

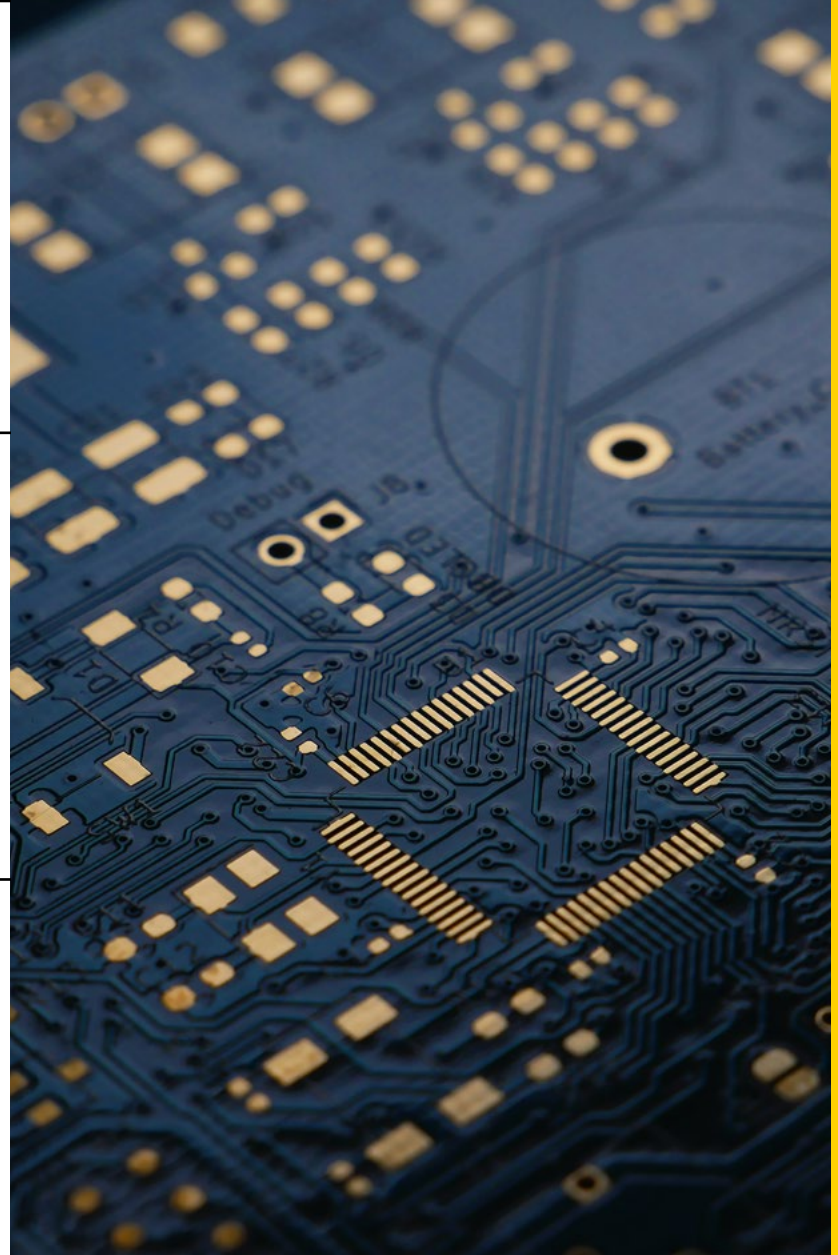
*Highlights*

# Quantum computing: Out of the box



**PROSEGUR**

# *Index*



01

# Technology of the impossible



The constant digital evolution present in our society, understood as the process of developing **tools and techniques focused on improving people's resources**, sustains numerous active fronts for innovation and technological progress. Among these is what is known as **quantum computing**, considered by **NATO** -among other institutions- as one of the most promising emerging technologies that currently exists.

In fact, the power and momentum of this technology will bring about a **revolution** in the way we process and store information. **It is estimated that it will reach its peak in 2035** by **projecting more than 2,000 zettabytes of information globally**, being when hardware and software capable of controlling these systems are expected to be available.

→  
A **But what exactly is quantum computing and why is it so revolutionary?**

The concept of quantum computing originated from Richard Feynman, an American physicist who, in a **paper** published in 1982, introduced the idea of **creating an environment based on quantum mechanics in order to solve complex algorithms that were impossible** for conventional computers.

Hence, according to the concept of quantum computing given by **IBM**, this technology refers to a **computer system that, based on physical principles of quantum mechanics, offers the possibility of developing or solving highly complex problems and algorithms.**

To quote Seth Lloyd – from his book *Programming the Universe*<sup>1</sup> – **A classical computation is like a solo voice** – one line of pure tones succeeding each other. A **quantum computation** is like a **symphony** – many lines of tones interfering with one another.

→ **How can they now solve calculations that were once believed impossible?**

ⓑ

Its foundation lies in a **new approach for the minimal units on which computational logic is based**, known as bits, which can be arranged as zeros or ones. Unlike classical computing, quantum computing uses qubits (quantum bits), which can represent 0, 1 or a simultaneous theoretical superposition thanks to a phenomenon called **quantum superposition**. Furthermore, qubits can be entangled, which means that the state of one qubit can depend on the state of another, **interacting and interfering** with each other and offering the possibility of **executing multidimensional algorithms**.

Therefore, qubits can be metaphorically represented as **switches** that can be on, off or possibly overlapping at the same time, similar to the way that you cannot know if a bedroom light is on or not until the moment you enter it.

→ ⓐ **So what does this entail?**

Quantum computing operates in an **extraordinarily larger domain** than classical computing. While classical computing performs individual calculations that lead to single results and a single change in any of the variables produces a new operation, **the quantum system generates a range of results by processing numerous operations simultaneously and at a faster rate**.

According to Aaronson and Weinersmith's<sup>2</sup> analogy, quantum computing is based on a choreography in which **the paths leading to incorrect answers interfere and cancel each other out, while the correct paths reinforce each other**, increasing the capacity of the computers for specific problems.

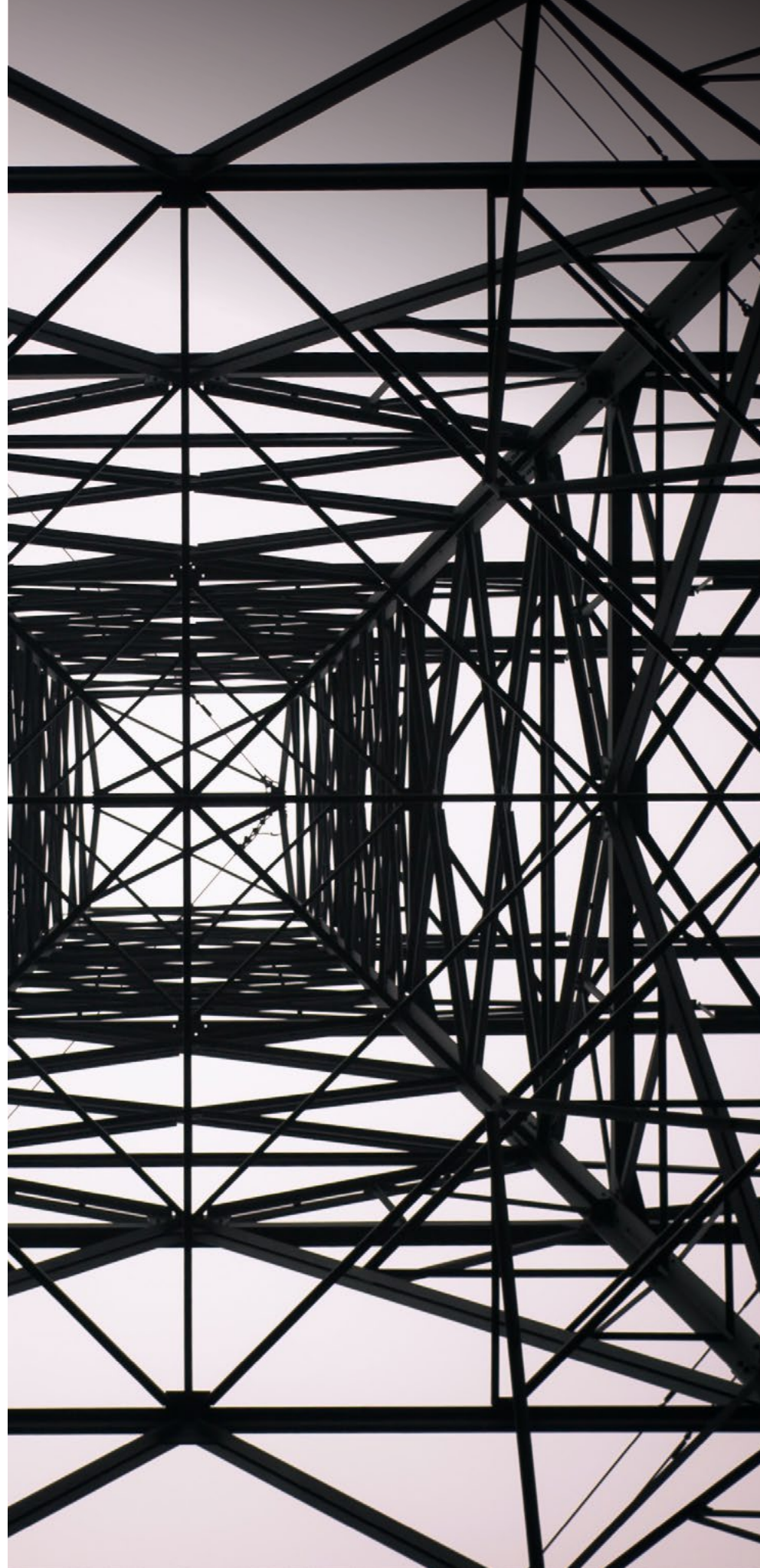
---

<sup>1</sup> See [Programming the Universe](#).

<sup>2</sup> See [The Talk](#).

All this, along with its small size, means that it requires **less energy consumption** compared to similar technology currently available: supercomputers. However, **quantum computing should not be reduced to a simple improvement in the processing speed** since there may be certain tasks where a conventional computer is more efficient.

Therefore, given the potential repercussions that this extraordinary revolution - previously considered impossible- presents for our society, **Prosegur Research** analyzes its possible **implications in the future**, both in terms of progress and aspects to consider regarding its security in order for this progress to be positive.



02

# From the qubit to the opportunity revolution



Computer scientists believe that in order to visualize **the true potential of quantum computers**, they must have a capacity of **1 million qubits**. As of June 2023, the computer that comes closest to this figure is IBM's Osprey, with 433 qubits. However, a recent **study** has found that, albeit in a restricted form, a quantum computer of only 127 qubits is capable of surpassing the capabilities of a state-of-the-art supercomputer. On the other hand, while it is true that systems with up to a 5,000-qubit architecture have been developed, such as D-Wave's Advantage System, some developers do not consider this to be quantum computing<sup>3</sup>, since they do not function as general-purpose computers - capable of performing a variety of tasks and operations -.

The main obstacle for the maximum exploitation of this quantum potential is due to the fact that, up to now, **the technology developed does not have the sufficient capacity to control these systems**, which causes **unstable conditions** when more sophisticated operations are carried out. Thus, the **challenges** that this technology currently presents are diverse:

## Graphic 1

### Challenges of quantum computing today

01



#### **Improving the stability and errors**

that qubits' present in order to increase their quantity in the process.

02



#### **Developing programming and software tools and techniques**

capable of adapting to quantum application.

03



#### **Reducing the cost involved**

in the construction and maintenance of these computers, as it currently requires significant financial capacity to be involved in this type of project.

**Source:** Prosegur Research, 2023 based on KPMG

<sup>3</sup> See **Protocol**.



However, despite the great room for improvement, quantum computing currently has **enormous benefits**<sup>4</sup>, covering a **wide range of domains and offering its application** in a variety of fields. Some of the main examples of its application include process optimization and the creation of new models or materials, improved cybersecurity in the creation of more advanced

encryption protocols, discovery of new drugs, improvement in the capabilities of artificial intelligence, or improvement of logistic and transportation operability, among others.

<sup>4</sup> See **Telos**.

<sup>5</sup> See **European Data Protection Supervisor (EDPS)**.

<sup>6</sup> See **Airbus**.

<sup>7</sup> See **IEEE - Spectrum**.

## Benefits and opportunities that quantum computing can provide

### 1 **Cryptography: privacy on the rise**

Quantum computing has the potential to **enhance security** by providing the ability to create more complex algorithms and protocols, which is a fundamental pillar in both military and civilian spheres. It is of particular interest with regards to **personal data protection**<sup>5</sup>.

### 2 **Process optimization in multiple industries**

Quantum computing can help tackle complex optimization problems, **exploring solutions more efficiently and finding optimal results faster and with greater diversity**. Thus, this optimization is expected to have a major impact on **simulation-related** operations, such as aeronautical **route planning or chemical development processes**. In the short term, it may have a major impact on the aeronautics<sup>6</sup> and energy<sup>7</sup> sectors. Ultimately, process optimization can lead to significant **cost reductions** for companies.

### 3 Machine learning and artificial intelligence: technological convergence

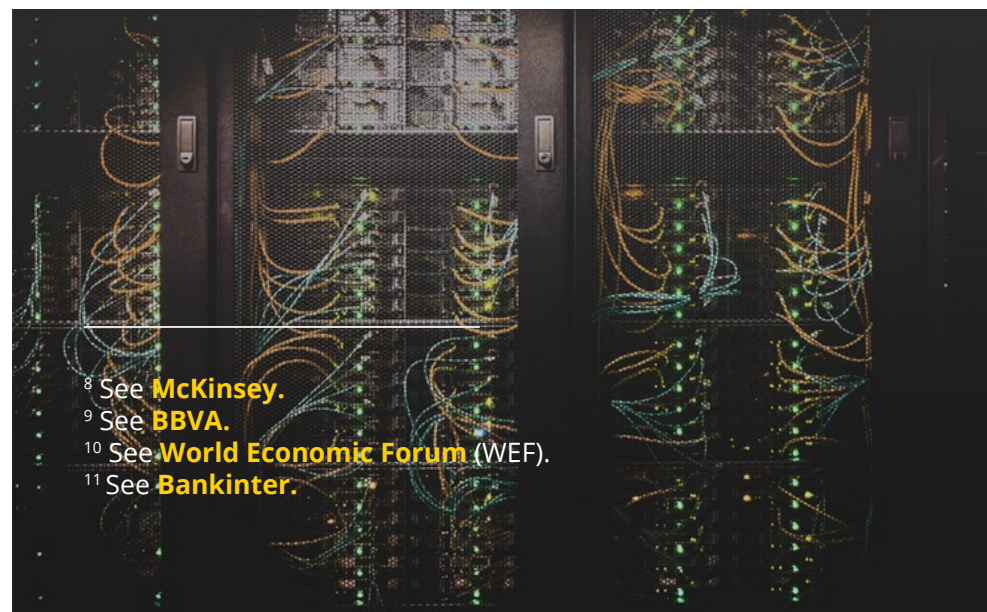
Quantum computing can improve machine learning algorithms and offer new techniques for **analyzing large data sets and recognizing complex patterns**, increasing the capabilities of technological convergence we have today. This can lead to advances in its application such as in **medical diagnostics, machine translation** and, in general, **for electronic instruments** that make use of artificial intelligence, which is particularly interesting for **weapons development**.

### 4 Managing risks and scenarios: enhanced creativity

Quantum computing can improve risk analysis and management through its ability to **measure and interconnect a large number of variables with a high degree of uncertainty**, as well as through the consideration and elaboration of multiple **scenarios**. This can be implemented in various contexts, among which **financial analysis**<sup>8</sup> stands out for its potentially significant benefits.

### 5 Sustainability as the axis of the future

**Preserving ecosystems** and action against the climate challenge should be one of the principal courses of action for all companies around the world. In this respect, quantum computing can benefit numerous sectors such as the **energy industry and data centers**, consuming less energy to maintain their operation<sup>9</sup>; **the research and chemical industry**, in the search for new fertilizers and various catalysts that reduce CO2 emissions into the atmosphere<sup>10</sup>; or the **automotive sector**, in the simulation of new water electrolysis models to generate green hydrogen and also design new batteries with more storage power<sup>11</sup>.



<sup>8</sup> See **McKinsey**.

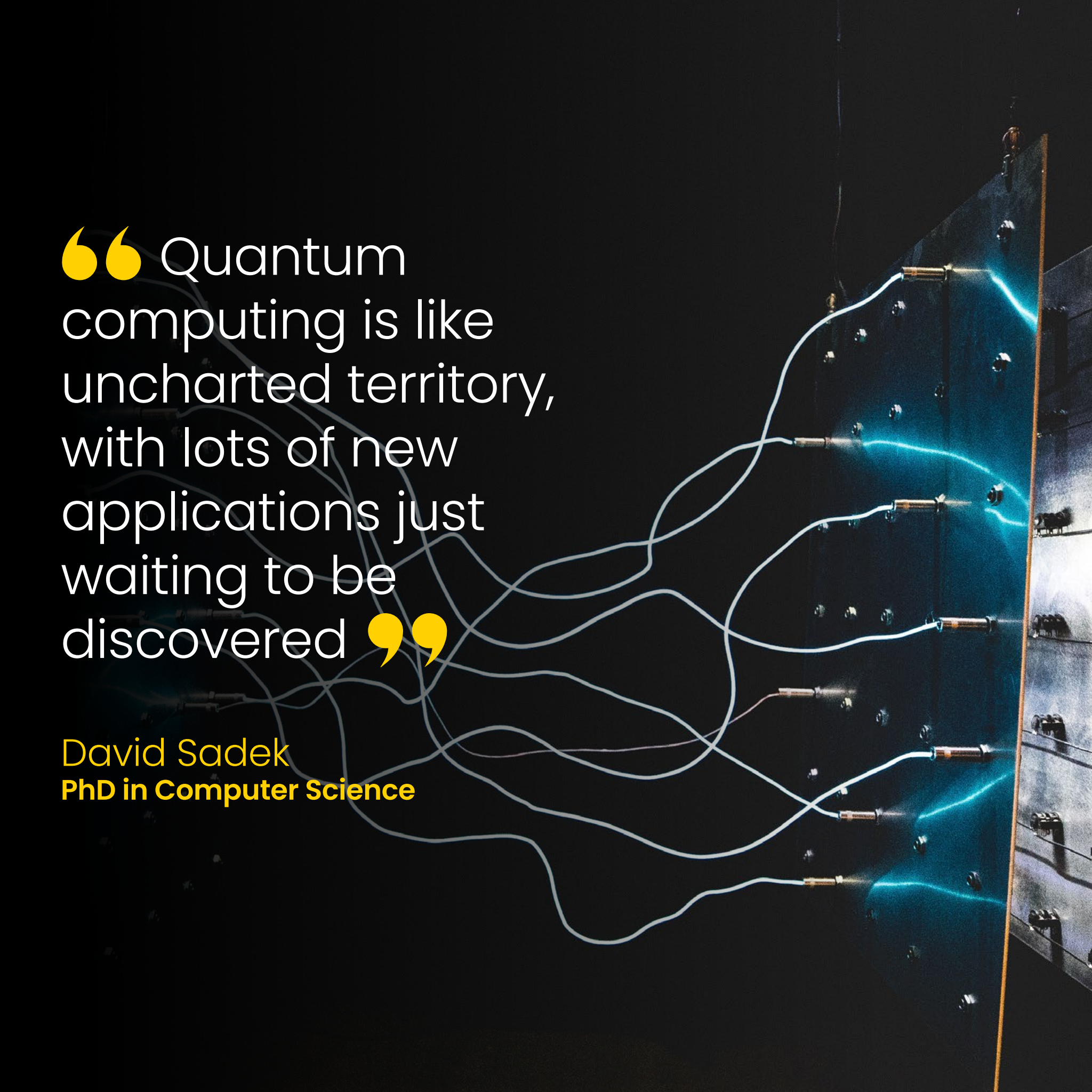
<sup>9</sup> See **BBVA**.

<sup>10</sup> See **World Economic Forum** (WEF).

<sup>11</sup> See **Bankinter**.

“ Quantum computing is like uncharted territory, with lots of new applications just waiting to be discovered ”

David Sadek  
PhD in Computer Science



03

**Security  
hotspots**  
related to  
quantum  
computing



Due to its technical characteristics, quantum computing presents a series of **important benefits** but also its **own risks and threats**. Additionally, like any technological advancement, **it helps to**

**empower citizens**, from its application in covering the individual needs or **boosting business** in companies and sectors, to **its use for criminal purposes**.

## IN ITS DESIGN



### Quantum precision

Qubits are fragile and prone to errors due to several factors, such as interactions with the environment and the effects of decoherence, resulting in the loss of quantum entanglement and generating a classical physical state - without entanglement. These quantum errors can propagate and **deteriorate the accuracy and trust in quantum calculations**. Consequently, this is likely to have a high impact in areas where accuracy is critical, such as drug development or decision making in the financial sector<sup>12</sup>.

### Thermal sensation -459°

A quantum computer requires specific conditions with a room temperature close to absolute zero (-459 °F; -273 °C) and isolation from the earth's magnetic field to prevent atoms from moving and colliding with each other or interacting with the environment. In addition to these unique conditions, in order to obtain them the quantum system needs helium<sup>13</sup>. Thus, in this regard, **the risks associated with the quantum computer supply chain become relevant**, where, in addition to the complexity of the infrastructure, possible alterations in the **helium supply** - such as shortages or price fluctuations - pose a risk to the operability of these machines and their operators.

<sup>12</sup> See [Medium](#).

<sup>13</sup> See [IBM](#).

## Legislative lag

The usual legal lethargy regarding the regulation of emerging technologies may materialize in the case of quantum computing. Considering its rapid development and potential capabilities, the absence of adequate regulatory

frameworks for its implementation and use could allow abusive or irresponsible practices that affect **privacy, security, and human rights**<sup>14</sup>. Without a solid regulatory framework, the risk of state and non-state actors using this technology in an aggressive and unrestricted manner is enhanced, which in turn **increases the vulnerability** of exposed systems.

# IN ITS IMPLEMENTATION



## Existential convergence

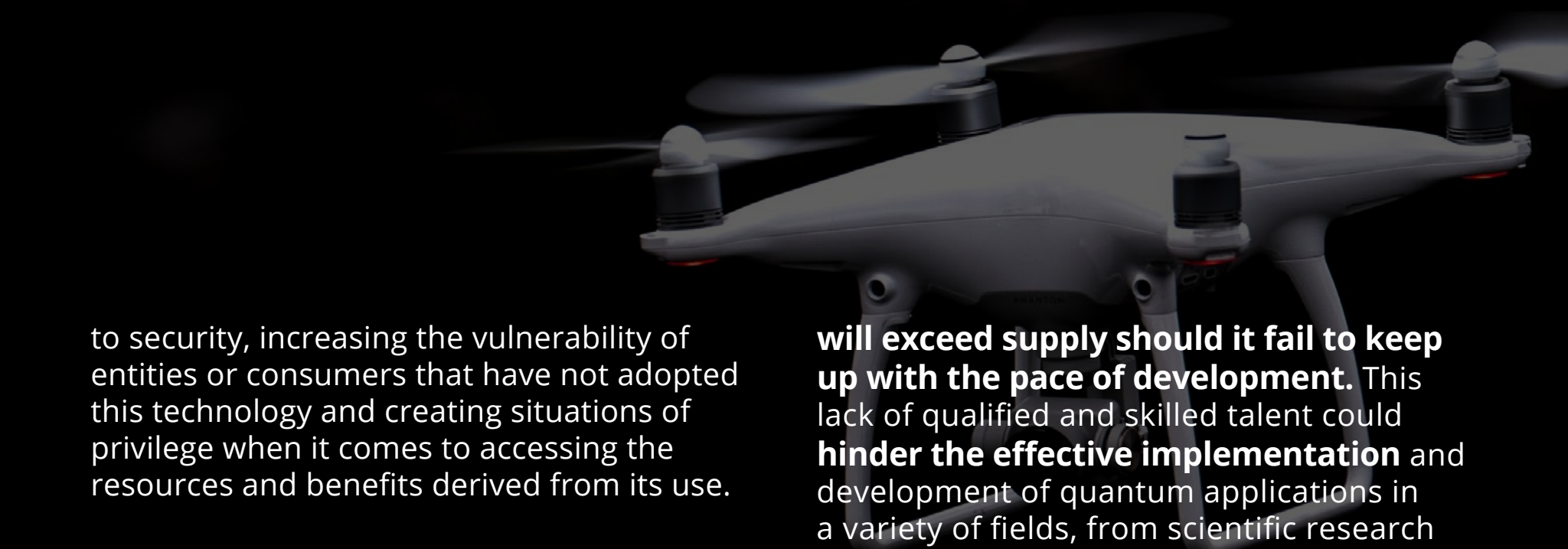
Although considerable progress has been made in building quantum computers, there are still significant challenges in making them practical and affordable. Current quantum systems face problems such as decoherence, lack of stability, and **high sensitivity to external interference**. In addition, availability and access to quantum computing is limited and highly restricted, as quantum systems are still in the **early stages of development** - which requires a high level of technological resources – leaving them in the hands of a limited number of organizations<sup>15</sup>.

## Quantum asymmetry

Whether it be due to its prohibitive development for most actors or to its high acquisition costs, **the asymmetric adoption of quantum computing** among users, companies and institutions can lead to situations of inequality in the market and the socioeconomic order. Moreover, this **technological gap** can be exploited by the malicious capabilities of quantum computing, exacerbating this inequality with regards

<sup>14</sup> See [European Data Protection Supervisor \(EDPS\)](#).

<sup>15</sup> See [The Quantum Insider](#).



to security, increasing the vulnerability of entities or consumers that have not adopted this technology and creating situations of privilege when it comes to accessing the resources and benefits derived from its use.

### Supercomputers need super-employees

As quantum computing advances and becomes a tangible reality, the **demand for highly skilled professionals**

**will exceed supply should it fail to keep up with the pace of development.** This lack of qualified and skilled talent could **hinder the effective implementation** and development of quantum applications in a variety of fields, from scientific research to industrial manufacturing and national security. Additionally, the absence of properly trained professionals heightens the **risk of implementing flawed solutions** that could be exploited by malicious actors or that simply do not meet the required security standards.

## IN ITS USE



### Communication integrity

The global Internet economy depends on cryptography as the basis for a secure network, which to date is vulnerable to the capabilities of quantum computing. Thus, the existence of a technology that allows the possibility of **quickly breaching**

**traditional encryption systems,** together with the lack of new methods capable of responding to this situation, represents an elevated risk for the security of both users and the entire IT infrastructure<sup>16</sup>.

---

<sup>16</sup> See **IBM**.

## Privacy of qubits

Given their value in today's society, one of the main objectives behind the violation of encryption systems may be to **obtain protected information**<sup>17</sup>. In this regard, the protection of personal data is exposed to a greater threat since the sensitive information stored or transmitted would be **exposed to unauthorized access**. This could ultimately have a severe impact on sectors that manage the most valuable personal data, such as banking, e-commerce, or healthcare.

## Quantum hacking

The use of quantum systems offers greater capabilities when it comes to **hacking computer systems** beyond the cryptographic component. Quantum computing techniques to exploit vulnerabilities are superior to those offered by a classic computer, generating a threat with a **higher impact given the lower detection and analysis** capacity offered by current defense systems<sup>18</sup>.

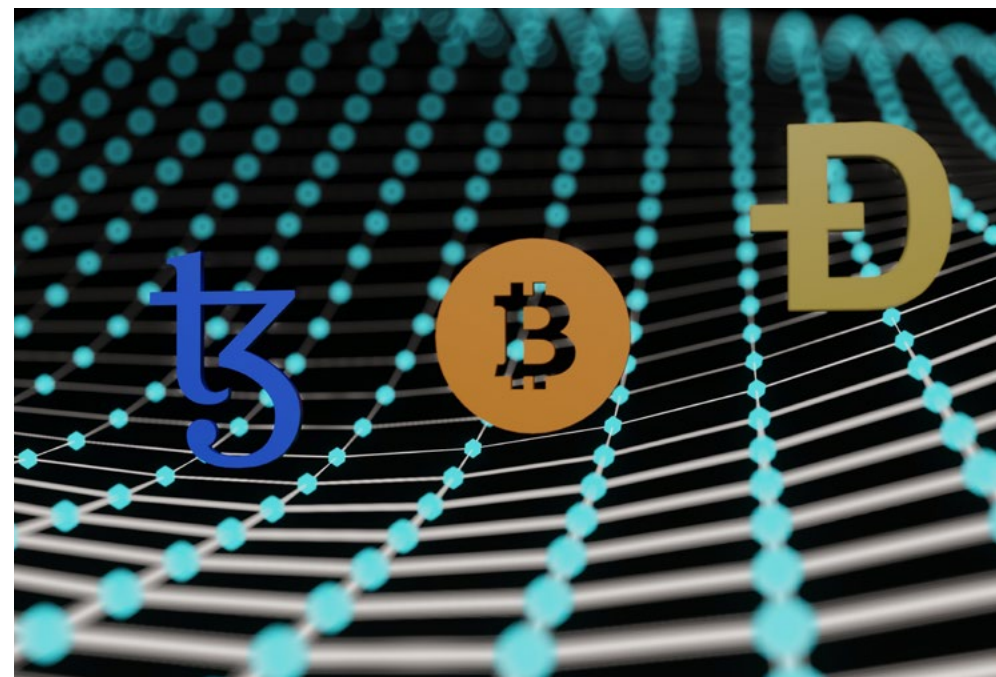
## Blockchain security

Quantum computing capabilities can also jeopardize the core of blockchain technology's success: its security. **The breach of its encryption and subsequent malicious manipulation** can mean not only the decline of this technology, but also a significant risk for companies and users that make use of it. For example, it is currently estimated that **25% of the cryptocurrencies** in circulation -based on blockchain- would be highly exposed to theft perpetrated through a quantum computer.

---

<sup>17</sup> See [European Data Protection Supervisor \(EDPS\)](#).

<sup>18</sup> See [Cloud Security Alliance](#).





## Multidimensional uncertainty

The greatest risk of quantum technology is its unpredictability. **The lack of knowledge and inability to fully measure its capabilities prevents making complete and effective forecasts of the potential threats and implications of its use for malicious purposes** in a variety of fields. Consequently, the possible development of **new criminal modus operandi** that would threaten the security of users and the industry as a whole will be particularly difficult to detect<sup>19</sup>.

---

<sup>19</sup> See [Forbes](#).



As has been made clear, quantum computing is a true revolution of the impossible, and offers us a promising future thanks to the transcendent technical advances that it will allow us to achieve, which were previously unthinkable. **Human technological empowerment with a vision of security is essential**, as well as a **positive impact** based on a systemic approach, which derives from the know-how of technicians, entrepreneurs, legislators, and citizens as a whole.

Generating **ecosystems of responsibility** through integrating the perspectives and needs of all stakeholders involved, as well as promoting sustainability at every level to ensure this progress makes a real contribution to global prosperity, will be two key challenges of this positive future.



# PROSEGUR

We ensure the security  
of individuals, businesses  
and society as a whole.

[research@prosegur.com](mailto:research@prosegur.com)

PROSEGUR RESEARCH

[www.prosegurresearch.com](http://www.prosegurresearch.com)