IDB

QUANTUM TECHNOLOGIES

Digital transformation, social impact, and cross-sector disruption

QUANTUM TECHNOLOGIES

Digital transformation, social impact, and cross-sector disruption

ITE TechLab

Author: Marcos Allende López
Supervisor: Marcelo Da Silva

Design: .Puntoaparte *Bookvertising*

Images: Wikicommons

QUANTUM TECHNOLOGIES

Digital transformation, social impact, and cross-sector disruption

This document is the result of the ongoing work of Marcelo Da Silva's team at the ITE TechLab to present new technologies to the Inter-American Development Bank, with an approach that is both technological and social. It is the first issue in a series of articles and audio-visual materials that will be presented together with the IDB Lab, as part of our joint effort to study the use of new technologies to foster development and social inclusion.

In many cases, the research and the learning necessary to write this document were done jointly. For the technical aspects, the technological trials conducted with Oscar Vazquez, Emiliano Colina, Ignacio Cerrato and Mariana Gutierrez, from IDB; Pau Velando and Guillem Sant from Entanglement Partners; and Bruno Huttner from IDQuantique were of fundamental importance.

In other aspects, the support received from Marcelo Da Silva, Nuria Simo, Vanessa Colina, Mario Casco, Maria Weisson, Melissa Panteliou, Isabel Ferro, Andrea Ortega and Sergio González, from IDB; and Alejandro Pardo, from IDB Lab was invaluable. We would also like to acknowledge the great job done by Mateo L. Zúñiga from .Puntoaparte *Bookvertising* and Melissa Julian in the edition.

TABLE OF CONTENTS

INTRODUCTION

Quantum technologies have been around since the middle of the 20th century and, for the past 60 years, they have contributed to small-scale developments and improvements, primarily in medicine. Over the past decade, however, the field of quantum technology has grown significantly and its technologies are becoming increasingly relevant across several industries and sectors, with an immeasurable potential impact on society. We are at the dawn of a new era, the age of quantum technology.

A new generation of quantum technologies will cut across most of the emerging technologies we know today, empowering many of them while threatening the security of others. They will disrupt current technology used in medicine, biology, genetics, education, economy and finance, energy, sustainable agriculture, transportation, and meteorology, among others, achieving a high social impact as well. Because of this, major global powers and the most prominent technology firms have already heavily invested in understanding, developing, and implementing these new technologies.

This document is divided into four sections that explain different aspects of quantum technologies, including the way they work, their inevitable impact at both the technological and social level, and the actions governments and technology firms are taking to incorporate them into their programs and infrastructure. While we recommend reading the entire document, each of the four sections are self-contained so that the reader has an opportunity to skip sections if needed. Because of this, some definitions may become redundant for those reading the entire document.

Section I aims to break down quantum computing and quantum information (including quantum cryptography), which are two of the most technologically disruptive quantum fields in the short and medium term. Section II discusses the impact of quantum technologies on existing digital technologies, such as cyber security, blockchain, artificial intelligence, the internet of things, drones, 5G, and 3D printing. Section III discusses the long-term social impact of quantum technologies for several different sectors, and it provides specific examples of use cases. To end on a topical note about the state of the quantum field, Section IV discusses some of the large programs currently being implemented by different international government institutions. Some more technical explanations have been reserved for the Appendices.

For the documentation and referencing of this publication, we have attempted to analyze and include the most relevant and impactful opinions, positions, and developments on quantum technologies. This has given way to a long list of references and recommended readings. However, it is possible that some might have been unintentionally left out; this will be corrected in future.

IDB

QUANTUM TECHNOLOGIES

Digital transformation, social impact,
and cross-sector disruption

THE QUANTUM ERA

00 01 10 11

THE QUANTUM ERA

The digital era we are currently living in has significantly changed our lives over the past few decades. It has allowed technology to take on larger and larger roles in our daily lives and at this point, it is hard for many of us to imagine what life would be like without our cell phones, computers, and televisions, for example. This digital era has shifted the way human beings interact and communicate with one another. Additionally, technology companies, such as Amazon, Google, and IBM, are quickly growing and have completely transformed the way we purchase goods, access information, and perform professional and personal tasks. As we start to move into a quantum era, we will see a similarly disruptive impact as we have seen in the digital one. Quantum technologies will infiltrate and influence our lives in unforeseeable ways. The specifics of their impending disruption and potential impacts will be discussed throughout this document.

QUANTUM TECHNOLOGIES

WHAT ARE QUANTUM TECHNOLOGIES?

In the first half of the 20th century, between 1900 and 1930, the study of elusive physical phenomena gave way to a new physical theory: Quantum Mechanics. This theory describes the workings of the microscopic world, the natural habitat of molecules, atoms, and electrons. Quantum Mechanics made it possible to understand that subatomic reality works in a completely counter-intuitive way where we can observe and measure processes that do not take place in the macroscopic world.

Throughout history, technological development has evolved as humanity has gained an understanding of the way in which nature works. The theory of Quantum Mechanics has allowed us to design technologies that can improve people's lives because through it, we now better understand the microscopic world. In particular, it has contributed to the development of **quantum technologies, which use the quantum properties of subatomic nature such as quantum superposition, quantum entanglement, and quantum teleportation.**

Without going into much technical detail, quantum superposition describes how a particle can exist within different states at the same time; quantum entanglement describes the way in which two separate particles can be correlated in such a way that, when one interacts with the other, the other becomes aware and reacts to it; and quantum teleportation uses quantum entanglement to send information from one place to another in space, without needing to travel through it.

Several existing technologies using quantum phenomena, including lasers and magnetic resonance imaging (MRI) machines, have made a small but important impact over the past half-century. However, it is only now that fields such as quantum computing, quantum information, quantum simulation, quantum optics, quantum metrology, quantum clocks, and quantum sensors are beginning to spearhead a technological revolution. Many of these already have relevant applications and active use cases that will be discussed in this document, while others are still in their infancy.

In this first section, we will only discuss quantum computing and quantum information; being the most complex and likely the most disruptive, they are worth a more detailed explanation. We will later discuss the social impact of the seven fields mentioned in the paragraph above in Section III.

QUANTUM COMPUTING

WHAT IS IT?

In order to understand how quantum computers work, it is convenient to explain how the computers we use every day -commonly referred to as digital or classical computers- work. Like all other electronic devices, their basic units of information are bits. This means their programs and applications are coded in bits, a binary language that uses 0s and 1s. Every time we interact with one of these devices, such as when touching a key on a keyboard, strings of 0s and 1s are created, destroyed, and modified inside the computer.

FIGURE 1. Examples of binary language characters.

Character	Bits
7	111
A	01000001
$	00100100
:)	0011101000101001

This may seem to be a fairly simple process, but the relevant question is, what exactly are these 0s and 1s within the computer? The 0 and 1 states of the bits correspond to an electrical current, which either circulates (1) or does not (0) through microscopic pieces. The microscopic pieces are called transistors, and act as switches. When the current is not circulating, the transistor is "off", and corresponds to a 0 bit in the computer. When the current does circulate, the transistor is "on," and it corresponds to a 1 bit in the computer. An easy way to understand the way bits work is by thinking about 0s as being empty holes and 1s being holes that are filled. What fills these holes are, in fact, electrons, which is why computers are called electronic devices. Each digital character corresponds to a specific string of 0s and 1s, shown in Figure 1.

Now that we understand better how classical computers work, we can try to understand the fundamentals of quantum computers. **Similar to bits in classical computing, the basic unit of information in quantum computing is the quantum bit, or qubit. Qubits are defined as two-level quantum systems.** They, like classical bits, can be at the lower level, marked by a state of low excitation or energy, defined as 0, and can also be at the higher level, marked by a state of higher energy or excitation, defined as 1. The fundamental difference here, in comparison to the binary nature of classical computing, is that qubits can also be at any of the infinitely many intermediate levels or states between 0 and 1 so that they are no longer binary as is the case with classical bits. For example, they can be in a state that is half 0 and half 1, or three-quarters 0 and one-quarter 1. This phenomenon of qubits being in intermediate states is an example of superposition, which stems from an important property of quantum systems known as quantum superposition.

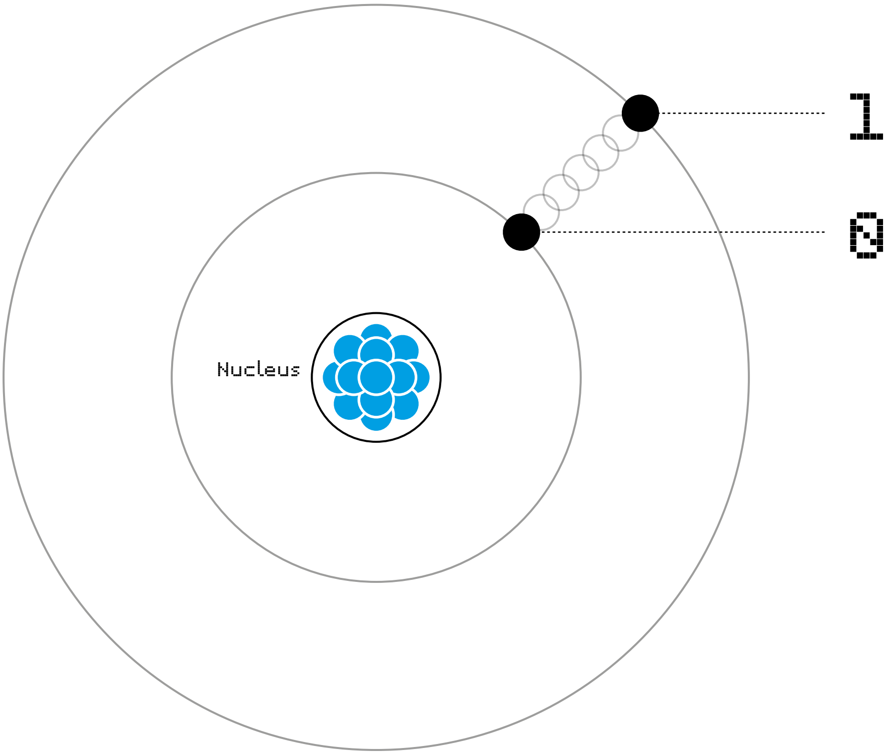
In order to understand how qubits work in a more tangible way, we will focus on an elementary physics model for demonstration. Imagine an electron orbiting around the nucleus of an atom. Recall that the more energy electrons have, the more freedom they have to stray away from the nucleus, orbiting at increasingly further levels. The less energy the electron contains, the closer it orbits around the nucleus. To model an atom as a qubit, we would need to lessen the energy of the system, so the electron can only be in the two lowest orbits possible. We achieve this by cooling the temperature of the atom down. If the electron has access to more than two orbits, it is not a two-level quantum system, and thus, not a qubit. Let us call the orbit that is closest to the nucleus "state 0" and the one farthest from it "state 1." In order for the electron to be able to pass from orbit 0 to orbit 1, it needs to receive energy, and in order to go from orbit 1 to orbit 0 it needs to lose or dissipate energy.

When we look at an electron in an atom, we can only find it orbiting in one of the defined orbits, and not in between. Once the electron is cooled down, it is only possible to find it in the two lowest orbits, previously defined as either state 0, the lowest orbit, or state 1, the next orbit. We can give electrons the exact amount of energy between state 0 and state 1 in order to get them to move from the lowest orbit to the next one. However, these orbits are not continuous, as there is a discrete energy gap between them. The key question here is: what happens when the electron is in its lowest state and is given an insufficient amount of energy to reach the next orbit?

When an electron does not receive enough energy to get from state 0 to state 1, it can then be described as being in an intermediate state. This intermediate state is known as the superposition, which is a combination of states 0 and 1. This is an undefined state in which the electron cannot be observed because the laws of nature do not allow it to be in between orbits. The very moment we try to measure the location of an electron in this undefined state, the superposition dissolves and the electron shows up either in state 0 or state 1, and not in between. This phenomenon is known as system collapse or decoherence.[1]

[1] The exact causes of the decoherence of quantum systems in nature still remain a topic of debate within the scientific community.

FIGURE 2.
Atom with two orbitals simulating the behaviour of a qubit.



This can be difficult to understand because we are used to observing the macroscopic world, where there is an observer-independent reality in which things are the way they are, regardless of whether they are observed and measured or not. However, in the subatomic world, different realities coexist until an interaction causes only one of them to "survive". In this case, nature only allows the electron to be in specific orbits around the atom which, for the purpose of this example, we have reduced to two. If we provide it with or withdraw from it a lower amount of energy than would allow it to go from one orbit to the other, the electron can be understood as being in an undefined position between the two orbits until we observe it.[2] The sub-atomic reality often remains indeterminate —as a simultaneous overlap of various realities— until there is an interaction. It then chooses what form to assume and which reality will prevail.

[2] The atomic model of circular electronic orbits was presented by N. Bohr in 1913, but with the advent of Quantum Mechanics, it was understood that the electrons are distributed around atomic nuclei in more complex orbitals. Added to that, if we analyze this example with Einstein's classical Theory of the Photoelectric Effect we would say that electrons in atoms can only take and dissipate amounts of energy that are proportional to the gap between levels. However, we think this simple example is very useful to explain the fundamentals of qubits. In practice, there are multiple ways to obtain these two-level quantum systems such as with trapped ions, defects in solids, semiconductors, superconductors or topological nanowires.

So, how do we determine which orbit the electron will appear in when we observe, or interact, with it? Unfortunately, the answer is that we can never know for sure. We can only know the exact probability that it will appear in orbit 0 or in orbit 1. This probability depends on the amount of energy the electron has when we observe it and at the moment it is observed, it "must decide"; the more energy it was given, the more probable it will be to find it in orbit 1 at the time of measurement.

Physicists came to this understanding of nature through their knowledge of Quantum Mechanics in the 20th century after decades of research and debates. It was initially rejected by scientists as important as Albert Einstein, who strongly believed in observer-independent reality and determinism. However, years of experiments have corroborated this theory of the microscopic world.

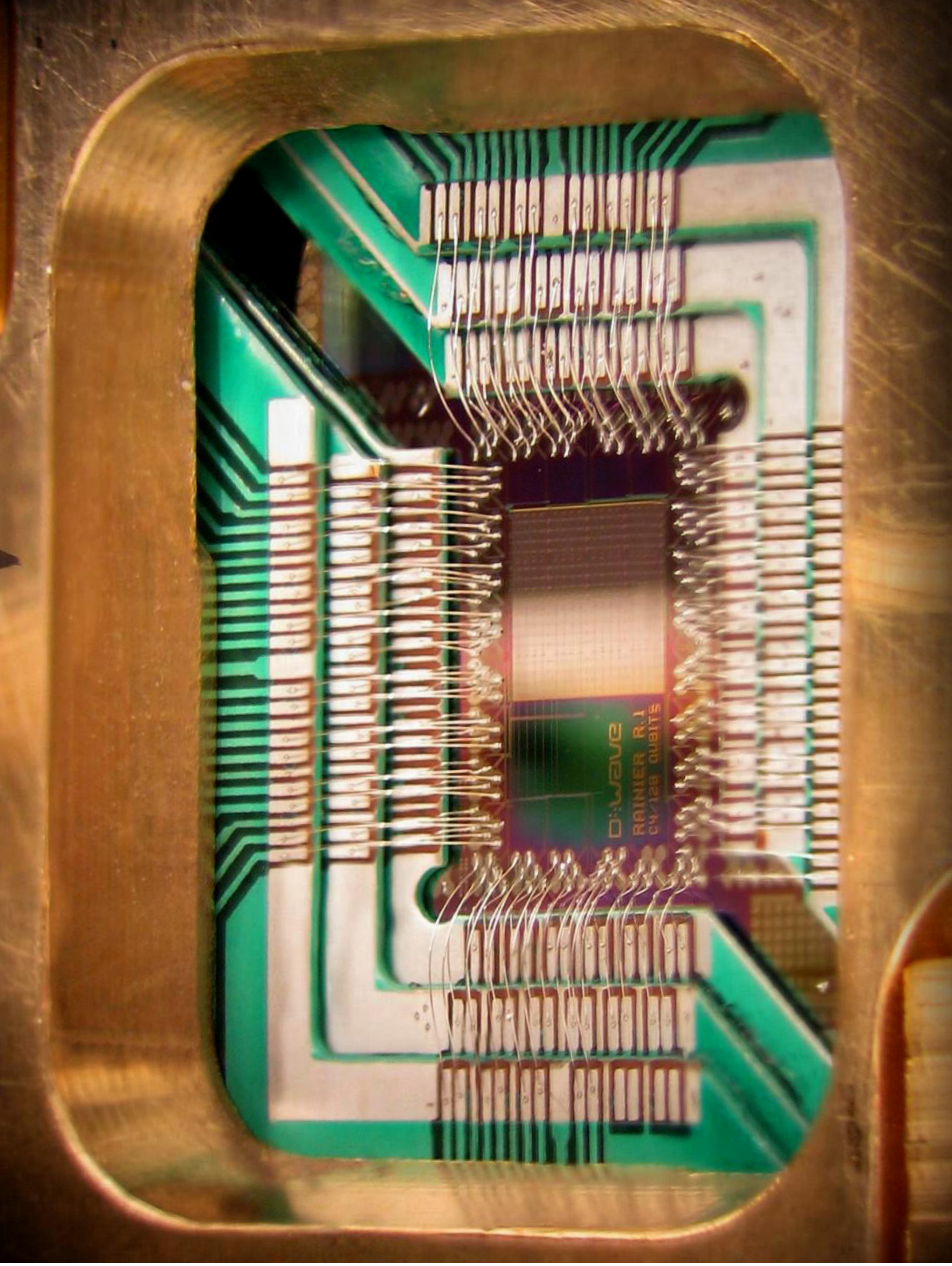
HOW DOES IT WORK?

Quantum computers allow us to use the quantum properties of qubits in order to run quantum algorithms. These algorithms use superposition and entanglement to offer a much higher processing capacity than classical computers. **It is important to note that the real change in paradigm is not that quantum computers are simply faster than classical computers,** as several publications erroneously suggest, **but that they allow for quantum algorithms that perform certain operations in a completely different, and importantly, much more efficient way.**

Let us look at a specific example of the efficiency of quantum computers over classical computers. Imagine we want to know which of the N=1,000,000 possible routes from Bogotá, Colombia to Lima, Perú is the fastest. To find the optimum route, a computer must start by digitalizing 1,000,000 options, meaning they need to be translated into bits for classical computers, and into qubits for quantum computers.[3] While a classical computer would need to analyze the routes, one by one, according to a specific algorithm in order to find the best route, a quantum computer would use a process called **quantum parallelism,** which allows it to consider all routes at the same time. In quantifying this, we can see that a classical computer needs $N/2$ steps (500,000 attempts in this case) to find the optimum route, while a quantum computer can perform the entire operation in only $\sqrt{N}$ steps (1,000 attempts in this case).

In many cases, the advantage of using a quantum computer is not simply but exponential, thanks to quantum parallelism. With only n qubits, we can obtain a computing capacity equivalent to 2^n bits. For example, with 270 qubits you could have more different and simultaneous combinations (base states) in a quantum computer than the number of atoms in the universe, estimated to be approximately 2^{80}.

[3] Classical or digital computers have a multi-layered architecture, meaning our interactions with them take place at many layers above the logical layer of bits. However, these are common discussions surrounding quantum computing as it is still in its infancy.



Photograph of a chip constructed by D-Wave Systems Inc. designed to operate as a 128-qubit superconducting adiabatic quantum optimization processor, mounted in a sample holder.

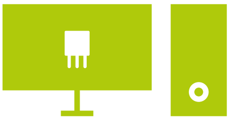
BITS

0 or 1
(one state at the same time)

00 or 01 or 10 or 11
(one state at the same time)

000 or 001 or 010 or 100 or 011 or 101 or 110 or 111
(one state at the same time)

↓



N bits → 1 state of N bits (at a time)

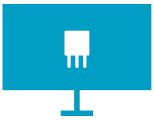
10 bits → 1 state of 10 bits (at a time)

50 bits → 1 state of 50 bits (at a time)

100 bits → 1 state of 100 bits (at a time)

↓

2^{80} bits



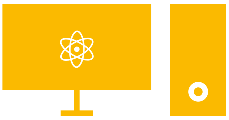
QUBITS

$\alpha \cdot 0 + \beta \cdot 1$
(2 simultaneous states)

$\alpha \cdot 00 + \beta \cdot 01 + \gamma \cdot 10 + \delta \cdot 11$
(4 simultaneous states)

$\alpha \cdot 000 + \beta \cdot 001 + \gamma \cdot 010 + \delta \cdot 100 + \zeta \cdot 011 + \eta \cdot 101 + \Theta \cdot 110 + \sigma \cdot 111$
(8 simultaneous states)

↓



N qubits → 2^n simultaneous states

10 qubits → 1024 simultaneous states

50 qubits → 1125899906842624 simultaneous states

100 qubits → 1267650600228229401496703205376 simultaneous states

↓

270 qubits

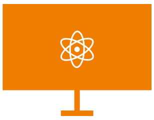
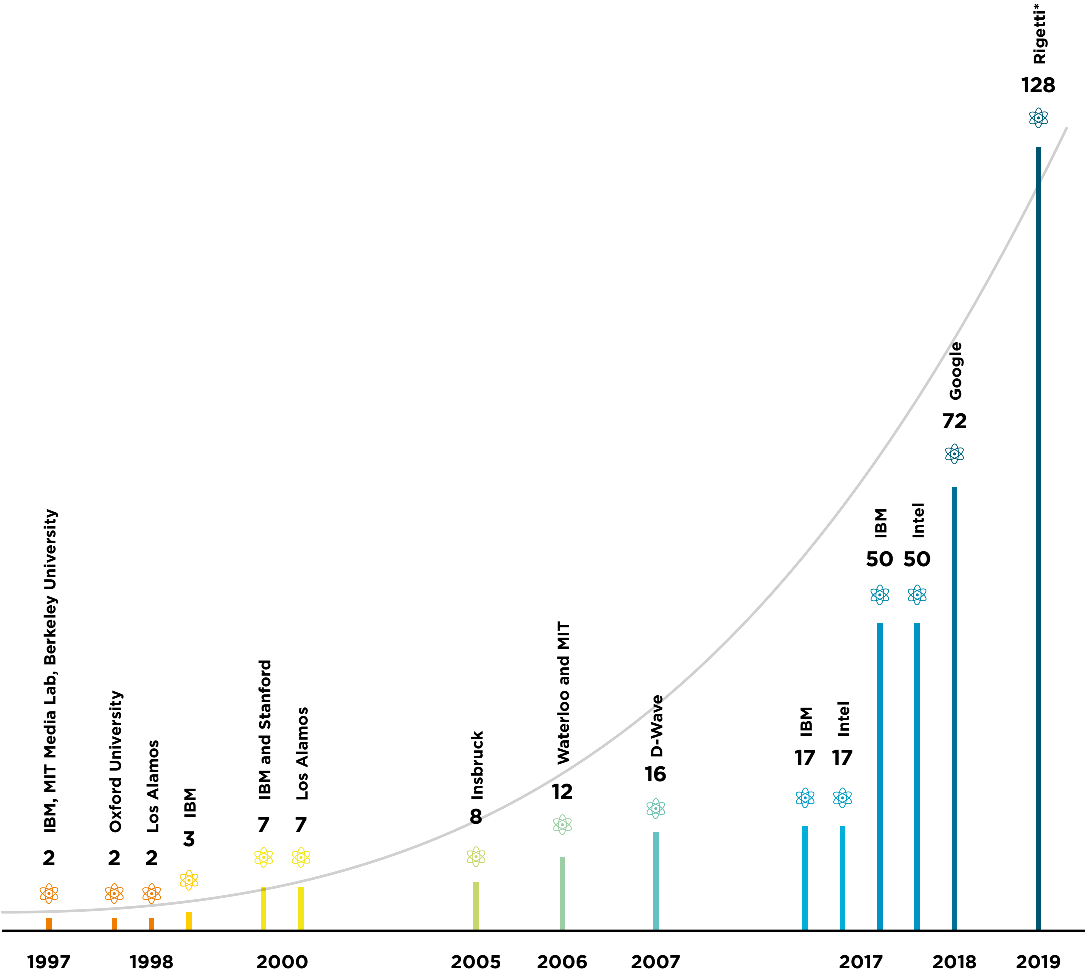


FIGURE 3.

Progresses in the development of quantum computers in terms of number of qubits

* Riggeti commited to reach 128 qubits in 2019



WHAT IS THE CURRENT STATE OF THIS TECHNOLOGY?

P. Benioff [1] and R. Feynman [2] were the first physicists to propose building computers based on the principles of Quantum Mechanics in the early 1980s. In the following 20 years, theoretical models for their architecture and the algorithms that could run within them were created. It was not until two decades later, in 1998, that the first 2-qubit quantum computers [3-7] were built, and the first algorithms were run on them [8]. Another two decades went by before the quantum computing race really accelerated; after 19 years of relatively small achievements in terms of the number of qubits quantum computers could contain, IBM took the lead in 2017, first with a 17-qubit, and later with a 50-qubit quantum computer [9]. In 2018, Google announced that it had a

72-qubit microprocessor [10] and Rigetti has committed to reaching 128 qubits in 2019 [11].[4] Figure 3 shows the most relevant milestones, regarding the number of qubits, that have been published thus far. This is discussed in more detail in Appendix A.

Qubit instability is the main challenge quantum computing is currently facing. Because qubits are so highly instable, controlling them is extremely difficult using current technology and this instability translates into computing "errors". Quantum error correction is very different from error correction in classical computing, which uses redundancy. Classical computers write or send the same sequence several times such that once all packages have been recovered, the errors can be identified and the message reconstructed. Given that quantum states cannot be cloned [14], in order to correct an error in a qubit, other qubits are needed to also carry the error.

The individual qubits are called physical qubits. The groups of qubits, which can take care of error correction and behave as a single qubit with no errors, are called logical qubits. For a quantum computer to function perfectly well, there needs to be error correction. Thus, the amount of qubits that really matter are in terms of logical, not physical qubits. The great leap in implementation of logical rather than physical qubits is yet to come. According to some experts, the number of physical qubits needed to obtain a logical one could be in excess of one thousand.

It is estimated that a quantum computer with 1500 to 2330 logical qubits will be capable of breaking all existing cyber security [12,13], which we will later discuss in more detail in Section II. When exactly this will happen still remains unknown. It is also worth noting that the number of qubits in Figure 3 correspond to physical and not logical qubits. Although the number of qubits is relevant, it is not the only important feature to determine which of two quantum computers is better.

We believe that the first quantum computing services to be provided to the general public will be offered by large technology companies in the form of software as a service (SaaS). Eventually, hybrid processors will allow the use of classical or quantum computing, depending on the problem and on the computing capacity needed by the user. In the same way that it is currently possible to run a virtual machine in different service providers' clouds, such as Amazon, Google, and Microsoft, in the future we might be able to rely on hybrid quantum and classical computing services in the cloud.

[4] The most popular quantum computers yet (only prototypes thus far) can be divided into two kinds: 1) Standard quantum computers, in which the qubits are quanta of magnetic flow in superconducting circuits, and 2) topological quantum computers, where qubits are pairs of quasi-particles called anions. Without going into too much detail, the advantage of the latter compared to the former is that, thanks to their architecture, topological quantum computers are more stable in terms of errors and noise. This poses one of the greatest challenges that quantum computing must overcome.

QUANTUM INFORMATION

WHAT IS IT?

The field of **quantum information** is the quantum equivalent to the field of classical information that studies how to quantify, store, and transfer information. Every time we access the Internet, make a telephone call, or pay with a credit card, we generate data that travels around the world at speeds close to the speed of light. Information currently travels primarily through one of two channels: (i) by cable, using primarily copper pairs and the network of fiber optics which cover the planet with more than one billion meters of underwater cable [15,16], or (ii) wirelessly, using the network of wireless telecommunications that employs different satellites as repeaters to send information to its destinations.

In order for the data generated in our electronic devices to be transferred either by cable or wirelessly, they are equipped with network cards that generate both analogue and digital signals that travel through the telecommunications networks in an orderly manner, following standardized protocols that have been developed and improved for decades. Analogue signals have a specific form and frequency, while digital signals consist of electric pulses.

Not only is it important to have effective and secure transmission of data, but it is also necessary to have effective and secure storage as well. There are several technological options to store data. Commonly, the hard drives of the electronic devices generating the data, such as computers, cell phones, and tablets, store the data themselves. Data can also be stored in USB memory sticks, external hard drives, or the cloud. Cloud storage, which involves the use of third-party storage in exchange for a fee, is being used more and more frequently.

There are two fundamentals in maintaining secure data transfer and storage: cryptography and authentication.

- **Cryptography consists of encrypting data so that only authorized users are able to access its contents.** Whenever we place a phone call or access a website that has the header "https", encryption protocols are running in the background. Signals containing data can be intercepted when travelling through cable, optical fibers, or wirelessly, and thus, encryption is necessary so that data content cannot be accessed through an interception.

- **Authentication enables us to confirm who we are communicating with when transferring data and is essential for cryptography to succeed.** If we receive an encrypted message but we are not able to verify the messenger's identity, we cannot be sure that the message was not sent or altered by someone else.

Cryptography techniques may be classified into two groups: **symmetric and asymmetric.** Symmetric techniques use the same key to encrypt and decrypt a given message or data set, and asymmetric techniques use different, but complementary, keys.

Symmetric cryptography

Symmetric cryptography is completely secure in theory, but not very practical; it either has to be combined with asymmetric cryptography or is carried out inefficiently. Simply, symmetric cryptography processes can be described in three steps:

1. The sender and recipient **agree upon and share** a **private key.**
2. The sender **encrypts** the message with the **private key** and sends it to the recipient.
3. The recipient **receives** the message and **decrypts** it with the same **private key.**

Symmetric cryptography demands the generation and exchange of a **private key** prior to the encryption, transmission, and decryption of the message. **This kind of encryption is completely secure only if (i) the keys are completely randomly generated, (ii) the channel used to share the keys is completely secure, and (iii) the keys are not used more than once.** However, using current or classical telecommunications, it is not viable to generate completely random keys because the algorithms that generate them always have a certain periodicity; they are repeated. Regarding the second requirement, the only classical way to have a completely secure channel to exchange these symmetric keys is to do so in person, which is highly inefficient. Doing it remotely implies trusting channels previously secured with asymmetric cryptography, which is not quantum-safe, as we will soon explain.

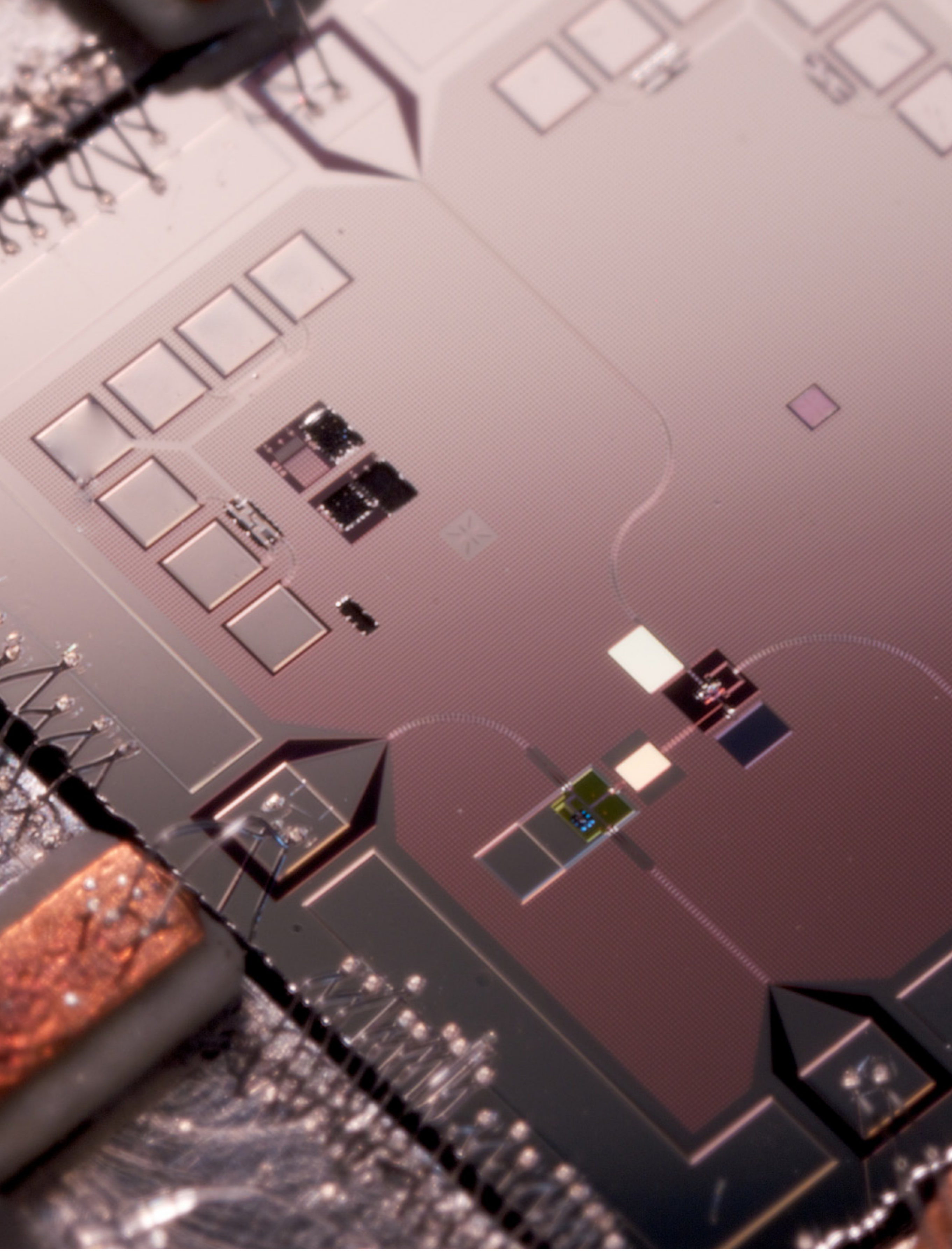
With the exception of some intelligence agencies and governments that generate a large number of keys periodically and distribute them physically using external drives, classical symmetric cryptography is not typically used unless it is combined with asymmetric cryptography which, as we will see, will be unsafe in the future.

One of the most famous historical examples of symmetric encryption is that of the Enigma machine used by the Germans in World War II. These machines had a set of rotors inside, allowing the machines to generate different sequences in the order of 10^{19} to encrypt messages. Each of these sequences were essentially symmetric keys. The machine's operator was given instructions once a month on how to place their rotors so that all the machines in use encrypted and decrypted with the same key. None of the three requirements for secure communication presented two paragraphs above was respected and The Allies were able to take advantage of the third in breaking Enigma's encryption.

The Germans set the key (the configuration of the rotors) arbitrarily, rather than completely randomly; instructions were sent by courier and, although insecure, this was not the weak point; the weak point that was harnessed by The Allies was the fact that the same keys were being used for different messages. The Allies were able to identify repeated phrases on the keys, such as the header or the date, allowing them to discard many of the 10^{19} possible keys, and find the right one.

Asymmetric cryptography

Given the inconveniences posed by symmetric keys, the development of asymmetric cryptography began in the 70s. Asymmetric cryptography allows for relatively secure



Photograph of a quantum machine. The mechanical resonator which was placed in a superposition is situated in the bottom left of the chip. The smaller white rectangle is the coupling capacitor between the mechanical resonator and the qubit.

point-to-point data transmission. This security relies on the difficulty to reverse certain mathematical operations, such as the factorization of prime numbers. Despite the fact that multiplying two prime numbers is a computationally simple operation, factoring the result of its product is exponentially more difficult. This involves the simple generation of pairs of "complementary" keys in such a way that a message encrypted by one of the keys can only be decrypted by the other.

The important thing to highlight here is that it requires an enormous computing capacity to find the key that decrypts the message based on the one that encrypts it, as is shown in Figure 4. This allows us to communicate securely with someone by requesting them to generate a pair of keys. They share a **public key** used to encrypt and send the message, which only they can decrypt with their **private key** when received. It works like a dropbox in a video rental shop; anyone can drop the film in the box but only authorized personnel can open the box to retrieve the videos. These processes can generally be described according to the following steps:

1. The recipient uses a given algorithm to **generate a pair of keys** periodically, which are known as the **public key** and **private key.** The **public key** is shared openly with the sender, and the private key is kept secret by the recipient.
2. The sender **takes** the **public key** offered by the recipient that they intend to send the message to, **encrypts** the message using the key, and then **sends** it to the recipient.
3. The recipient **receives** the encrypted message and **decrypts it** using the **private key,** which only they have access to.

Among the many problems that quantum computing will be able to solve in a much more effective manner than current computing in the future, are those that lie in the foundation of all the asymmetric cryptography used today. **Quantum computing will eventually break all current asymmetric cryptography techniques used over the Internet and phones.**

The three main algorithms used to generate keys in asymmetric cryptography are (i) RSA (based on the factorization of prime numbers, shown in Figure 4), (ii) discreet logarithms, and (iii) elliptic curves, all of which are described in Appendix D. In 1994, P. Shor presented a quantum algorithm that effectively reverses each of these three algorithms and warned that there may come a time when keys used in asymmetric cryptography will be broken faster with a quantum computer than they can be generated with a digital or classical one [17].

Luckily, the field of quantum information will eventually render asymmetric cryptography obsolete. **Quantum cryptography allows for the generation of completely random symmetric keys that can be shared securely and effectively without having to use asymmetric cryptography to secure the channel or having to communicate in person to exchange them. In other words, it provides a secure channel to send completely random keys.** This can be done by means of two processes: quantum random number generation (QRNG) and quantum key distribution (QKD).

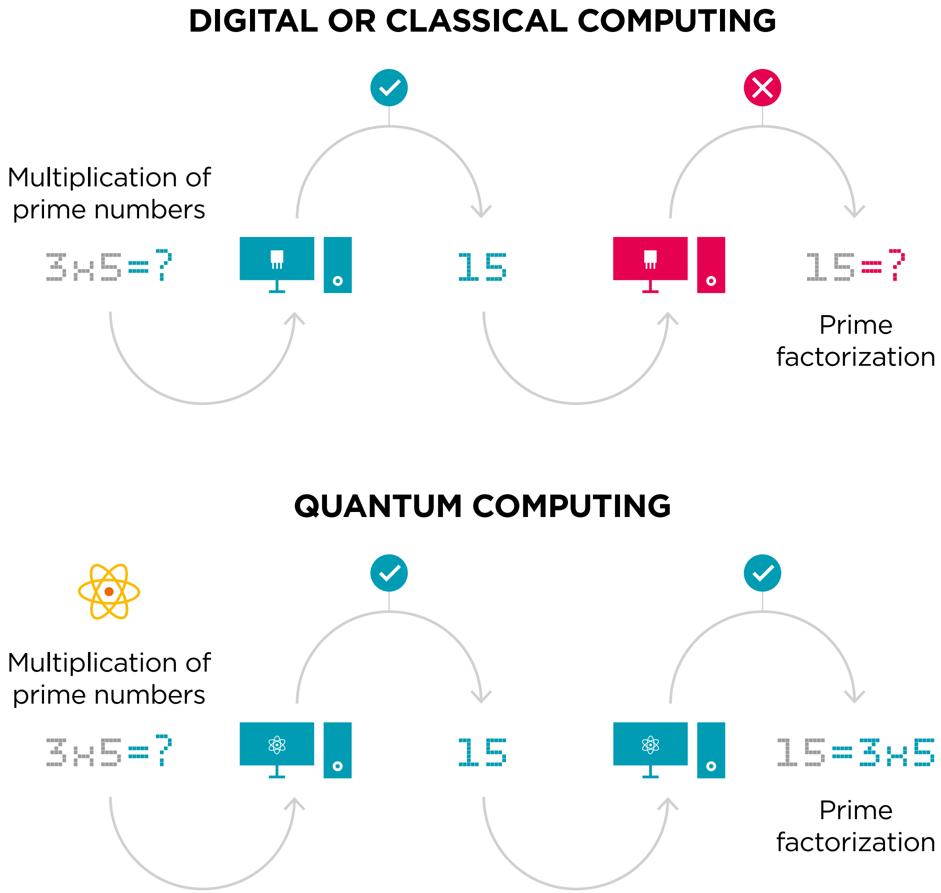

DIGITAL OR CLASSICAL COMPUTING
Multiplication of prime numbers
3x5=?
15
15=?
Prime factorization
QUANTUM COMPUTING
Multiplication of prime numbers
3x5=?
15
15=3x5
Prime factorization

FIGURE 4. Example of the prime factorization problem, the basis of many current encryption protocols. All the computational capacity in the entire world could not factor extremely large numbers within a reasonable amount of time.

HOW DOES IT WORK?

The success of these processes, described in more detail in Appendix B, lies in the fact that they are implemented at the hardware level -in the physical structure of computers and channels- rather than at the software level -by means of programs- as is the case with classical random number generation and classical cryptography algorithms. **This allows us to benefit from the advantages of physical processes with quantum properties which a) have complete uncertainty and are not deterministic, allowing for the generation of truly random keys,[5] and b) exploit the fact that interception affects the result of the key**

[5] A simple example is that of a semi-reflective mirror which lets through half of the light it receives, so that each particle of light that reaches it has a 50% chance of passing through. If we write 1 every time a photon goes through, and 0 every time a photon is reflected, we obtain a 100% random key.

measurement; keys are coded into quantum states and thus, change when observed, enabling us to detect eavesdroppers that may observe the key during the transmission.[6]

Quantum symmetric cryptography is completely secure and resistant to quantum computing because its security relies on the laws of nature that govern physical processes taking place at the hardware level, rather than the software level, where security relies on the difficulty of reversing mathematical algorithms.

WHAT IS THE CURRENT STATE OF THIS TECHNOLOGY?

While quantum computing is still under development, quantum cryptography is already in use.

IDQuantique is the world's leading manufacturer of quantum devices and sells quantum random number generators that are only a few millimeters in size. In terms of key exchange, the first QKD protocols were conceived of and published in the 1980s. The most widely used QKD protocol is BB84, proposed by C. Bennett and G. Brassard in 1984 [19]. It is described further in Appendix B. The second most relevant QKD protocol is E91, proposed by A. Eckert in 1991 [20].

For the implementation of these protocols, it is necessary to have quantum systems to code into the randomly generated 0s and 1s that constitute the symmetric keys. For practical reasons, mainly photons are used as the quantum systems.

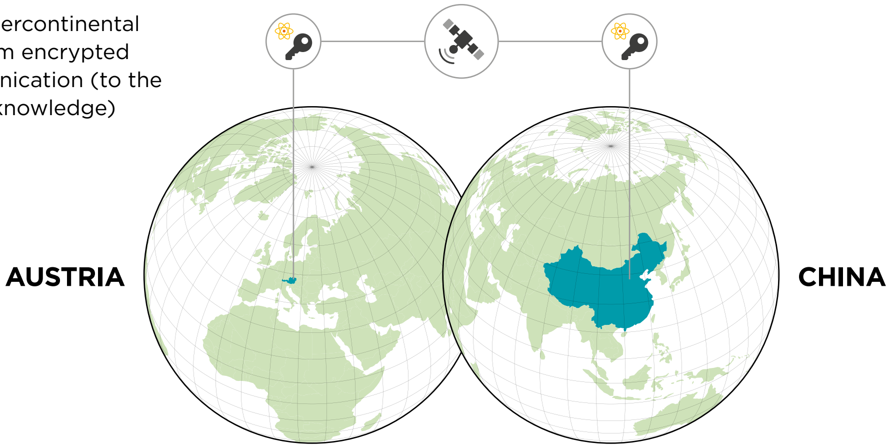
Photons, or light particles, can travel through both optical fiber and free space. However, optical fiber has a much higher attenuation than free space when above the densest layers of the atmosphere. Currently, the limit when actually transferring these keys through an optical fiber channel is a few hundred kilometers. **The first documented transfer consisted of a network of six nodes which were 29 kilometers in length, between Harvard University and Boston University in 2004** [21,22]. A recent experiment succeeded in exchanging keys via optical fiber between nodes at more than 400 kilometers of distance [23] in very favorable conditions. The scalability of these networks depends on the development of quantum repeaters, [24] which require very sophisticated quantum memories which are still being developed [25,26]. China owns the longest existing network, with 32 nodes more than 2,000 km in length between the cities of Beijing and Shanghai [27].

[6] Most frequently, the polarization of light particles, photons, are used as quantum states. If we think of photons as arrows, their direction of polarization can be understood as the direction of the arrow. We can think of a 0 as a horizontal photon, and a 1 as a vertical photon. If an eavesdropper observes the key when it is being transmitted, the polarization of the photon (the direction of the arrow) changes, and so does the key. When a piece of that key is later exchanged, and thus sacrificed in order to check if both have the same key, it is possible to detect potential eavesdroppers. The rest of the key is used to encrypt information only if no eavesdroppers are detected.

Satellites are used as nodes in wireless communications. The first country to launch a satellite for Earth-to-space and space-to-Earth quantum communication purposes was also China. In 2016, the QUESS (Quantum Experiments at Space Scale) space mission launched a 600 kg satellite known as MICIUS and the estimated total cost of the mission was $100 million [28,29]. **In communication with three Earth stations in Delingha, Nanshan, and Lijiang, it was possible to generate and share quantum keys for the first time over long distances exceeding 1,200 km** [30,31].

Because of this satellite, on September 17, 2017, one of the greatest milestones in the field of quantum information was achieved: **a successful 90-minute quantum encrypted videocall between China and Austria over a distance of 7,600 km.** To public knowledge, this was the first intercontinental communication encrypted using secure quantum technology. After the quantum key was successfully generated and exchanged, the videocall data traveled over a regular optical fiber wire, and was encrypted and decrypted in China and Austria with the quantum secret key [32].

First intercontinental quantum encrypted communication (to the public knowledge)



In a few years, all internet-connected devices, and even some that are not connected to the internet, will encrypt the information they exchange using quantum keys that have previously been generated securely. When quantum computers are powerful and robust enough, any communication done without these quantum keys will no longer be secure. When quantum computers are ready to break classical keys, it will not only be unsafe to have new files which are classically encrypted, but **any existing sensitive or confidential file which has already been downloaded or intercepted in the present time, may be kept until a quantum computer is able to decrypt it.** This is already known as “hack today, crack tomorrow.” For this very alarming reason, governments and private companies are joining forces in the race to adapt quantum technology at an increasing speed in order to guarantee the safety of their data, as we will discuss in Section IV.

Appendix C contains a detailed summary of the most relevant initiatives in this area by governments, universities, and the private sector to date.

IDB

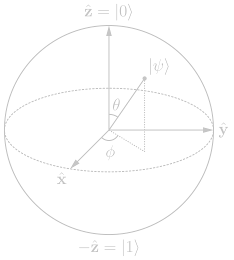
QUANTUM TECHNOLOGIES

Digital transformation, social impact,
and cross-sector disruption

IMPACT ON EMERGING TECHNOLOGIES

00 01 10 11

IMPACT ON EMERGING TECHNOLOGIES



Emerging technologies, such as blockchain, AI, the Internet of Things (IoT), drones, virtual reality, 5G, 3D printing, robots, and self-driving vehicles are becoming increasingly relevant across various fields and sectors in this time of digital transformation. These technologies aim to improve our quality of life by accelerating other technological developments and generating social impact. However, each of these technologies are growing in parallel for the most part. There are only a few companies developing products combining two or more of these technologies, such as blockchain and IoT or drones and AI. Eventually, these technologies will merge to generate an exponentially bigger impact than they would be able to alone. However, because they are still at a very early stage of development and because there is a shortage of developers and personnel with enough technical knowledge to make innovations, these convergences are still missing.

Quantum technologies will significantly disrupt the current progress and future development of the emerging technologies described in the previous paragraph and will provide cross-cutting influence. This section will describe how quantum computers will threaten data authentication, exchange, and storage, having the greatest impact on areas where cryptography plays a fundamental role, such as cyber security and blockchain. 5G and IoT technologies also require secure data authentication and exchange and thus, quantum computing will be significantly threatening for them as well. Despite the significant threats they pose, quantum computing and the other emerging technologies will allow for necessary technological evolution and growth.

CYBER SECURITY

WHAT IS CYBER SECURITY?

Cyber security **is defined as the practice of protecting systems, networks, and programs.** When the Internet appeared in the 1980s, it was necessary to develop universal standards and protocols so that people around the world speaking different languages and using different systems could communicate with one another on it in a unified way. With this aim, in 1984 the International Organization for Standardization (ISO) created and published the OSI model (Open Systems Interconnection), which defines seven theoretical layers [34], shown in Figure 5.

Each of these layers present the different risks that cyber security addresses. With the arrival of quantum computing and quantum cryptography, they will change completely.

FIGURE 5. OSI Model.

Software

Layer	Type	Function	Cyber security risk
7 Aplication	Data	High level APIs, programs and applications	Virus and trojan
6 Presentation	Data	Data representation & encryption	Personal information theft and attacks on BIOS
5 Session	Data	Interhost communication	
4 Transport	Segments	End-to-end connections and reliability	IP faking, authentication, MITM, data decrypting, reinjection attacks
3 Network	Packages	Path determination, routing and logical addressing (IP)	
2 Data link	Infrastructure	Physical addresing (MAC & LLC)	Eavesdropping, saturation attacks, ARP spoofing
1 Physical	Bits	Medial, signal and binary transmission (logical bits)	Undue access to the physical layer and data theft

Hardware

THE FUTURE OF CYBER SECURITY IN THE QUANTUM ERA

There are a wide array of risks associated with the use of Internet-connected devices, the most relevant of which are presented in Figure 5 within the framework of the OSI model. Note that many security breaches occur because of inadequate or unsafe behaviors on the part of users, which will not be discussed in this document. Outside of this, the two core categories in regards to security issues are cryptography and authentication, as you may recall from Section I. If network access for users is not forged, and the information is stored and shared using completely secure cryptography so that no unauthorized person can access it, most potential security breaches do not happen. Thus, this section focuses on the significant changes that cryptography and authentication will need to undergo in the quantum era.

Changes in cryptography and authentication will become crucial as the advent of quantum computing will put cyber security in serious danger. **When quantum computers are robust enough, they will be capable of breaking every single cryptography and authentication protocol that rests unconditionally on asymmetric cryptography algorithms.**[7] Quotes from two of the most reputable standards agencies, the National Institute for Standards in Technology (NIST) and the National Security Agency (NSA), highlight the seriousness of this issue:

> “If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use” - *NIST* [36]

> “A sufficiently large quantum computer, if built, would be capable of undermining all widely-deployed public key algorithms used for key establishment and digital signatures.” - *NSA* [37]

Both agencies call attention to the problems quantum computing will engender for current cryptography and authentication, and they also propose similar solutions to these problems. Both agencies are still reluctant to adopt new standards that rely on symmetric quantum cryptography (described in Section I) probably because they believe is not yet mature enough and would require a massive renewal of hardware to implement. Instead, their recommendations **focus on Post-Quantum Cryptography (PQC).**

PQC proposes the use of new asymmetric mathematical algorithms that are more difficult to reverse than those currently in existence. This approach does not require hardware renewal; it only requires software updates. NIST proposes the use of lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, hash-based signature, among other algorithms to be researched for this use [36]. They also commend the European initiatives, PQCrypto [38] and SAFEcrypto [39], and the Japanese initiative, CREST Crypto Math [40], that have already begun work in this area.

[7] In 1994, P. Shor [17] published a quantum algorithm to effectively reverse cyber security protocols based on discrete logarithms and factorization of prime numbers. This algorithm has already been successfully implemented in quantum computers, and once quantum computers have a large enough number of qubits, it will be possible to use them to effectively break the cryptography we use currently.

Additionally, in 2017, NIST called for proposals on PQC algorithms [41]. Their intention was to involve the community in playing a leading role in their search for an international consensus on the standardization of secure encryption methodologies after the widespread implementation of quantum computing is underway.

PQCrypto has already made specific recommendations on the use of new symmetric cryptography algorithms known as SPHINCS and XMSS [42].

The biggest problem posed by PQC algorithms is that they will never be completely secure. Their security relies on the fact that classical computers are not capable of efficiently solving very difficult mathematical problems, which are the basis of the PQC algorithm. Once quantum computers become larger and more capable, algorithm reversal will become much easier to achieve, threatening the security of devices and networks secured by PQC algorithms. Quantum algorithms that are ready to break today's cryptography already exist, and are simply awaiting quantum computers that are robust enough to run them.

Cryptography

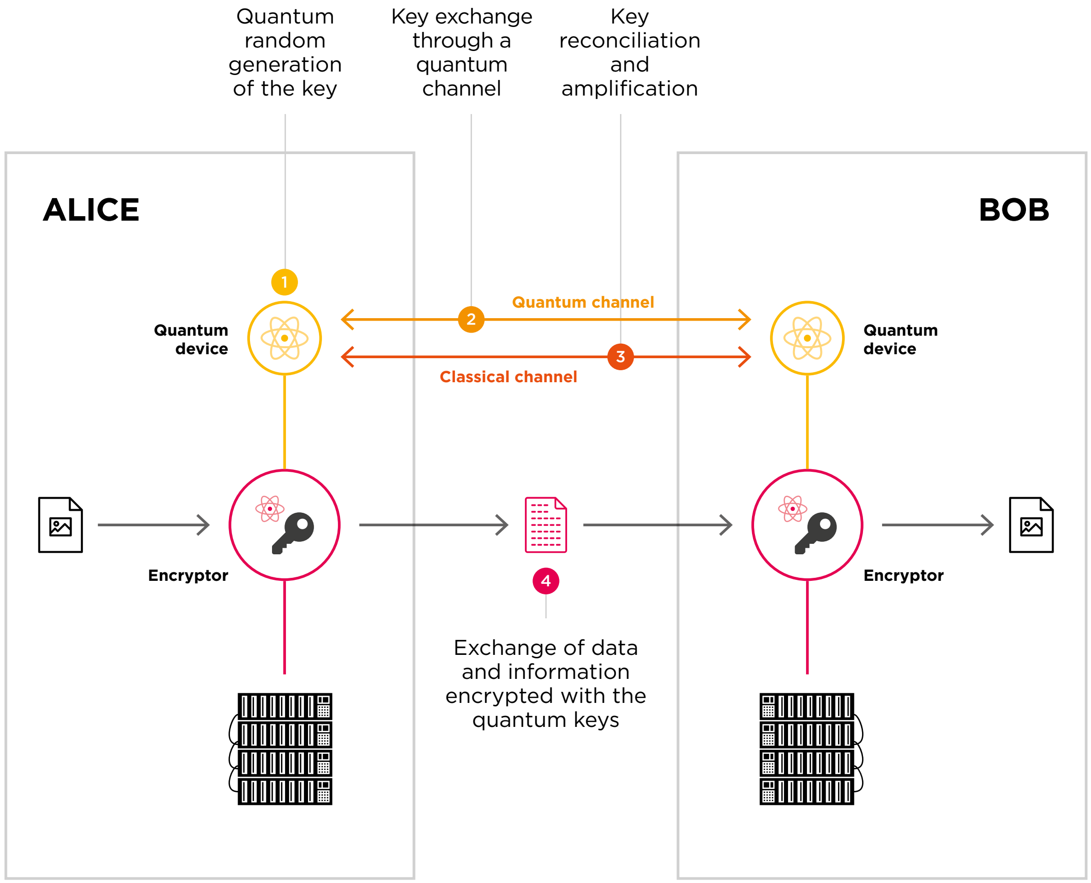
The PQC algorithm reversal problem described above does not exist with quantum asymmetric cryptography because quantum cryptography protocols (QKD) simply do not use mathematical algorithms. Rather, they consist of physical processes whose violability go against the laws of nature.

> **"QKD as a cryptographic primitive offers security that is guaranteed by the laws of physics [...]. This means that even assuming an adversary to have unlimited computational resources, including unlimited classical and quantum computing resources, QKD is secure now and always will be." –** ETSI [43]

In a much more complete document than those from the NSA and NIST, the European Telecommunications Standards Institute (ETSI) stated in 2015 that **quantum cryptography is the only alternative for long term secure encryption.** They analyze quantum cryptography's functioning, advantages, and challenges. Further, it describes use cases for QKD, including encryption and authentication, network infrastructure, cloud storage, and artificial intelligence, as well as areas of application, such as medicine and health, financial services, and mobile apps. [43]

Explained in Section I, the security enabled by quantum cryptography relies on the laws of physics because it takes place at the hardware level, rather than at the software level, which corresponds to layers 1 and 2 in the OSI model. **The advantages afforded by the use of quantum processes in making quantum cryptography completely safe are that (i) the generation of keys is completely random, and (ii) keys are impossible to be spied on in an exchange without being detected. However, as mentioned before, quantum cryptography also has a disadvantage in that it requires hardware modifications and upgrades to incorporate quantum equipment, but devices are substituted and improved all the time so it should not be a strong barrier.**

FIGURE 6. Alice and Bob using quantum random number generators (QRNG) and quantum key distribution (QKD) to generate and share keys in a secure way.


Quantum random generation of the key
Key exchange through a quantum channel
Key reconciliation and amplification
ALICE
BOB
1
2
3
4
Quantum device
Quantum channel
Classical channel
Quantum device
Encryptor
Encryptor
Exchange of data and information encrypted with the quantum keys

There are readily available commercial options for this type of equipment. They typically consist of devices connected with one another to:

- Generate quantum random keys using quantum random number generators (QRNG).
- Exchange keys coded into quantum states, such as through the polarization of photons.
- Carry out a reconciliation process to detect potential eavesdroppers and debug the key.
- Transfer the key locally to a traditional encryptor, which is connected to the electronic device generating the information to be encrypted, shown in Figure 6.

IDQuantique is the current leading world manufacturer of these devices. Other companies, such as MagiQ, SeQureNet, and QuintessenceLabs, also have products; others, such as Toshiba, NEC, Mitsubishi, and IBM, have research programs in this area.

Appendix C presents some of the most commonly used asymmetric cryptography techniques and compares the ability of classical and quantum computers in breaking them. It can take from thousands or millions of years to days, hours, or minutes to break them, depending on the type of device being used.

Authentication

Through quantum processes, quantum cryptography offers security that is not possible to achieve with classical cryptography. However, there is still no clear solution to the authentication problem. In regard to information encryption, asymmetric cryptography is used to authenticate and perform digital or electronic signatures. Specifically, a digital signature is simply a pair of public-private keys. In order to sign messages, we need to encrypt the messages with the private key so the recipient gets it encrypted with the public key, allowing them to verify that it is our message, as:

- Without our private key it is impossible to generate our public key.
- A trustworthy third party has previously verified that out electronic identity matches with our real identity and issued a certificate stating that the public key belongs to us. This certificate is attached to the messages we send.

The problem here lies in the fact that quantum computing allows us to discover the private key using the public key, making the safety of the whole process disappear. It is difficult to provide a quantum solution to authentication because the authentication of servers, which happens at a network level (layer 3 in the OSI model) and authentication of users, which takes place at the application level (layer 7 of the OSI model) are not easily translated to the physical level (layer 2 in the OSI model).

To understand this difficulty, it is important to keep in mind that **authentication involves (i) generating an identity, (ii) validating that identity (by a trusted party), (iii) the possibility of verifying that identity (checking that it was validated by a trusted party), (iv) the possibility of repudiating that identity, (iv) reusing that identity and (v) recovering that identity, among others.** In order to meet all of these requirements, records -or the use of memory- is required. However, the nature of the microscopic world makes it impossible to clone quantum states and it is very challenging to record something when copying it is not possible. Thus, quantum memory is extremely complex and is presently only under development [14]. Most quantum memories that have been developed to date are capable of only storing the states of a few photons at a time. The current record is held by a research group at the University of Warsaw, with 665 simultaneous states at a time, accomplished in 2017 [44]. Quantum memories will also have implications for data storage but there is a long to go before quantum data storage becomes a reality.

Despite these difficulties, there are some floating ideas on how to develop secure quantum digital signatures (QDS). In 2001, D. Gottesman at the University of California, Berkeley and I. Chuang at the MIT Media Lab [45] proposed the first theoretical model of quantum digital signatures.[8] The most successful experimental accomplishments in this area have been carried out without using memories or quantum repeaters, both of which make the

[8] Without going into too much technical detail, these signatures work similarly to Lamport signatures and Merkle trees, but use (i) random number generators for private keys and (ii) quantum mappings instead of hash functions to generate public keys from the private keys.

process difficult. In 2015, the first implementation was able to transmit QDS at a distance of more than 2 km [46]. One year later, a transmission of over a 1.6 km distance [47,48] was made through the air. In the same year, the 100 km barrier was broken using a 102 km long optical fiber. This is the longest distance covered to date [49]. The problem posed by these signatures is that despite being completely secure, they are not reusable. When they are used, part of the private key is revealed. This makes them less practical than originally expected, even after overcoming their complex implementation in terms of infrastructure. For further information on the experimental progress of QDS we recommend referring to the publication, "Progress in experimental quantum digital signatures" [50].

An extremely interesting idea, whose implementation will be equally important for cryptography and authentication is that of a quantum internet. Some technology firms, such as QuTech, are working on roadmaps to achieve interconnected quantum computer networks that combine all the advantages of quantum technologies, such as secure symmetric cryptography or synchronicity, through atomic clocks. Their working group has already published a paper defining six stages in the development of a quantum internet [51].

The development of quantum computer networks will require further development of viable and optimal quantum computer architecture that can utilize quantum properties in order to be secure at all levels. In 2000, D. DiVincenzo identified five criteria for the development of robust quantum computers, namely: (i) a scalable physical system with well-defined qubits, (ii) the ability to initialize the state of the qubits to a simple fiducial state, such as, for example, state $|000 \ldots \rangle$, (iii) long enough coherence times (longer than the operational time of quantum gates) (iv) a universal set of quantum gates, and (v) a qubit-specific measurement capability [52]. In 2017, M.F. Brandl published what he called a Von Neumann quantum architecture, which combined Von Neumann's classical architecture with DiVincenzo's five criteria [53].

Ultimately, **it is a fact that cyber security will change radically in the next few years in order to withstand attacks from quantum computers.** The proposed solution to improve asymmetric cryptography algorithms that are currently widely used is either the ideation of new asymmetric algorithms known as PQC, or quantum symmetric cryptography, consisting of QRNG and QKD. While the latter has proven to be completely secure, it is currently only useful for cryptography purposes and requires infrastructure adaptations. On the other hand, PQC offers only short-term guarantees but for the time being, it seems to be the most viable solution in terms of authentication. **In the long run, we are likely to witness the birth of a new concept of the Internet, consisting of a completely different network of interconnected quantum or hybrid computers.**

In Section IV, we will discuss how the great world powers are aware of this threat and are implementing billion-dollar programs to dominate and fight against it. Additionally, universities, start-ups, and large technology firms are increasingly seeking to play an important role in this emerging quantum field.

BLOCKCHAIN

WHAT IS BLOCKCHAIN?

Blockchain technology was initially presented in 1991 by physicists S. Haber and W.S. Stornetta, who introduced the idea of a ledger to digitally record audio, image, video, and text files in an immutable and decentralized way [54].

In 2008, blockchain rose to fame with the advent of Bitcoin [55], a cryptocurrency whose security and functioning are guaranteed through blockchain technology. Since then, blockchain has provided technological support to more than 2,000 cryptocurrencies and to other digital solutions outside the area of non-fiduciary money. Some examples of the wide range of applications in which this technology can be utilized include supply chains, transparent voting systems, energy supply traceability, financial inclusion, remittances, digital identity, humanitarian aid, medical and property records, and academic certifications, among others.

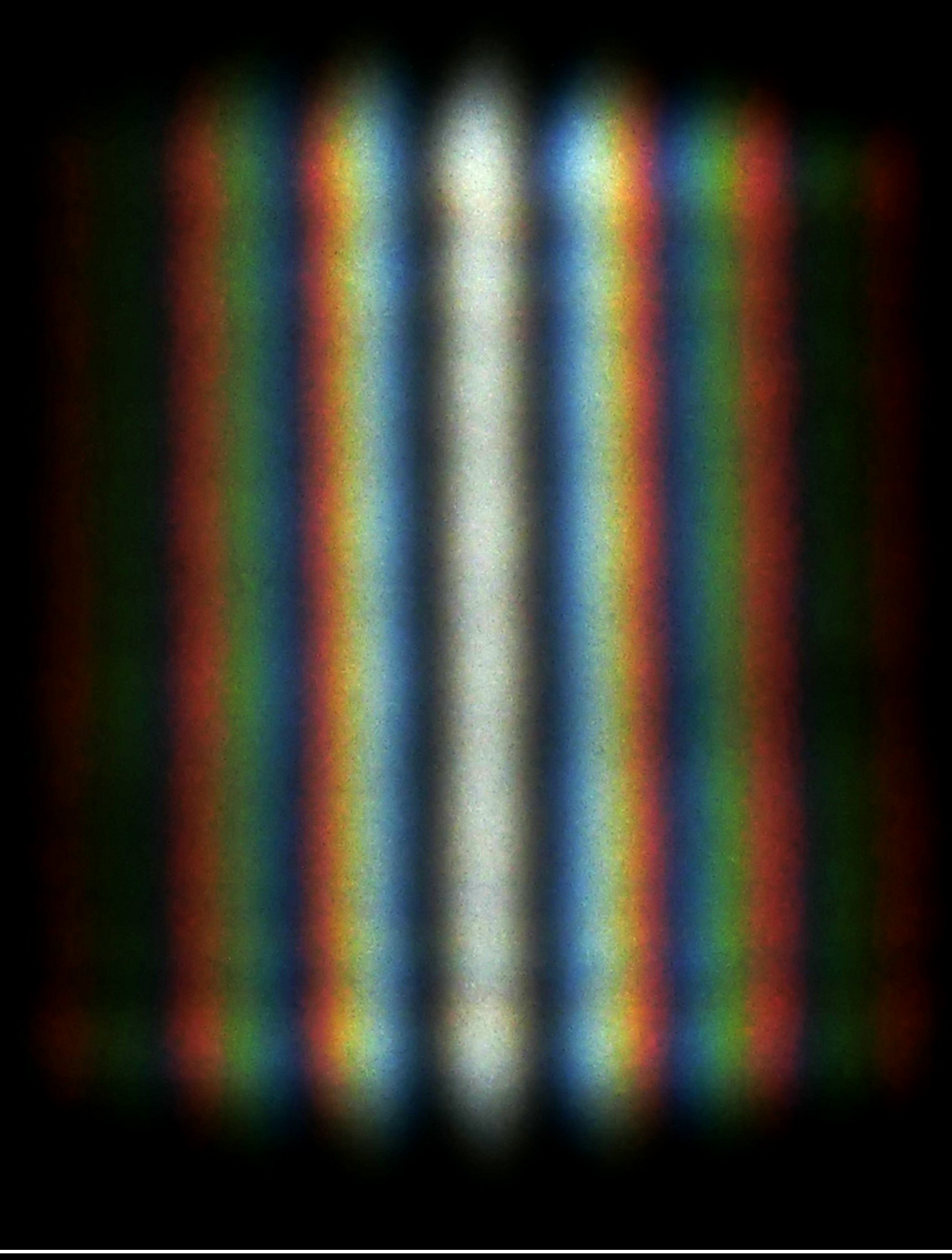
Blockchain technology's utility lies in the fact that it allows us to keep an unchangeable, decentralized, and consensual record of transactions. A transaction is defined as anything that is registered in the blockchain, including tasks such as the creation of a user, the updating of a document, or the sale of an asset, among many others. When blockchain is used as it is meant to, all participants, or nodes, of the blockchain share a synchronized ledger. Any information that is pushed to the shared ledger by any of the participants must be previously validated by the other participants according to the rules defined in the consensus protocol.[9]

For more information on blockchain technology, we recommend reading "Blockchain: How to develop trust in complex surroundings to generate social impact value," a document we published with the ITE Tech Lab, which explains its functioning from a thorough, but not overly technical, point of view. This publication answers questions about how to best utilize blockchain in digital solutions [56]. For lighter reading, we also recommend two related articles published in *Abierto al Público* [57,58].

WHAT IS BLOCKCHAIN'S SECURITY BASED ON?

There are two outstanding elements that need to be addressed regarding blockchain security. The first one has to do with participant keys, and the second with the encryption of transactions and blocks; we will again see that security revolves around authentication and cryptography.

[9] In practice, many blockchain networks, commonly known as private or federated, (or permissioned), have one or several entities that control the network. These entities decide who can have access to the network and what each authorized user's read and write rights are.



A double-slit interference of the sunlight passing through two slits ~1 cm long and ~0.5 mm apart. At the top and the bottom of the image the interference on the edge of the slit produces noticeable variation of the brightness. Aleksandr Berdnikov.

Participant keys

In blockchain, a pair of keys is generated for the two participants involved in a transaction and are known as **public key** or **wallet** and **private key,** which define and characterize their identification and authentication.[10]

The **public key** or **wallet** is the key that each participant displays for others to see when signing transactions, sending information, receiving information or in any way interacting with the blockchain. The **private key** is the key with which each participant authenticates themselves in the system. Only the holder of a **private key** can issue signatures with the public key.

The pairs of keys are generated by the blockchain for each participant, using asymmetric key algorithms. As previously explained in this section, quantum computers will be able to run quantum algorithms -specifically, Shor's algorithm [17]- capable of efficiently reversing asymmetric algorithms to effectively find a user's private key from their public key.

Block mining, consensus protocols, and reversibility of hash functions

In terms of security, another strong point of blockchain technology is the **mining** process. **Mining** is the process by which **transactions** that are grouped to create a **block** are **encrypted** using a hash function, which generates an irreversible alphanumeric string as output. This process is done according to the rules set out in the consensus protocol, which varies within each blockchain network.

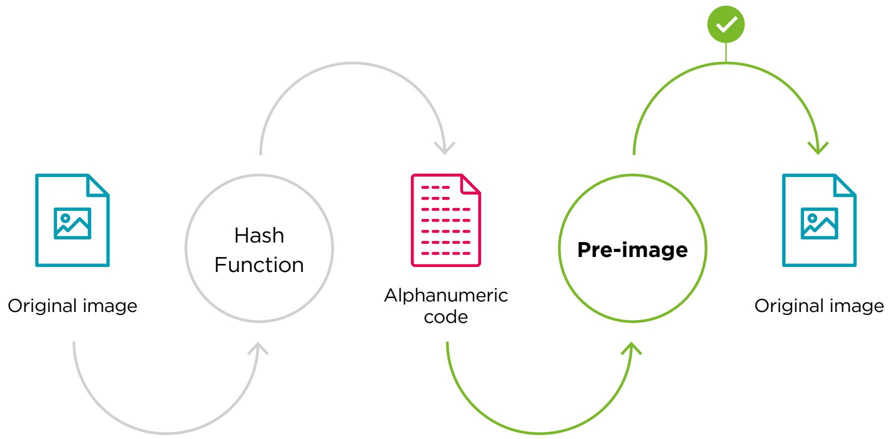
The blockchain will be secure as long as the hash function used for encryption meets two known conditions: **pre-image and collision resistance.**

[10] To be precise, the public key and the wallet are not always the same. In fact, it is important to highlight the difference, which will be explained in the following section. In the most important networks, the public key is generated with asymmetric cryptography from the private key and then hashed to give way to the wallet, so that the wallet is the hashed public key. This is due to space limitations, not security.

Pre-image resistance

A hash function is said to be pre-image resistant if the message that contains a specific hash value is impossible to find within a reasonable timeframe. Hash functions are required to disable a hacker from having a better strategy than brute-force to reverse them.

FIGURE 7. Concept of pre-image.

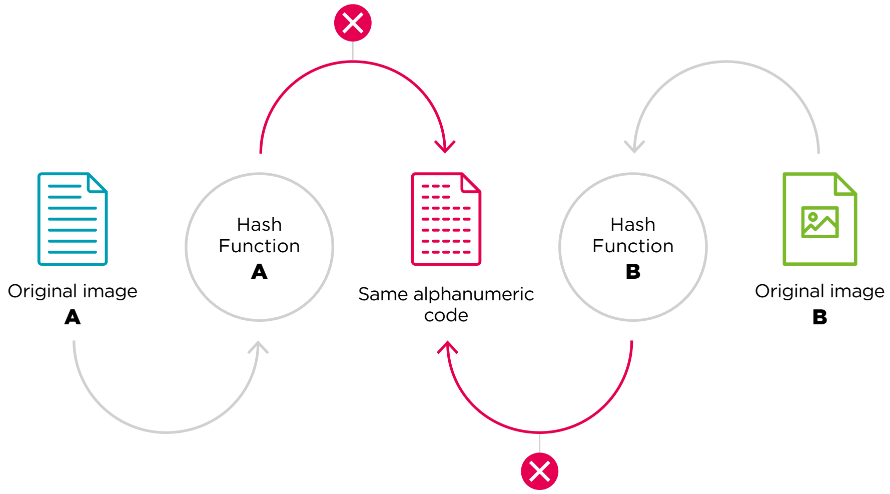


Collision resistance

A hash function is said to be collision resistant if two different messages (transactions or blocks) cannot get the same hash within a reasonable timeframe.

Note that the number of combinations of transactions that define the content of a block are infinite, while the number of possible hashes resulting from the encryption of the blocks are finite because they are alphanumeric codes of a certain length. They are also restricted in that they must start with a given number of zeros. As any string of any size that is passed as an input to a specific hash function gives as an output another string of a fixed size, the input space is much bigger than the output space. In fact, it is infinitely bigger. Because of this, you cannot require a hash function to always give two different outputs for two different inputs. However, you do require it to be rare enough not to happen within the time you will be using that hash function; that is the timeframe mentioned above.

FIGURE 8. Concept of collision.



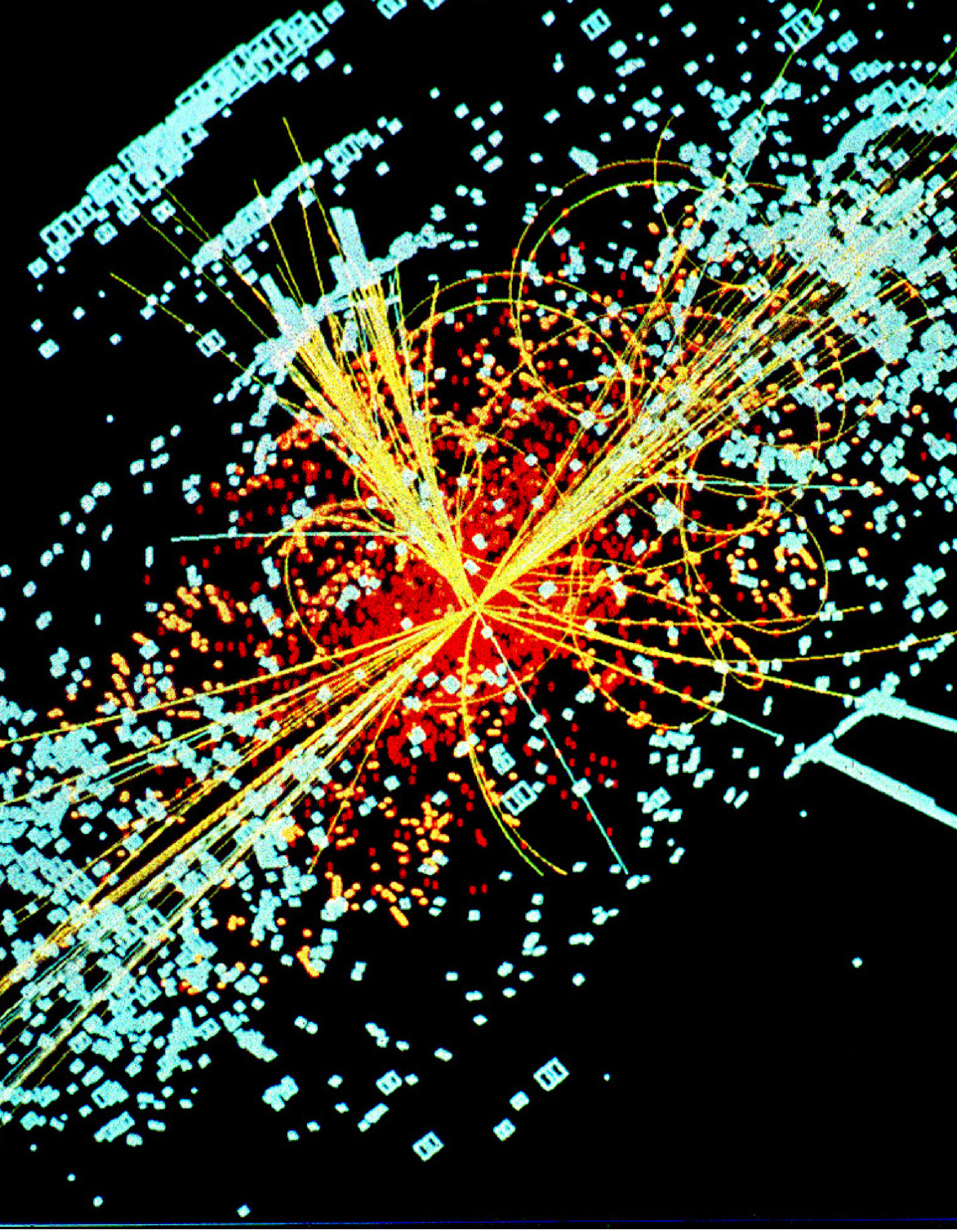
THE FUTURE OF BLOCKCHAIN IN THE QUANTUM ERA

Quantum technologies will affect blockchain technology in at least 4 different areas. The influence of quantum technologies on blockchain will primarily be related to the two security pillars, pre-image resistance and collision resistance, described on the previous page, cryptography, and to blockchain's use of the Internet and classical servers or computers. These four areas are: **(i) authentication, (ii) block mining, (iii) reversibility of hash functions, and (iv) the use of the Internet and its protocols for the communication between nodes and wallets.**

Quantum technologies and authentication in blockchain

Blockchain technology uses asymmetric cryptography to generate **public key - private key** pairs for participants. Elliptic Curve Digital Signature Algorithms (ECDSA) are the most widely used algorithms for blockchain asymmetric cryptography.[11] As stated several times throughout this document, quantum computing will be able to effectively break this kind of encryption (thanks to the Shor algorithm [17]) with critical consequences. End-user level blockchain authentication is only safe if hackers are unable to find the end-user's private key, which gives access to their assets stored in the wallets.

[11] Specifically, the two main public networks, Bitcoin and Ethereum, use the parameters in the secp256k1 ECDSA curve proposed by Certicom [60,61,62] and Hyperledge. The most widely used network software for private and federated (permissioned) networks uses the prime256v1 curve, with the authorization of Ethereum [63].



An example of simulated data modeled for the CMS particle detector on the Large Hadron Collider (LHC) at CERN. Here, following a collision of two protons, a Higgs boson is produced which decays into two jets of hadrons and two electrons. The lines represent the possible paths of particles produced by the proton-proton collision in the detector while the energy these particles deposit is shown in blue. Lucas Taylor / CERN. October 1997.

There is still no known way to reverse hash functions with quantum algorithms. Because wallets are not the public keys in themselves, but rather the result of hashing them, knowing a wallet does not allow a hacker with a quantum computer to find the blockchain user's **private key** that gives access to the wallet. They would have to reverse a hash function to get the public key from the wallet and then reverse the asymmetric cryptography algorithm to get the private key from the public one. With digital or classical computers, none of these two processes are feasible, but quantum computing offers an advantageous solution for the latter. Quantum computers can find private keys, as public keys are disclosed in the blockchain network when the user makes a transaction. At the moment in which the public key is disclosed, **a quantum computer that is powerful enough can use Shor's algorithm** [17] **to apply reverse engineering and find a user's private key within minutes,** as there is no longer a hash function protecting the public key. The moment this happens, that user's identity and assets in the blockchain can be stolen and sent to a different account without any possible way of claiming them back.

One way to minimize the threat this poses is to regenerate the pairs of keys following each transaction. Even if this practice was always followed, the threat still remains while the transactions are in the process of being accepted and incorporated into the synchronized copies of the ledger. For the transaction to be accepted by the blockchain nodes, it must be incorporated into a block, which must be supported by the network. In some instances, there are blocks that are not supported by the network, and the transactions, despite having been able to enter the block, have not reached the longest version of the chain and thus, are not accepted by the blockchain. In the Bitcoin network, one block is published every 10 minutes on average. The acceptable amount of time for the blockchain node pushing the transaction to wait is until the other six blocks have been added subsequently in order to make sure that the block and its transactions have been accepted by the network. This process takes close to one hour. During that period, the **public key** is disclosed to the network, and a quantum computer that is sufficiently fast and powerful enough could use it to find out the **private key,** access the account, and steal the property -including that which is being transferred in the intercepted transaction - before it is consolidated in the blockchain and the key is changed and secure again.

According to the calculations made by two studies conducted at Waterloo University and the Microsoft Research Center, **the estimated number of logical qubits needed to implement quantum algorithms that are capable of breaking 256 bit-long encrypted digital signatures generated with ECDSA currently used in these networks, are 1500** [12] **and 2330** [13]. It remains uncertain the amount of physical qubits this is equal to, but experts estimate that a logical qubit could require more than a thousand physical qubits. According to extrapolations made by a third study conducted by researchers in Singapore, Australia, and France, **in 2027 there will be quantum computers powerful enough to break private keys in less than 10 minutes** [64]**.**

Thus, there is a pressing need to change the key-generating algorithms in blockchain. There are three ways to do this, as we discussed in the section on cyber security:

- **Using more sophisticated algorithms to generate asymmetric keys,** also known as ***"post-quantum cryptography"*** **(PQC).** However, the security of PQC is temporary because eventually, they will be broken. Discussed in the previous section, the NIST is in the process of evaluating a public call for proposals [41] for a better solution and the European initiative, PQCrypto, has identified the hash-based algorithms, SPHINCS [65] and XMSS [66], as being the best alternative candidates so far [42].

- **Using quantum symmetric cryptography.** As it stands, quantum technology allows us to (i) generate completely random symmetric keys with quantum random number generators and (ii) share them in a completely secure manner by coding them into quantum states that change when observed. However, it is still unclear how to use quantum properties to develop asymmetric cryptography schemes, such as those currently used for authentication and digital signatures, as we are still at a very early stage in the development of quantum memories and quantum repeaters. The same is true in regard to quantum signature schemes, where progress is very slow, and the longest implementation distance for one of these protocols so far was 102 km in 2017 [49], discussed in the previous section.

- **Developing a new digital signature methodology that can use the quantum symmetric cryptography that is already available** to allow for completely different authentication and digital signature schemes, without the need for **public-private** key pairs. Although this has not yet been proposed, it would be more complex at the beginning because it involves a change in paradigm and the generation of new equipment, as quantum cryptography takes place at a hardware level. However, it would also be simpler in practice because it does not require the use of quantum symmetric cryptography to forcibly perform the asymmetric cryptography of authentication and digital signatures, as is the case with current quantum digital signature protocols.

So far there has not been a single documented initiative that has implemented one of these alternatives, or any others, to improve the lack of security surrounding authentication in blockchain. The most remarkable proof of concept thus far might be one conducted by Russian researchers in July 2018. It reports the use of quantum digital signatures [67], which corresponds to the second bulleted solution described above. In their November 2018 issue, Nature published the same group's analysis of the threats quantum computing poses for blockchain, as well as the potential quantum solutions that need to be developed [68].

Surprisingly, the reaction and movement from the blockchain community in response to warnings of these impending threats has been minimal to non-existent. In fact, a significant part of the blockchain community is not even interested in understanding the threat that quantum computing poses for blockchain. For example, at the largest blockchain event of the year, Consensus 2018, which gathered more than 8,500 people together in New York City, there were no presentations or panels about the issue. The same was true at the most important blockchain event in Latin America, Labitconf 2018, held in Santiago, Chile.

Despite the majority of the blockchain community's ignorance to the threat of quantum computing, some blockchain community leaders have reacted. For example, one of the most important and well respected figures in this community, Vitalik Buterin, who established Ethereum in 2015 [69], has acknowledged the concerns surrounding the threats of quantum computing. He has also showed his satisfaction with Lamport signatures [70], a hash-based scheme, and has spoken of his intentions to include it in his digital signatures once quantum computers become a tangible threat [71,72].

We must note that any proposed solution will pose extra challenges to the blockchain community. It will be difficult to reach consensus on making major changes to the public networks or on updating all the digital signatures of all active accounts. However, it is very important that these debates become real as soon as possible because **all downloaded data that is currently encrypted with classical asymmetric cryptography will be vulnerable to decryption through future quantum computers.**

Quantum technologies and the reversibility of hash functions

For now, blockchain is in luck as there are no known quantum algorithms that can optimally reverse hash functions, even though there is no mathematical proof that they are *not* reversible [73,74]. Thus, the **resistance to pre-images is safe for now but there is no guarantee that this will always be the case.** The day this happens, blockchain technology as we now know it will become obsolete.

In regard to **collision resistance,** the other significant security feature of hash functions, safety **depends exclusively on the "quality" of the hash functions and therefore, the safety of collision resistance will not change with the advent of quantum computing.** If the functions are good enough, and are not used for too long, it will be highly improbable for two different chains of data to have the same hash.

Quantum technologies and block mining

Another area that will be impacted by quantum technologies is block mining. Quantum computers will be able to run Grover's quantum algorithm [75], which allows us to find a specific element in a disorganized list of N elements in $\sqrt{N}$ number of steps. Classical computing needs $N/2$ steps on average to do the same. Mining blocks in blockchain is similar in a way to finding a specific element on a list. Mining involves searching for a random piece, called a **nonce.** The nonce is concatenated to the rest of the elements in the block (block number, transactions, hash of the previous block, etc.) and gives a valid hash.[12] Therefore, quantum computers will be able to mine blocks by running a quantum algorithm a fewer number of times to find the hash.

[12] In public networks, such as Bitcoin or Ethereum, there is a competition to find the hash in each block, for it entails a reward in the form of cryptocurrency. In Bitcoin, that reward is currently 12.5 Bitcoins, equivalent to about $50,000, in March, 2019. At its highest point, in January of 2018, it reached $237,500. It is this reward that motivates the computational and energy expense undertaken by these miners.

Bitcoin, the most popular public network to date, requires the average number of hashes that need to be attempted in order to find the valid one and win the consensus protocol, or "proof of work," to be $2^{256}/t$, where t is a parameter that is recalculated every 2016 blocks. It is recalculated this often so that the difficulty to hack is maintained according to the mining community's guideline that, on average, it takes them 10 minutes to find the valid hash. The difficulty can be defined as $D = 2^{224}/t$, which is the number above divided by the number of nonces available, which is 2^{32} [23]. As of January 2019, the difficulty is $D = 5 * 10^{12}$ [76], which, using the formula above, means that a classical computer will have to make about $4.19 * 10^{29}$ attempts on average. In theory, a quantum computer would only need to make approximately $6.48 * 10^{14}$.

A study conducted by institutions in Singapore, Australia, and France determined that quantum computing will not be capable of mining blocks faster than the classical devices currently used for this process (ASIC) [77] within the next decade. They establish that the number of logical qubits[13] needed to mine blocks efficiently would be 2024, which they expect to become a reality between the years 2025 and 2030. They do not expect quantum computers to be able to do this before 2030 because ASIC devices have been very efficiently designed for this purpose and will continue to be better than quantum computers in doing so until then. Once quantum computers are able to efficiently mine blocks, they will do so 100 times faster than the ASIC devices [64].

Once this happens, the problem it will cause will not be critical and the solution to safeguarding blockchain security will remain simple. In the case that the current consensus protocols are maintained, **it is always possible to increase the level of difficulty to make up for the increase in speed offered by quantum computing. Cuckoo Cycle** [78]**, Momentum** [79] **and Equihash** [80] **are proposing new consensus protocols** which offer a higher resistance to quantum computing. Although they continue to apply hash functions to the information in the blocks, the validity conditions of the blocks now apply not only to the nonce, but also to the header [81], in such a way that it will not be enough to simply iterate over a succession of elements until the valid hash is found.

Quantum technologies and the use of the Internet

In the section on cyber security, we analyzed some Internet security threats that will come with the rise of quantum computing. These same threats directly affect blockchain because it uses the Internet. Two adverse consequences will affect blockchain in the context of using an unsafe Internet network:

- Node and wallet identity thefts.
- Practices known as "man in the middle" (MITM), which consist of an unauthorized third party that intercepts and changes information exchanged between a wallet and a node or between nodes.

[13] Logical qubits are used for the processing. However, for error correction, each one of these qubits is accompanied by several other qubits, known as physical qubits.

For details on the possible ways to obtain a secure Internet in the era of quantum computing, please refer to the discussion in the cyber security section.

Finally, it is worth briefly mentioning the existence of proposals to build entirely quantum blockchains that are based on the entanglement phenomenon and on the impossibility of copying quantum states [82]. Recall that quantum systems change when observed, rendering cloning impossible, as we explained in the section on quantum technologies [14]. Once developed, quantum blockchain technology will be significantly different from current blockchain technology and will offer complete security because it will be based on physical processes, rather than on the mathematical difficulty of reversing hashes or digital signatures. Recall that this is the same reason quantum cryptography is naturally more secure than the limited security offered by classical cryptography, explained in the section on quantum cryptography. In the event that quantum computing eventually allows for effective reversal of hash functions, a quantum blockchain solution seems to be the only viable one for blockchain's future.

ARTIFICIAL INTELLIGENCE

WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence (AI) has been defined in many ways. For the purposes of this paper, we will refer to AI as the ability for machines to exhibit behaviors that are similar to those of human beings, such as reasoning, learning, perceiving, planning, being creative, and solving problems.

There are certain disciplines in the field of AI such as machine learning, neuronal networks, language processing, image recognition, voice recognition, etc., which, together, provide the machine with the ability to display human behaviors. With increasing frequency, the algorithms behind these subcategories are designed to learn autonomously, as they are fed with data.

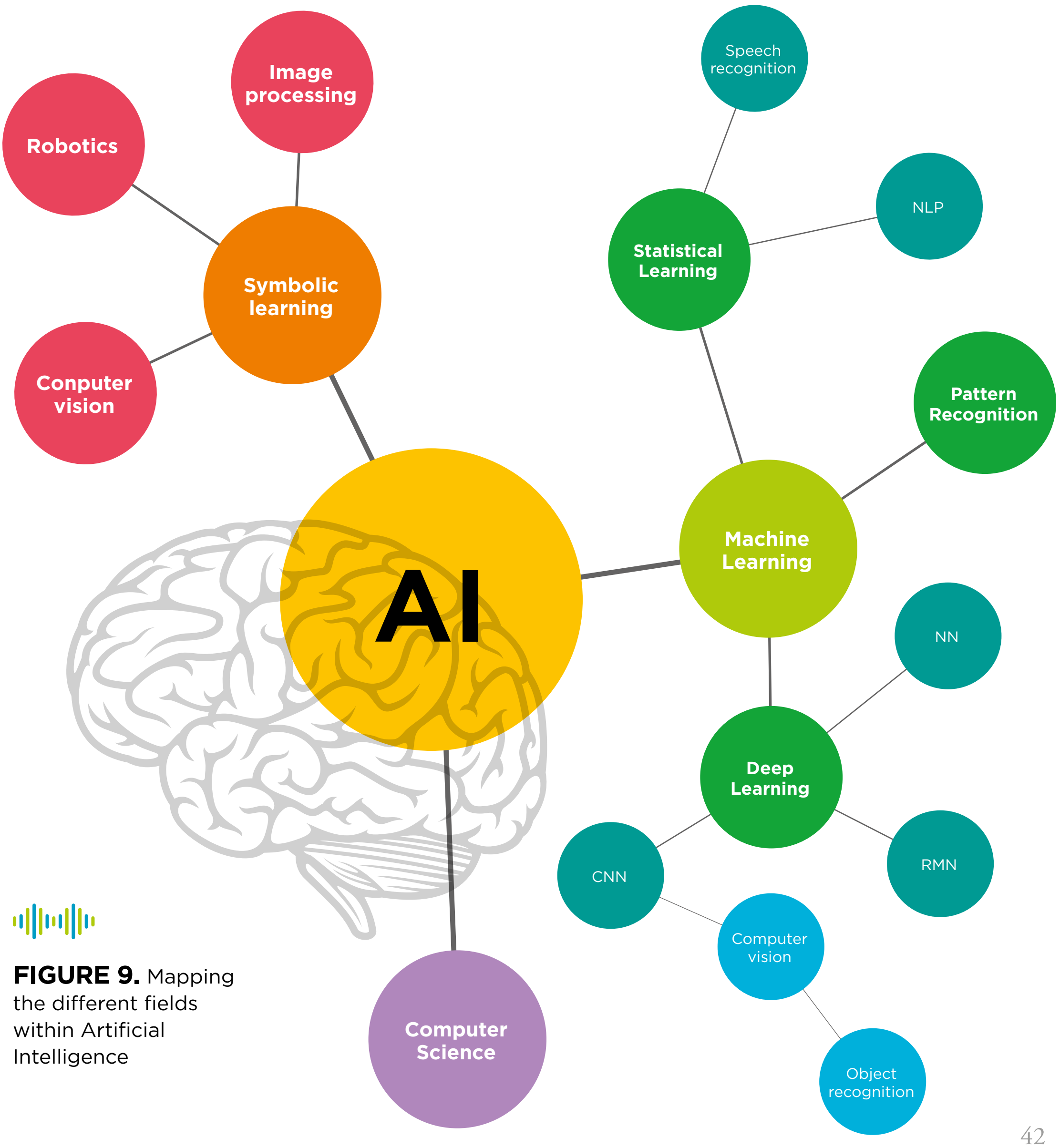


FIGURE 9. Mapping the different fields within Artificial Intelligence

The abilities of AI machines are usually classified into four levels depending on the degree of the machine's behavioral sophistication:

- Reactive: Ability to respond to stimuli or input in real time without taking into account past experiences or memorizing processes.
- Limited memory: Ability to respond to stimuli or input by making decisions that take past experiences that are stored in a memory into account.
- Theory of mind: Ability to have their own thoughts and feelings which influence their decisions and their interaction with the world.
- Awareness of self: Ability to be aware of their own consciousness and existence, and to understand themselves apart from simply understanding human beings.

The last of the four levels is associated with the ideal concept of artificial intelligence, in which machines are capable of fully simulating an intelligence that is similar to that of human beings. However, thus far, it has only been possible to develop AI machines with the capacity for the first two levels. This has been a significant point of frustration and disappointment.

THE FUTURE OF AI IN THE QUANTUM ERA

It is possible that the implementation of quantum computing is just what AI needs to reach more advanced stages [83-85]. There is currently a growing active field of research in quantum artificial intelligence and quantum machine learning.

Since the year 2000, research has been published on the ways in which quantum computing can be applied to the mapping of language expressions [86], game theory [87], image classification [88], coordination problems [89], natural language processing [90], economic strategies in the context of public goods games [91], and even quantum artificial life [92].

A study showed that the main areas in which quantum computing could be applied to AI in the short term with a processor of around 1,000 logical qubits are **(i) problems that are currently hard and intractable for the ML community, for example generative models in unsupervised and semi-supervised learning, (ii) datasets with potentially intrinsic quantum-like correlations, as in cognitive sciences (iii) hybrid algorithms where a quantum routine is executed in the intractable step of the classical ML algorithm pipeline** [93]**.**

The ability to address exponentially complex problems in AI rests on the premise that quantum computing will be able to do mathematical operations which are not yet possible. For instance, current social platforms collect massive amounts of data per second that cannot be used to make real-time recommendations because the necessary computing capacity to do so is not available. This also applies to traffic regulation in the transport sector and to the prediction of financial crashes in the financial sector, as we will discuss later in this document.

In 2014, four Chinese researchers published the first implementation of a machine-learning quantum algorithm in a four-qubit processor [94]. The algorithm they implemented was the quantum version of the support vector machine (SVM) technique, a supervised algorithm capable of classifying new data from existing data that have been pre-divided in groups. The technique they implemented is known as quantum support vector machine (QSVM), and it was applied to the problem known as optical character recognition (OCR), used for text digitalization. The aim of the experiment was for the quantum processor to identify the numbers 6 and 9 in writing. To do this, a machine was trained with images so that it could understand a written 6 and a written 9, and succeeded in classifying them.

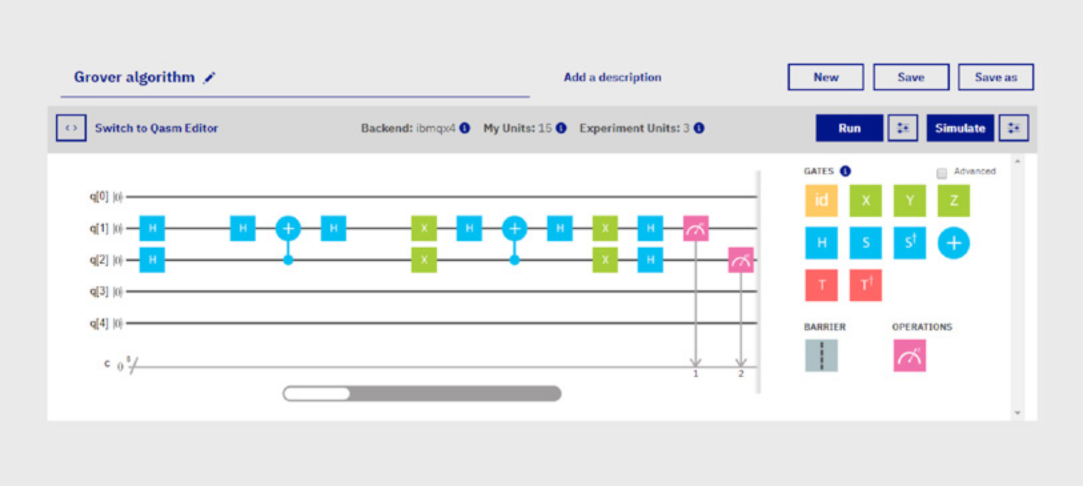
There are several theoretical studies that discuss the fusion of AI and quantum computing, proposing algorithms in the areas of deep learning and neural networks, among others [95-107].

There are already many online quantum computer simulators that can start testing these kinds of algorithms. They use various existing programming languages such as C, C++, Java, Matlab, Maxima, Python and Octave, and new ones, such as Q# [108]. The Rigetti Forest [109] and the IBM QISKit [110] stand out among the most popular platforms to play with a virtual quantum machine.

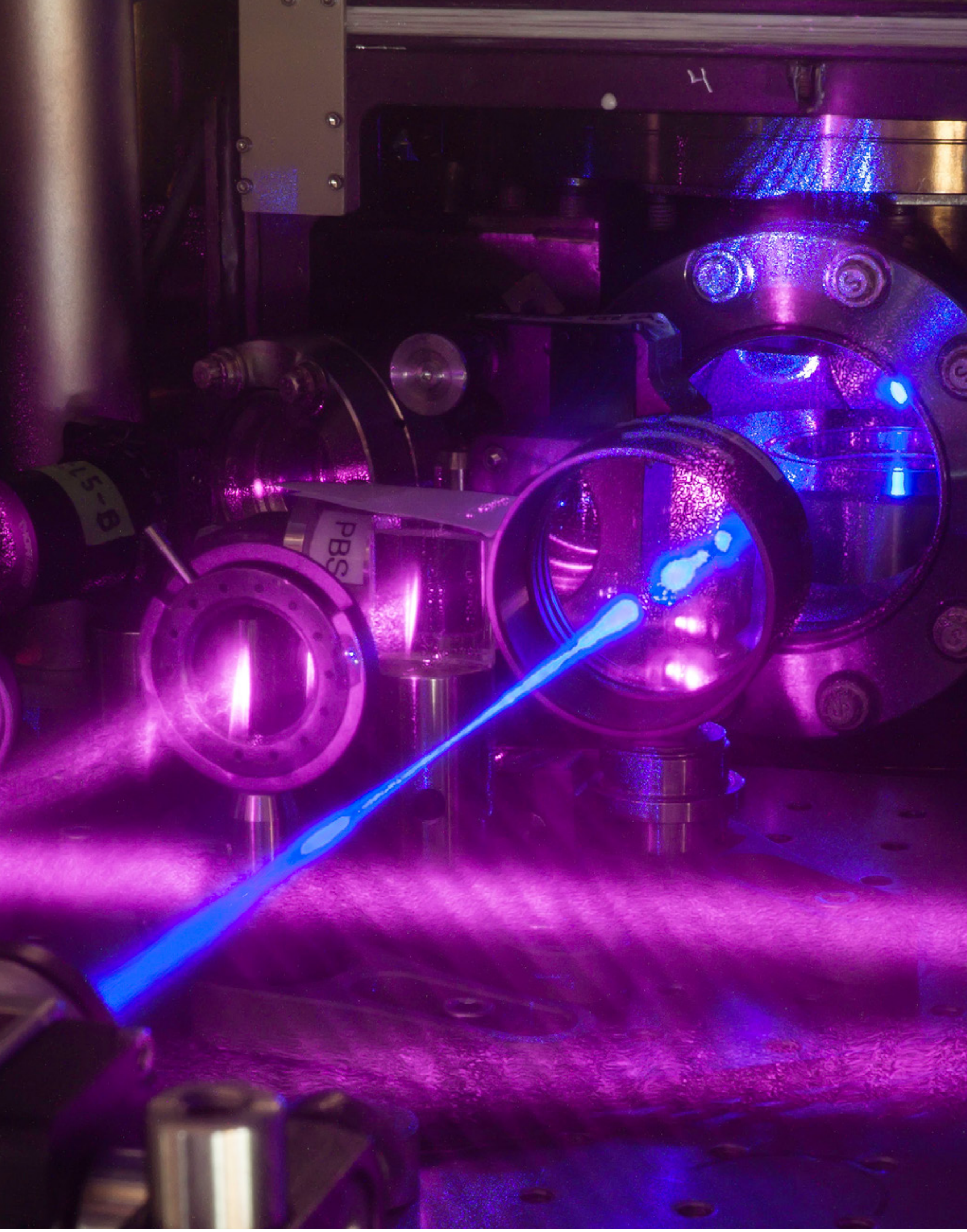
A very interesting study [111] simulates **quantum artificial life** [92], which consists of imitating the processes of reproduction, mutation, interaction, and death. In it, pairs of qubits serve as individuals, with one qubit representing the genotype and the other, the phenotype. The information is coded in the genotype and communicated generation after generation.

In concluding this section, we want to highlight that although this is a very new field (most of the literature consists of 2018 publications), there is a growing community of researchers who are quickly generating large amounts of knowledge in this area. As virtual machines and real quantum computers introduce more qubits and become more robust, quantum AI will become a reality. Because of this, it is possible that machines may eventually develop the capacity for emotions and consciousness. The effect this development could have on the world is immeasurable.

FIGURE 10. Grover's algorithm for 2 qubits running on IBM's online quantum simulator.


Grover algorithm

Backend: ibmqx4 My Units: 15 Experiment Units: 3



JILA’s three-dimensional (3-D) quantum gas atomic clock consists of a grid of light formed by three pairs of laser beams. A stack of two tables is used to configure optical components around a vacuum chamber. Shown here is the upper table, where lenses and other optics are mounted. A blue laser beam excites a cube-shaped cloud of strontium atoms located behind the round window in the middle of the table. Strontium atoms fluorescence strongly when excited with blue light. Credit G.E. Marti/JILA

OTHER TECHNOLOGIES

THE INTERNET OF THINGS (IOT) AND DRONES

One of the fastest growing emerging technologies is the Internet of Things (IoT), which refers to a network of devices connected through the Internet. According to Ericsson, the number of these devices will exceed 25 billion in 2020 [112] and according to Bain, it will generate more than 300 billion US dollars per year, [113] primarily in the sectors of agriculture, automobiles, and infrastructure [114].

The company, QLM Technology, has developed an application combining IoT, drones, and quantum sensors. They mounted a quantum sensor on a drone that is capable of detecting natural gas leaks at a 150-meter distance, moving at a speed of up to 38 km/h. Quoting its founder, this provides "10 times more sensitivity than its competitors to detect these leaks, which cause losses between 6 and 35 billion US dollars for the natural gas industry per year" [115].

An article published by Telefónica in 2017 discussed the great impact that quantum technologies are expected to have on the IoT, highlighting the need to use quantum information to create quantum telecommunication channels connecting these devices in a secure manner, and quantum computing to make them smarter and more efficient [116]. Furthermore, it agreed with GrowthEnabler in the idea that Smart Cities will be one of the sectors that benefit the most from the IoT [117]. Articles published in Forbes [118] and IDQuantique's [119] contain further information.

5G

The rapid increase in the number of devices connected to the Internet has created an urgency for the development of 5G, the fifth generation of mobile communications. 5G will offer higher speed at a lower latency in data upload, traffic, and download. The efforts to develop this technology are geared towards making it quantum-safe so that it is resistant to the threat of quantum computing in hacking communications.

A study published by Deloitte in 2018 acknowledges 5G development efforts by several countries including the USA, South Korea, Japan, and Germany. They note that China stands out from the pack as it has made significant investments in infrastructure and towers and is considered to be the current leader in terms of development and implementation of 5G networks. For example, since 2015, China Tower, the largest telecommunications tower manufacturer in the world, has invested 17.7 billion US dollars in capital and added more than 350,000 infrastructure points in China [120].

South Korean company, SK Telecom, has made significant movements in merging 5G technology with quantum cryptography. In 2017, at the Mobile World Congress in Barcelona, they signed an agreement with the German company, Deustche Telekom, to “guarantee secure telecommunications in the quantum era” [121] as well as another agreement with Nokia to “work jointly in quantum cryptography” [122]. One year later, at the same event, they announced a 65 million US dollar investment in the leading quantum technology manufacturer for cryptography, IDQuantique [123].

These alliances have already proven to be successful. In June 2018 Deutsche Telekom announced [124] that it would be running trials involving quantum cryptography systems (quantum random number generators and quantum symmetric cryptography protocols) in its test network in Germany [125,126]. A few months later, in September 2018, satisfactory interoperability tests were reported between IDQuantique’s asymmetric cryptography systems and the Nokia Secure Optical Transport solution [127] on SK Telecom’s commercial telecommunications network in Seoul, to connect real data in production in Korea, between the Bundang and Jung-gu districts [128].

Furthermore, in South Korea, SK Telecom, KT and LG Uplus have agreed to work collaboratively with one another in the development of a 5G infrastructure for the entire country [129]. Together, these three telecommunication companies are advising the International Telecommunications Union (ITU), the UN agency responsible for information and communications technologies in the drafting of documents [130]. The ITU develops standards for governing the establishment of telecommunications networks, including 5G and quantum cryptography technologies that are interoperable across the world. These kinds of standards are essential to ensuring the various emerging initiatives in different countries are scalable and interoperable.

In the United States, Quantum Xchange is the country’s first company to develop a commercial network that incorporates quantum cryptography [131]. It will “connect the financial markets on Wall Street with back office operations in New Jersey, helping banks keep high-value transactions and mission-critical data safe and secure” [132]. This telecommunications company entered into an 8.9 million US dollar agreement with SK Telecom [133] for it to provide quantum cryptography systems.

3D PRINTING

The development of quantum sensors has already been empowered by 3D printing, which consists of building three-dimensional objects by adding material layer by layer under computer control.

In the last few years, there has been significant progress in the preparation, control, and measurement of atomic gases. This has allowed for the development of unprecedented quantum sensors that provide significantly higher precision to the measurement of magnetic and gravitational fields. It can be used in biomedical scanners, non-invasive underground mapping, or GPS navigation [134,135]. 3D printing can effectively manufacture portable quantum sensors for these applications. Different working groups have already been using additive manufacturing techniques (the industrial name for 3D printing) to manufacture atom traps, vacuum chambers, and magnetic shields [136,137], which are essential devices in the fields of quantum sensors and metrology.

IDB

QUANTUM TECHNOLOGIES

Digital transformation, social impact,
and cross-sector disruption

IMPACT ON SECTORS AND INDUSTRIES

00 01 10 11

IMPACT ON SECTORS AND INDUSTRIES

In the previous sections, we discussed quantum information and quantum computing in detail. While these might be the two most disruptive fields for the future of quantum technologies, there are many others that will also be impactful across several industries and governments. Thus, in this section we will discuss the social impact of quantum simulators, quantum optics, quantum metrology, atomic clocks, and quantum sensors in addition to that of quantum information and quantum computing. Sectors and industries as medicine, biology, genetics, education, finances, economy, agriculture, transport and meteorology will be provided with a new set of useful quantum tools. We consider it necessary to begin this section with a brief description of all these emerging quantum technologies.

QUANTUM COMPUTING

Quantum computing is the most widely known quantum technology. It has the potential to crush the computing capacity currently available with classical computing and has potential applications in all fields imaginable. Since the year 2000, universities and large technology firms such as IBM, Google, Microsoft, and Rigetti have been racing to develop quantum computers that can hold more and more qubits. As of late 2018, Google holds the record, with 72 qubits. Despite the fact that some smaller issues have been resolved on a case-by-case basis, none of these new quantum computers have shown an advantage over digital or classical computing yet. Once they are able to surpass classical computing in their problem-solving abilities, we will have reached what is known as quantum supremacy, which is expected to happen very soon. Several experts have predicted that in only 10 years' time, sufficiently robust quantum computers will exist that are capable of achieving significant milestones, including the breaking of all existing asymmetric cryptography.

QUANTUM INFORMATION

Quantum information is the field that studies quantum quantification, storage, and data transfer. It includes the area of quantum cryptography, which will offer a completely new way of protecting information and data from both classical and quantum computing interception efforts. Quantum cryptography was successfully tested for the first time more than 10 years ago. Switzerland, for example, has been using quantum encryption to protect national election data between the data counting and storage centers since 2007. Currently, China is the leader in this field. In 2016, it launched the first satellite that enabled quantum encrypted intercontinental communications that eventually allowed for a 90-minute long videocall to Austria in 2017. It hosts and operates the largest ground-based quantum commercial network that is more than 2,000 km long. Predictions expect a quantum telecommunications network between Asia and Europe within the next decade, and a global network by 2030.

QUANTUM SIMULATORS

A quantum simulator is a quantum physical system that can be prepared or manipulated to allow for the study of the properties of a complex quantum or classical system. This is achieved either by reproducing the systems at a smaller scale under controlled conditions or by working effectively with the mathematical function describing the system's dynamics. There are different types of quantum simulators that can solve problems that classical computing cannot, but unlike quantum computers, they are not universal. This means that they cannot solve "any solvable problem". They are programmed to tackle specific problems or situations.

ATOMIC CLOCKS

Atomic clocks measure time based on natural microscopic processes with extremely small periodicities and extremely high precision. In contrast, traditional clocks are based on the frequency of mechanical processes far less precise. Since 1967, a second has been defined as the duration of 9,192,631,770 oscillations of a ^{133}Ce atom. The natural frequency of atoms of the same element -in this case, Caesium- is constant and does not depend on the environment surrounding it. Atomic clocks using this phenomenon have already been built. As an example of its precision, it is worth noting that if two atomic clocks had been built and synchronized during the Big Bang, there would not be a second's difference between them today.

QUANTUM METROLOGY

Quantum metrology is the study of the use of physical systems with quantum properties, such as entanglement, used to make precise and sensitive measurements. Again, this field is very important for quantum information, communication, and cryptography.

QUANTUM OPTICS

Quantum optics is the field that deals with the quantum processes and phenomena occurring at the microscopic level in the interaction of photons and matter. This field is essential to the fields of quantum information, communication, and cryptography because it is at the very basis of understanding photons. It is also useful in the manufacturing of all kinds of high-precision light sensors that are cheaper, smaller, and easier to manipulate than traditional light sensors. Quantum sensors are becoming very useful in several industrial processes.

QUANTUM SENSORS

Quantum sensors use quantum properties in physical systems to obtain high sensitivity and resolution. As we will discuss later, they are widely used in medicine. Quantum imaging is an example of a quantum sensor and can be used in very high sensitivity cameras, essential for self-driving vehicles.

IMPACT ON MEDICINE, BIOLOGY, AND GENETICS

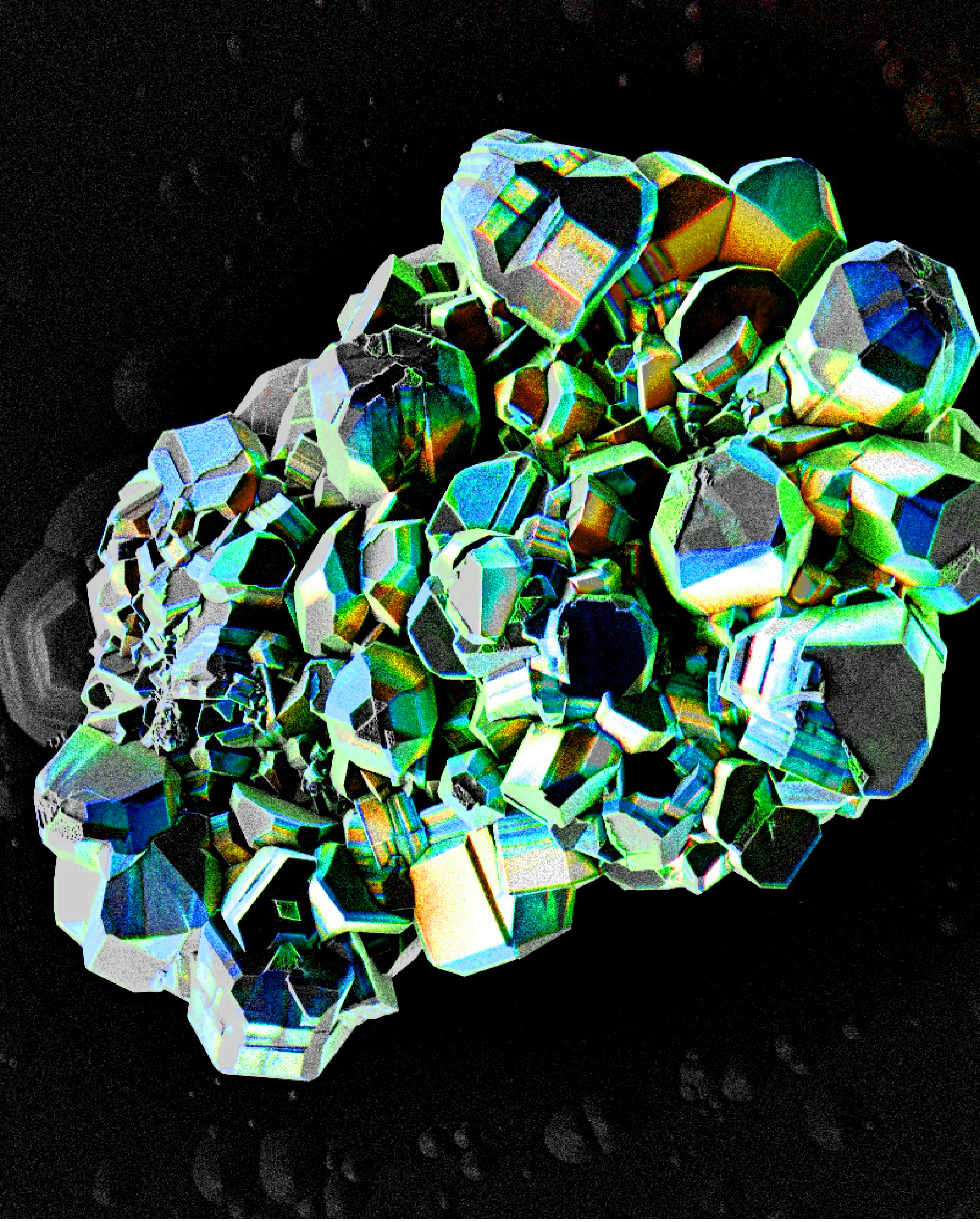
The various fields within the biomedical sciences have already taken advantage of quantum technologies. For example, magnetic resonance imaging (MRI), which helps detect tumors and other diseases in a non-invasive manner, and lasers, which are used in multiple kinds of high-precision surgeries, are two types of quantum technologies that have been used successfully for decades in this field. Quantum technologies will open doors to new techniques and processes that are impossible to reach with the existing biomedical technology.

Simulation and quantum computing have the potential to reproduce the biochemical interactions of drugs within organisms, allowing scientists to design targeted drugs. Currently, it is impossible to simulate even the dynamics of a simple molecular system with classical computers.[14] In most cases, drug development involves years of clinical testing on animals and humans in the discovery, clinical, and pre-clinical stages [140]. The use of this technology would cause a disruptive leap in drug design.

Quantum optics will also offer significant biomedical applications. The branch of quantum optics with surface plasmons —quasiparticles corresponding to quantum plasma oscillations— makes it possible to conduct very precise studies on and measurements of the dynamics of live cells. Not only does this allow us to make non-invasive nanospectroscopies, but also to **disrupt, manipulate, and ultimately, control, live organisms at the molecular level.** The use of this technology for molecular diagnostics, precision medicine, and nanobiology are limitless [141-143]. The Japanese National Institute for Quantum and Radiological Science and Technology (QST) **has already started using non-invasive techniques capable of detecting a solid tumor in 30 minutes.** They can map out the area at molecular level, defining the size and properties of the nanoplatforms that must be sent to obtain the best possible treatment and predicting their therapeutic efficiency. [144].

In 2017, the international consulting firm, Accenture, the quantum software company, 1Qbit, and the biotechnology firm, Biogen, started a collaboration to **"design the first quantum molecular comparison application** with potential to significantly improve

[14] When simulating microscopic processes, such as drug interactions within an organism, current computers are not capable of processing the interactions between atoms and molecules efficiently. If we increase the number of molecules, the number of steps a digital or classical computer will have to process increases exponentially. The simulation of a few molecules can take several years, making it impossible to simulate complex processes with the goal of making actual progress in the medical field. With quantum computing, however, the difficulty becomes polynomial rather than exponential: the amount of steps the computer must take increases at the same ratio as the number of molecules, allowing for these simulations to become achievable.



Indium-gallium nitride is a semiconductor alloy that emits light when irradiated by energetic particles. A small crystal cluster has accidentally grown during the w:MOVPE process. The lightness corresponds to its standard w:SEM image, whereas the colour overlayers were added according to the light emitted under the electron beam. Blue and green channels are roughly natural colours, while red encodes the ultraviolet emission. The image demonstrates that InGaN/GaN structures are highly anisotropic, and so are their cathodoluminescence properties. FDominec. 16 October 2017.

advanced molecular design to **accelerate the development of drugs to treat complex neurological diseases such as multiple sclerosis, Alzheimer's, Parkinson's or Lou Gehrig's disease"** [145]**.**

Another application of quantum technologies to the medical field will be the use of quantum cryptography to safeguard medical data. According to IDQuantique, world leader in hardware manufacturing for quantum cryptography, in the first semester of 2016, the medical records of more than 30 million patients were stolen in a total 263 security breaches from cyberattacks, which took an average of 233 days to be discovered and another 111 to be communicated [146].

In sum, quantum technologies will allow for more efficient clinical drug discovery, aid in elucidating mechanisms of complex diseases, help to further uncover the biology and the genome of living beings, and support better protection against medical record breaches, among many other applications.

IMPACT ON EDUCATION AND JOBS

As we mentioned earlier, we are witnessing an era of fast digitalization, which creates great demand for technological innovations in every sector. Currently, in Latin America and the Caribbean, most technological and computer science education in elementary, middle and high schools is either too basic or non-existent for the complexity of knowledge needed for a successful scientific and technical career. Undergraduate and graduate courses in relevant science and technology subjects seem to evolve at much slower speeds than the market demands, leading to an alarming number of vacancies in technology-related positions around the world. According to the consultancy firm Allen & York, the number of vacancies will reach 800,000 in 2020 in the UK alone [147]. Further, in "The Future of Jobs", the World Bank highlights the need to educate and create technology-related jobs in Latin America and the Caribbean in order to maintain growing levels of productivity and prosperity and to decrease poverty levels [148].

Regarding jobs related to quantum technologies in particular, the issue is much more serious. While it is possible to succeed in many different technology-related jobs after having studied various bachelors and masters degrees, **jobs in the field of quantum technology require an understanding of Physics that is difficult to acquire without studying it in depth.** There is already unmet demand for personnel who understand quantum physics in companies supplying software and hardware services, as well as in start-ups and consultancy positions. Because the depth of knowledge one must have in order to succeed in most of these careers is so necessary, the growing demand for these positions will be even harder to meet than it already is for technology careers that are not related to quantum physics. According to a report published in 2018 by BBCReport, the Compound Annual Growth Rate (CAGR) for the commercial market in quantum technologies will be 37.3% until 2022, reaching 161 million US dollars, and **a 53% CAGR between 2022 and 2027, reaching a total of 1.3 billion US dollars** [149]**.**

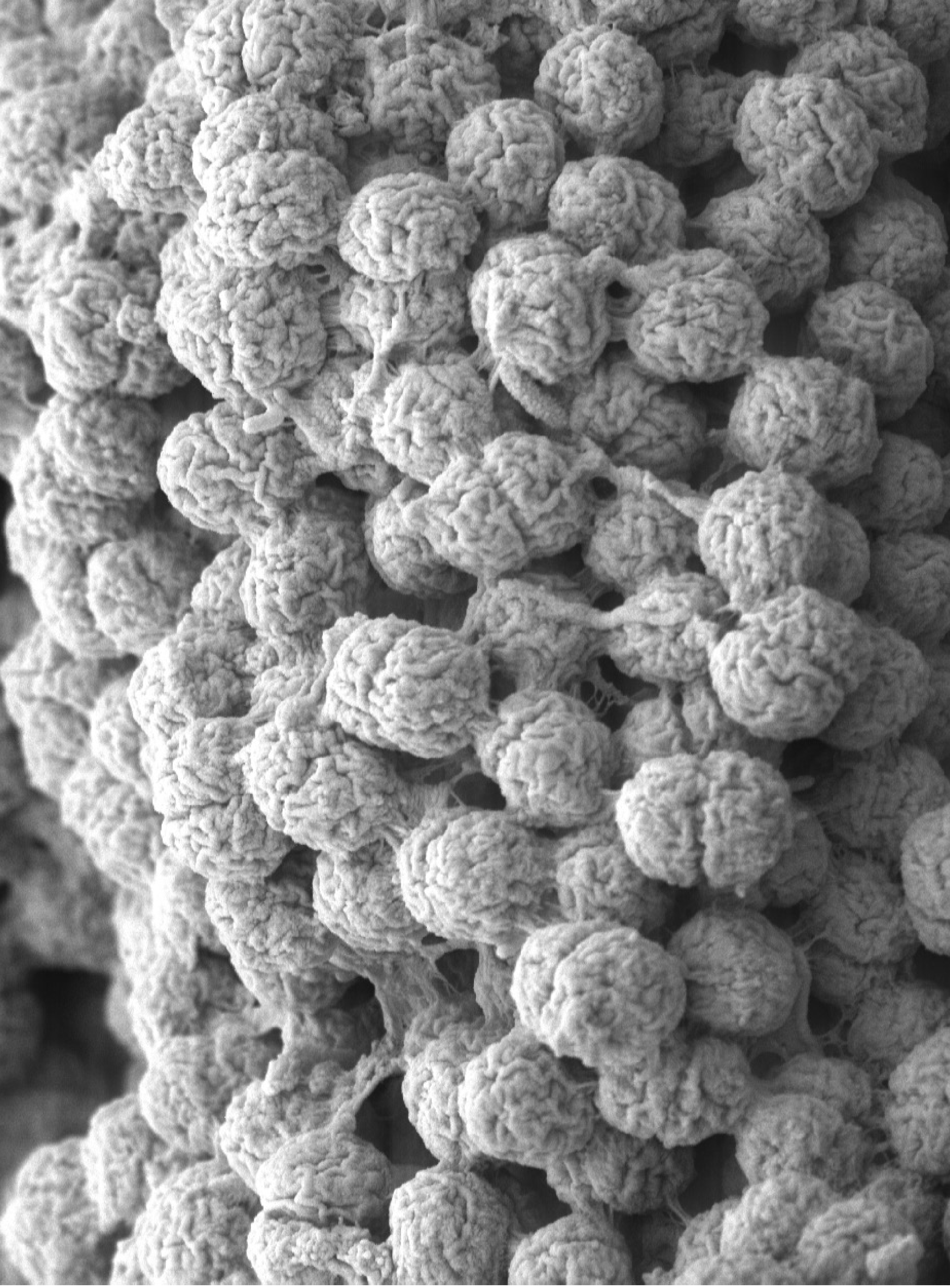
IMPACT ON ECONOMY AND FINANCE

Economics and finance will also change in the era of quantum technologies. **The capacity of quantum computers and simulators to solve complex problems and process large numbers of possibilities quickly and effectively will allow us to build, simulate, and improve financial models using quantum algorithms.** As we mentioned in Section I, quantum computing does not operate in the same way as classical computing. By exploiting quantum parallelism, quantum computers can evaluate various options simultaneously, rather than in sequence, cutting time and efficiently processing resources significantly. **Those who build financial models can also benefit from quantum randomness.**

Simulators, such as quantum annealers, are already operating in the market, effectively solving real problems with a large number of variables. To be able to effectively solve these problems, we must find the mathematical function that describes the real model. Then, optimization can be achieved by minimizing the function to find the optimum values of the variables.

Quantum annealers can be used to predict financial crashes. A 2017 study provided mathematical proof that predicting a financial crash is a problem that cannot be solved computationally, as it belongs to the NP-complete complexity class [150]. Specifically, it proves that even in simple financial networks where "the regulator has complete information about the entire structure of the financial network, and the only uncertainty is in which specific assets may decline in value […] calculating the number of institutions that can fail in a network is NP-Hard". This year, three members of the Quantum World Association (QWA) -R. Orús, E. Lizaso (both researchers and partners at Entanglement Partners), and S. Mugel- proved that "the equilibrium market values of institutions after a sudden shock to the network can then be calculated via adiabatic quantum computation and, more generically, by quantum annealers [...] providing a potentially more efficient way to predict financial crashes" [151].

Atomic clocks also have important applications in this field. Currently, the timestamp on economic transactions, requiring extreme precision and synchronization, depends on the GNSS in computational networks and on local atomic clocks, according to a report from the European Union [152]. Because of their high precision, they recommend the regulation and use of this technology more widely.



Algae in Scanning Electron Microscope, magnification 5000x. SecretDisc.

IMPACT ON SUSTAINABLE ENERGY AND AGRICULTURE

One of the most relevant quantum technologies in the areas of energy and agriculture can be seen in the production of ammonia, essential for the manufacturing of fertilizers. The ammonia production process consumes 2% of the world's energy per year [153]. According to the International Fertilizer Industry Association's annual report, 187 million tons of fertilizer were used in 2018. Between 2018 and 2022, growing demand will motivate a 98 billion US dollar investment in initiatives to build 60 new production units to produce 78 million tons more each year [154]. In Latin America and the Caribbean, the petrochemical industry is led by Brazil, Mexico, Venezuela, Trinidad and Tobago, Argentina [155,156].

Ammonia is essential for fertilizer production. The ammonia production process, known as the Haber-Bosch process, in honor of its inventors in the early 20th century, involves a reaction that results from the combination of hydrogen and nitrogen. It requires the dissociation of nitrogen, which only happens **under extreme pressure and temperature conditions, consuming close to 2% of the world's energy annually** [157]**.**

A new method to obtain ammonia at room temperature, using the enzyme nitrogenase, already exists [153]. Quantum computers allow us to simulate the process of ammonia synthesis using this method at a molecular level. It is impossible to do this same simulation using classical computers. **This new process will save 2% of the world's energy, will reduce the environmental impact of the ammonia production process, and will potentially lower the price of food.**

The energy sector will also directly benefit from quantum computers and simulators to process huge amounts of data and information. This will enable a much more efficient distribution of resources and aid in lowering the price of food.

OTHER IMPACTS

These will not be the only sectors and fields to benefit from quantum technologies.

For example, we will eventually be able to model the circulation of vehicles and citizens by using the large amount of data captured by applications, such as Waze and Google Maps, in real time. By optimizing mathematical models to simulate real situations based on existing data, quantum simulators can more accurately suggest optimum routes, better coordinate traffic lights to provide routes for emergency vehicles, simulate catastrophes, and analyze the necessary improvements to avoid them or minimize their consequences, etc. The advent of self-driving vehicles absolutely requires this quantum processing capacity and is one of the many future technologies in the field of transportation that will rely on quantum processes.

Quantum simulation will also facilitate major changes in meteorology. It will allow us to address complex weather phenomena more precisely and will give us the tools necessary to predict natural disasters.

QUANTITATIVE TRADING

Enhanced understanding of correlated variables and phenomena and their impacts on capital markets

MACHINE LEARNING

Enhanced training processes and power to calculate scenarios, alternatives and complex math

ROUTE OPTIMIZATION

Thanks to the ability to evaluate multiple scenarios with enhanced parallelism

PERSONALISED DRUGS

Ability to develop new drugs based on the better understanding of molecules information formation of genomics

POST-QUANTUM SECURITY

Crypto resistant to quantum computing thanks to the principle of non-observability and true randomness

SINTHESYS OF NEW MOLECULES

Based on the enhanced capacity to understand chemical reactions and simulate atomic interactions

WEATHER FORECASTING

Capacity to understand atmospherical phenomena thanks to the enhanced parallel computation

NEW MATERIALS

Development of new materials thanks to the ability to simulate molecule interactions and physical properties

IDB

QUANTUM TECHNOLOGIES

Digital transformation, social impact,
and cross-sector disruption

COUNTRY PROGRAMS AND STRATEGIES

00 01 10 11

COUNTRY PROGRAMS AND STRATEGIES

The major global powers and the most successful technology companies are aware of the potential of quantum technologies. Over the past few years, many have invested billions of dollars in the research and development of quantum technologies in hopes of leading the race to quantum power.

CHINA

The Chinese government is currently the international leader in the field of research and development for quantum technologies. They have allocated a quantum technology budget that is 10 times higher than that of its closest competitors (United States and the European Union).

Mentioned in Section I and detailed in Appendix C, China has been at the forefront of quantum telecommunication network development both ground-based and satellite-based. Launching the MICIUS satellite in 2016 for Earth-to-satellite and satellite-to-Earth telecommunications within the QUESS *(Quantum Experiments at Space Scale)* program was a worldwide historical landmark and it allowed for the first quantum encrypted intercontinental video call between Chinese and Austrian Academies of Science to be conducted on September 17, 2017 [30]. QKDs were also conducted at a distance of 719 km between the Tiangong-2 space laboratory and the Nanshan land station in 2017 [158]. China foresees launching 10 additional satellites that will allow for a network of intercontinental communications between Europe and Asia by 2020 with plans to expand into a worldwide network by 2030 [48]. According to the MIT magazine, the mind behind all of these projections is that of Jian-Wei Pan, the quantum physicist known as "the Father of Chinese Quantum science" [159].

Among the ground-based initiatives mentioned in Appendix C, it is worth highlighting one led by the University of Science and Technology. They developed a quantum network connecting four cities from Beijing to Shanghai with 2000 km of optical fiber, making it the biggest quantum network for quantum telecommunications on land [160].

Additionally, in 2017, it was announced that the construction of a 37-hectare National Laboratory for Quantum Information Sciences in Hefei is currently underway. The budget was 76 billion Yen (11.5 billion US dollars) for this 2.5 year construction project, estimated to be completed by 2020. [161,162].

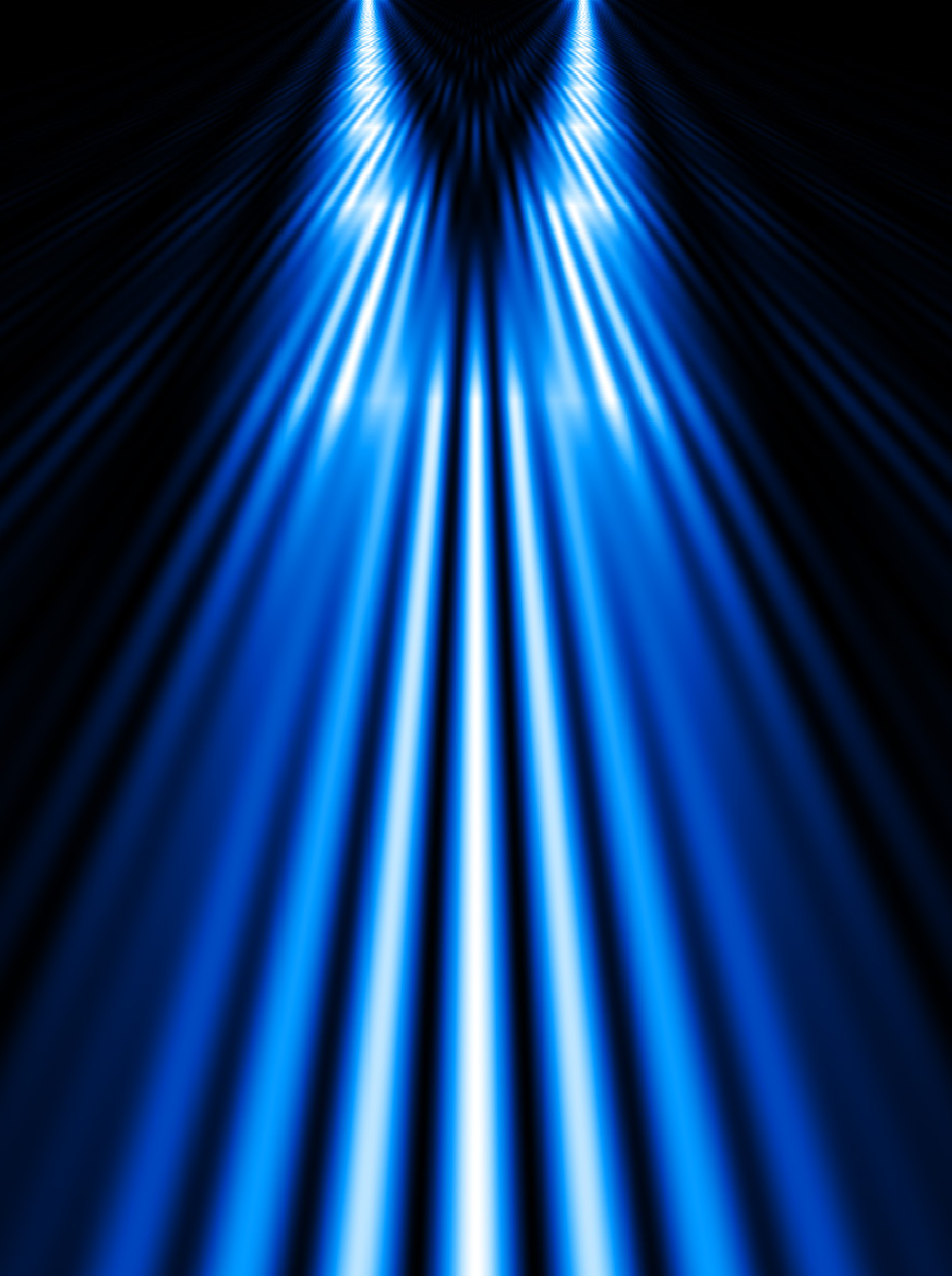
EUROPEAN UNION

As a result of the collaborative effort of over 3,400 representatives from academia and industry in Europe, The Quantum Manifesto was released in May 2006 [163]. This is a short document supported by researchers from almost every European country to raise awareness about the need to invest in quantum technology research, development and adoption in the European Union. The goals of this collaborative effort were to (i) promote a competitive European quantum industry to make Europe a global leader, (ii) expand European scientific leadership and excellence in quantum research, (iii) turn Europe into a dynamic, attractive region for innovative quantum technology research, and (iv) benefit from quantum technology improvements to promote better energy, health, safety and environmental solutions. Specifically, the Manifesto suggested six key activities:

- Supporting growth in scientific activities linked to quantum technologies.
- Create a favorable ecosystem of innovation and business creation for quantum technologies.
- Facilitate a new level of coordination between academia and industry to move advances in quantum technologies from the laboratory to industry.
- Create a new generation of quantum technology professionals in Europe through focused education at the intersection of science, engineering and business, and by strengthening public awareness of key ideas and capabilities.
- Coordinate public investments and strategies in quantum technologies at the European level.
- Promote the involvement of member regions that do not currently have a strong quantum technologies research program.

The document highlights the importance of quantum technologies and calls for the "launch [of] an ambitious European initiative in quantum technologies, needed to ensure Europe's leading role in a technological revolution now under way."

Because of the Manifesto, the Quantum Flagship program was launched by the European Union in October 2018 in Vienna [164] with a 1-billion euro budget (1.15 billion US dollars) to be invested over 10 years. Currently, their website presents information regarding calls for proposals and conference information. It also contains informative material



Simulation of the double-slit experiment with electron - Young interference with two slits. Alexandre Gondran. 1 November 2001.

about quantum technology, including a section that explains misconceptions surrounding quantum technologies and promotes what they call the Second Quantum Revolution.[15]

The European State Agency (ESA) also has multiple initiatives. One of such initiatives, the Space-QUEST (Quantum Entanglement for Space Experiments), proposes to perform space-to-ground quantum communication tests from a transmitter on the outer wing of the Columbus module in the International Space Station (ISS) [165,166]. Another initiative is Eutelsat Quantum, which is "a pioneering mission that will influence how telecom satellites are procured and manufactured in Europe." A software-defined satellite will be put into orbit for ground-to-space and space-to-ground quantum telecommunications during the second half of 2019 [167].

UNITED STATES

In recent years, several leaders in the United States have called for the establishment of a government level program that can coordinate the development of quantum technologies, similar to those in China and Europe. For example, William Hurd, a re-elected Congressman from Texas and director of the Information Technologies Subcommittee [168], has claimed that "whoever gets to true quantum computing first will be able to negate all the encryption that we have ever done to date. That is why China, this is why Russia is sucking up ciphertext that they will eventually be able to decrypt" [169]. In 2014, the MIT magazine published an article on the space race for quantum telecommunications, pinpointing China as the leader and indicating that the "U.S. plans are much less clear. This may be because the work is being done behind closed doors. On the other hand, the U.S. may be dragging its feet" [170].

By the end of 2018, some changes in the U.S. took place [171,172] with the publication of a document summarizing a national strategy for the Science of Quantum Information [173] and the launching of the National Quantum Initiative Act [174]. After approval by the Senate, President Trump signed off on December 21st, and it became Public Bill 115-368 [175]. This legislation proposes devoting 1.3 billion US dollars to fund research on quantum technologies. In particular, the Department of Energy, the NIST, the National Science Foundation (NSF), and NASA, among others, will participate in this research. According to the journal, Science, the "U.S. government is currently investing approximately 250 million US dollars a year, mostly through the Army Research Office, but the new budget will go mostly to its national laboratories"[176].

[15] The Second Quantum Revolution refers to the current era that presents a high number of infant quantum technologies of highly expected impact. Depending on the author, the First Quantum Revolution corresponds either to a) the stage between 1900 and 1930 in which Quantum Mechanics was born along with an understanding of its value and usefulness to describe the microscopic world, or to b) the creation of the first quantum technologies, such as lasers or MRI. In this document, we do not use the term First Quantum Revolution because we believe there is no consensus on which of these events constitutes the First Quantum Revolution. In addition, we believe none of them relates to the current revolution.

This bill "directs the President to implement a National Quantum Initiative Program to, among other things, establish the goals and priorities for a 10-year plan to accelerate the development of quantum information science and technology applications". The bill defines quantum information science as "the storage, transmission, manipulation, or measurement of information that is encoded in systems that can only be described by the laws of quantum physics" [175].

There are initial plans for each of the primarily organizations involved in research under this bill. The NIST will conduct specific activities in quantum science and organize a workshop to discuss the development of a quantum information and technology industry. The NSF will conduct basic research with a research program focused on quantum information and engineering. It will share this task with the Department of Energy. The NSF will also grant scholarships for Multidisciplinary Centers for Quantum Research and Education. The Science Agency will establish and operate Centers for National Research.

Within the private sector in the United States, movement has been much quicker. American companies have been at the forefront of quantum technology development since the beginning, especially in the field of quantum computing

In a collaboration led by renowned physicist I. Chuang, IBM and Stanford University ran Grover's quantum algorithm [75] for the first time using a 3-qubit quantum computer in 2000. Since then, the number of qubits in their processors has increased and, in 2017, the company managed to develop the first 50-qubit quantum computer [178]. Additionally, IBM has a 20-qubit quantum computer that is open to the public, so that any person accessing the Internet can send IBM an algorithm to run on it. They also have a quantum software development kit (SDK) called QISKit [179]. In 2019, IBM released the first 20-qubit commercial quantum computer under the name Q System One [180]. Regardless of its limited capacity, this is a great step in the quantum computing race [181].

Google has also strongly committed to advancements in quantum computing, ending the year 2018 as the company with the most powerful quantum computer, with 72-qubits [182]. Google has made an agreement with NASA for the joint exploration of quantum processors [183]. They have also joined an alliance between NASA and D-wave. In 2017, the D-Wave 2000-qubit quantum annealer, known as D-Wave 2000Q, was installed in one of Google's centers.

Rigetti, has been developing and granting access to an online platform of 8 and 19-qubit processors and, in August 2018, the company committed to developing a 128-qubit quantum computer by August 2019 [185,11]. Their platform offers the ability to "develop and execute quantum-classical programs in a virtual, classical compute environment that is side-by-side with our real quantum hardware" [186].

Intel has also played a significant role in the United States, collaborating with QuTech, a Dutch research institute, and developing a 17-qubit processor in 2017 and a 49-qubit processor in 2018 [187].

Finally, Microsoft is also in search of the first robust quantum computer, but with a different architecture than the others. Instead of using conductive qubits used by IBM, Google, Intel, and Rigetti, which are harder to scale, they are opting for the development of a topological quantum computer. Their website also contains a Quantum Development Kit to start programming quantum algorithms and they promise to provide quantum services in their Azure cloud [188,189].

Recently, an American company, Quantum Xchange, announced that it will develop the first commercial network in the United States with quantum cryptography that "will connect the financial markets on Wall Street with back office operations in New Jersey, helping banks keep high-value transactions and mission-critical data safe and secure" [177].

JAPAN

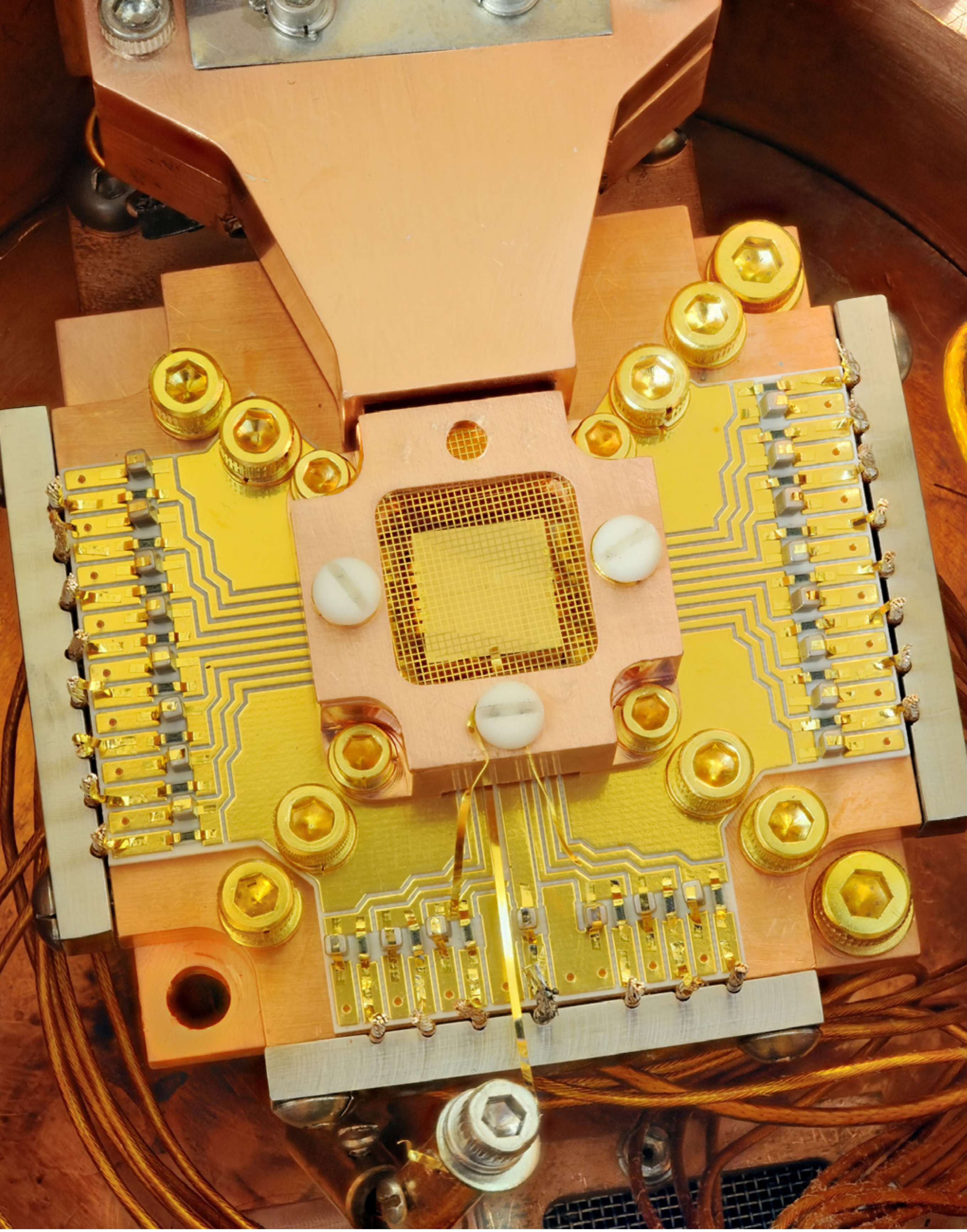
In 2017, the Japanese government launched a program to join the quantum computing race with a 30 billion Yen (332 million US dollars) budget for a 10-year plan that began in April, 2018 [190].

Japan has also shown special interest in developing a quantum neural network (QNN). In October 2016, a year after the official announcement by the Japan Science and Technology Agency (JSP) [191], it was revealed that the technological company NTT supported the development of a QNN capable of solving combinational optimization problems with social and medical applications, among others. The prototype consists of a closed circular fiber loop, a phase-sensitive amplifier (PSA), and a field-programmable gate array (FPGA). It has the capacity to solve the Max Cut problem among many others. The Max Cut problem involves separating people into two groups while avoiding, in the most efficient way possible, incompatibilities between pairs thus, creating the two groups in the most compatible manner. The QNN is able to solve this problem for 2,000 people with 20,000 incompatibilities in 5 milliseconds at an energy cost of 1kW, rather than the 10kW a quantum computer would consume [192-194].

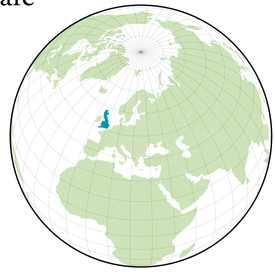
Japan has also made significant progress in the field of quantum telecommunications, further detailed in Appendix C. The country has developed a six-node land network between Koganei, Otemachi, Hakuson, and Hongo with connections of over 90 km [195]. In 2017, the micro-satellite Small Optical Transponder (SOTA), orbiting at an altitude of 600 km, was able to conduct ground-to-space telecommunications [196].

UNITED KINGDOM

In 2013, the United Kingdom announced it would invest 270 million pounds sterling (equivalent to 350 million US dollars) to finance the first five years of the National Quantum Technologies Programme to "create a coherent government, industry and academic quantum technology community that gives the UK a world-leading position in the emerging multi-billion-pound new quantum technology markets" [197].



NIST physicists used this apparatus to coax two beryllium ions (electrically charged atoms) into swapping the smallest measurable units of energy back and forth, a technique that may simplify information processing in a quantum computer. The ions are trapped about 40 micrometers apart above the square gold chip in the center. The chip is surrounded by a copper enclosure and gold wire mesh to prevent buildup of static charge. Credit: Y. Colombe/NIST.



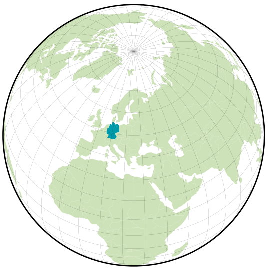
They will begin by developing applications in the areas of defense, safe communications, information technologies, and oil and gas, among others, and then will move on to broader market applications. The program foresees applications in different industries, markets and sectors. In particular, they note the importance of quantum computing devices, quantum enhanced imaging, quantum secure communications, quantum acceleration and navigation devices, quantum gravity sensing devices, and quantum timing devices [198].

Currently, the UK program is co-led by EPRSC, Innovate UK, BEIS, NPL, GCHQ, Dstl, and KTN, with a vision that is highly focused on research within academia. They have already invested 120 million pounds sterling (160 million US dollars) in 4 hubs that have been operational since 2014. These hubs tackle the areas of sensors and metrology [199], quantum image processing [200], quantum information technologies [201] and quantum telecommunications technologies [202] and are led by Birmingham, Glasgow, Oxford, and York, Universities, respectively, with a total of 17 universities and 132 companies involved.

In 2015, The Quantum Technologies Strategic Advisory Board led by Prof. D. Delpy reported on the program. They estimated the cost of developing commercial prototypes, such as biological microscopes, space applications for environmental monitoring and earthquake prediction, and medical diagnosis between 2015 and 2025 and predicted that the first robust and resilient quantum computers would be available by 2025 [203].

The UK government's chair of scientific advisory, Prof. Sir M. Walport, estimates that, in the long term, the quantum technology industry will be comparable to the electronic component industry, valued at 240 billion US dollars [204].

GERMANY



In September 2018, Germany became the European Union country with the highest investment in quantum technologies at the national level after approving QUTEG, a national initiative comprising a 5-year program and 650 million US dollars in funding [205]. The QUTEG initiative will span from 2018 to 2020 and will attempt to (i) expand the research landscape of quantum technologies, (ii) create research networks for new applications, (iii) establish lighthouse projects for industrial competitiveness, (iv) ensure security and technological sovereignty, (v) shape international cooperation, and (vi) engage the people of their country [206].

This initiative has already produced two flagship documents. The first is titled, "Quantum Technologies: Foundations and Applications" [207] and the second is titled, "Quantum Technologies: From Foundation to Market" [208].

In addition, several German agencies, including the Max Planck Institute and the German Aerospace Center (DLR), collaborated in 2016 with the goal of conducting an experimental study to test the transmission of photon signals between the portable space stations located at the Teide Observatory, Tenerife, and the Alphasat I-XL stationary satellite distanced 38,600 km apart [209].

LATIN AMERICA AND THE CARIBBEAN

There are currently no countries in Latin America and the Caribbean (LAC) launching programs with direct investments in the research and development of quantum technologies.

Dr. S. Venegas, who received his doctorate in theoretical physics from Oxford University, is one of the fathers of quantum computing in Mexico. He created the research group on quantum image processing at Monterrey Institute of Technology and has taught many free and open courses for students all over the region. He sees Brazil and Mexico as the two leading countries in LAC in number of researchers and publications on topics related to quantum technologies. He also highlights that, despite there being no specific funds from national programs in any LAC country, there are research centers and universities in some of them that offer MA and PhD programs on quantum technologies, such as the PhD program in nanotechnology at Monterrey Technology Institute.

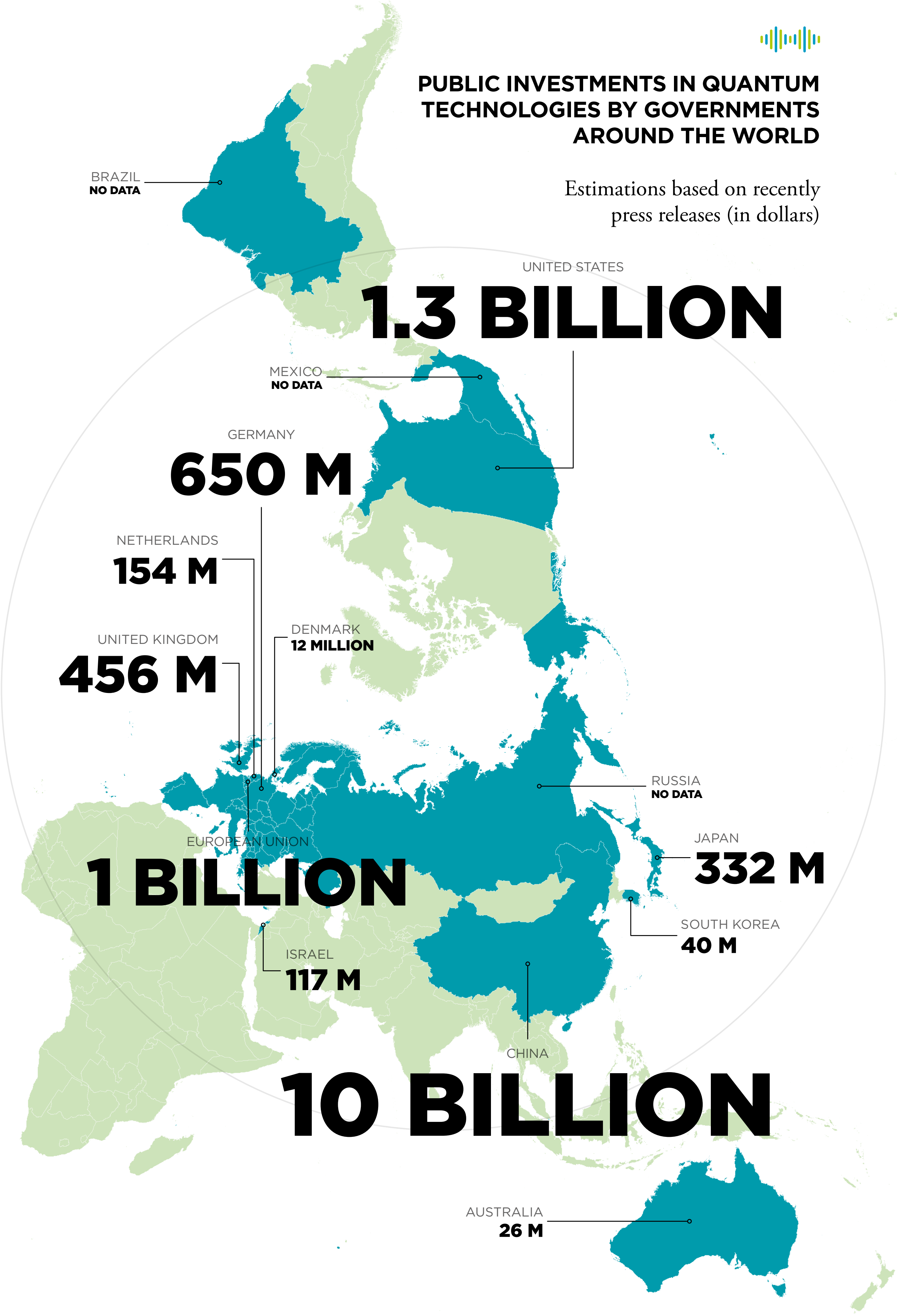
In Brazil, the primary institution in this field is the Quantum Computing Group at the National Laboratory for Scientific Computing, whose mission is to "develop original research in the areas of quantum computing and information, supervise Doctoral and Masters students, to propose new techniques, to follow, and if possible to participate in the development of the quantum hardware" [211]. According to a study released in 2015, 11 million euros (12.6 million US dollars) were dedicated to quantum technologies with 104 authors publishing on the matter between 2013 and 2015 [210].

REST OF THE WORLD

The countries described in this section are not the only ones making an effort in the race to explore, develop, and adopt quantum technologies. Some other countries have also started national programs and dedicated public funds in this disruptive field. University of Waterloo in Canada proudly recognizes having invested over 1.5 billion US dollars in quantum technologies over the last 15 years [212]; Russia has founded the Russian Quantum Center, where various institutions and universities are collaborating [213]; France has the Paris Centre for Quantum Computing (PCQC) [214]; Denmark contains the Quantum Innovation Centre (Qubiz) [215]; Singapore holds the Centre for Quantum Technologies (CQT) [216]; Australia has Centre for Quantum Computation & Communication Technology [217]; the Netherlands is being guided by QuTech [218]; and Israel is focusing on defense [219].

PUBLIC INVESTMENTS IN QUANTUM TECHNOLOGIES BY GOVERNMENTS AROUND THE WORLD

Estimations based on recently press releases (in dollars)



CONCLUSIONS

In this document, we discussed past, present, and future developments of quantum technologies and their important social, industrial, and governmental implications. We have explained their mechanisms and functions, as well as the ways in which they will potentially impact digital technologies such as cyber security, blockchain, artificial intelligence, the Internet of things, drones, 5G, and 3D printing. We have also analyzed and presented examples of their potential impact on sectors such as medicine, biology, genetics, education, economy and finance, energy, transportation, and meteorology. Finally, we presented the various programs and strategies being adopted by countries around the world in the race to quantum supremacy.

Quantum computing opens doors to the computational treatment of processes which are simply impossible using current classical computers; this poses both threats and immense opportunities at the same time. On one hand, it threatens data authentication, exchange, and storage, having the greatest impact on areas where cryptography plays a fundamental role, such as cyber security and blockchain. Other technologies, such as 5G, drones, and IoT also require secure data authentication and exchange; thus, quantum computing will be a significant threat for them as well. On the other hand, the computational capacity it offers will be essential in speeding up the development of many emerging technologies, especially those related to artificial intelligence. It will also be remarkably beneficial in the fields of medicine, biology, and genetics where, for example, quantum technologies will allow for the simulation of the effects of clinical drugs, exponentially reducing time and resources. More efficient research can be done in the quest to find cures for cancer and other diseases, including Alzheimer's, Parkinson's, and multiple sclerosis, among many others. In the field of finance, it will be possible to create much more precise mathematical models and to process data in real time in a more efficient manner for decision making. In energy and sustainable agriculture, it will be possible to explore new techniques for ammonia production at a lower energy and economic cost, replacing the current process that consumes 2% of the world's energy and drives up the cost of food.

The field of quantum information offers a completely safe way to store and share information because its processes are based on the physical properties of nature, rather than on the complexity of mathematical problems. This means breaking their encryption would entail breaking the laws of physics. In quantum cryptography, all processes happen at the hardware level rather than at the software level. Several countries already host the quantum telecommunications networks that use quantum cryptography. In 2016, China was the first country to deploy a satellite for quantically encrypted space telecommunications, which covered more than 2,000 km between Beijing and Shanghai. It is likely that within a few years, all daily devices we use to store or share data and information will do so using quantum generated keys and all communications will also be secured using this technology. Further, the first ideas for a quantum Internet have already been proposed and might become a reality in the near future as well.

Within the areas of public investment, business, and entrepreneurial development, the possibilities quantum technologies can offer are endless and the expansion they will create in these fields is undeniable. Emerging quantum technologies will be responsible for a technological revolution already in process, with a 37% CAGR until 2022, reaching a net worth of 161 million US dollars as an industry, and a 53% CAGR between 2022 and 2028, when it will reach 1.3 billion US dollars.

The major global powers have not overlooked the potential of these technologies, and some are already investing billions of US dollars in them. China, the USA, and the European Union are at the forefront, with programs amounting to 10 billion, 1.3 billion, and 1 billion US dollars, respectively. In Latin America and the Caribbean, the most active communities of researchers are in Brazil and Mexico. However, there are currently no known government initiatives dedicating funds to research and development in quantum technologies in the region.

Alliances between governments and large technology firms will become increasingly necessary in the development and implementation of these technologies into various systems. Overall, the education sector will need to educate future professionals; the industrial and technological sectors will need to understand, support, and develop new products that use quantum technologies; and governments will need to be protected and prepared. Quantum technologies have only begun to open the doors to a new era and all industries and sectors must get on board.

REFERENCES

1. P. Benioff. *The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines*. J. Stat. Phys. 22, 563 (1980). DOI: https://doi.org/10.1007/BF01011339.
2. R.P. Feynman. *Simulating physics with computers*. International journal of theoretical physics 21 (1982).
3. https://www-03.ibm.com/press/us/en/pressrelease/965.wss#release
4. I.L. Chuang, N. Gershenfeld and M. Kubinec. *Experimental implementation of fast quantum searching*. Phys. Rev. Lett. 80, 3408 (1998).
5. J.A. Jones y M. Mosca. *Implementation of a quantum algorithm to solve Detsch's problem on a nuclear magnetic resonance quantum computer*. J. Chem. Phys. 109 (1998):
6. 1648.DOI: https://doi.org/10.1063/1.476739.
7. R.J. Hughes et al. *The Los Alamos trapped Ion quantum computer experiment*. Fortschr. Phys. 46 (1998): 329-361.
8. D.F.V. James et al. *Trapped ion quantum computer research at Los Alamos*. NASA International Conference on Quantum Computing and Quantum Communications (1998): 426-437.
9. I.L. Chuang. *Experimental realization of a quantum algorithm*. Nature 393 (1998): 143-146.
10. https://www-03.ibm.com/press/us/en/pressrelease/52403.wss https://research.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html
11. https://medium.com/rigetti/the-rigetti-128-qubit-chip-and-what-it-means-for-quantum-df757d1b71ea
12. J. Proos y C. Zalka. *Shor's discrete logarithm quantum algorithm for elliptic curves*. Journal Quantum Information & Computation 3 (2003): 317-344.
13. M. Roetteler, M. Naehrig, K.M. Svore and K. Lauter. *Quantum resource estimates for computing elliptic curve discrete logarithms*. Advances in Cryptology – ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II (241-270).
14. W. K. Wootters and W. H. Zurek. *A single quantum cannot be cloned*. Nature, 299 (1982): 802.803.
15. https://www.submarinecablemap.com
16. https://www.xataka.com/historia-tecnologica/1-000-millones-de-metros-de-cable-submarino-son-los- responsables-de-que-tengas-internet-en-casa
17. P. W. Shor. *Algorithms for quantum computation: Discrete logarithms and factoring*. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA (1994): 124-134.
18. https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/.
19. C.H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore (New York, IEEE, 1984).
20. A.K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
21. C. Eliot. *The DARPA Quantum Network*. arXiv:quant-ph/0412029v1 (2004).
22. C. Elliott et al. *Current status of DARPA Quantum Network*. arXiv:quant-ph/0503058v2 (2005).
23. A. Boaron et al. Secure quantum key distribution over 421 km of optical fiber. Phys. Rev. Lett. 121, 190502 (2018).
24. H.J. Brieget, W. Dür, J.I. Cirac and P. Zoller. *Quantum repeaters: The role of imperfect local operations in quantum communication*; Phys. Rev. Lett. 81, 5932 (1998).
25. Y-F Pu et al. *Experimental realization of a multiplexed quantum memory with 225 individually accessible memory cells*. Nature Communications 8, 15259 (2017).
26. N. Jiang et al. *Experimental realization of random access quantum memory of 105 qubits*. Am. Phys. Soc. F26.00004 (2018).
27. https://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete
28. P. Jianwei. *Quantum Science Satellite*. Chinese Journal of Space Science 34, 5 (2014) pp. 547-549.
29. http://spaceflights.news/quess-launched-form-cosmodrome-on-gobi-desert/

30. S.K. Liao et al. *Satellite-to-ground quantum key distribution*. Nature 549 (2017): 43-47.

31. J. Yin et al. *Satellite-based entanglement distribution over 1200 kilometers.* Science 356, 6343 (2017): 1140-1144. DOI: 10.1126/science.aan.

32. S.K. Liao et al. *Satellite-relayed intercontinental quantum network*. Phys. Rev. Lett. 120, 030501 (2018).

33. E. Conover. *A quantum communications satellite proved its potential in 2017*. Science News 192, 11 (2017): 27.

34. 34. ISO-IEC 7498-1:1994

35. K. Holl. *Global Information Assurance Certification Paper. OSI Defense in depth to increase application security.* (2003)

36. L. Chen et al. *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology Internal Report 8105 (2016).

37. National Security Agency (NSA). *CNSA suite and quantum computing FAQ*. MFQ-U-OO-815099-15 (2016).

38. https://pqcrypto.org/

39. https://www.safecrypto.eu/

40. https://cryptomath-crest.jp/english/

41. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

42. http://pqcrypto.eu.org/docs/initial-recommendations.pdf

43. M. Campagna et al. *Quantum safe cryptography and security. An introduction, benefits, enablers and challenges*. ETSI White Paper No. 8. ISBN No. 979-10-92620-03-0.

44. https://phys.org/news/2017-12-quantum-memory-record-breaking-capacity-based.html

45. D. Gottesman and I. Chuang. arXiv:quant-ph/0105032v2 (2001).

46. R.J. Donaldson et al. *Experimental demonstration of kilometer-range quantum digital signatures*. Phys. Rev. A 93, 012329 (2016).

47. C. Croal et al. *Free-space quantum signatures using heterodyne measurements*. Phys. Rev. Lett. 117, 100503 (2016).

48. C. Peuntinger et al. *Distribution of squeezed states through an atmospheric channel*. Phys. Rev. Lett. 113, 060502 (2014).

49. H.L. Yin et al. *Experimental quantum digital signature over 102 km*. Phys. Rev. A 95, 032334 (2017).

50. R.J. Collins, R. J. Donaldson and G. S. Buller. *Progress in experimental quantum digital signatures*. Proc. SPIE 10771, Quantum Communications and Quantum Imaging XVI, 107710F (2018). doi: 10.1117/12.2319015.

51. https://qutech.nl/wp-content/uploads/2018/10/Quantum-internet-A-vision.pdf

52. D. Vinzenzo. *The Physical interpretation of quantum computation*. Fortschritte der Physik 48 (2000): 9-11.

53. M. F. Brandl. *A quantum von Neumann architecture for large-scale quantum computing*. arXiv:1702.02583v3 [quant-ph].

54. S. Haber and W.S. Stornetta. *How to time-stamp a digital document.* Journal of Cryptology 3, 2 (1991): 99- 111.

55. Bitcoin: A peer-to-peer electronic cash system.

56. M. Allende López and V. Colina Unda. Blockchain: *Cómo desarrollar confianza en entornos complejos para generar valor de impacto social.* Inter-American Development Bank (IDB). DOI: 10.18235/0001139.

57. M. Allende López and V. Colina Unda. *Aprende los tres elementos clave de blockchain con este ejemplo práctico*. IDB Blog: Abierto al público (2018).

58. M. Allende López and V. Colina Unda. *Conoce los distintos tipos de blockchain.* IDB Blog: Abierto al público (2018).

59. https://www.nature.com/articles/d41586-018-07449-z

60. https://en.bitcoin.it/wiki/Secp256k1

61. G. Wood. Ethereum: *A secure decentralized generalized transaction ledger*. EIP-150 REVISION.

62. D.R.L. Brown. *SEC 2: Recommended elliptic curve domain parameters*. Standards for Efficient Cryptography 2 (SEC 2).

63. http://hyperledger-fabric-ca.readthedocs.io/en/latest/users-guide.html

64. 64. D. Aggarwal et al. *Quantum attacks on Bitcoin and how to protect against them*. arXiv:1710.10377v1 [quant-ph].

65. 65. D.J. Bernstein et al. *SPHINCS: Practical stateless hash-based signatures*. Advances in Cryptology -- EUROCRYPT (2015): 368-397.

66. J. Buchmann, E. Dahmen and A. Hulsing. *XMSS: A practical forward secure signature scheme based on minimal security assumptions*. PQCrypto 2011: Post-Quantum Cryptography (2011): 117-129.

67. E.O. Kiktenko et al. *Quantum-secured blockchain*. Quantum Science and Technology 3, 3 (2018).

68. https://www.nature.com/articles/d41586-018-07449-z#ref-CR8

69. https://www.ethereum.org/

70. https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150/

71. https://blog.ethereum.org/2015/07/05/on-abstraction/

72. https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150/

73. L. Tessler and T. Byrnes. *Bitcoin and quantum computing*. arXiv:1711.04235v2 [quant-ph].

74. M. Amy et al. *Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3*. Selected Areas in Cryptography – SAC (2016): 317-337.

75. L.K Grover. *A fast quantum mechanical algorithm for database search*. Proceedings of the twenty-eigth anual ACM symposium on Theory of computing (1996): 212-219.

76. https://www.blockchain.com/charts/difficulty?timespan=30days

77. https://asicminermarket.com/product/antminer-s9-14t-1600w-psu-14ths-2-fan-2/

78. J. Tromp. *Cuckoo cycle: A memory bound graph-theoretic proof-of-work*. Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30 (2015). Revised Selected Papers pp. 49-62. DOI 10.1007/978-3-662-48051-9_4.

79. D. Larimer. *Momentum – A memory-hard proof-of-work via finding birthday collisions*.

80. A. Birykov and D. Khovratovich. *Equihash: Asymmetric proof-of-work based on the generalized birthday problem*.

81. https://www.cryptocompare.com/coins/guides/what-is-a-block-header-in-bitcoin

82. https://www.technologyreview.es/s/10211/blockchain-se-vuelve-cuantico-para-sobrevivir-al-ordenador-del- futuro

83. https://www.technologyreview.com/s/610624/ibms-dario-gil-says-quantum-computing-promises-to- accelerate-ai/

84. https://www.wired.com/story/job-one-for-quantum-computers-boost-artificial-intelligence/

85. https://www.forbes.com/sites/bernardmarr/2017/09/05/how-quantum-computers-will-revolutionize- artificial-intelligence-machine-learning-and-big-data/#54faca725609

86. P. Benioff. *Languaje is physical.* Quantum information processing 1, 6 (2002) pp. 495-509. https://doi.org/10.1023/A:1024074616373.

87. E.W. Piotrowski and J. Sladkowski. *The next stage: quantum game theory*. arXiv:quant-ph/0308027v1.

88. Y. Dang et al. *Image classification based on quantum KNN algorithm*. arXiv:1805.06260v1 [cs.CV].

89. B.A. Huberman and T. Hogg. *Quantum solution of coordination problems*. Quantum Information Processing 2, 421 (2003). https://doi.org/10.1023/B:QINP.0000042201.34328.61.

90. W. Zeng and B. Coecke. *Quantum algorithms for compositional natural language processing*. SLPCS@QPL (2016). DOI:10.4204/EPTCS.221.8

91. KY. Chen, T. Hogg and R. Beausoleil. *Quantum Information Processing* 1, 449 (2002). https://doi.org/10.1023/A:1024070415465.

92. U. Alvarez Rodriguez, M. Sanz, L. Malata and Enrique Solano. *Artificial Life in Quantum Technologies*. Scientific Reports 6, 20956 (2016).

93. Perdomo-Ortiz, M. Benedetti, J. Realpe-Gómez and R. Biswas. *Opportunities and challeges for quantum-assisted machine learning in near-term quantum computers.* Quantum Science and Technology 3, 3 (2018).

94. L. Zhaokai, L, Xiaomei, X. Nanyang and D. Juangeng. *Experimental realization of quantum artificial intelligence*. Phys. Rev. Lett 114, 140504 (2015).

95. V. Dungjo and H. J Briegel. *Machine learning 7 artificial intelligence in the quantum domain*. Rep. Prog. Phys. 7, 074001 (2018).

96. S. Dernbach et al. *Quantum walk inspired neural networks for graph-structured data*. Proceedings the 7th international conference on complex networks and their applications VII (2018): 182-193.

97. G. Verdon, J. Pye and Michal Broughton. *A universal training algorithm for quantum deep learning*. arXiv:1806.09729v1 [quant-ph].

98. M.V. Altaisky, N.E. Kaputkina and V.A. Krylov. Symmetry and decoherence-free subspaces in quantum neural networks. arXiv:1802.05710v1 [quant-ph].

99. E. Farhi and Harmut Neven. *Classification with quantum neural networks or near term processors*. arXiv:1802.06002v1 [quant-ph].

100. J. Bausch and Felix Leditzky. *Quantum codes from neural networks.* arXiv:1806.08781v1 [quant-ph].

101. H. Chen et al. *Universal discriminative quantum neural networks.* arXiv:1805.08654v1 [quant-ph].

102. Z. Zhao et al. *A note on state preparation for quantum machine learning.* arXiv:1804.00281v1 [quant-ph].

103. W. Huggins, P. Patel, B. Whaley y E.M Stoudenmire. *Towards quantum machine learning with tensor networks*. Quantum Science and technology 4, 2 (2019).

104. B. Huang, N.O. Symonds and O.A. Von lilienfeld. *The fundamentals of quantum machine learning*. arXiv:1807.04259v2 [physics.chem-ph].

105. J. Biamonte. *Quantum machine learning matrix product states*. arXiv:1804.02398v1 [quant-ph].

106. M. Schuld y Nathan Killoran. *Quantum machine learning in feature Hilbert spaces*. arXiv:1803.07128v1 [quant-ph].

107. J. Biamonte et al. *Quantum machine learning*. Nature 549 (2017): 195-202.

108. https://quantiki.org/wiki/list-qc-simulators

109. https://www.rigetti.com/products

110. https://qiskit.org/

111. U. Alvarez Rodriguez, M. Sanz, L. Lamata and E. Solano. *Quantum artificial life in an IBM quantum computer*. Scientific Reports 8, 14793 (2018).

112. https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

113. http://www.bain.com/publications/articles/choosing-the-right-platform-for-the-industrial-iot.aspx

114. https://www.rvo.nl/sites/default/files/2017/11/Matrix_Final%20report_20042017.pdf

115. https://iot.telefonica.com/es/node/6646

116. https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

117. https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#649469391480

118. https://marketing.idquantique.com/acton/attachment/11868/f-025f/1/-/-/-/-/2017%2011%20DefTech_IDQ%20paper.pdf

119. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf

120. https://www.prnewswire.com/news-releases/sk-telecom-and-deutsche-telekom-establish-quantum-alliance- for-worldwide-quantum-safe-network-ecosystem-300413853.html

121. https://www.netmanias.com/en/post/korea_ict_news/11572/5g-nokia-sk-telecom-security/sk-telecom-and- nokia-sign-cooperation-agreement-for-quantum-cryptography

122. https://www.idquantique.com/id-quantique-sk-telecom-join-forces/

123. http://www.ajudaily.com/view/20180726104931947

124. http://www.ajudaily.com/view/20180726104931947

125. https://www.zdnet.com/article/sk-telecom-applies-quantum-key-to-deutsche-telekom-network/

126. https://networks.nokia.com/solutions/secure-optical-transport

127. https://www.idquantique.com/idq-sk-telecom-nokia-secure-optical-transport-system-using-qkd

128. https://www.zdnet.com/article/south-korean-telcos-agree-to-launch-5g-at-the-same-time/

129. https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14600

130. https://quantumxc.com/quantum-safe-security-in-a-5g-world/

131. https://www.businesswire.com/news/home/20180626005289/en/Quantum-Xchange-Launches-Quantum- Network-United-States

132. https://www.zdnet.com/article/sk-telecom-applies-quantum-key-to-deutsche-telekom-network/

133. https://quantic.ac.uk/quantic-researcher-spins-off-quantum-technologies-for-gas-detection/, https://www.qlmtec.com/technology/

134. Keil, M. et al. *Fifteen years of cold matter on the atom chip: promise, realizations, and prospects*. Journal of Modern Optics 63 (2016): 1840-1885. DOI: https://doi.org/10.1080/09500340.2016.1178820 (2016).

135. Barrett, B. et al. Mobile and remote inertial sensing with atom interferometers. In IOS Press (ed.) Proceedings of the International School of Physics “Enrico Fermi” 188 (2014): 492-555.

136. 136.https://www.nature.com/articles/s41598-018-26455-9

137. 137.J. Vovrosh et al. *Additive manufacturing for quantum technologies*. Scientific Reports 8, 2023 (2018).

138. https://www.nibib.nih.gov/science-education/science-topics/magnetic-resonance-imaging-mri

139. https://spie.org/membership/spie-professional-magazine/archives/2011jan-archive/lasers-in-medicine?SSO=1

140. https://www.msdsalud.es/recursos-de-salud/guias-para-pacientes/proceso-investigacion-desarrollo- aprobacion-farmaco.html

141. L. P. Lee. *Quantum bionanophotonics for life science and medicine*. International Conference on optical NEMS and nanophotonics (2015).

142. G. L. Lio et all. *Quantized plasmon quenching dips nanospestroscopy via plasmon resonance energy transfer*. Nature Methods 4, 1015-1017 (2017).

143. K. Lee, Y. Cui and L. P Lee. *Quantitative imaging of single MRNA splice variants in living cells*. Nature Nanotechnology 9, 474-480 (2014).

144. https://www.nature.com/articles/d42473-018-00265-z

145. https://newsroom.accenture.com/news/accenture-labs-and-1qbit-work-with-biogen-to-apply-quantum-computing-to-accelerate-drug-discovery.htm

146. https://www.idquantique.com/protecting-health-care-data-motion/

147. https://www.allen-york.com/blog/2018/04/uk-will-have-800000-unfilled-it-jobs-by-2020

148. M.A. Dutz, K. R. Almeida and T.G. Packard. *The jobs of tomorrow: Technology, Productivity, and Prosperity in Latin America and the Caribbean.* Directions in Development;; Directions in Development--Information and Communication Technology;. Washington, DC: World Bank. © World Bank.

149. A. McWilliams. *Quantum computing: Technologies and global markets to 2022*. Icc Research (2018).

150. B. Hemenway and S. Khanna. *Sensitivity and computacional complexity in financial networks*. Algorithmic Finance 5, 3-4 (2016): 95-110.

151. R. Orús, S. Mugel and E. Lizaso. *Forecasting financial crashes with quantum computing*. arXiv:1810.07690v1 [q-fin.GN]

152. A. M. Lewis. *The impact of quantum technologies on the EU's future policies*. European Commission: JRS Science for policy report. Part 1: Quantum time (2018).

153. M. Reiher et. al. *Elucidating reaction mechanisms on quantum computers*. Proceedings of the National Academy of Sciences (2017).

154. https://www.ifastat.org/market-outlooks

155. http://www.eldiario.net/noticias/2016/2016_01/nt160124/principal.php?n=92&-produccion-de-amoniaco-y-urea-en-manos-de-seis-paises

156. http://www.ssecoconsulting.com/industria-petroquiacutemica-en-ameacutericalatina.html

157. M. Kitano et. al. *Electride support boosts nitrogen dissociation over ruthenium catalyst and shifts the bottleneck in ammonia synthesis*. Nature Communications 6, 6731 (2015). DOI: 10.1038/ncomms7731.

158. Sk. Liao et al. *Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 Space Lab*. Chin. Phys. Lett. 34, 090302 (2017). DOI: 10.1088/0256-307X/34/9/090302.

159. https://www.technologyreview.com/s/612596/the-man-turning-china-into-a-quantum-superpower/

160. https://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete

161. https://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility

162. https://superposition.com/2017/10/31/china-goes-big-92-acre-10-billion-quantum-research-center/

163. *Quantum Manifesto. A new era of technology* (2016).

164. https://ec.europa.eu/digital-single-market/en/news/quantum-flagship-kickoff

165. Ursin et al. Space-QUEST. *Experiments with quantum entanglement in space.* Europhysics News 40, 3 (2009): 26-29.

166. S.K. Joshi et al. Space QUEST mission proposal. *Experimentally testing decoherence due to gravity.* New Journal of Physics 20 (2018).

167. https://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Quantum

168. https://hurd.house.gov/about/committees-and-caucuses

169. https://hurd.house.gov/media-center/in-the-news/best-piece-legislation-dc-about-quantum-computing

170. https://www.technologyreview.com/s/528671/the-space-based-quantum-cryptography-race

171. https://www.forbes.com/sites/arthurherman/2018/08/20/at-last-america-is-moving-on-quantum/#23cbc4f45327

172. https://www.forbes.com/sites/astanley/2018/06/26/is-the-u-s-getting-its-act-together-on-quantum- computing/#638d553b704f

173. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum- Information-Science.pdf

174. *https://www.congress.gov/bill/115th-congress/house-bill/6227/related-bills*

175. https://www.congress.gov/bill/115th-congress/house-bill/6227

176. https://www.sciencemag.org/news/2018/01/after-years-avoidance-department-energy-joins-quest-develop-quantum-computer

177. https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/

178. https://quantumexperience.ng.bluemix.net/qx/experience

179. https://newsroom.ibm.com/2019-01-08-IBM-Unveils-Worlds-First-Integrated-Quantum-Computing-System- for-Commercial-Use#assets_all

180. https://www.research.ibm.com/ibm-q/system-one/

181. https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

182. https://www.nasa.gov/saa/domestic/27787_Fully_Executed_NRSAA_Google_Quantum_Computing.pdf

183. https://www.dwavesys.com/press-releases/d-wave-2000q-system-be-installed-quantum-artificial-intelligence-lab-run-google-nasa

184. M. Reagor et. Al. *Demonstration of universal parametric entangling gates on a multi-qubit lattice*. Science Advances 4, 2 (2018).

185. https://www.rigetti.com/qcs

186. https://newsroom.intel.com/news/intel-delivers-17-qubit-superconducting-chip-advanced-packaging- qutech/#gs.pYDbTmrp

187. https://www.microsoft.com/en-us/quantum/technology

188. https://www.microsoft.com/en-us/quantum/development-kit

189. https://www.businesswire.com/news/home/20180626005289/en/Quantum-Xchange-Launches-Quantum- Network-United-States

190. https://www.thedailystar.net/world/asia/japan-launches-its-first-quantum-computer-prototype-nii-ntt- university-of-tokyo-1494877

191. http://www.jst.go.jp/pr/announce/20161021/index.html

192. https://www.datacenterdynamics.com/news/japanese-govt-and-ntt-announce-quantum-neural-network/

193. https://asia.nikkei.com/Business/Technology/Japan-enters-quantum-computing-race-and-offers-free-test-drive

194. https://www.hpcwire.com/2017/11/22/japan-unveils-first-quantum-computer-prototype/

195. M. Sasaki et al. *Field test of quantum key distribution in the Tokyo QKD Network*. Optics Express 19, 11 (2011): 10387-10409.

196. H. Takenaka et al. *Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite*. Nature photonics 11 (2017): 502-508.

197. http://uknqt.epsrc.ac.uk/about/overview-of-programme

198. http://uknqt.epsrc.ac.uk/applications/

199. https://www.quantumsensors.org/

200. https://quantic.ac.uk/

201. http://nqit.ox.ac.uk/

202. https://www.quantumcommshub.net/

203. https://epsrc.ukri.org/newsevents/pubs/quantumtechstrategy/

204. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/564946/gs- 16-18-quantum-technologies-report.pdf

205. http://www.qutega.de/en/home/

206. https://www.laserfocusworld.com/articles/2018/09/650-million-for-quantum-research-in-germany.html

207. http://www.qutega.de/fileadmin/qutega/Qutega_Grundlagenpapier.pdf

208. https://www.bmbf.de/pub/Quantentechnologien.pdf

209. K. Gunther et al. *Quantum-limited measurements of optical signals from a geostationary satellite*. Optica 4, 6 (2017): 611-616.

210. http://colnal.mx/events/correlaciones-cuanticas-escuela-latinoamericana-de-fisica-marcos-moshinsky-2017-6

211. F. Heijman-te Paske. *Global developments in Quantum Technology*. Netherlands Ministry of Economic Affairs (2015).

212. https://uwaterloo.ca/global-impact/canadas-stake-quantum-race

213. http://www.rqc.ru/

214. http://www.pcqc.fr/

215. http://qubiz.dk/

216. https://www.quantumlah.org/page/key/whatwedo

217. http://www.cqc2t.org/

218. https://www.nwo.nl/en/news-and-events/news/2015/135-million-euros-for-development-of-quantum- computers.html

219. https://www.jpost.com/Israel-News/Israel-joins-the-race-to-become-a-quantum-superpower-574510

220. https://www-03.ibm.com/press/us/en/pressrelease/965.wss#release

221. L.M.K. Vandersypen et al. *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*. Nature 414 (2001): 883-887

222. H.Häffner et al. *Scalable multiparticle entanglement of trapped ions*. Nature 438 (2005): 643-646.

223. C. Negrevergne et al. *Benchmarking quantum control machine methods on a 12-qubit system*. Phys. Rev. Lett. 96, 170501 (2006).

224. https://www.nature.com/news/2007/070215/full/news070212-8.html

225. https://physicsworld.com/a/ibm-offers-20-qubit-quantum-computer-to-clients/

226. .https://ai.googleblog.com/2018/05/the-question-of-quantum-supremacy.html

227. https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/

228. https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/

229. R. Alleaume et. al. *SECOQC. White paper on quantum key distribution and cryptography*. arXiv:quant- ph/0701168v1

230. M. Peev et al. *The SECOQC quantum key distribution network in Vienna*. New Journal of Physics 11, 075001 (2009).

231. A. Mirza and F. Petruccione. *Realizing long term quantum cryptography*. Society of America B 27, 6 (2010). DOI: 10.1364/JOSAB.27.00A185.

232. T.Y. Chen. *Metropolitan all-pass and inter-city quantum communication network*. Optical Express 18, 26 (2010): 27217-27225.

233. W. Chen et al. *Field experimental "star type" metropolitan quantum key distribution network*. IEEE Photonics Technology Letters 21, 9 (2009): 575-577.

234. Y. Pu et al. *Experimental entanglement of 25 individually accessible atomic quantum interfaces. Science Advances* 4, 4 (2018).

235. D. Dequal et al. *Experimental single photon exchange along a space link of 7000 km*. Phys. Rev. A 93, 010301 (2016).

236. L. Calderaro. *Towards quantum communication from global navigation satellite system*. Quantum Science and Technology 4, 1 (2018).

237. Teunissen, Peter J. G. and Oliver Montenbruck. *Springer Handbook of Global Navigation Satellite Systems*. Springer International Publishing (2017).

238. E. Kerstel. Nanobob. *A cubesat mission concept for quantum communication experiments in an uplink configuration*. EPJ Quantum Technology 5:6 (2018).

239. R. Bedington, J.M. Arrazola and A. Ling. *Progress in satellite quantum key distribution*. Quantum Information 3, 30 (2017).

240. R.C. Merkle. *Secure communications over insecure channels*. Communications of the ACM 21, 4 (1978).

241. W. Diffie and M.E. Hellman. *New directions in cryptography*. IEEE Transactions on information theory 22, 6 (1976).

242. J. Ellis. *The possibility of secure non-secret digital encryption*. CESG Communications-electronics security group Research Report No. 3006.

243. W. Diffie. *The first ten years of public key cryptography*. Proceedings of the IEEE 72, 5 (1988).

244. R.L. Rivest, A. Shamir and L. Adleman. *A method for obtaining digital signatures and public key cryptosystems*. Communications of the ACM 21, 2 (1978): 120-126.

245. http://www.bbc.com/news/uk-england-gloucestershire-11475101

246. http://unsolvedproblems.org/index_files/RSA.htm

247. T. Kleinjung et al. Factorization of a 768-bit RSA modulus. In: Rabin T. (eds) Advances in Cryptology – CRYPTO 2010. Lecture Notes in Computer Science 6223 (2010). Springer, Berlin, Heidelberg.

248. T. Elgamal. *A public key cryptosystem and a signature scheme based on discrete logarithms*. IEEE Transactions on information theory 31, 4 (1985).

249. https://www.certicom.com/content/certicom/en/code-and-cipher/development-of-core-ecc-standards-by- ansi.html

250. NIST. *Digital signature standards*. FIPS Publication 186-2 (2000).

251. A.I. Ali. *Comparison and evaluation of digital signature schemes employed in NDN network*. International journal of embedded systems and applications (IJESA) 5, 2 (2015).

APPENDICES

APPENDIX A

THE EVOLUTION OF QUANTUM COMPUTING

In the early 1980s, P. Benioff [1] and R. Feynman [2] first proposed the idea of using computers to simulate physical phenomena. For the next 20 years, several researchers published on the potential ways these computers could be built and proposed algorithms that could run on them, giving birth to the field now known as quantum computing. In 1998, three independent research groups managed to build the first 2-qubit quantum computers. One was built at the University of California, Berkeley by a partnership led by IBM researcher, I. Chuang, between IBM, the MIT Media Lab, and UC Berkeley [3, 4]. Another was built by J.A. Jones and M. Mosca at Oxford University [5], and the third one was built in Los Alamos, California by R.J. Hughes and D.F.V. James et al [6,7].

Within months of these huge accomplishments by the quantum community, a team again led by I. Chuang developed the first 3-qubit quantum computer and implemented Grover's algorithm on it at the IBM Research Center in San Jose, CA [8].

The first 7-qubit quantum computer was developed between 2000 and 2001 and was able to implement Shor's algorithm for the first time. This 7-qubit quantum computer was developed through a collaboration between IBM and Stanford University. They used the algorithm to factor the number 15 into its primes, 3 and 5 [221]. Researchers at the University of Los Alamos also achieved this milestone in 2000.

In 2005, the first qubyte quantum computer (8-qubits) was implemented by the University of Insbruck [222]. A year later, researchers from Waterloo and MIT managed to increase the number to 12 qubits [223]. Again, it only took a year for this record to be broken; in 2007, D-Wave managed to reach 16 qubits [224].

After these rapid breakthroughs, there were 10 years of relative frustration in this field. Finally, in May 2017, IBM announced a new record with the first 17-qubit quantum computer [9], which was promptly matched by Intel in October [188]. A few months later, IBM reached the 50-qubit [179] milestone and also offered online access to a 20-qubit computer for any user to run simulations and provide feedback on its functioning [225].

In April 2018, Google led this ongoing race with their development of a 72-qubit quantum computer, the computer with the greatest capacity to date [10].

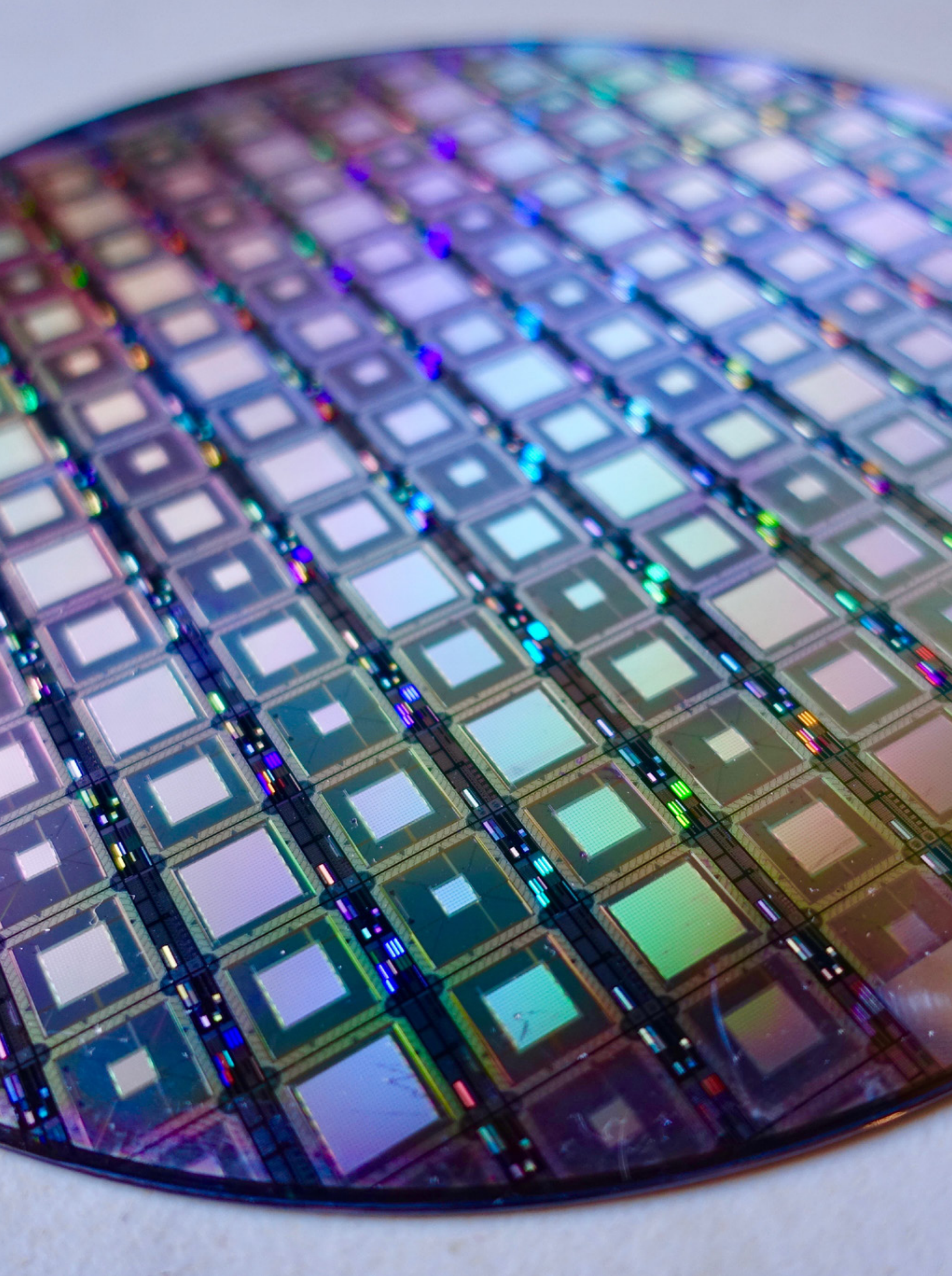
The quantum community is now racing toward quantum supremacy, defined as the existence of a quantum computer executing a process faster than any digital or classical computer. Google believes this could be done with a 50-qubit quantum computer

[226]; thus, news of a quantum computer outperforming a classical one is expected in the near future.

Since the first quantum processors were built in 2000, the year 2030 has been estimated to be the year in which quantum processors will achieve quantum supremacy. As previously stated, some believe that a quantum computer with between 1500 [12] and 2330 [13] logical qubits would be enough to break keys currently used in cybersecurity in a reasonable amount of time. Another study claims that, by 2027, it will be possible to break digital signatures used in blockchains in less than 10 minutes [64], posing a major threat to the security of blockchain technology.

Figure 3 demonstrates the exponential rate at which quantum computer development is growing. In fact, IBM released the first commercial quantum computer under the IBM Q System One [181,182] program in January 2019 with a 20-qubit processor; it cannot yet be purchased. To date, only quantum annealers have been marketed for specific applications (generally for optimization issues). The 2000-qubit D-Wave 2000Q is one such example [185].

It is unlikely that domestic quantum computers will be in existence for several decades. Further, in the future, computers may not be exclusively either quantum or classical, but hybrid, with two processors that take on tasks based on their individual characteristics and required capabilities. The first contact the general public will likely have with quantum computing will be probably through services provided in the cloud, known as “software as a service” (SaaS). With varying fares, quantum hardware and software from big technology companies will be available for commercial use.



A zooming in on a wafer of D-Wave Quantum Computers, Steve Jurvetson from Menlo Park, USA. 1 February 2018.

APPENDIX B

QUANTUM CRYPTOGRAPHY

The greatest change in paradigm offered by quantum cryptography in comparison to classical cryptography is the use of processes occurring at the physical level (hardware level), rather than at the software level, to guarantee data safety. **Quantum cryptography allows for completely safe transmission of data through random key generation and safe key exchange.**

Random Number Generation

Classical random number generation is based on deterministic algorithms, originating from seeds. It is impossible to achieve true randomness with classical algorithms, which take place at the software level. However, there are random physical processes in nature that we can understand and control due to our understanding of Quantum Mechanics. These processes can be used to generate random numbers and in turn, random keys. One simple way of doing so is by working with light particles (photons) and semi-reflective mirrors. If a photon falls on a mirror with a 50% chance of being reflected and a 50% chance of passing through, we can agree to write 0 when the photon is reflected and write 1 when it goes through the mirror, creating a 100% random key.

Currently, it is relatively simple to use these physical processes. The company IDQuantique manufactures commercial devices of millimetric dimensions that do so [18].

Quantum Symmetric Cryptography (QKD)

At present, all processes and protocols used to transfer data, including the Internet, depend on asymmetric cryptography to establish a safe connection between two users, frequently referred to as Alice and Bob. This cryptography enables Alice to send Bob a public key to encrypt data so that Alice can decrypt it using a private key. Bob can send her a symmetric encrypted key so that only Alice and Bob know such key. They can then start using this key to encrypt messages. This is how the Internet's https protocol works. With the advent of quantum computing, however, eavesdroppers will be able to find private keys and decrypt them from the public key, which is explained in Section I [36,37,43].

Again, quantum cryptography allows users to create a fully secure symmetric key because it involves physical, rather than software, processes.

This is due to the uncertainty and no-cloning principles that apply in the microscopic world and make it impossible to observe without modifying or copying a quantum state and, as a result, the data encrypted in that state. This means that if Alice somehow codes a 0 or a 1 into the polarization of a photon and sends it to Bob, once Bob receives and measures that photon and speaks to Alice, they will know if someone has observed that photon along the way. That is, they will know for certain whether a key is safe or not before using it and will also be able to completely dispose of an unsafe asymmetric encryption if they want. This quantum process is known as quantum key distribution (QKD).

Let us further explore QKD at the physical level. It is well known that light has the ability to be polarized. For example, polarized sunglasses are used to filter light, making it easier on our eyes. Understanding the process of polarization is easier when we think of photons as arrows with a determined direction, the direction of polarization. Polarizers measure, detect, and interact with photons and let them pass (or not) through based on their direction of polarization. Because all particles are quantum systems, quantum phenomena such as superposition and entanglement apply to light particles.

For example, if we release a photon that has diagonal polarization, one of the following cases can occur through the process of throwing a photon through a polarizer:

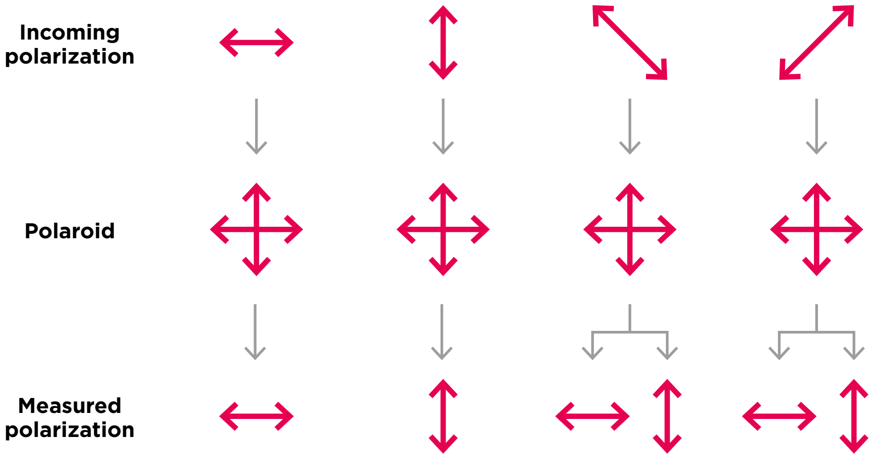
a. If the polarizer is also diagonal, the photon passes through with 100% probability. This happens in macroscopic cases when the object is shaped and sized like a hole. This can be compared to taking a couch at a diagonal angle through a diagonally faced door.
b. If the polarizer is vertical, the photon will not go through with 50% probability. If it does pass through, it will do so as a vertically polarized photon, so that someone who sees the photon coming through will not know its previous direction of polarization. This happens because diagonal photons are a combination (a quantum superposition) of a vertical and horizontal photon. Thus, when the photon reaches the polarizer, it is "forced" to stop being diagonal and must decide whether to become its horizontal "projection",[16] so that it will not go through the polarizer, or choose to be vertical, so that it goes through the polarizer as a vertical photon. This always happens when the polarizer differs by 45° in the direction of polarization. Thus, the same phenomenon happens when the polarizer is horizontal. This has no classical analogue, as a couch in a diagonal position will never go through a door with a vertical shape.
c. If the polarizer is vertical but at a 90° angle to the photon, the photon never goes through.
d. With any other polarization, the likelihood of the photon going through the polarizer depends on the difference between the photon and polarizer's angles of polarization. The probability starts from 0% when those directions are orthogonal and up to 100% when they are parallel.

Cases B and D only occur within quantum systems and are the processes that underlie QKD to allow for the safe sharing of keys between two individuals. If the keys are intercepted (measured by an eavesdropper using polarizers), they become modified from their original state. That modification can be detected by Alice and Bob who can confirm that eavesdropping took place. The most widely used QKD protocol is the BB84 [19] scheme:

[16] Referring to "projections" is wrong as it would seem that half the photon corresponds to each projection, meaning only half of the photon passes through and that is not what happens. The photon truly exists in a superposition of polarizations and, if decanted through the polarization of the polarizer, it goes through it as a whole.

1. Alice and Bob agree on the polarizations that will be their 0s and 1s and on the polarizers they will use to measure them. For example, they determine that photons polarized at 45º and 90º correspond to 0s and photons polarized at 0º and 135º correspond to 1s. This negotiation takes place through a classical channel and does not reveal data about the future key to a potential eavesdropper.
2. Alice randomly sends polarized photons in one of the four predetermined directions through a quantum channel to Bob. If the eavesdropper intercepts the photon, they can be detected because 50% of the time, they use the wrong polarizer, which changes the polarization.
3. Bob measures the photons sent by Alice, registers the polarizer used, and if, based on the initial agreement, the photon polarization is polarized at 45° or 90°, he writes down a 1. If, on the contrary, it is polarized at 0° or 135° he writes down a 1.

FIGURE 10. Schematic representation of polarizer action on photons.

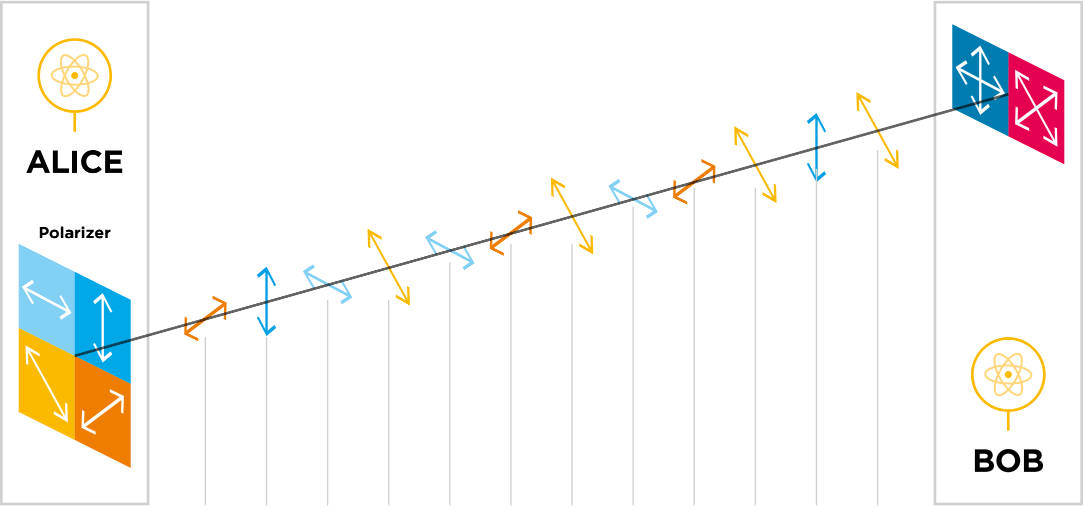


In the two cases on the left, the photon passes through, keeping its polarization because the correct base (polarizer) was chosen. In the two cases on the right, the photon goes through with a different polarization with a 50% probability of being either vertical or horizontal.

4. Alice and Bob communicate again through a classical channel and Bob tells Alice which polarizers he used. Because of the quantum superposition phenomena explained above, if Bob uses the horizontal-vertical polarizer and the photon has a diagonal polarization, Bob will have either a vertical or a horizontal photon with 50% likelihood for each option. However, in no case will he be able to know that the original photon was diagonal, so he loses the 1 or 0 data coded by Alice in that diagonal polarization. This is why Alice and Bob delete the 1s and 0s corresponding to the measurements Bob took with the wrong polarizer from their key.

5. Once Alice and Bob have a clean key with 1s and 0s corresponding to the proper measurements, they use the classical channel to share part of that key. If their keys differ from each other by a percentage above the estimated intrinsic error percentage for that channel, they can then confirm that an eavesdropper has observed the key when it was sent and added an error with their random selection of polarizers.
6. If the key has not been observed by an eavesdropper, Alice and Bob will use the rest of it (which was not exchanged in Step 5) to encrypt and decrypt data. If the key has been observed, they can delete it or use techniques to reduce the information the eavesdropper has on the key.

This process's safety lies in the fact that the eavesdropper will never be able to predict the key Alice sent because it is 100% random (something only quantum technology allows for). Further, the eavesdropper will also never be able to guess the results of Bob's measurements without adding detectable errors to them. Hence, the eavesdropper will never have information about the key communicated through the quantum channel and will always be detected when spying on quantum communications.



Bit Sequence	1	1	0	0	0	1	0	0	1	0	1	0	Bit Sequence
Photon Sequence	⤢	↕	↔	⤡	↔	⤢	⤡	↔	⤢	⤡	↕	⤡	Photon Sequence
Bases Sequence	+	+	×	×	+	×	+	×	×	+	+	×	Bases Sequence
Detection Result	0	1	1	0	0	1	1	0	1	0	1	0	Detection Result
Compatibility	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✓	✓	Compatibility
Key	-	1	-	0	0	1	-	-	1	-	1	0	Key

FIGURE 11. High level representation of the BB84 schema, the most used quantum key distribution (QKD) protocol.

APPENDIX C

EVOLUTION OF QUANTUM ENCRYPTED COMMUNICATION NETWORKS

Ground-based QKD using optical fibers

The field of quantum telecommunications started making real accomplishments with the development of the first testnets at the beginning of the 21st Century. The DARPA (Defense Advanced Research Projects Agency) Quantum Network was the first known quantum network on earth. It was developed by researchers at Harvard and Boston Universities in 2003. It measured 29 km long initially connecting six, and later ten nodes in 2005 [21,22].

According to IDQuantique, Switzerland was the first country to install a quantum network for a real case in 2007. They used it to protect national election data when transmitted from the storage room to the location in which the votes were tallied.

Not long after, in 2008, a robust quantum network was developed in Vienna for the SECOQD (Secure Communication based on Quantum Cryptography) European project. The Austrian Institute of Technology received 11 million euro in funding from the European Union to coordinate the project. This quantum network had six nodes. Five were located in the Siemens facilities and the sixth one was located in a relay station. In total, the network was 285 km long and was divided into optical fibers between nodes measuring from 6 km to 85 km [229,230].

Another interesting project in this field is Quantum City in South Africa. The Quantum City project is the result of a collaboration between the Center for Quantum Technology from KwaZulu-Natal University, the Innovation Company from that University, eThekwini Municipality, and the Innovation Fund. This quantum network was developed in 2009 with four initial nodes distributed in multiple suburbs of the eThekwini district and wired in a star configuration with fiber lengths between the nodes, ranging from 2.6 km to 27 km [231].

There have also been several quantum network initiatives in China. One of those initiatives, in operation since 2007, comprised of a network in the metropolitan area of Beijing. It consisted of four operational nodes separated by 32 km and up to 42.6 km in a star configuration, in the areas of Wangjing, Dongxiaokou, Nanshatan, and Huangchenggen [232]. A network that became operational in 2009 in Heifei is also worth mentioning. This network also had four nodes placed in a star configuration and a fifth additional node, which were located in UTSC, Wan'an, Meilan, Wanxi and Feixi respectively. The network allowed for real-time quantum encrypted phone calls between any pair of the five nodes with a distance of up to 60 km [233]. A third network between the metropolitan areas of Heifei, Chaohu, and Wuhu was operational for over 5,000 hours from December 2011 until July 2012. Five of the nodes were in Heifi, three more nodes were installed in

Wuhu, and a ninth node was operating in Chaohu. The total length of the installed optical fiber was close to 200 km [234]. Other initiatives have followed, the most outstanding of which is led by the University of Science and Technology of China that intends to create a quantum connection between four cities through a 2,000 km long optical fiber from Beijing to Shanghai [27].

The best documented quantum network to date was developed by Tokio and structured in three layers [195]. The first layer is the quantum layer, made up of six nodes generating keys through different protocols, distributed between the cities of Koganei, Otemachi, Hakuson, and Hongo, connected point by point. The second layer is for administration and control. A key management agent (KMA) located in each node that physically corresponds to a protected server. The KMA receives a key through an application interface (API) developed by NEC Corporation and the National Institute of Information and Communications Technology of Japan (NICT). This key makes it possible for different systems and protocols that make up the network to interoperate. The servers corresponding to the KMAs are responsible for collecting quantum keys

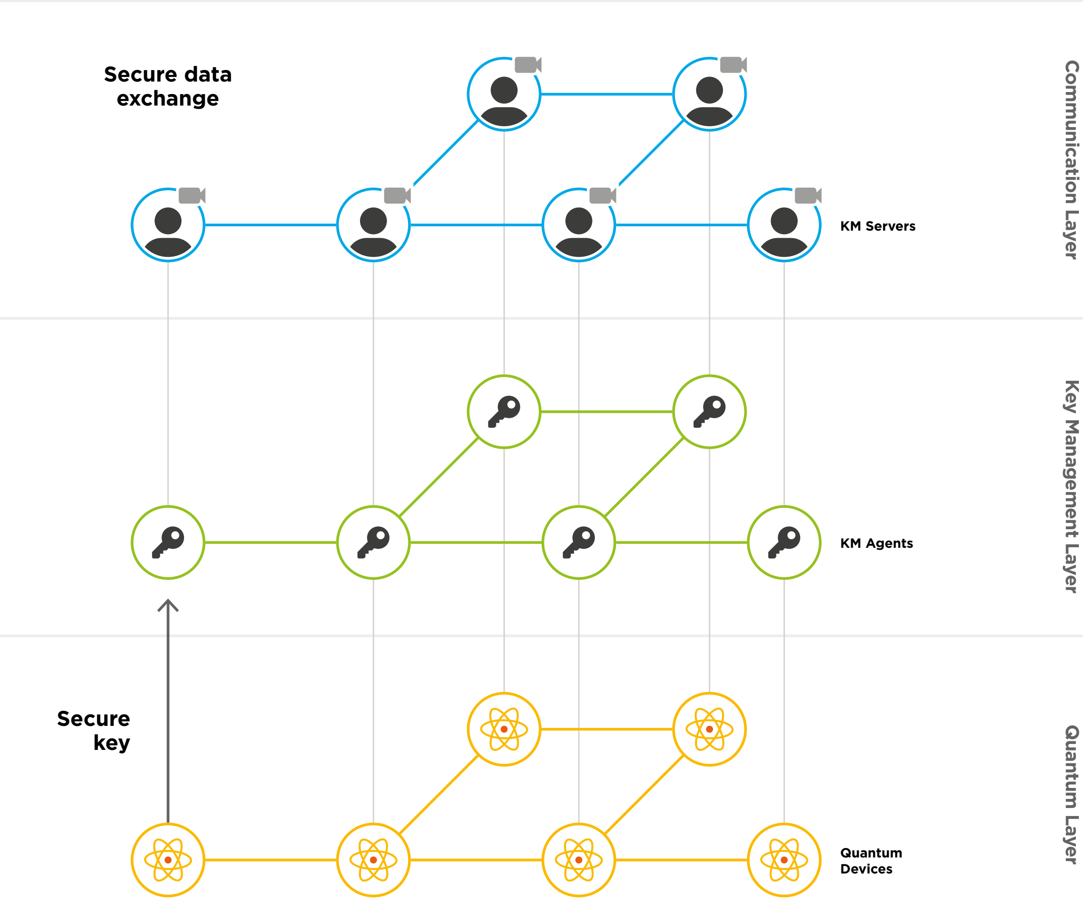


FIGURE 12. Schematic representation of the 3-layer quantum network in Tokio, divided into 3 layers.

and the data on them. They can collect the quantum error ratio per qubit (QBER), for example, and then send it to a centralized server for key management (KMS). The third layer is a communication layer in which the generated quantum keys are used to encrypt and decrypt audio, text, video, or other types of data produced by different applications per the AES-256 standard. The different connections use cables ranging from 1 km to 90 km in length.

The United States just started testing this technology. Quantum Xchange is developing the country's first commercial network with quantum cryptography [131] that "will connect the financial markets on Wall Street with back office operations in New Jersey, helping banks keep high-value transactions and mission-critical data safe and secure" [132]. This telecommunications giant entered into an 8.9 million US dollar agreement with SK Telecom [126] for Quantum Xchange to provide SK Telecom with its quantum cryptography systems.

Space-based QKD using satellites

As mentioned in Section I, wireless networks have a broader range than wired networks. Wireless networks have a lower attenuation because keys are able to be transmitted travelling above the atmosphere most of the time and up there, there are only a few particles to interact with. Orbiting satellites are needed to enable these wired networks and because of this, the first space-based test was under way for a while longer than the first ground-based networks.

China was the first country to place satellites in orbit for Earth-to-space and space-to-Earth quantum communication purposes. In 2016, the QUESS (Quantum Experiments at Space Scale) space mission launched a 600 kg satellite, known as MICIUS. The estimated overall cost of the mission was 100 million US dollars [28,29]. With communication between Earth stations in Delingha, Nanshan, and Lijiang, MICIUS was able to generate and share the first quantum keys over long distances that exceeded 1200 km [30,31].

Because of MICIUS, the greatest milestone in the field of quantum information was achieved on September 17, 2017: a quantically encrypted 90-minute videocall was placed between China and Austria at a distance of 7,600 km. It was the first instance of encrypted intercontinental communication using secure quantum technology. After the key was generated using the MICIUS satellite, it was used by China and Austria to encrypt and decrypt a videocall that traveled through regular optical fibers belonging to classical networks [32].

China foresees launching 10 additional satellites that are expected to allow for a quantum network of intercontinental communications between Europe and Asia by 2020 that would be worldwide by 2030 [33].

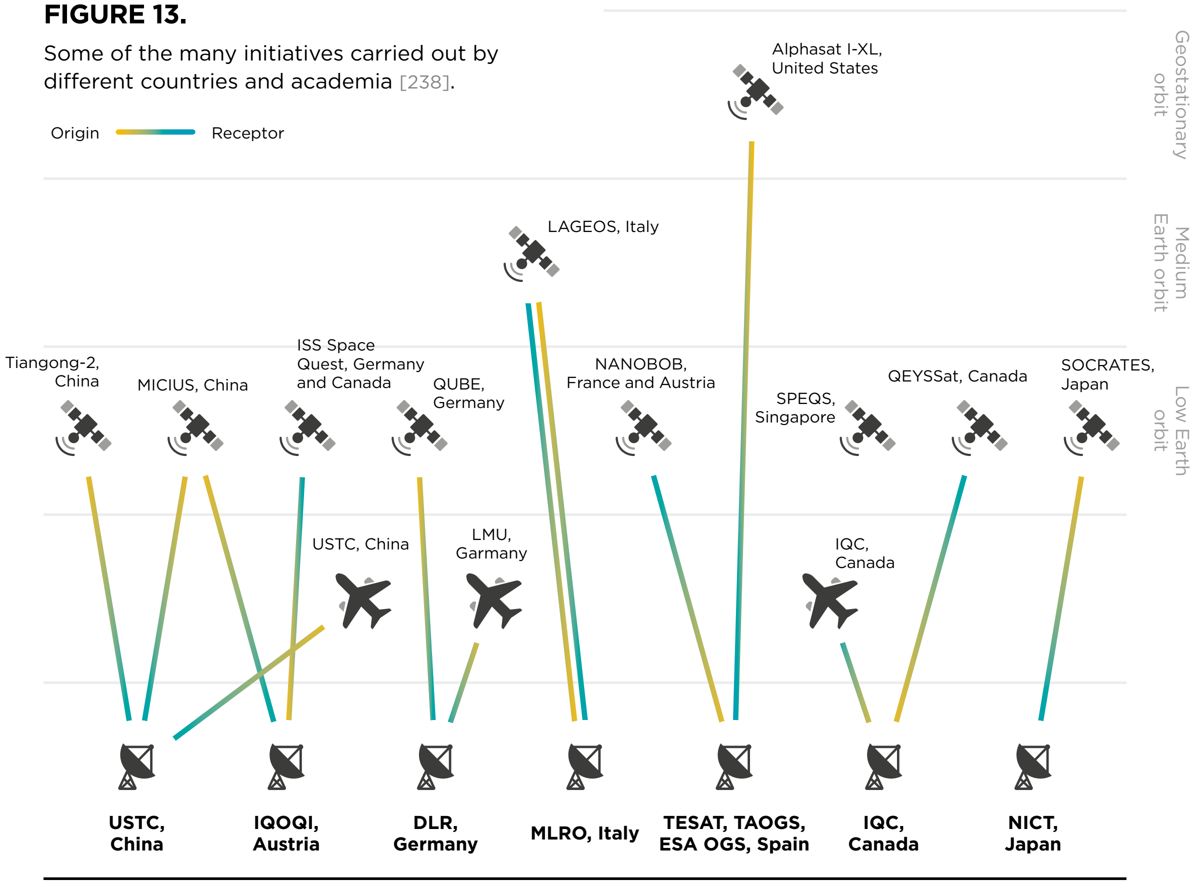
China is also focused on studying the feasibility of conducting Earth-to-space and space-to-Earth communications using devices in space stations, rather than satellites, in order to avoid generating a satellite constellation. Thus, in 2017, QKDs were conducted between the Tiangong-2 space laboratory and the Nanshan land station, which are 719 km apart [159].

Likewise, in 2017, Japan managed to conduct QKDs using a micro-satellite called Small Optical Transponder (SOTA). SOTA weighs 6 kg, is 17.8 cm long, 11.4 cm wide, and 26.8 cm tall, and orbits at an altitude of 600 km [196].

In 2016, a collaboration between academic institutions and Italian observatories carried out optimal photon transmissions from a 7,000 km distance between the LAGEOS-2 satellite, orbiting at an altitude of 5,620 km, and the Matera Laser Ranging Observatory. This feat pave the way for the conduction of QKDs at longer distances [235].

FIGURE 13.

Some of the many initiatives carried out by different countries and academia [238].



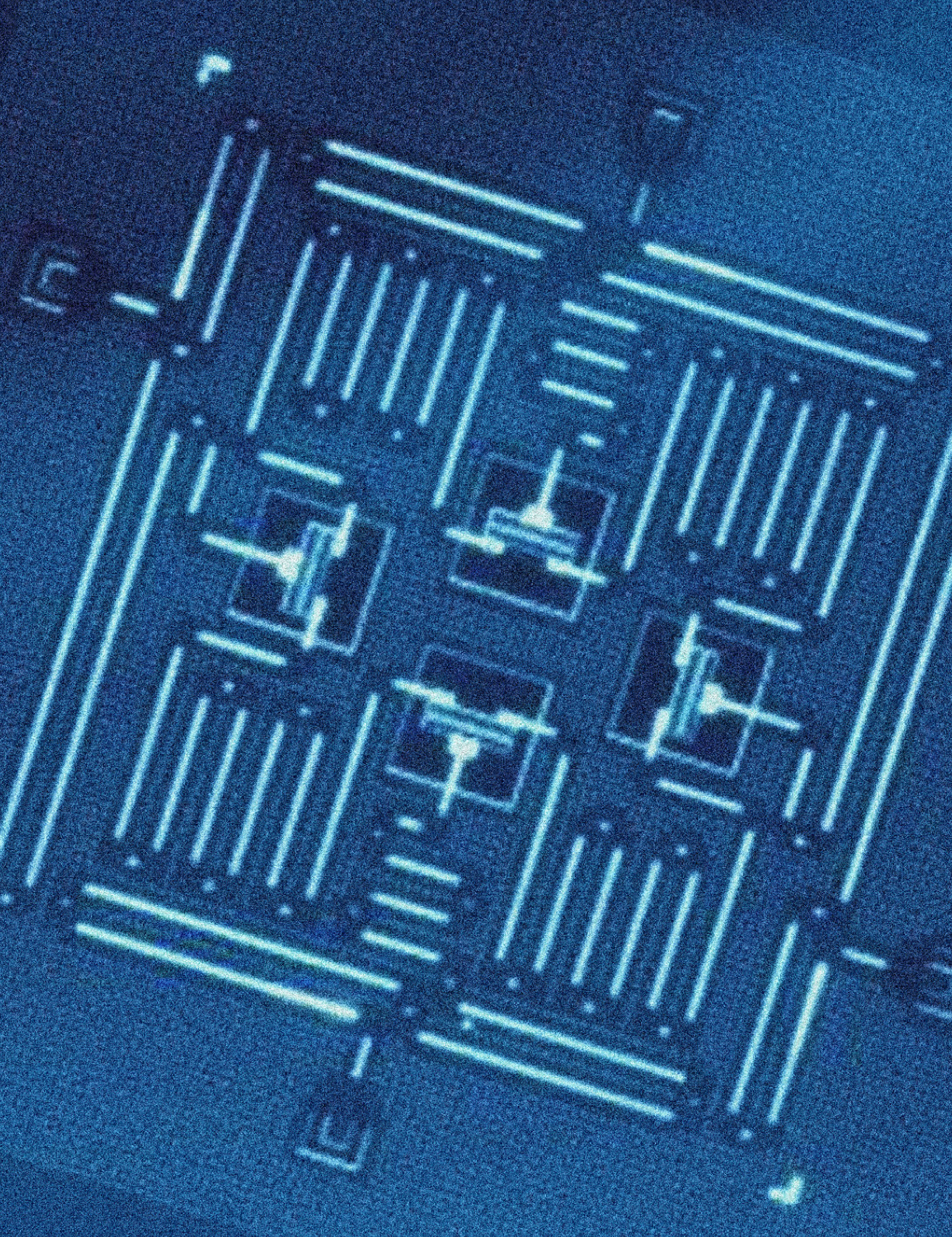
In April 2018, the group announced they were able to surpass the 20,000 km threshold in photons exchanged [236]. They established communication between two satellites from the GLANOASS constellation, which has over 20 satellites, operates in three orbital planes, and was developed during the second half of the 20th Century for Russian satellite geo-localization [237].

Space-QUEST (Quantum Entanglement for Space Experiments) run by the European Space Agency (ESA) [53,54] is another interesting European initiative. It proposes the placement of a transmitter on the outer wing of the Columbus module at the International Space Station (ISS). The ESA is also running the Eutelsat Quantum initiative, “a pioneering mission that will influence how telecom satellites are procured and manufactured in Europe”. In the second half of 2019, a satellite will be launched for Earth-to-space and space-to-Earth quantum telecommunications [166].

Several German agencies, including the Max Planck Institute and the German Aerospace Center, collaborated in 2016 to conduct their own experimental study to test the transmissions of photon signals at a distance of 38,600 km between the portable space stations located at the Teide Observatory, Tenerife, and the Alphasat I-XL stationary satellite [209].

France and Austria have also collaborated in an initiative called NanoBob, an attempt to offer more precise data on the optimal system arrangement for QKDs using satellites and to precisely synchronize two watches; one is located on a space ship and the other is on Earth [238].

These are only some of the many projects being conducted around the world so far [239]. While China is in the lead for now, several countries are eager to develop quantum telecommunication technology. Thus, most countries in Asia and Europe are making major investments in quantum technologies so as not to fall behind in the quantum telecommunications race led by China. While many other countries in other parts of the world are conducting concept tests within their governments, technology companies, and financial institutions, we have not been able to find sufficient data on equally ambitious initiatives as those described in this section. Unfortunately, we are not aware of a single program or concept test in Latin America and the Caribbean.



A device consisting of four transmon qubits, four quantum busses, and four readout resonators fabricated at IBM and appearing in the paper "Building logical qubits in a superconducting quantum computing system" by Jay M. Gambetta, Jerry M. Chow and Matthias Steffen. Jay M. Gambetta, Jerry M. Chow & Matthias Steffen. 13 January 2017.

APPENDIX D

ASYMMETRIC CRYPTOGRAPHY

The idea of asymmetric cryptography, also known as public key encryption, emerged in the 1970s. While it was first believed that R. Merkle [240] and W. Diffie and M. Hellman [241] developed this method in 1976, it seems that it was actually J. Ellis, a cryptographer from the British Intelligence, who explored this field for the first time in 1970 in a classified manner [242].

Among the different asymmetric cryptography techniques, the RSA algorithm, the elliptic-curve cryptography, and the discrete logarithm cryptography are most important and will be briefly covered in this section [243].

RSA Algorithm

The RSA Algorithm relies on the exponential difficulty for classical computers to factor large integer numbers; there is a log-linear relationship between the number of steps the computer must conduct and the integer's size. It is believed that R. Rivest, A. Shamir, and L. Adleman from MIT developed the RSA Algorithm in 1978 [244]. In fact, the algorithm was named in their honor. However, a document from the British intelligence service was declassified in 1996, proving that C. Cocks and M. Williamson had actually proposed a similar method in 1973 [245].

The idea behind the algorithm is that, given the integer numbers *e*, *d* and *n* so that for any integer *m* complying with $0 \leq m \leq n$ the following applies:

$$(m^{\mathrm{e}})^{\mathrm{d}} \equiv m \ (\mathrm{mod\ n})$$

It is extremely difficult to find *d* given *e* and *n,* , or even *m* with classical algorithms. In the algorithm, *m* is the message to be encrypted, *e* is the public key given to the person sending the message to be encrypted, and *d* is the private key to decrypt it that only the receiver of the message possesses.

The classical algorithm that solves the problem most efficiently is the general number field sieve (GNFS). It is the fastest algorithm that can factor numbers higher than 10^{100}. The problem to be solved is, given the integer *n*, one must find prime integers *p* and *q* (related to *e* and *d*) so that:

$$n=pq$$

Between 1991 and 2007, RSA Laboratories ran an active challenge where they financially rewarded people that were able to factor RSA numbers of different lengths [246].

RSA-768 is the longest known number to be factored, with 768 binary digits and 232 decimal digits. The team responsible for factoring it -the team that won the challenge- had to perform more than 10^{20} operations to find the number. They used the GNFS algorithm and hundreds of computers with very powerful processors for two years to do so. In 2009, they received the 50,000 US dollar award. They said that using a single AMD Opteron processor at 2.2 GHz with 2 GB of RAM, it would have taken them 1500 years to do the same thing and estimated that factoring a 1024-bit number would be 1,000 times more difficult [247].

In 2015, the NSA advised against continuing to use this encryption technique

Discreet Logarithms Problem (DLP) and Elliptic-Curve Cryptography (ECC)

Given a finite cyclical group, G, and a group generator, the discreet logarithms problem on G entails finding the only $d \in [0, |G| -1]$ which, given any element of the group $\beta \in G$, fulfils:

$$\alpha^d=\beta$$

That is, finding the logarithm of β with base α:

$$d=log_\alpha\beta$$

There are certain groups G with specific properties that allow us to develop algorithms that solve this problem in polynomial time. For example $G=Z_N$. However, for other groups G, the difficulty is exponential or sub-exponential, so that those groups are more appropriate in developing cryptographic algorithms because they will be harder to reverse.

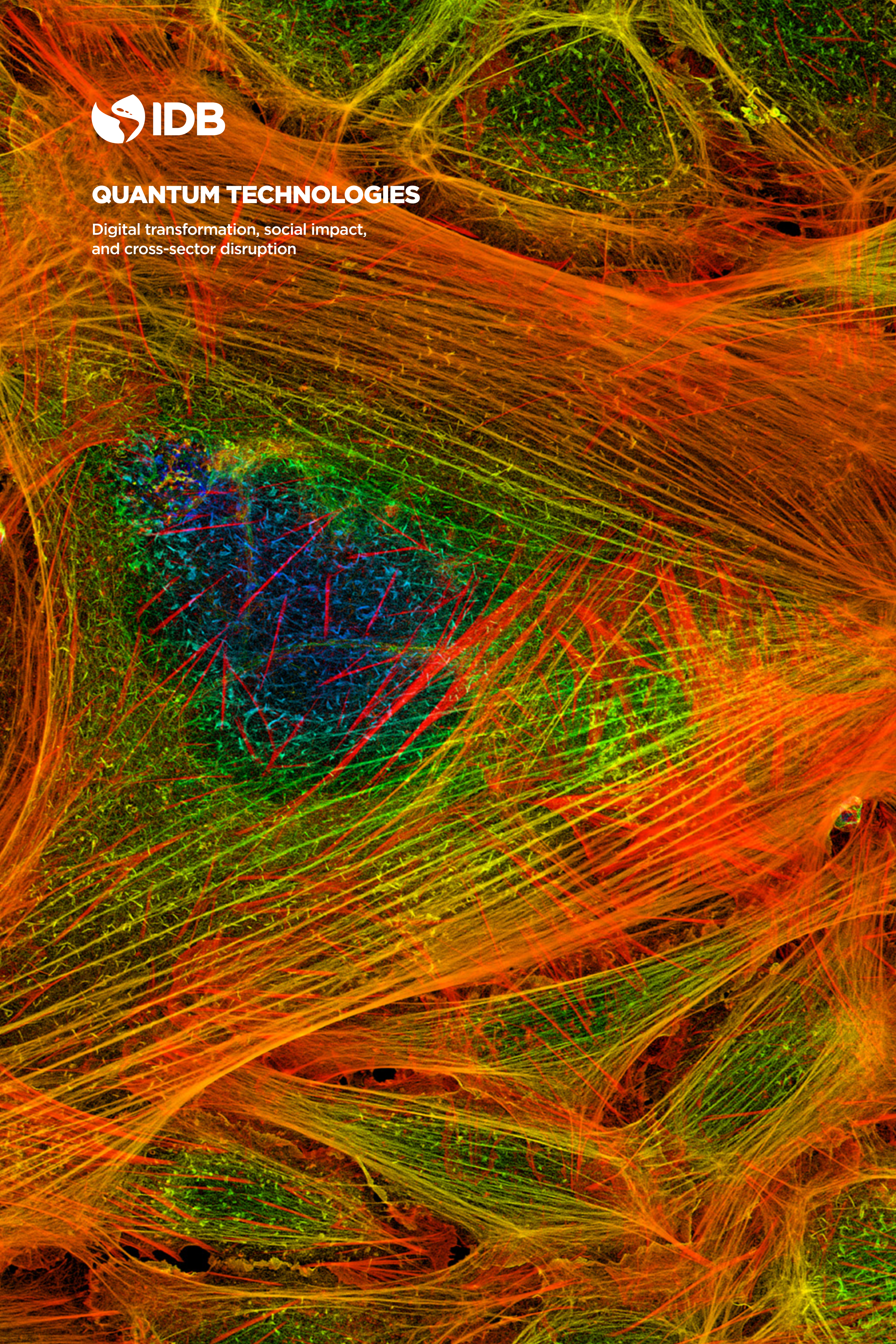
Some popular algorithms, such as the ElGamal encryption [248], known as *Digital Signature Algorithm* (DSA), or the Diffie-Hellman key exchange, propose using the multiplicative group module p, $G=(Z_p)^*$. Others propose using finite abelian groups of elliptic curves $G=GF(p^n)$, as, for example, the Diffie-Hellman version on elliptic curves (ECDSA).[17]

In 1999, ANSI sponsored the use of elliptic curves and proposed the standard ANSI X9.62 [249]. A year later NIST also supported the use of elliptic curves proposed by ANSI and proposed additional elliptic curves to be used [250].

[17] The elliptic algorithm is the additive formulation for the discreet algorithm. The elliptic algorithm has exponents and products while the discrete algorithm has products and sums.

ECDSA is slightly more sophisticated than RSA. It is also safer because it achieves the same complexity of RSA, but with shorter keys. For those readers interested in a more detailed comparison, we recommend the document by Al.I. Ali [251] where more information, including the following chart, may be found:

RSA key length (bits)	ECDSA key length (bits)
1024	192
2048	256



IDB

QUANTUM TECHNOLOGIES

Digital transformation, social impact,
and cross-sector disruption