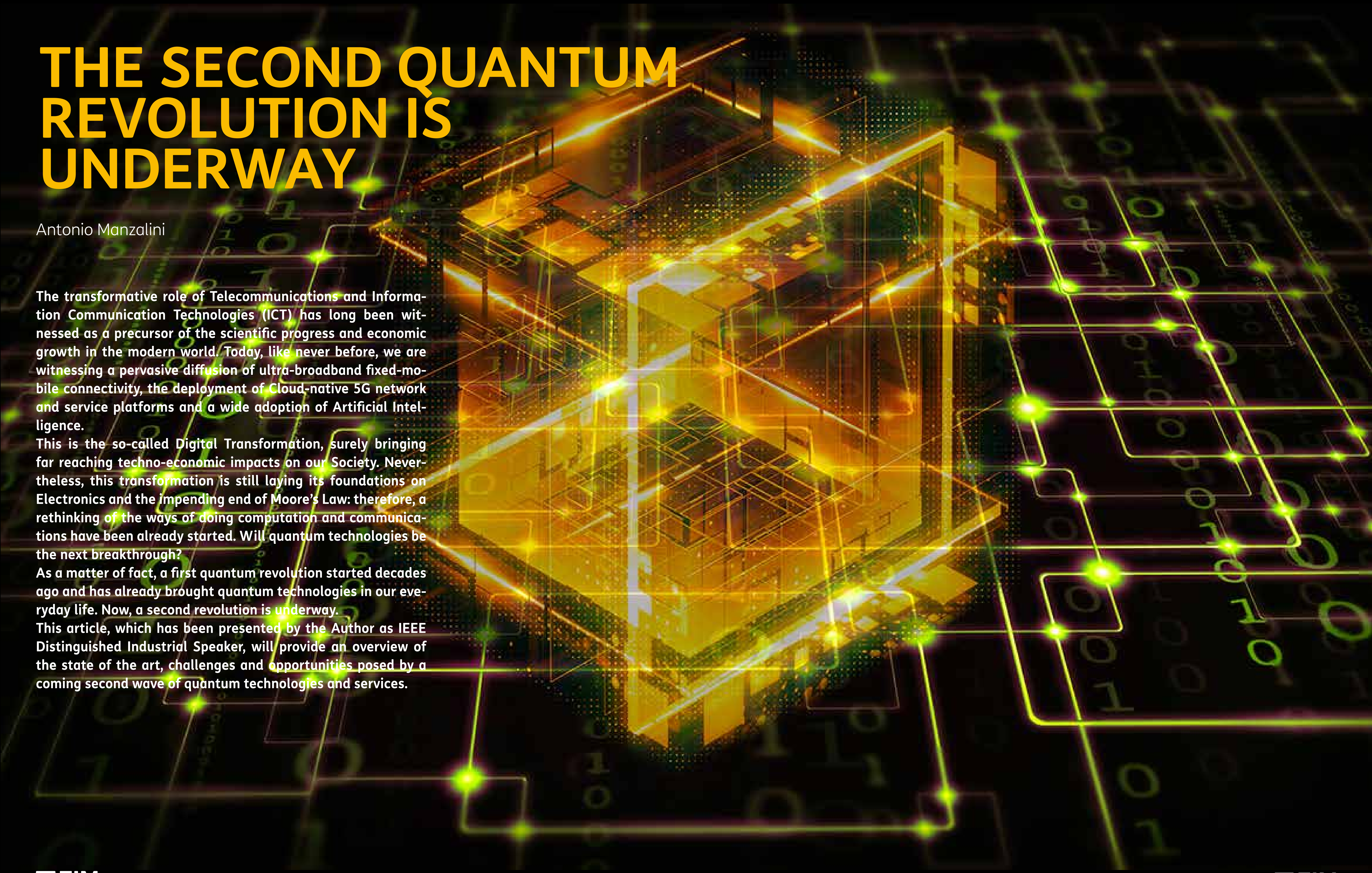


THE SECOND QUANTUM REVOLUTION IS UNDERWAY

Antonio Manzalini

The transformative role of Telecommunications and Information Communication Technologies (ICT) has long been witnessed as a precursor of the scientific progress and economic growth in the modern world. Today, like never before, we are witnessing a pervasive diffusion of ultra-broadband fixed-mobile connectivity, the deployment of Cloud-native 5G network and service platforms and a wide adoption of Artificial Intelligence.
This is the so-called Digital Transformation, surely bringing far reaching techno-economic impacts on our Society. Nevertheless, this transformation is still laying its foundations on Electronics and the impending end of Moore's Law: therefore, a rethinking of the ways of doing computation and communications have been already started. Will quantum technologies be the next breakthrough?
As a matter of fact, a first quantum revolution started decades ago and has already brought quantum technologies in our everyday life. Now, a second revolution is underway.
This article, which has been presented by the Author as IEEE Distinguished Industrial Speaker, will provide an overview of the state of the art, challenges and opportunities posed by a coming second wave of quantum technologies and services.

Quantum technologies are already here

Today, Software Defined Network (SDN) and Network Function Virtualization (NFV) are offering the opportunity of designing and operating 5G infrastructures with unprecedent flexibility. In fact, an orchestrated use of Cloud, Edge-Fog computing and network virtual resources can deliver a continuum of capabilities, functions and microservices through the so-called 5G Cloud-native infrastructures.

Sustainability of future network scenarios will have to face several techno-economic challenges, such as: the transmission and processing of enormous, and increasing, quantity of data with ultra-low latencies, automation of management and control processes, the fulfilment of the strict requirements of resilience, security and privacy, optimization of energy consumption, and so on.

Indeed today we are living a Digital Transformation, bringing far reaching techno-economic impacts on our Society. Nevertheless, this transformation is still laying its foundations on Electronics and the impending end of Moore's Law: therefore, a rethinking of the ways of doing computation and communications have been already started. Will quantum technologies be the next breakthrough?

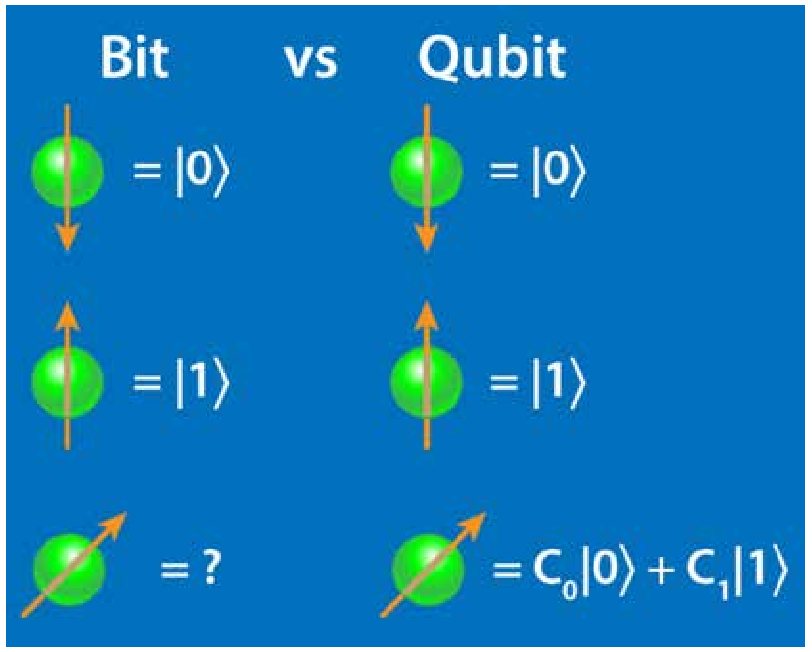
As a matter of fact, a first quantum revolution started decades ago and has already brought quantum technologies in our everyday life. Chips for computers and smart-phone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc. are all based on technologies exploiting the quantum mechanics principles.
Now a second revolution seems to be underway: in fact, there is a new impressive grow of interests for quantum, with several investments from public and private organizations worldwide (see Box 1) targeting new horizons of applications. In particular, there are three quantum phenomena, well known and well tested in Physics, which are not fully exploited yet by Industry.
These phenomena are: superposition, entanglement and measurement.

- Superposition concerns the property of quantum objects to stay in linear combination of multiple states until they are observed.
- Entanglement is defined as the possibility that two or more quantum objects to stay intrinsically linked, into an intertwined composite state, regardless of how far apart the objects are from one another. Recently hyper-entanglement has been discovered, defined as the entanglement in multiple degrees of freedom (DOFs) of a quantum system, such as polarization, spatial-mode, orbit-angular-momentum, time-bin and frequency DOFs of photons.
- Measurement regards the collapse and disruption of a quantum state from coherent probabilistic superposition state into a discrete one.

When quantum technologies will become mature enough to control and exploit these three phenomena, then there will be the impact of this second revolution over many markets, ranging from Telecom and ICT, to Medicine, to Finance, to Transportation, and so on. Significant work is still needed but, in light of the potential opportunities and threats of this second revolution, a lot of investments are being made worldwide.

Bits, Qubits and Quantum Gates

As a digital system manipulates Bits, a quantum system manipulates Qubits. A Qubit is the well-known basic unit of quantum information. A Qubit can be coded by a quantum system having two-states (or two-levels), for example: the spin of an electron (spin up and spin down).
Photons are special qubits in that they possess several independent properties such as polarization, spin angular momentum or orbital angular momentum. These degrees of freedom can all be employed to encode quantum information. The number of accessible qubits can be increased beyond the number of particles by the simultaneous entanglement of multiple photons and multiple degrees of freedom (hyperentanglement). The three degrees of freedom of six photons, for example, can provide control over an 18-qubit ensemble.



1
Bits vs quantum bits (qubits)

A weird and remarkable property of quantum information is that a qubit can stay simultaneously with two values 0 and 1 (superposition of states), until it collapses, for example when a measurement is made.
In other words, while a Bit is either 0 or 1, a qubit can be seen as a linear combination of the two states (0, 1) with coefficients which are complex numbers. This allows representing the interactions between quantum states in terms of constructive and destructive interference of quantum information waves.

This means that two qubits can be in a superposition of four states, three qubits can be in a superposition of eight states... and so on. Therefore, generalizing while N bits can take one of 2N possible permutations, N qubits can stay in a superposition of all 2N possible permutations. This have remarkable consequences in computation.

A quantum register - associated to N qubits - may have a state which is the superposition of all 2N values simultaneously: therefore, by applying a quantum operation to the quantum register would result in altering all 2N values at the same time. This property allows quantum computers to elaborate qubits with "a sort of parallel computation" reducing the processing time (from exponential to polynomial time) for solving certain complex problems.
In general, there are two main classes of quantum computers: analog and gate-based.

Analog quantum computers include annealers, adiabatic computers, i.e., systems which solve problems by directly manipulating the interactions between qubits rather than breaking actions into more abstract gate operations.

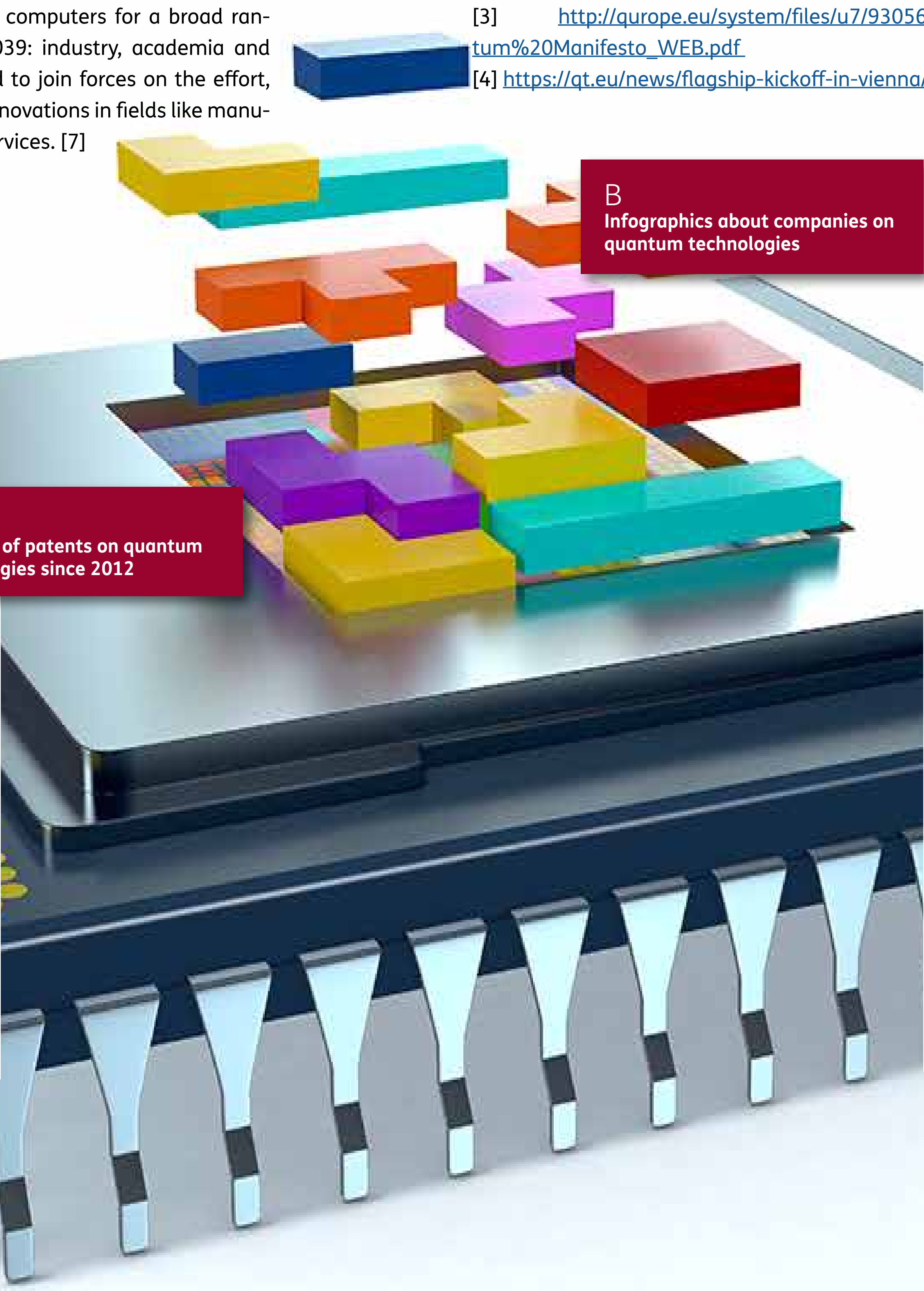
Gate-based quantum computers, sometimes referred to as universal quantum computers, use logical gate operations (AND, OR, etc.) on qubits. Quantum logic gates are the building blocks of quantum circuits:

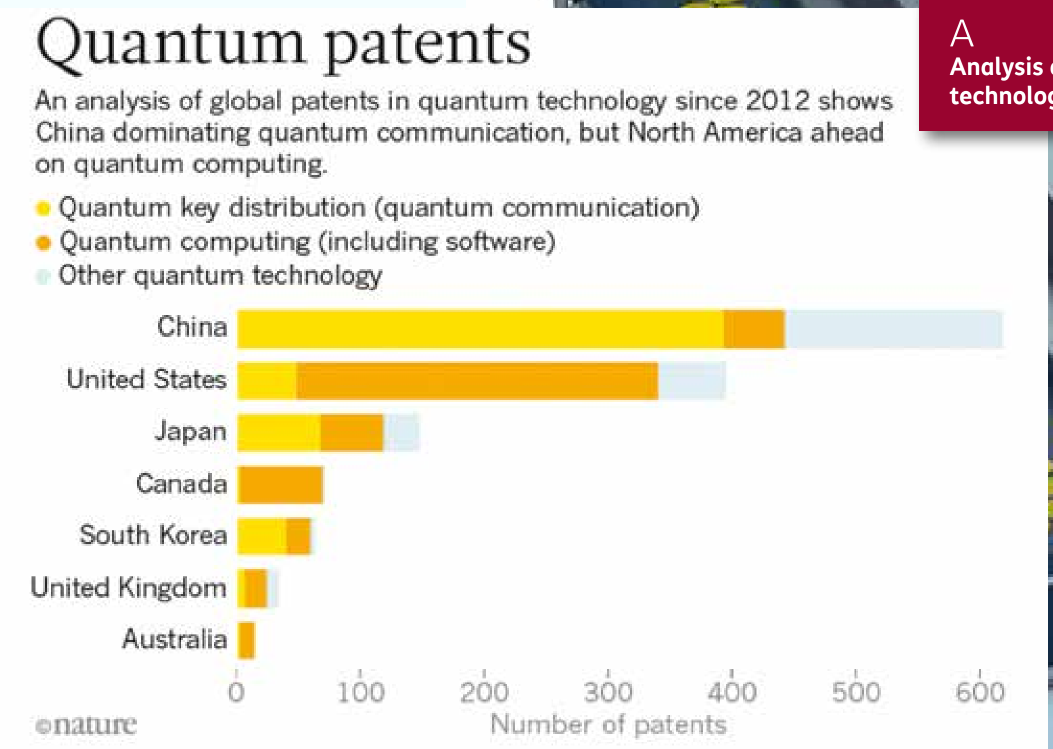
A growing interest on Quantum

We are witnessing increasing efforts and investments on innovation activities about quantum technologies and services. Notable examples of industries include: Microsoft, IBM, HP, Toshiba, Google, Intel, Alibaba, Tencent, Baidu, but also several Network Operators.

According to a new report from McKinsey & Partners, in partnership with the Viva Technology show, that quantum technologies will have a global market value of $1 trillion by 2035 [1]. The Journal Nature recently published [2] an overview about published patents on quantum methods and systems and the development of start-ups. Data and information have been extracted from various market-research websites and consultancy reports.

Also, public and governative sectors are announcing investments. European Commission has launched a €1 billion Flagship Initiative in Quantum Technology, starting in 2018 within the European H2020 research and innovation framework programme [3], [4]. U.S. Government has enacted legislation to coordinate and accelerate U.S. quantum research and development [5]. China has announced plans to spend more than $10 billion to build a national laboratory for quantum science, to open in 2020 [6]. Japan will aim to develop full-fledged quantum computers for a broad range of uses by around 2039: industry, academia and government are expected to join forces on the effort, which promises to yield innovations in fields like manufacturing and financial services. [7]




Quantum patents
An analysis of global patents in quantum technology since 2012 shows China dominating quantum communication, but North America ahead on quantum computing.
● Quantum key distribution (quantum communication)
● Quantum computing (including software)
● Other quantum technology
China
United States
Japan
Canada
South Korea
United Kingdom
Australia
0
100
200
300
400
500
600
Number of patents
©nature

A
Analysis of patents on quantum technologies since 2012

References

[1] https://www.consultancy.uk/news/24361/quantum-computing-market-to-reach-1-trillion-by-2035

[2] Quantum gold rush: the private funding pouring into quantum start-ups – Nature News Features 02nd October 2019 available at https://www.nature.com/articles/d41586-019-02935-4

[3] http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf

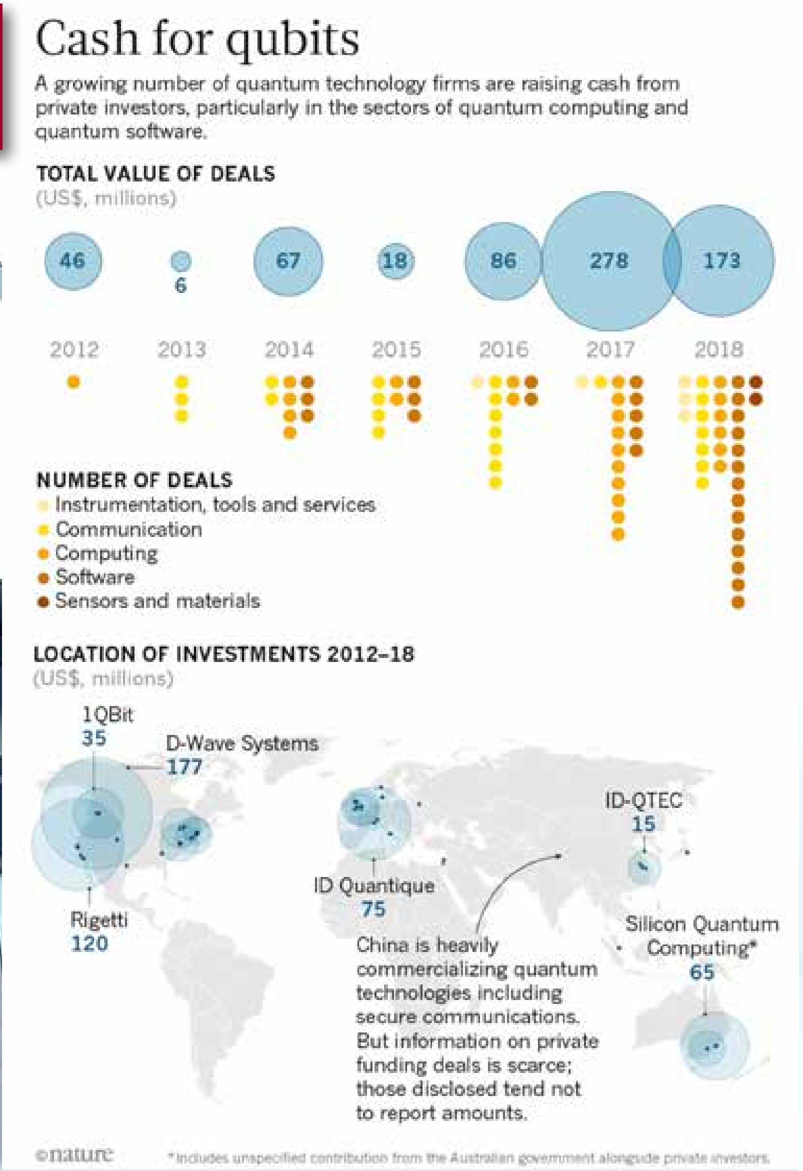
[4] https://qt.eu/news/flagship-kickoff-in-vienna/

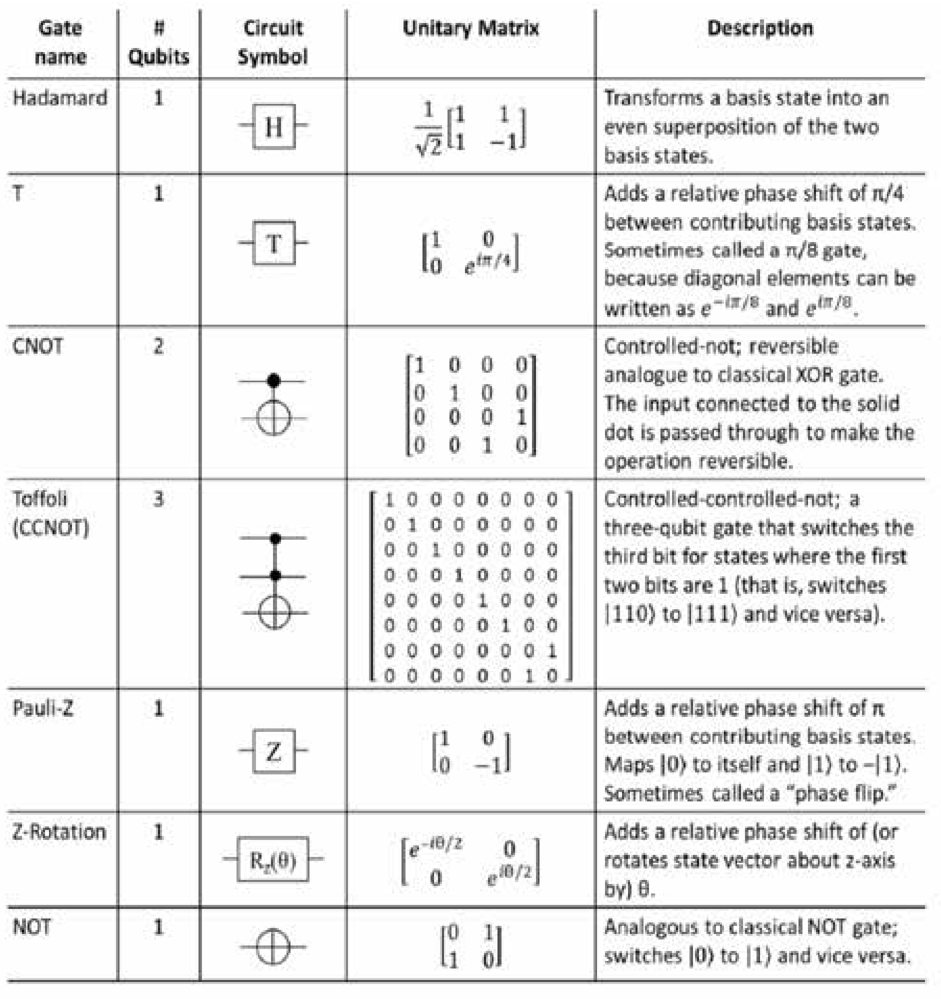
[5] https://www.computer.org/csdl/magazine/co/2019/10/08848174/1dAq2PvlBkI

[6] https://www.economist.com/business/2018/08/18/the-race-is-on-to-dominate-quantum-computing?cid1=cust/ednew/n/bl/n/2018/08/16n/owned/n/n/nwl/n/n/EU/144433/n

[7] https://asia.nikkei.com/Business/Technology/Japan-plots-20-year-race-to-quantum-computers-chasing-US-and-China

B
Infographics about companies on quantum technologies





Gate name	# Qubits	Circuit Symbol	Unitary Matrix	Description
Hadamard	1	H	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$	Transforms a basis state into an even superposition of the two basis states.
T	1	T	$\begin{bmatrix}1 & 0\\0 & e^{i\pi/4}\end{bmatrix}$	Adds a relative phase shift of π/4 between contributing basis states. Sometimes called a π/8 gate, because diagonal elements can be written as $e^{-i\pi/8}$ and $e^{i\pi/8}$.
CNOT	2	● ⊕	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$	Controlled-not; reversible analogue to classical XOR gate. The input connected to the solid dot is passed through to make the operation reversible.
Toffoli (CCNOT)	3	● ● ⊕	$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$	Controlled-controlled-not; a three-qubit gate that switches the third bit for states where the first two bits are 1 (that is, switches $\|110\rangle$ to $\|111\rangle$ and vice versa).
Pauli-Z	1	Z	$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$	Adds a relative phase shift of π between contributing basis states. Maps $\|0\rangle$ to itself and $\|1\rangle$ to $-\|1\rangle$. Sometimes called a "phase flip."
Z-Rotation	1	$R_z(\theta)$	$\begin{bmatrix}e^{-i\theta/2} & 0\\0 & e^{i\theta/2}\end{bmatrix}$	Adds a relative phase shift of (or rotates state vector about z-axis by) θ.
NOT	1	⊕	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	Analogous to classical NOT gate; switches $\|0\rangle$ to $\|1\rangle$ and vice versa.

2
Quantum Logic Gates

for example, CNOTs and unitary single qubit operations form a universal set of quantum computing.

It should be mentioned that it is also possible to simulate quantum–gates computers by using classical computers. There exists a variety of software libraries that can be used, each with different purposes: a comprehensive list of tools is available on Quantiki [1].
Simulation can be made, for instance, using OpenCL (Open Computing Language) [2] which is a general-purpose framework for heterogeneous parallel computing on standard hardware, such as CPUs, GPUs, DSP (Digital Signal Processors) and FPGAs (Field-Programmable Gate Arrays).

There are multiple ways to build gate-based quantum computers manipulating qubits.

Table 1 provides an overview (not exhaustive): superconductors and trapped ions are presently the most advanced implementations [3].

Quantum Algorithms and Software

Most of the optimization problems in the fields of ICT and Telecommunications are currently solved with algorithms for finding suboptimal solutions, because of the excessive cost of finding an optimal solution.

Some of these problems includes: e.g., network planning, joint optimization of multiple functions, such as radio channel estimation, data detection and synchronization, Data Center resources and energy optimization.

Today, Quantum annealers (e.g., D-Wave) are already being used to solve some combinatorial and optimization problems. Nevertheless, quantum annealers are not properly quantum computers: they are specialized computing systems based on quantum heuristics.

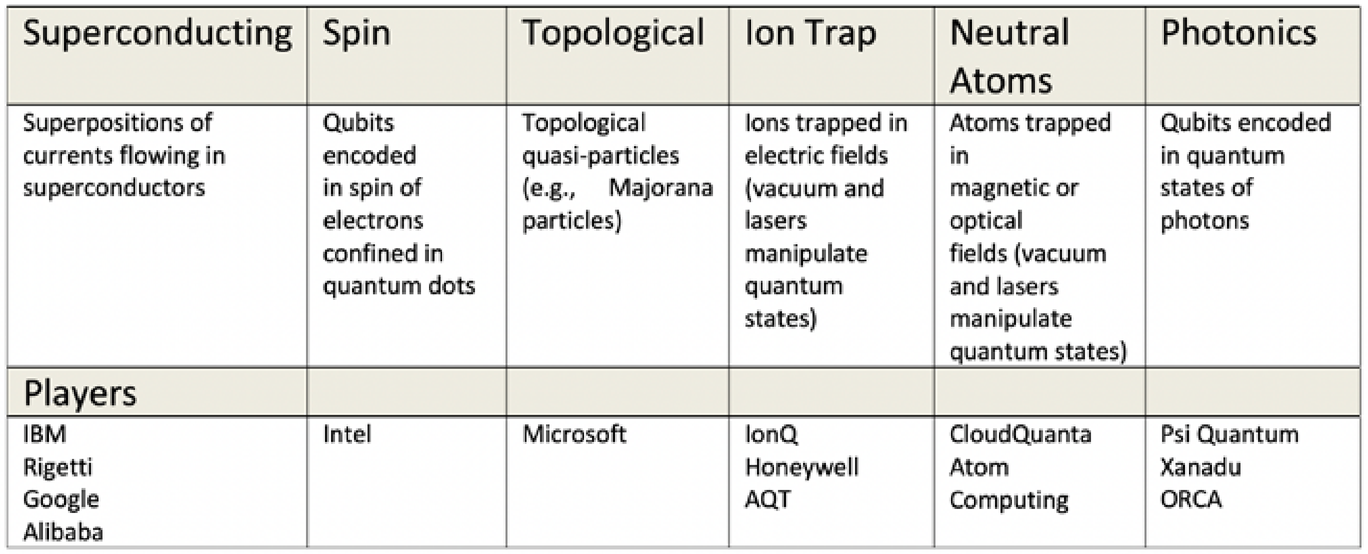
In most cases, the problem to be solved is encoded into an Ising-type Hamiltonian, which is then embedded into a quantum hardware graph to be solved by a quantum annealer.

Gate-based quantum computers use another approach. For instance, figure 3 shows the comparison of the two approaches for the execution of quantum algorithms workflows. In the gate-based approach the problem is formulated in a way for selecting a proper quantum algorithm. Then the quantum algorithm is transformed in a quantum circuit (i.e., using quantum gates) which is either executed on a quantum processor or simulated.

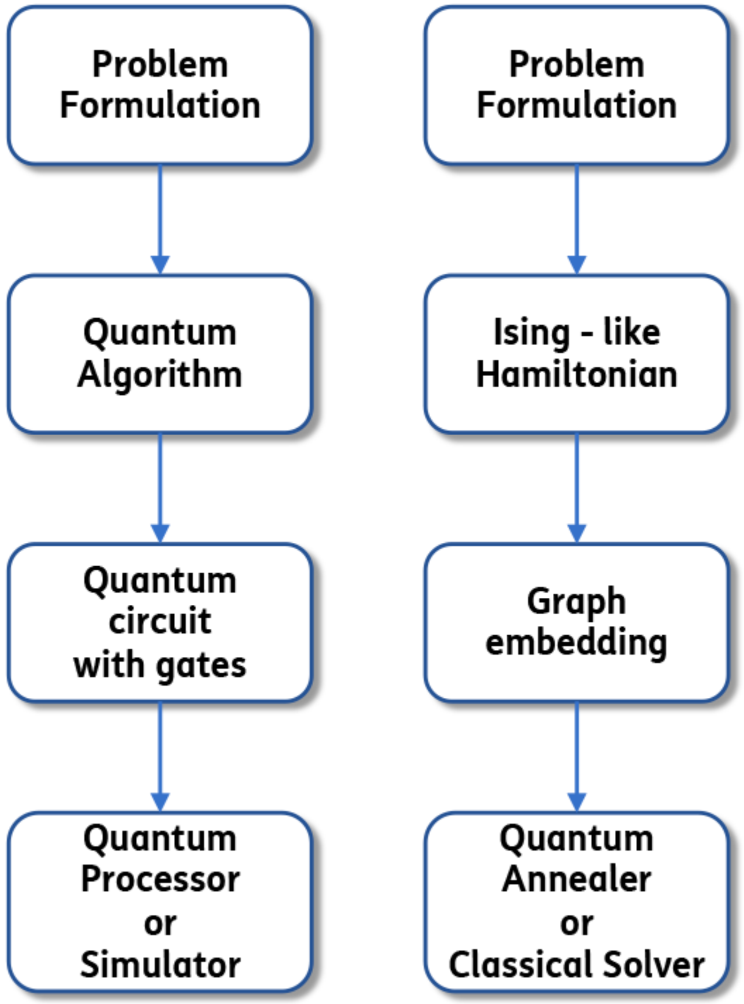
In both cases, random fluctuations (e.g., heat or quantum-mechanical phenomena), could occasionally flip or randomize the state of qubits: this is introducing errors and potentially derailing the validity of the calculations. This is why many of these quantum systems require special vacuum environments, the adoption of cryogenic systems and error corrections methods. In particular, quantum error correction involves a substantial multiplication of resources: the number of physical qubits required may be orders of magnitude greater than the number of error-free logical qubits seen by the algorithm.

In general, we may say that there are two main classes of quantum algorithms, derived as generalization from the Shor's algorithm for factoring (capable of breaking a lot of public-key cryptography) and the Grover algorithm for searching. The website "Quantum Zoo" [4] has gathered a comprehensive list of said classes of algorithms, briefly describing their operation.

Table 1
Examples of gate-based approaches for developing quantum computers



Superconducting	Spin	Topological	Ion Trap	Neutral Atoms	Photonics
Superpositions of currents flowing in superconductors	Qubits encoded in spin of electrons confined in quantum dots	Topological quasi-particles (e.g., Majorana particles)	Ions trapped in electric fields (vacuum and lasers manipulate quantum states)	Atoms trapped in magnetic or optical fields (vacuum and lasers manipulate quantum states)	Qubits encoded in quantum states of photons
Players					
IBM Rigetti Google Alibaba	Intel	Microsoft	IonQ Honeywell AQT	CloudQuanta Atom Computing	Psi Quantum Xanadu ORCA



3
Quantum algorithms workflows: on a gate-model computer (left), on a quantum annealer (right)

It should be mentioned that for near term quantum applications, hybrid quantum/classical algorithms are also very promising.

A common characteristic of these approaches is that the quantum computer is rather simplified: it is only in charge of carrying out a subroutine, acting as a "coprocessor" while the larger scale algorithm is governed by a classical computer. In this case a higher error rate per operation is tolerable.

It may even be possible to implement such quantum algorithms without quantum error correction.
In summary, when comparing quantum algorithms with their classical counterparts, it appears that employing quantum systems specific performance targets may be reached at a lower computational complexity: on the other hand, an analytical demonstration of the levels of efficiency of quantum computers and algorithms in addressing computational complexity require further studies.

Concerning software languages and tools, the scenario is very active but still rather fragmented: the reference [5] provides an overview of open-source software projects and encourages the coalition of larger communities.

Sliq [6] is an example of recent progresses in the definition of a simple and powerful quantum language.

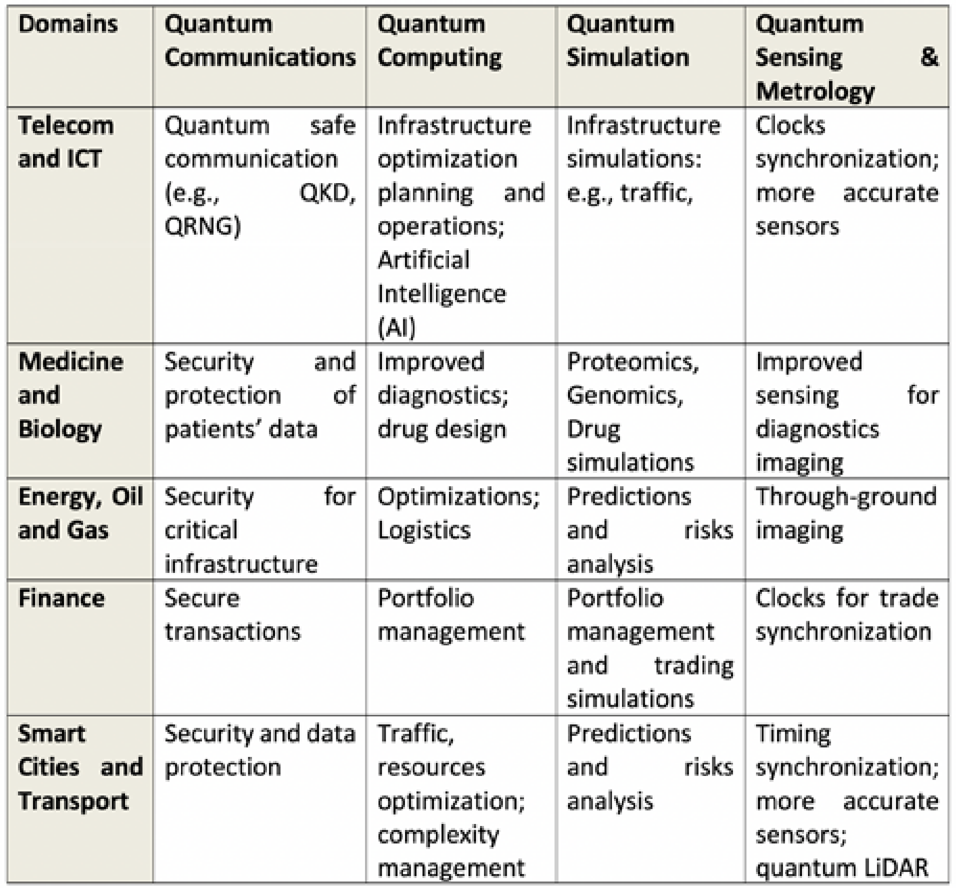
Sliq has been designed to address the challenge to enable Programmers to work at high level of abstraction. An intuitive semantics allows implicitly to drop temporary values, as in classical computation.
Soon we may even expect the emergence of quantum app stores. Not app stores like the one we access with our smartphone, but similar to code repositories, such as GitHub, types of library where quantum software developers make the code they have written available to anyone [7].

For more details see the article by M. Amoretti "Quantum Software", in this volume.
We conclude noting that the interest in quantum software is very high. The number and value of venture capital deals, particularly in quantum software and computing startups, is increasing, reaching a total of 32 deals in 2018 at a total value of US$173 million in 2018 [8].

Application areas for Quantum

International innovation activities and Standardization Bodies are pretty aligned in identifying four main applications areas of quantum technologies and services: commu-

Table 2
Examples of applications for quantum technologies (not exhaustive)



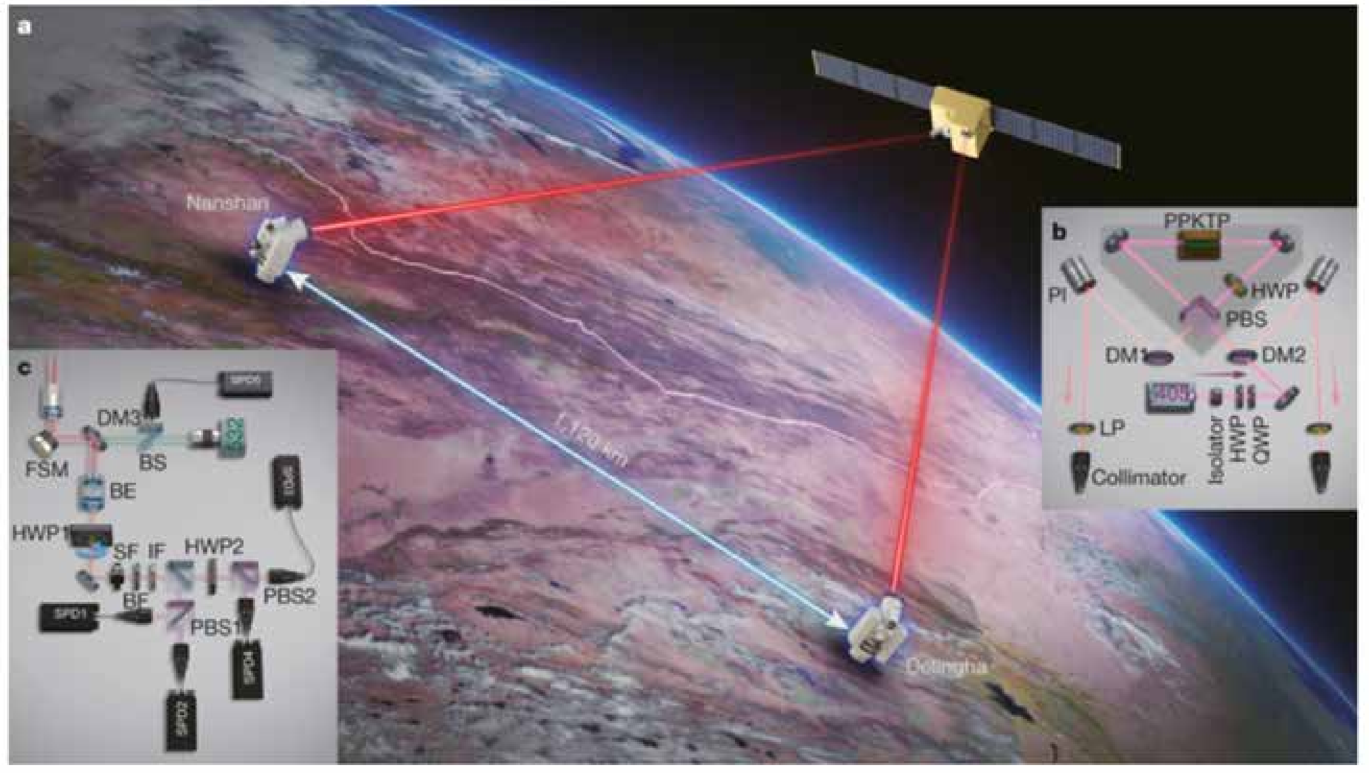
Domains	Quantum Communications	Quantum Computing	Quantum Simulation	Quantum Sensing & Metrology
Telecom and ICT	Quantum safe communication (e.g., QKD, QRNG)	Infrastructure optimization planning and operations; Artificial Intelligence (AI)	Infrastructure simulations: e.g., traffic,	Clocks synchronization; more accurate sensors
Medicine and Biology	Security and protection of patients' data	Improved diagnostics; drug design	Proteomics, Genomics, Drug simulations	Improved sensing for diagnostics imaging
Energy, Oil and Gas	Security for critical infrastructure	Optimizations; Logistics	Predictions and risks analysis	Through-ground imaging
Finance	Secure transactions	Portfolio management	Portfolio management and trading simulations	Clocks for trade synchronization
Smart Cities and Transport	Security and data protection	Traffic, resources optimization; complexity management	Predictions and risks analysis	Timing synchronization; more accurate sensors; quantum LiDAR

Entanglement-based QKD over 1,120 km

Quantum Key Distribution (QKD) is secure way of sharing cryptographic keys between remote users, leveraging on the quantum principles. The potential applications of QKD include not only securing communications networks but also critical infrastructures (for instance, the Smart Grid), transactions of financial institutions and national defense.

QKD has a TRL 7-9: there are some pieces of equipment already commercially available even if as today the distances covered over optical fibres are still relatively limited (about 50 to 80 km) owing to the channel loss that occurs when using optical fibres (or terrestrial free space) that exponentially reduces the photon transmission rate.

Long-distance entanglement distribution can be realized using quantum repeaters: on the other hand, the technology is still immature for practical implementations but there are intensive innovation activities. For example, innovation activities demonstrated the feasibility of QKD over a coiled optical fibre of about 500 km.



In satellite communications, longer distances have been achieved, owing to the negligible photon loss and decoherence experienced in empty space. Therefore, tj satellite-based QKD has the potential to help to establish a global-scale quantum network: for example, a 1,200 km point-to-point QKD has been already demonstrated from a satellite to a ground station, even if with limited efficiency.

Recently [1] entanglement-based QKD has been demonstrated between two ground stations over 1,120 km at a finite secret-key rate of 0.12 bits per second, without the need for trusted relays. In particular, entangled photon pairs were distributed via two bidirectional downlinks from the Micius satellite to two ground observatories in Delingha and Nanshan in China.

Reference

[1] Yin, J., Li, Y., Liao, S. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature (2020). https://doi.org/10.1038/s41586-020-2401-y

nications, computing, simulations, sensing and metrology.

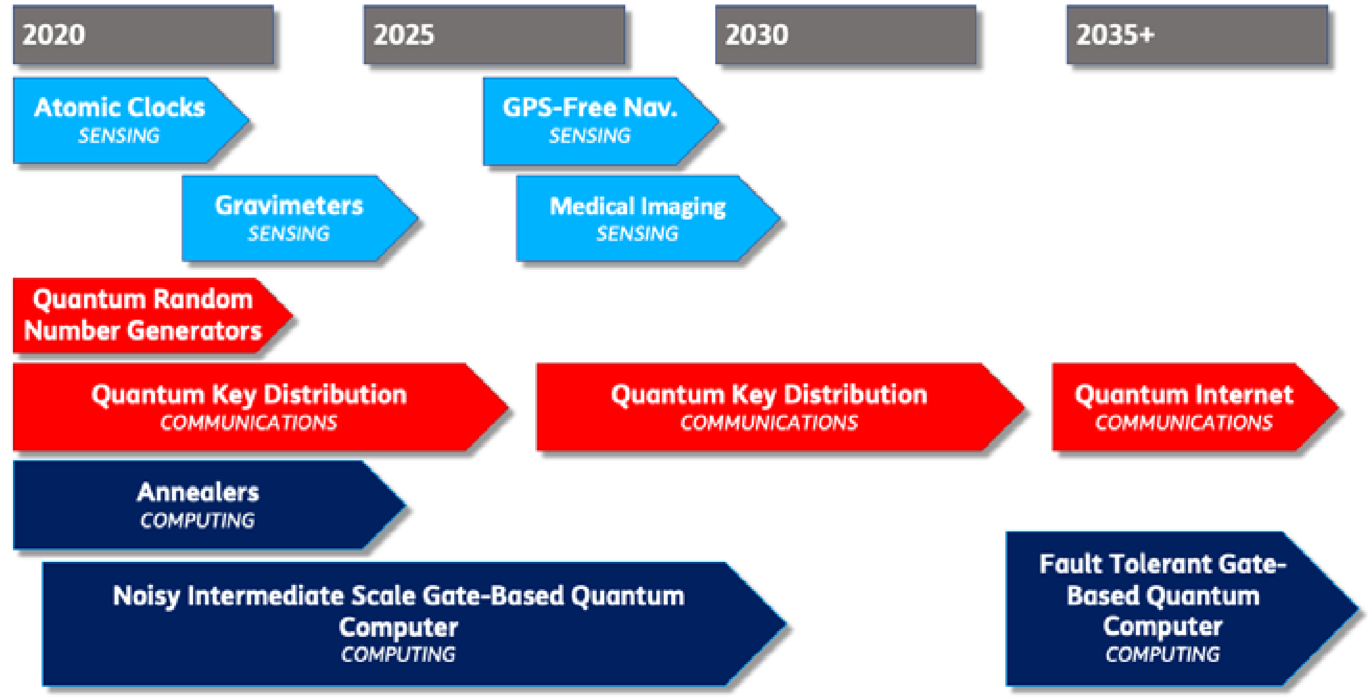
The area of Quantum Communications includes two main sub-domains: the so-called quantum-safe communications and the “teleporting” of qubits (e.g. Quantum Internet, whose TRL is 1-2). Quantum-safe communications leverage on systems such as Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG) which have a TRL 7-9. Regarding the status of the developments of the Quantum Internet see the article by S. Cacciapuoti and M. Caleffi “The Quantum Internet: the next ICT revolution”, in this volume.

Quantum Computing has been already touched in the previous section. The area concerns the exploitation of the three principles of superposition, (hyper)entanglement and measurements, to speed up over classical computers in solving complex optimization and combinatorial problems.

Quantum simulations concerns all those applications where well-controlled quantum systems are used to simulate the behavior of other systems, which are less accessible and more complex for a direct simulation (TRL 6-9). Table 2 provides some examples of applications.
Quantum sensing and metrology includes those applications where high sensitivity of quantum systems to environmental influences can be exploited to measure physical properties and timing with more precision (e.g. magnetic and heat sensors, gravimeters, GPS-free navigators, clocks; TRL is 4-9).

Overall, while some quantum applications are already commercially available today (e.g., QKD and QRNG, quantum annealers, quantum simulations, atomic clocks and some quantum sensors) the current use of the second wave of quantum technologies is still relatively limited. This is due to both technical limitations and tradeoffs between technical performance and costs. Further progresses are needed. On the other hand, international community is recognizing the disruptive potentialities of these technologies in several markets when a breakthrough will be reached.

4
Tentative roadmap for quantum technologies and services [3]



*Chevron placement represents anticipated start date of commercialization
Source: Expert interviews, Newry analysis

Conclusions

A first quantum revolution has already brought quantum technologies in our everyday life, since decades. Chips for computers and smartphone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc. are all based on technologies exploiting the quantum mechanics principles.

Now a second revolution seems to be underway, leveraging on the three quantum principles of superposition, (hyper-)entanglement and measurement. It is safe to predict that a second wave of quantum technologies could potentially have a major impact in many markets, ranging from Telecom and ICT, to Medicine, to Finance, to Transportation, and so on. Significant work is still needed to develop enabling components and systems but in light of the potential opportunities and threats, quite a lot of investments are being made worldwide across the public and private organizations.

In quantum communications, a technological breakthrough is need for developing quantum repeaters: this would be a key step for both long-distance QKD and distributed quantum computing. Concerning quantum computing, a roadblock is mitigating the random fluctuations that could occasionally flip or randomize the state of qubits during processing. Innovative qubits coding (e.g., in topological computing) and availability of efficient methods of quantum error correction are two to the main expected key milestones. Quantum software scenario is very active but rather fragmented: major efforts are directed to define languages to enable Programmers to work at high level of abstraction.

Standardization efforts are also set to help coordinating and accelerating progresses of quantum technologies. Multiple groups such as ANSI, ITU, IETF, ETSI, GSMA and IEEE are producing significant efforts. One key aspect concerns the integration of future quantum nodes and equipment (today for example QDK systems) in classic infrastructure (e.g., 5G): this requires the definition of interfaces and abstraction for management and control. The topics is also under study and experimentation in the Quantum Flagship projects of H2020 (e.g., QIA, CIVIQ and UNIQORN).

In conclusion, the following figure 4 provides a tentative roadmap for quantum technologies and services [3] ■

References

1. Quantum Information Portal and Wiki, available at https://quantiki.org/wiki/list-qc-simulators
2. Kelly, A. Simulating quantum computers using OpenCL. arXiv preprint arXiv:1805.00988 (2018).
3. OIDA QUANTUM PHOTONICS ROADMAP, Every Photon Counts - March 2020
4. Quantum Algorithms Zoo, available at http://quantumalgorithmzoo.org/#acknowledgments
5. Fingerhuth, M.; Babej, T.; Wittek, P. Open source software in quantum computing. PLoS ONE 2018, 13, e0208561.
6. https://ethz.ch/en/news-and-events/eth-news/news/2020/06/the-first-intuitive-programming-language-for-quantum-computers.html
7. The Quantum App Store Is Coming, Scientific American 9th June 2020, available at https://www.scientificamerican.com/article/the-quantum-app-store-is-coming/
8. Quantum gold rush: the private funding pouring into quantum start-ups, Nature News Features 02nd October 2019, available at https://www.nature.com/articles/d41586-019-02935-4

Antonio Manzalini *antonio.manzalini@telecomitalia.it*

Ingegnere elettronico, Ph.D è entrato in Telecom Italia nel 1990. Ha partecipato a diversi progetti di ricerca internazionali riguardanti reti di trasporto SDH ed ottico (WDM), occupando varie posizioni di responsabilità. Ha inoltre contribuito a molte attività di standardizzazione, guidando alcuni gruppi di lavoro in ITU-T, IEEE e GSMA. Attualmente si occupa di tecnologie ed architetture di reti 5G, basate sull'integrazione di SDN, NFV con Cloud-Edge Computing e sistemi di Intelligenza Artificiale. Nel 2019, IEEE gli ha assegnato il premio Industrial Distinguished Lecturer Award. È autore di oltre un centinaio di pubblicazioni internazionali e di sette brevetti ■