrid models allow applications to be hosted by quantum software and simulators in the cloud as a service. Algorithms for optimization, simulations and machine learning are already available. Error correction will bring the utility of quantum computing sooner than anticipated. From carbon sequestration to electrolysis of water and the invention of new batteries, quantum computing has the potential to harness nature to help reverse climate change. Communities need to be educated early so they can reach quantum competency from different angles and help such as building applications and web interfaces and be part of the development via open source.

Barriers to entry are shown below all of which are being addressed today -

- Quantum error correction and environmental sensitivity.
- Post-quantum cryptography is a national security concern.
- Quantum-powered AI could create unintended consequences.

Quantum is a deep technology so long-term thinking is a must. Straight out of the starting blocks are use cases for consumer engagement and commercial access. Firstly, **Quantum advantage** needs to be achieved which is the demonstrated ability for a quantum computer to outperform a classical computer by an order of magnitude, achieving results in minutes that would otherwise take millions of years to complete. A million qubits are needed for quantum advantage and so far, only 1000 has been achieved. Next stages are to higher qubits which are expensive requiring super cooling and error correction to control the quantum particles (qubits). Secondly, **Quantum utility** needs to be reached which shows improved outcome to the status quo through the application of quantum technology, reaching a state of heterogeneity where quantum accelerator technology sits alongside classical computers. This will make quantum computing more accessible by aggregating access to quantum compute capability, delivering tools for software developers/researchers, providing a platform with access to a catalog of quantum solutions and AI. This needs to stay engaged in hybrid fashion to classical compute devices such as a NVIDIA[liv] GPU. Quantum computers then become general purpose computing devices in the same way as GPU. Finally, the state of **Quantum Supremacy** is sought by all nations and large companies from the point of view of computing power and the ability to calculate faster.

While maintaining healthy competition, it is hoped that collaboration will occur making quantum supremacy a shared success because climate change, new drugs, new energy sources and supply chain optimizations need this technology. It would be ironic to create a quantum divide before the digital divide which still exists in emerging and rural communities, though leapfrog could be beneficial. The number of quantum algorithms is growing, and material innovations are critical to enable practical applications. With advanced materials, quantum technologies offer functionalities such as superconductivity and manipulation of quantum information. Promising host materials for quantum systems include silicon, diamond, rare-earth minerals and many more.

As data volume increases, quantum computing can make better predictions about where markets are going. Quantum computing is already used for risk assessment in the financial industry for sales forecasting and financial market behaviour. Quantum computing will change the way we use data, adding exponential value to the data that's already being collected through cloud-based technology. Quantum software as a service is available in the cloud to keep the costs down and make technology available to all.

Quantum computing is a revolutionary technology that could allow for precise molecular-level simulation and a deeper understanding of nature's basic laws. McKinsey estimates the quantum computing market to be worth anywhere between 9 billion and 93 billion, quantum sensing 1 to 7 billion and quantum communications 1 to 6 billion from investment perspective[lv]. The market opportunity is high as is the technical risk. Those who do not understand how quantum computers work because of the in depth physics will soon appreciate that quantum computers solve very complex known problems in a short amount of time with high accuracy and they will be using quantum computing in their daily lives under the hood without knowing the technology, just like the telephone and Internet in the past.

REFERENCES

[i] https://en.wikipedia.org/wiki/Richard_Feynman

[ii] https://www.nature.com/articles/nphys2258

[iii] https://thelephant.io/the-quantum-computing-market/

[iv] https://aws.amazon.com/what-is/quantum-computing/#:~:text=Quantum%20computing%20is%20a%20multidisciplinary,hardware%20research%20and%20application%20development.

[v] https://generativeai.net/

[vi] https://www.un.org/en/climatechange/cop26

[vii] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-just-might-save-the-planet#:~:text=Quantum%20computing%20could%20be%20a,the%201.5°C%20target.

[viii] https://scienceexchange.caltech.edu/topics/quantum-science-explained/entanglement

[ix] https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-superposition#:~:text=When%20an%20electron%20is%20in,in%20two%20places%20at%20once.

[x] https://www.symmetrymagazine.org/article/what-is-a-photon?language_content_entity=und

[xi] https://docs.dwavesys.com/docs/latest/c_gs_2.html

[xii] https://iopscience.iop.org/article/10.1088/0034-4885/76/7/076001/meta

[xiii] https://www.youtube.com/watch?v=uLnGp1WTNFQ

[xiv] https://thequantuminsider.com/2023/03/13/what-is-nisq-quantum-computing/

[xv] https://ionq.com/resources/what-is-hybrid-quantum-computing

[xvi] https://www.ibm.com/cloud/blog/what-is-quantum-safe-cryptography-and-why-do-we-need-it

[xvii] https://www.evolutionq.com/

[xviii]https://www.techtarget.com/searchsecurity/definition/RSA#:~:text=RSA%20is%20a%20type%20of,is%20used%20to%20decrypt%20it

[xix] https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD

[xx] https://onlinelibrary.wiley.com/doi/abs/10.1002/sat.1392

[xxi] https://spectrum.ieee.org/amp/ibm-condor-2658839657

[xxii] https://en.m.wikipedia.org/wiki/Shor%27s_algorithm

[xxiii] https://www.nist.gov/

[xxiv] https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard#:~:text=The%20Advanced%20Encryption%20Standard%20(AES)%20is%20a%20symmetric%20block%20cipher,cybersecurity%20and%20electronic%20data%20protection

[xxv] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[xxvi] https://en.wikipedia.org/wiki/Trust_anchor

[xxvii] https://www.techtarget.com/searchenterpriseai/definition/generative-AI

[xxviii] https://en.m.wikipedia.org/wiki/Moore%27s_law

[xxix] https://www.gpsworld.com/the-role-of-atomic-clocks-in-data-centers/#:~:text=The%20atomic%20clock%20time%20transmitted,transmitted%20time%20is%20not%20available

[xxx] https://encyclopedia.pub/entry/34723

[xxxi] https://www.linkedin.com/pulse/why-we-need-quantum-digital-twins-ian-gordon

[xxxii] https://www.osti.gov/servlets/purl/1640593?ref=blog.taurushq.com

[xxxiii] https://cointelegraph.com/news/quantum-miners-would-yield-massive-energy-savings-for-blockchain-study

[xxxiv]https://www.internationalinsurance.org/insights_cyber_embedded_artificial_intelligence_in_financial_services

[xxxv] https://www.quantum-alliance.de/

[xxxvi] https://www.allaboutcircuits.com/news/ibm-accelerates-germany-as-a-quantum-hub-with-eus-first-quantum-computer/

[xxxvii] https://www.qutac.de/?lang=en

[xxxviii] https://qureca.com/quantum-initiatives-worldwide-update-2023/

[xxxix] https://phys.org/partners/niels-bohr-institute/

[xl] https://www.hudson.org/policy-centers/quantum-alliance-initiative

[xli] https://qureca.com/

[xlii] https://www.nqcc.ac.uk/

[xliii] https://www.gov.uk/government/groups/regulatory-horizons-council-rhc

[xliv] https://www.qcaustralia.org/

[xlv] https://en.wikipedia.org/wiki/DARPA

[xlvi] https://entanglementexchange.org/

[xlvii] https://www.canada.ca/en/innovation-science-economic-development/news/2023/01/government-of-canada-launches-national-quantum-strategy-to-create-jobs-and-advance-quantum-technologies.html

[xlviii] https://quantum-internet.team/

[xlix] https://en.m.wikipedia.org/wiki/Sycamore_processor

[l] https://tadviser.com/index.php/Product:Zuchongzhi_(quantum_computer)

[li] https://www.scmp.com/news/china/science/article/3223364/chinese-quantum-computer-180-million-times-faster-ai-related-tasks-says-team-led-physicist-pan

[lii] https://www.dwavesys.com/

[liii] https://www.globenewswire.com/news-release/2019/01/10/1686297/0/en/Market-for-Post-Quantum-Cryptography-Software-and-Devices-to-Reach-3-9-billion-by-2028.html

[liv] https://www.nvidia.com/en-us/

[lv]https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20funding%20remains%20strong%20but%20talent%20gap%20raises%20concern/quantum-technology-monitor.pdf

6.2023

David Piesse
CRO of Cymar

About the Author:
David Piesse is CRO of Cymar. David has held numerous positions in a 40-year career including Global Insurance Lead for SUN Microsystems, Asia Pacific Chairman for Unirisx, United Nations Risk Management Consultant, Canadian government roles and staring career in Lloyds of London and associated market. David is an Asia Pacific specialist having lived in Asia 30 years with educational background at the British Computer Society and the Chartered Insurance Institute.