

TECNOLOGÍAS CUÁNTICAS

Una oportunidad transversal
e interdisciplinar para la transformación
digital y el impacto social

TECNOLOGÍAS CUÁNTICAS

Una oportunidad transversal
e interdisciplinar para la transformación
digital y el impacto social

ITE TechLab

Autor: Marcos Allende López

Supervisor: Marcelo Da Silva

Diseño: .Puntoaparte *Bookvertising*

Imágenes: Wikicommons

TECNOLOGÍAS CUÁNTICAS

Una oportunidad transversal e interdisciplinar
para la transformación digital y el impacto social



Este trabajo es resultado del esfuerzo que, desde el ITE TechLab, hemos venido realizando en el equipo de Marcelo Da Silva para poder presentar nuevas tecnologías al Banco Interamericano de Desarrollo con un enfoque técnico y social al mismo tiempo. Esta publicación es la primera de una serie de artículos y materiales audiovisuales que se ofrecerán de manera conjunta con el BID Lab, en el marco de nuestra colaboración para el análisis de la utilización de nuevas tecnologías para el desarrollo y la inclusión social.

El aprendizaje y la investigación realizada para la redacción de este documento ha sido muchas veces conjunto. En la parte técnica, han sido fundamentales las pruebas tecnológicas con Oscar Vazquez, Emiliano Colina, Ignacio Cerrato y Mariana Gutierrez, del BID; Pau Velando y Guillem Sant de Entanglement Partners; y Bruno Huttner de IDQuantique.

En otros aspectos ha sido igualmente valioso el apoyo de Marcelo da Silva, Nuria Simo, Vanessa Colina, Mario Casco, María Weisson, Melissa Panteliou, Isabel Ferro, Andrea Ortega y Sergio Gonzalez del BID; y Alejandro Pardo, del BID Lab. También queremos reconocer el gran trabajo de Mateo L. Zúñiga y el equipo de .Puntoaparte *Bookvertising* en la maquetación, y el apoyo de Melissa Julian en la edición.



Copyright © 2019 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercialSinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (<http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) y puede ser reproducida para cualquier uso no comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas. Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID, no están autorizados por esta licencia CC-IGO y requieren de un acuerdo de licencia adicional. Note que el enlace URL incluye términos y condiciones adicionales de esta licencia. Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.

TABLA DE CONTENIDOS

INTRODUCCIÓN	5	IMPACTO EN SECTORES E INDUSTRIAS	50
LA ERA CUÁNTICA	6	IMPACTO EN MEDICINA, BIOLOGÍA Y GENÉTICA	53
TECNOLOGÍAS CUÁNTICAS	7	IMPACTO EN EDUCACIÓN Y TRABAJO	55
¿Qué son las tecnologías cuánticas?	7	IMPACTO EN ECONOMÍA Y FINANZAS	56
COMPUTACIÓN CUÁNTICA	8	IMPACTO EN ENERGÍA Y AGRICULTURA SOSTENIBLE	58
¿Qué es?	8	OTROS IMPACTOS	58
¿Cómo funciona?	11	PROGRAMAS Y ESTRATEGIAS POR PAÍS	60
¿Cuál es el estado actual de la tecnología?	14	CHINA	61
INFORMACIÓN CUÁNTICA	16	UNIÓN EUROPEA	62
¿Qué es?	16	ESTADOS UNIDOS	64
¿Cómo funciona?	20	JAPÓN	66
¿Cuál es el estado actual de la tecnología?	20	REINO UNIDO	68
IMPACTO EN TECNOLOGÍAS EMERGENTES	24	ALEMANIA	69
CIBERSEGURIDAD	26	AMÉRICA LATINA Y EL CARIBE	69
¿Qué es la ciberseguridad?	26	RESTO DEL MUNDO	70
El futuro de la ciberseguridad en la era cuántica	27	CONCLUSIONES	72
BLOCKCHAIN	32	REFERENCIAS	75
¿Qué es blockchain?	32	ANEXOS	81
¿En qué basa blockchain su seguridad?	34	ANEXO A: Evolución de la computación cuántica	81
El futuro de la blockchain en la era cuántica	37	ANEXO B: Criptografía cuántica	85
INTELIGENCIA ARTIFICIAL	43	ANEXO C: Evolución de las redes de comunicación cuánticamente encriptadas	88
¿Qué es la inteligencia artificial?	43	ANEXO D: Criptografía asimétrica	94
El futuro de la inteligencia artificial en la era cuántica	44		
OTRAS TECNOLOGÍAS	46		
Internet de las cosas (IoT) y drones	47		
5G	47		
Impresión 3D	49		

INTRODUCCIÓN

Estamos ante la llegada de una nueva era, la era de las tecnologías cuánticas. Este tipo de tecnologías, que llevan entre nosotros desde mediados del siglo XX, ha estado aportando mejoras y avances a pequeña escala durante más de 60 años, principalmente en medicina.

Sin embargo, actualmente está naciendo una nueva generación de tecnologías cuánticas altamente disruptivas con potencial para afectar transversalmente a la mayoría de las tecnologías emergentes que conocemos, empoderando a muchas de ellas y amenazando la seguridad de otras. De igual manera, se prevé que ofrezcan un alto impacto social por sus aplicaciones directas en medicina, biología, genética, educación, economía y finanzas, energía, transporte o meteorología, entre otros. Es por ello que varias de las principales potencias mundiales y muchas de las empresas tecnológicas líderes están iniciando programas y realizando grandes inversiones económicas para no quedarse atrás en esta nueva era tecnológica, la era cuántica.

El presente documento se estructura en cuatro secciones independientes que tienen como objeto explicar en qué consisten estas tecnologías, cómo funcionan, de qué manera van a causar ese impacto tanto a nivel tecnológico como a nivel sectorial y qué están haciendo gobiernos y empresas tecnológicas al respecto. Hemos tratado de construir la publicación de manera que cada una de las cuatro secciones pueda leerse de manera independiente, lo que ha obligado a introducir alguna pequeña redundancia en cuanto a definiciones para el lector que se atreva con el documento completo, como recomendamos hacer.

En la primera sección se presentan en un tono divulgativo la computación cuántica y la información cuántica -que incluye la criptografía cuántica-, los dos campos cuánticos posiblemente más disruptivos a nivel tecnológico a corto y medio plazo. En la segunda sección se discute el impacto previsto de las tecnologías cuánticas sobre tecnologías digitales, presentando un análisis más detallado sobre el futuro de ciberseguridad, blockchain e inteligencia artificial y comentando de manera más superficial qué cambiará en IoT, drones o 5G. En la tercera se aborda el impacto sectorial que las tecnologías cuánticas tendrán a medio y largo plazo en medicina, biología, genética, educación, economía y finanzas, energía, agricultura, transporte o meteorología. Finalmente, y para cerrar con una nota de plena actualidad sobre el estado de la carrera cuántica, en la cuarta y última sección se comentan algunos de los programas más importantes que distintos gobiernos están llevando a cabo. Algunas explicaciones más técnicas se han reservado para los anexos.

Para la documentación y referenciación de esta publicación se ha tratado de analizar e incluir las opiniones, las posturas y los desarrollos de mayor relevancia y repercusión sobre estas tecnologías, lo que ha dado lugar a una extensa sección de bibliografía con lecturas de interés. Es posible, sin embargo, que algunas hayan sido obviadas de manera no intencionada, lo que se intentará corregir en versiones futuras.



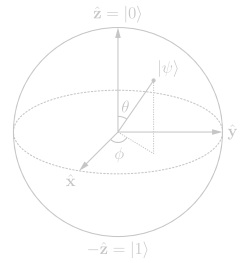
TECNOLOGÍAS CUÁNTICAS

Una oportunidad transversal e interdisciplinar
para la transformación digital y el impacto social

LA ERA CUÁNTICA



LA ERA CUÁNTICA



A lo largo de las últimas décadas hemos ido acostumbrándonos a tener tecnología cada vez más presente en nuestras vidas, hasta el punto de no saber vivir sin ella en muchas ocasiones. Esta revolución digital que estamos experimentando ha ocasionado grandes cambios sociales, como la manera en la que nos relacionamos, nos comunicamos o nos exponemos en las redes sociales. Por otro lado, el crecimiento exponencial que algunas compañías tecnológicas han experimentado les ha dado la capacidad de poder modificar tanto directa como indirectamente nuestros patrones de comportamiento. En los próximos años vamos a adentrarnos en una nueva era, la era cuántica, cuyo potencial presentaremos en este documento. Si bien es imposible saber con certeza cuál será su impacto social y tecnológico, se espera que haya un antes y un después de la adopción de esta nueva generación de tecnologías, tal y como ocurrió con las tecnologías digitales.

TECNOLOGÍAS CUÁNTICAS

¿QUÉ SON LAS TECNOLOGÍAS CUÁNTICAS?

En la primera mitad del siglo XX -más concretamente entre 1900 y 1930- el estudio de algunos fenómenos físicos que aún no estaban bien entendidos dio lugar a una nueva teoría física, la Mecánica Cuántica. Esta teoría describe y explica el funcionamiento del mundo microscópico, hábitat natural de moléculas, átomos o electrones. Gracias a ella no solo se ha conseguido explicar esos fenómenos, sino que ha sido posible entender que la realidad subatómica funciona de forma completamente contra intuitiva, casi mágica, y que en el mundo microscópico tienen lugar sucesos que no ocurren en el mundo macroscópico.

A lo largo de la historia, el ser humano ha ido desarrollando tecnología a medida que ha ido entendiendo el funcionamiento de la naturaleza a través de la ciencia. En este caso, es el entendimiento del mundo microscópico a través de la Mecánica Cuántica el que nos permite inventar y diseñar tecnologías capaces de mejorar la vida de las personas. **Las tecnologías cuánticas, por tanto, son aquellas que tienen como base propiedades cuánticas de la naturaleza subatómica como la superposición cuántica, el entrelazamiento cuántico y el teletransporte cuántico.**

Sin entrar en detalles muy técnicos, la superposición cuántica describe cómo una partícula puede estar en diferentes estados a la vez; el entrelazamiento cuántico describe cómo dos partículas tan separadas como se desee pueden estar correlacionadas de forma que, al interactuar con una, la otra se entera; y el teletransporte cuántico utiliza el entrelazamiento cuántico para enviar información de un lugar a otro del espacio sin necesidad de viajar a través de él.

Hay muchas y muy diferentes tecnologías que utilizan fenómenos cuánticos y, algunas de ellas, como el láser o las imágenes por resonancia magnética (IRM), llevan ya entre nosotros más de medio siglo. Sin embargo, **actualmente estamos presenciando una revolución tecnológica en áreas como la computación cuántica, la información cuántica, la simulación cuántica, la óptica cuántica, la metrología cuántica, los relojes cuánticos o los sensores cuánticos.** En algunos de estos campos, como discutiremos a lo largo de este documento, ya existen aplicaciones y casos de uso en activo. En otros, sin embargo, aún tardarán algunos años en llegar.

En esta primera sección vamos a hablar solamente de la computación cuántica y la información cuántica puesto que, al ser los más complejos y -quizás- disruptivos, merecen una explicación más detallada. Será en la tercera sección, cuando nos centremos en el impacto social, donde abordaremos los siete campos cuánticos mencionados en el párrafo anterior.

COMPUTACIÓN CUÁNTICA

¿QUÉ ES?

Para entender cómo funcionan los computadores cuánticos es conveniente explicar primero cómo funcionan **los computadores que utilizamos a diario**, a los que nos referiremos en este documento como computadores digitales o clásicos. Estos, al igual que el resto de los dispositivos electrónicos como *tablets* o teléfonos móviles, **utilizan bits como unidades fundamentales de memoria.** Esto significa que los programas y aplicaciones están codificados en bits, es decir, en lenguaje binario de ceros y unos. Cada vez que interactuamos con cualquiera de estos dispositivos -por ejemplo pulsando una tecla del teclado- se crean, destruyen y/o modifican cadenas de ceros y unos dentro de la computadora.



FIGURA 1.
Ejemplos de caracteres en lenguaje binario.

Caracter	Bits
7	111
A	01000001
\$	00100100
:)	0011101000101001

La pregunta interesante es, ¿qué son físicamente estos ceros y unos dentro de la computadora? Los estados cero y uno de los bits se corresponden con corriente eléctrica que circula, o no, a través de unas piezas microscópicas denominadas transistores, que actúan como interruptores. Cuando no circula corriente, el transistor está “apagado” y se corresponde con un bit 0, y cuando circula está “encendido” y se corresponde con un bit 1. De forma

más simplificada, es como si los bits 0 y 1 se correspondiesen con huecos, de manera que un hueco vacío es un bit 0 y un hueco ocupado por un electrón es un bit 1. Es por este motivo que estos dispositivos se llaman electrónicos. A modo de ejemplo, en la figura 1 se muestra la escritura en lenguaje binario de algunos caracteres.

Ahora que tenemos una idea de cómo funcionan los computadores actuales, tratemos de entender cómo funcionan los cuánticos. **La unidad fundamental de información en computación cuántica es el *quantum bit* o *qubit*. Los *qubits* son, por definición, sistemas cuánticos de dos niveles** -ahora veremos ejemplos- que pueden estar en el nivel bajo, que se corresponde con un estado de baja excitación o energía definido como 0, o en el nivel alto, que se corresponde con un estado de mayor excitación o definido como 1, pero -y aquí radica la diferencia fundamental con la computación clásica- también pueden estar en cualquiera de los infinitos estados intermedios, como por ejemplo un estado que sea mitad 0 y mitad 1, o tres cuartos de 0 y un cuarto de 1. Este fenómeno se conoce como superposición cuántica y es natural en sistemas cuánticos.

Para hacernos una idea de cómo conseguir un sistema de este tipo físicamente, imaginemos un electrón orbitando alrededor de un átomo. Cuanta más energía tienen los electrones en un átomo, mayor es su capacidad para alejarse del núcleo que los atrae electromagnéticamente, pudiendo situarse en órbitas más alejadas de este. Para que el átomo se comporte como un sistema cuántico de dos niveles -un qubit-, necesitamos reducir la energía del electrón para que no pueda escaparse de las dos órbitas más bajas. Esto se consigue enfriando el sistema, y tiene relación con que los computadores cuánticos que se están desarrollando hoy en día sean los lugares más fríos del universo, ya que solo a temperaturas extremadamente bajas se consigue controlar estos procesos cuánticos. Denominamos entonces a la órbita más cercana al núcleo el estado o nivel 0 y a la más alejada el estado o nivel 1. Para que el electrón pueda pasar de la órbita 0 a la 1 necesita recibir energía, y para descender de la 1 a la 0 necesita disipar o ceder energía.

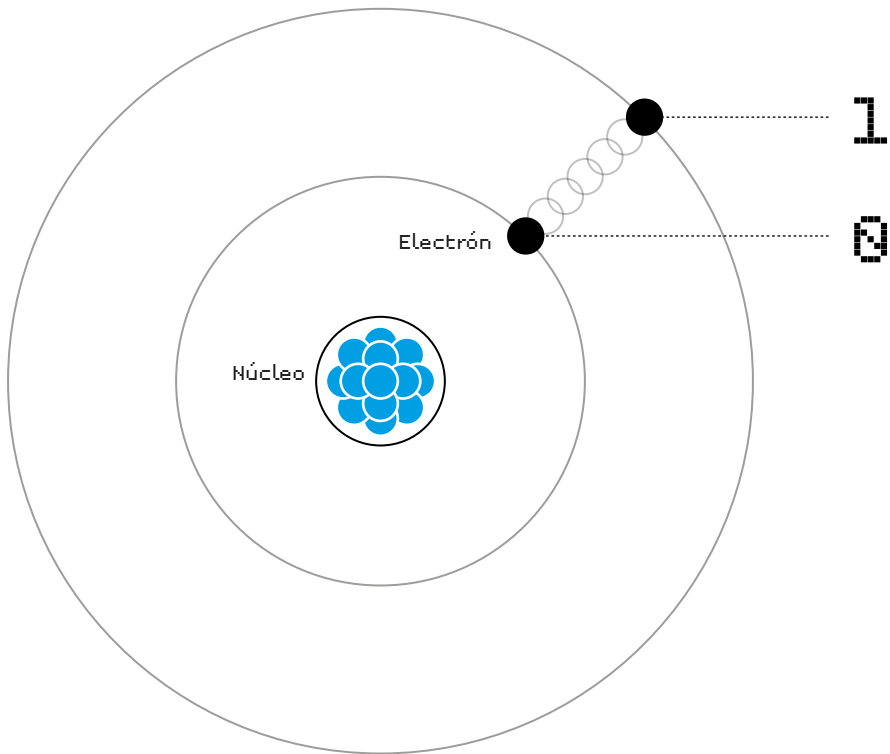
Cuando observemos el electrón, siempre vamos a encontrarlo en una de las órbitas predefinidas alrededor del núcleo. Si el sistema se ha enfriado lo suficiente, lo encontraremos o bien en el estado 0 -en la órbita más cercana al núcleo- o en el estado 1 -la siguiente-. Sin embargo, estas órbitas no son continuas, sino que hay una diferencia de energía entre ambas. La pregunta clave es, ¿qué pasa si cuando el electrón está en la órbita baja le damos una energía que no es suficiente para llegar a la órbita 1?

Pues ocurre que desde el momento en que el electrón recibe la energía hasta el momento en que nosotros lo observamos para ver en cuál de las dos órbitas está, el electrón está en un estado intermedio que podemos entender como una superposición de los estados 0 y 1 de las que mencionábamos antes. En el momento que observamos -interactuamos con- el electrón, se rompe esa superposición en lo que se conoce como colapso o decoherencia¹ del sistema, y el electrón se presenta o bien en la órbita que denominamos 0 o bien en la que denominamos 1.

1. Las causas exactas de la decoherencia de sistemas cuánticos en la naturaleza son aún motivo de debate en la comunidad científica.

**FIGURA 2.**

Átomo con dos orbitales simulando el comportamiento de un *qubit*.



Dado que esto es contraintuitivo, tal y como adelantábamos al principio, no está de más insistir sobre ello. Lo que ocurre con la realidad subatómica es que en muchos casos permanece indefinida -como superposición simultánea de varias realidades- hasta que tiene lugar una interacción y entonces elige qué forma tomar -cuál de las realidades prevalece-. Esto resulta difícil de entender ya que estamos acostumbrados a observar el mundo macroscópico, donde percibimos una realidad independiente del observador en la que las cosas son como son sin importar que alguien las observe o mida. En el mundo subatómico, diferentes realidades coexisten hasta que una interacción hace que solo una “sobreviva”. En este caso, el electrón solo tiene permitido -por la naturaleza- estar en órbitas específicas alrededor del átomo, que para nuestro ejemplo hemos reducido a dos. Sin embargo, si le damos o le quitamos una cantidad de energía menor que la que le permitiría pasar de una órbita a otra, entonces el electrón pasa a tener una posición indefinida entre las dos órbitas hasta que lo observamos.²

-
2. En realidad, el modelo atómico de órbitas electrónicas circulares fue propuesto en 1913 por N. Bohr pero con la llegada de la Mecánica Cuántica se comprendió que los electrones se distribuyen alrededor de los núcleos atómicos en orbitales más complejos. Por otro lado, si estudiamos clásicamente este mismo fenómeno con la teoría del efecto fotoeléctrico descrito por Einstein, diríamos que el electrón no puede recibir o disipar energía en cantidades que no sean proporcionales a la diferencia entre orbitales. Sin embargo, este ejemplo simple que hemos presentado nos parece muy útil para explicar los fundamentos de un *qubit*. En la práctica hay múltiples maneras de conseguir estos sistemas cuánticos de dos niveles, como por ejemplo con iones atrapados, defectos en sólidos, semiconductores, superconductores o nano-hilos topológicos.

La pregunta que surge entonces es: ¿En qué órbita va a aparecer el electrón al observarlo? La respuesta a esta pregunta es que no podemos saberlo. Podemos conocer la probabilidad exacta de que aparezca en la órbita 0 o en la órbita 1 en función de la energía que posea en el momento en que lo observemos y tenga que “decidir”, de forma que cuanta más energía le hayamos dado, más “cerca” estará de la órbita 1 y en consecuencia mayor será la probabilidad de encontrarlo ahí al medir, y viceversa.

Este entendimiento de la naturaleza ofrecido por la mecánica cuántica al que llegaron los físicos del siglo pasado tras décadas de investigaciones y debates fue rechazado inicialmente por científicos de la talla de Albert Einstein, que creía firmemente en una realidad determinista e independiente del observador. Sin embargo, años de experimentos han refutado las explicaciones y predicciones de esta teoría del mundo microscópico.

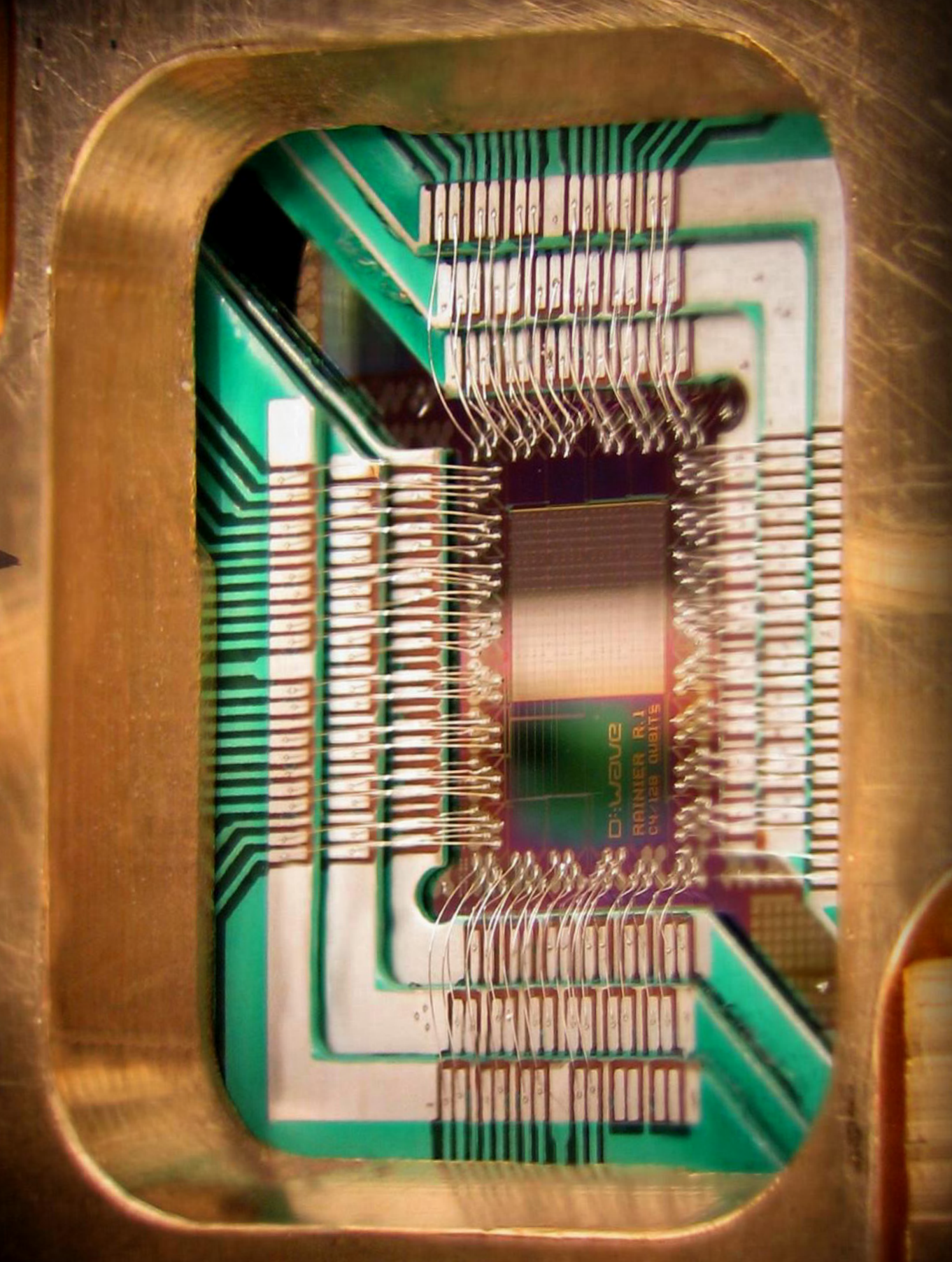
¿CÓMO FUNCIONA?

El propósito de los computadores cuánticos es aprovechar estas propiedades **cuánticas** de los *qubits*, como sistemas cuánticos que son, para poder correr **algoritmos cuánticos** que utilizan la superposición y el entrelazamiento para ofrecer una **capacidad de procesamiento mucho mayor** que los clásicos. **Es importante indicar que el verdadero cambio de paradigma no consiste en hacer lo mismo que hacen las computadoras digitales o clásicas -las actuales- pero más rápido**, como de forma errónea se puede leer en muchos artículos, **sino que los algoritmos cuánticos permiten realizar ciertas operaciones de una manera totalmente diferente que en muchos casos resulta ser más eficiente** -es decir, en muchos menos pasos-.

Veamos un ejemplo concreto de lo que esto implica. Imaginemos que estamos en Bogotá y queremos saber cuál es la mejor ruta para llegar a Lima de entre $N=1.000.000$ candidatas. De cara a poder utilizar computadoras para encontrar el camino óptimo necesitamos digitalizar 1.000.000 opciones, lo que implica traducirlas a lenguaje de bits para el computador clásico y a *qubits* para el computador cuántico.³ Mientras que una computadora clásica necesitaría ir uno por uno analizando todos los caminos hasta encontrar el deseado, una computadora cuántica se aprovecha del proceso conocido como **paralelismo cuántico** que le permite considerar todos los caminos a la vez. Esto implica que, si bien la computadora clásica necesita del orden de $N/2$ pasos o iteraciones, es decir, 500.000 intentos, la computadora cuántica encontrará la ruta óptima tras solo \sqrt{N} operaciones sobre el registro, es decir, 1.000 intentos.

En muchos casos la ventaja no es cuadrática sino exponencial ya que, gracias al paralelismo cuántico, con n *qubits* podemos obtener una capacidad computacional equivalente a 2^n bits. Para ejemplificar esto, es frecuente contar que con unos 270 *qubits* se podrían tener más estados base en un computador cuántico -más cadenas de caracteres diferentes y simultáneas- que el número de átomos en el universo, que se estima en torno a 2^{80} .

3. En un computador clásico o digital, a diferencia de los cuánticos dada su etapa prematura, se dispone de una arquitectura con múltiples capas, de forma que nosotros interactuamos con ellos muchas capas por encima de la capa lógica de los bits, pero es interesante pensarlo a este nivel para entender las diferencias.



Chip construido por D-WAVE Systems Inc. diseñado para operar como un procesador cuántico superconductor y adiabático de optimización, montado sobre un soporte de muestra.

BITS



0 or 1
(un estado cada vez)



00 or 01 or 10 or 11
(un estado cada vez)



000 or 001 or 010 or 100 or 011
or 101 or 110 or 111
(un estado cada vez)



N bits → 1 estado de N bits cada vez

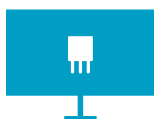
10 bits → 1 estado de 10 bits cada vez

50 bits → 1 estado de 50 bits cada vez

100 bits → 1 estado de 100 bits cada vez



2^{80} bits



QUBITS



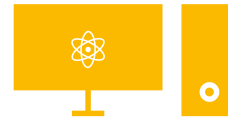
$\alpha \cdot 0 + \beta \cdot 1$
(2 estados simultáneos)



$\alpha \cdot 00 + \beta \cdot 01 + \gamma \cdot 10 + \delta \cdot 11$
(4 estados simultáneos)



$\alpha \cdot 000 + \beta \cdot 001 + \gamma \cdot 010 + \delta \cdot 100 +$
 $\zeta \cdot 011 + \eta \cdot 101 + \theta \cdot 110 + \sigma \cdot 111$
(8 estados simultáneos)



N qubits → 2ⁿ estados posibles cada vez

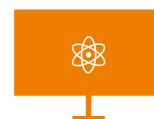
10 qubits → 1024 estados simultáneos

50 qubits → 1125899906842624
estados simultáneos

100 qubits →
1267650600228229401496703205376
estados simultáneos



270 qubits



¿CUÁL ES EL ESTADO ACTUAL DE LA TECNOLOGÍA?

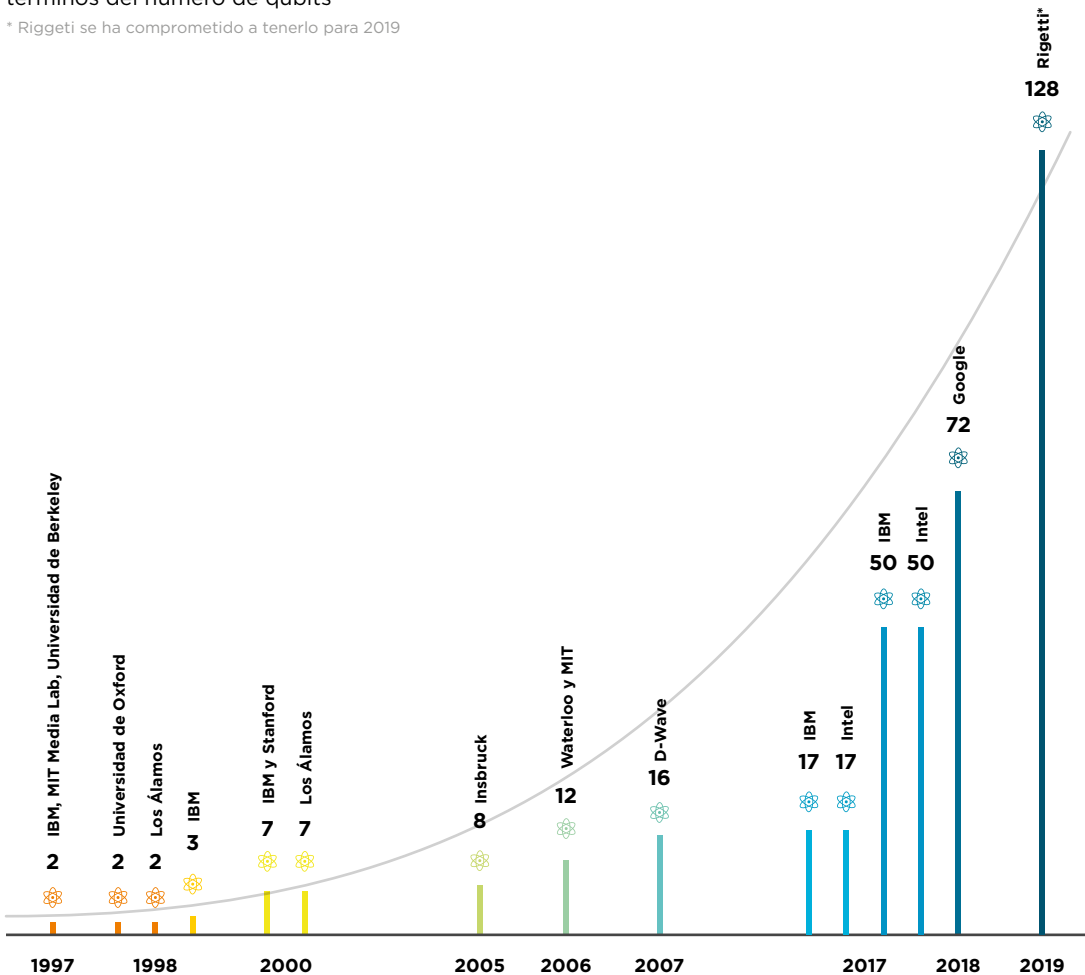
Las primeras ideas sobre construir computadoras utilizando principios de la Mecánica Cuántica se atribuyen a P. Benioff [1] y R. Feynman [2] a principios de los años 80. Durante las dos décadas posteriores comenzaron a proponerse modelos teóricos sobre la arquitectura de las mismas y algoritmos cuánticos que podrían correr en ellas. No fue, sin embargo, hasta el año 1998, que se construyeron las primeras computadoras cuánticas de 2 *qubits* [3-7] y se corrieron los primeros algoritmos [8]. De nuevo dos décadas tuvieron que pasar hasta que, tras un avance lento en el número de qubits operando en procesadores cuánticos, se comenzó a acelerar la carrera de la computación cuántica. En 2017 IBM se ponía a la cabeza de la carrera primero con 17 y después con 50 *qubits* [9] y en 2018 Google anunciaba tener un microprocesador de 72 [10] y Rigetti prometía alcanzar los



FIGURA 3.

Evolución del desarrollo de computadores cuánticos en términos del número de qubits

* Rigetti se ha comprometido a tenerlo para 2019



128 para 2019 [11].⁴ En la figura 3 se presentan los hitos más relevantes -que se hayan hecho públicos- en cuanto a número de *qubits*, cuya discusión detallada se reserva para el anexo A.

El principal reto al que se enfrenta la computación cuántica hoy en día es la inestabilidad de los *qubits*. El control del estado de los *qubits* es harto complicado con la tecnología existente ya que tienen un nivel de inestabilidad muy elevado, lo que se traduce en “errores” computacionales. La corrección de errores cuántica es muy diferente a la clásica, en la que se suele recurrir a la redundancia -es decir, se escribe o se envía varias veces la misma secuencia de manera que cuando se recuperan todos los paquetes se reconstruye el mensaje identificando los errores-. Dado que los estados cuánticos no se pueden clonar [14], para corregir errores en un *qubit* se necesita de otros *qubits* a los que se les va propagando el error. Los *qubits* individuales se denominan físicos y los conjuntos de *qubits* que se comportan como uno solo con corrección de errores se denominan qubits lógicos. Para el correcto funcionamiento de un computador cuántico se necesita que haya corrección de errores, ergo que los *qubits* sean lógicos, y el gran salto que la implementación de esto supone aún está por llegar. Según algunos expertos, el número de *qubits* físicos para conseguir uno lógico podría ser superior a 1000.

Si bien, como comentaremos más adelante, se estima que con un computador cuántico de entre 1500 y 2330 *qubits* lógicos se podría romper toda la ciberseguridad actual [12,13], cuándo tendremos estos computadores es aún una incógnita. Además, es importante indicar que las cifras de *qubits* de la figura 3 corresponden a *qubits* físicos y no lógicos. Por esa y otras razones, si bien el número de *qubits* es relevante y tiene un impacto mediático grande, no es el único factor determinante a la hora de decir si un computador cuántico es mejor que otro.

Lo que parece claro para el autor de este documento es que los primeros servicios de computación cuántica para el público general serán provistos por grandes compañías en la forma *software as a service* (SaaS) y que en cuanto la tecnología sea lo suficientemente madura se fabricarán procesadores híbridos de manera que, en función del problema a resolver y la capacidad computacional requerida, se pueda computar indistintamente de manera clásica o cuántica. Al igual que ahora en el plazo de unos minutos podemos correr una máquina virtual en la nube de varios proveedores como Amazon, Google o Microsoft, quizás en el futuro podamos disponer de servicios híbridos de computación cuántica y clásica.

4. Las computadoras cuánticas más populares hasta la fecha -que hasta el momento son más bien prototipos- son de dos tipos. Las computadoras cuánticas estándar, en las que los *qubits* son cuantos de flujo magnético en circuitos superconductores, y las computadoras cuánticas topológicas, en las que los *qubits* son parejas de quasi-partículas llamadas aniones. Sin entrar en demasiado detalle, la ventaja de la segunda con respecto a la primera es que, gracias a su arquitectura, los sistemas son más estables con respecto a errores -o ruido-, que es uno de los grandes desafíos a superar en la computación cuántica.



INFORMACIÓN CUÁNTICA

¿QUÉ ES?

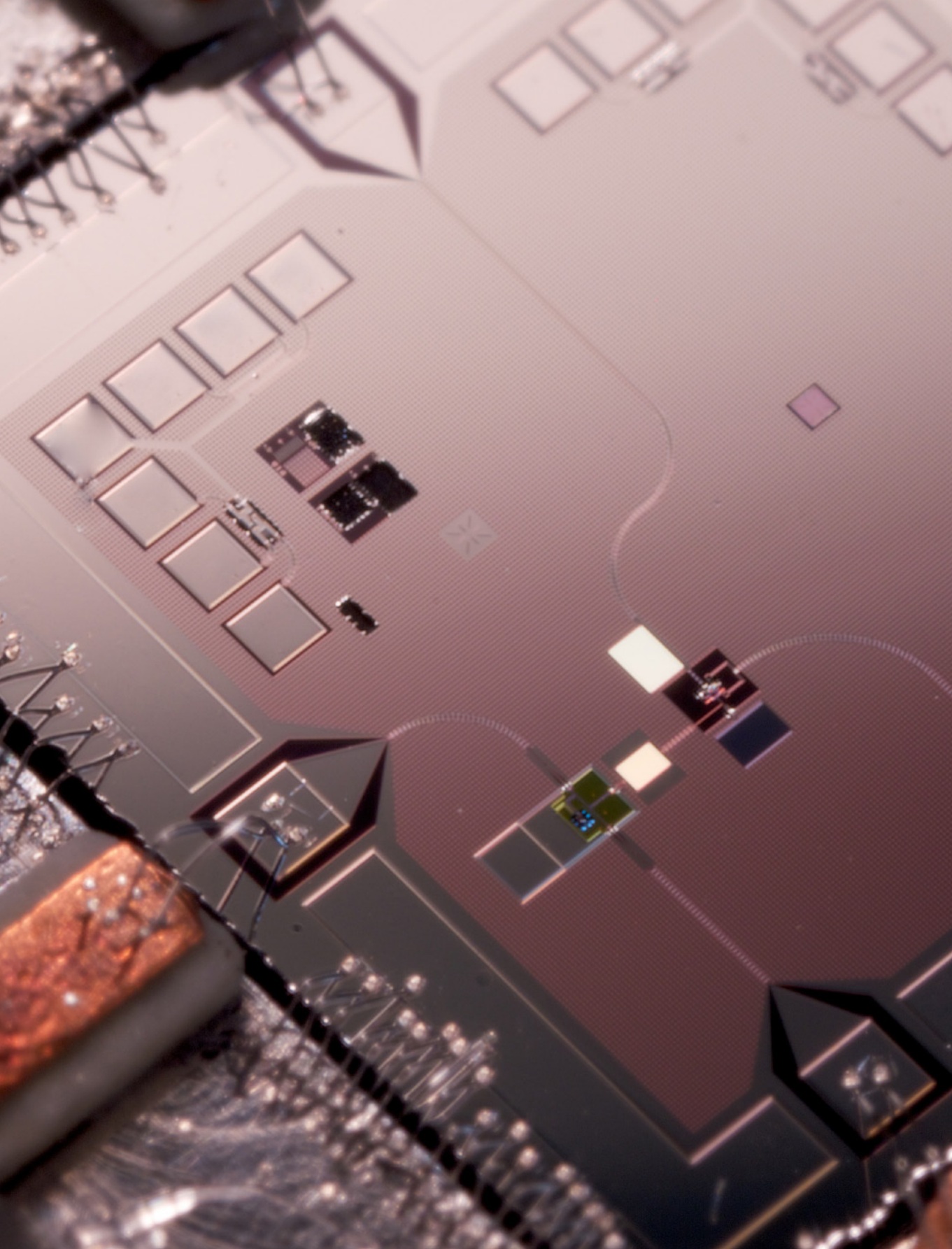
El campo de la información cuántica es el análogo cuántico al campo de la información clásica que estudia cómo cuantificar, almacenar y transferir información. Cada vez que accedemos a internet, hacemos una llamada telefónica o pagamos con nuestra tarjeta de crédito, estamos generando datos que viajan por todo el mundo a velocidades cercanas a las de la luz. En la actualidad, la información viaja principalmente por dos canales; (i) por cable, donde destacan los denominados pares de cobre y el conjunto de redes de fibra óptica que recorre el planeta, con más de 1000 millones de metros de cable submarino [15,16], y (ii) sin cables, gracias la red de telecomunicaciones inalámbrica que utiliza diferentes satélites como repetidores para hacer llegar la información a su destino.

Para que los datos que generamos a partir de dispositivos electrónicos se puedan transferir tanto por cable como sin él, estos disponen de unas tarjetas de red que se encargan de generar señales tanto analógicas -con forma y frecuencia específicas- como digitales -pulsos eléctricos- que viajan por las redes de telecomunicaciones de manera ordenada siguiendo los protocolos estandarizados que se han ido desarrollando y mejorando durante décadas.

Si bien lo relativo a la transmisión eficiente y segura de estos datos es primordial, también lo es lo que concierne al almacenamiento de los mismos. Son varias las opciones tecnológicas para almacenar datos, como los discos duros de los mismos dispositivos electrónicos que generan la data -computadores, teléfonos o tabletas-, memorias extraíbles como discos duros externos y USB y, cada vez con más frecuencia, el almacenamiento de datos en la nube, consistente en utilizar servidores de un tercero para guardar nuestra información con un determinado costo.

Hay dos áreas fundamentales para la consecución de almacenamiento y transferencia de datos segura: criptografía y autenticación.

- **La criptografía consiste en el cifrado de información de manera que solo las personas autorizadas puedan acceder a su contenido.** Cuando realizamos una llamada de teléfono o cuando accedemos a una página web que comienza con https, por detrás se están aplicando protocolos de encriptación de forma que la información viaja cifrada a través de los canales mencionados anteriormente para que, si alguien interceptase las señales que contienen dicha información, no pudiesen acceder a su contenido.
- **La autenticación es esencial para saber con quién nos estamos comunicando y es imprescindible para que el cifrado pueda tener éxito** ya que, en un ejemplo sencillo, si recibimos un mensaje cifrado pero no podemos verificar que el mensajero es quien dice ser, el mensaje puede haber sido enviado o modificado por un tercero.



Fotografía de una máquina cuántica. El resonador mecánico, en superposición, está situado en la esquina inferior izquierda del chip. El rectángulo blanco pequeño es el capacitor de acoplamiento entre el resonador mecánico y el qubit.

Las técnicas de encriptación pueden clasificarse en dos grandes grupos; **simétricas y asimétricas**. Se denominan simétricas a las que utilizan la misma clave para encriptar y desencriptar un determinado mensaje o conjunto de datos, y asimétricas a las que utilizan claves diferentes pero “complementarias”.

Encriptación simétrica

La encriptación simétrica es completamente segura en la teoría, pero a la vez insegura o ineficiente en la práctica. El proceso de encriptación simétrica puede describirse de forma sencilla en los siguientes tres pasos:

1. El emisor y el destinatario **acuerdan y comparten** una **clave privada** que van a usar para encriptarlo antes de ser enviado y desencriptarlo al ser recibido.
2. El emisor **encripta** el mensaje con la **clave privada** acordada y se lo envía al destinatario.
3. El destinatario **recibe** el mensaje y lo **desencripta** con la misma **clave privada**.

La criptografía simétrica necesita de la generación y el intercambio de la **clave privada** previo a la encriptación, transmisión y desencriptación del mensaje. **Este tipo de cifrado es completamente seguro si (i) las claves son completamente aleatorias, (ii) el canal utilizado para compartir las claves es completamente seguro y (iii) las claves no se utilizan más de una vez.** En las telecomunicaciones actuales -o clásicas- la generación de claves completamente aleatorias no es viable, puesto que los algoritmos que las generan tienen siempre una determinada periodicidad -se repiten-. Por otro lado, la única manera de tener un canal completamente seguro para el intercambio de estas claves es hacerlo presencialmente, lo que es altamente ineficiente. Hacerlo a distancia implica confiar en canales que hayan sido asegurados con criptografía asimétrica que dejará de ser segura con la llegada de la computación cuántica, como ahora veremos.

Es por este motivo que, a excepción de algunas agencias de inteligencia o gobiernos que generan grandes cantidades de claves periódicamente y las distribuyen físicamente utilizando memorias externas -como USB-, la criptografía simétrica no se usa hoy en día sin ser combinada con criptografía asimétrica, lo que la vuelve insegura.

El ejemplo más conocido de criptografía simétrica a lo largo de la historia son, posiblemente, las máquinas Enigma. Estas tenían unos rotores que les permitían generar del orden de 10^{19} secuencias distintas con las que cifrar mensajes. Cada una de esas secuencias era una posible clave simétrica. El operador de cada máquina recibía instrucciones una vez al mes sobre cómo colocar los rotores de manera que todos utilizaran la misma secuencia, y por tanto la misma clave, para encriptar y desencriptar. Si bien ninguno de los tres requisitos identificados dos párrafos más arriba fue respetado, el tercero fue la razón por la cual los Aliados consiguieron descifrar Enigma. La clave -el orden de los rotores- era establecido de manera no totalmente aleatoria pero sí suficientemente arbitraria por humanos; el canal utilizado para compartir las claves era el correo ordinario, y aunque inseguro, tampoco fue la causa del éxito americano; las claves, sin embargo, eran reutilizadas ya que no se cambiaban tras cada mensaje. Los Aliados conocían ciertas frases que se repetían en los

mensajes encriptados -como el saludo o la fecha-, lo que les permitía descartar un gran número de las 10^{19} claves posibles, y gracias a ello conseguían dar con la correcta.

Encriptación asimétrica

Dados los inconvenientes de las claves simétricas, en los años 70 se comenzaron a desarrollar técnicas de encriptación asimétricas. La criptografía asimétrica permite la transmisión relativamente segura de información de punto a punto. Esta seguridad descansa en la dificultad para invertir ciertas operaciones matemáticas, como por ejemplo la factorización de números primos; si bien multiplicar dos números primos es una operación computacionalmente sencilla, factorizar el resultado de su producto es extremadamente -para ser precisos, exponencialmente- más difícil. Este procedimiento permite generar parejas de claves “complementarias” de manera sencilla de forma que lo que una encripta la otra lo desencripta, pero con la particularidad de **se necesita una enorme capacidad computacional para dar con la clave que desencripta a partir de la que encripta**, como se ilustra en la figura 4.

Esto permite que, para comunicarnos de manera segura con alguien, le podamos pedir a ese alguien que genere una pareja de claves y nos comparta la **clave pública** para que nosotros encriptemos y enviemos el mensaje, y solo él o ella pueda desencriptarlo con la **clave privada**. Funciona como un buzón de un videoclub; todos podemos insertar películas, pero una vez dentro solo el personal autorizado tiene la llave para abrirlo y acceder a ellas. Estos procesos pueden describirse de forma genérica según los siguientes pasos:

1. El destinatario **genera** periódicamente **una pareja de claves** conocidas como **clave pública** y **clave privada** haciendo uso de un algoritmo determinado. La **clave pública** es compartida abiertamente con el emisor y la **clave privada** mantenida en secreto por el destinatario.
2. El emisor **toma** la **clave pública** ofrecida por el destinatario al que quiere enviarle un mensaje, **encripta** con ella dicho mensaje y se lo **envía** al destinatario.
3. El destinatario **recibe** el mensaje encriptado y lo **desencripta** con la **clave privada** que solo él conoce y ha mantenido en secreto.

Entre los muchos problemas que la computación cuántica conseguirá resolver de manera mucho más eficiente que la computación actual se encuentran los que son base de toda la criptografía asimétrica utilizada hoy en día. Es decir, **la computación cuántica pondrá en riesgo toda la criptografía asimétrica utilizada en internet, telefonía, por gobiernos o por agencias de inteligencia.**

Los tres principales algoritmos utilizados en criptografía asimétrica para la generación de claves son RSA -basado en la factorización de números primos-, logaritmos discretos y curvas elípticas, descritos en el anexo D. En 1994 P. Shor presentó un algoritmo cuántico que invierte estos algoritmos de manera eficiente y llegó a afirmar que puede llegar el momento en que será más rápido romper claves de este tipo con un computador cuántico que generarlas con uno tradicional o clásico [17].

El campo de la información cuántica da solución a este gran desafío al que se enfrenta la humanidad, ya que permite renunciar a la criptografía asimétrica cuya seguridad nunca será completa. **La criptografía cuántica ofrece la posibilidad de generar claves simétricas completamente aleatorias y compartirlas de manera completamente segura y eficiente sin necesidad de utilizar criptografía asimétrica para asegurar el canal ni de intercambiarlas en persona. Es decir, ofrece un canal seguro a través del cual enviar claves completamente aleatorias.** Esto se consigue mediante dos procesos, la generación cuántica de números aleatorios (QRNG por sus siglas en inglés) y la distribución de claves cuánticas (QKD por sus siglas en inglés).

¿CÓMO FUNCIONA?

El éxito de estos procesos, que se detallan en el anexo B, consiste en que son implementados a nivel de hardware -es decir de la propia estructura física del equipamiento- y no a nivel de software -es decir con programas, como ocurre con la generación de números aleatorios clásica y los algoritmos de criptografía clásicos-. **Esto permite aprovecharse de procesos físicos con propiedades cuánticas que (i) tienen una incertidumbre real y no son deterministas, de manera que permiten generar claves verdaderamente aleatorias⁵ y (ii) los datos codificados cuánticamente cambian cuando alguien los observa, permitiendo enviar una clave codificada en estados cuánticos y detectar si alguien observó la clave en su transmisión.⁶**

Al basar su seguridad en las leyes de la naturaleza que están presentes en los procesos físicos que tienen lugar a nivel de hardware y no en la dificultad de invertir algoritmos matemáticos que se implementan a nivel de software, **la criptografía simétrica cuántica es completamente segura y resistente ante computación cuántica.**

¿CUÁL ES EL ESTADO ACTUAL DE LA TECNOLOGÍA?

Si bien la computación cuántica aún no está ofreciendo productos comerciales, la criptografía cuántica ya está entre nosotros.

La compañía IDQuantique, líder mundial en la fabricación comercial de dispositivos cuánticos, ya desarrolla y comercializa generadores cuánticos de números aleatorios con

-
5. Un ejemplo muy sencillo consiste en un espejo semi-reflector que deja pasar la mitad de la luz que llega, de manera que cada partícula de luz que lo encara tiene un 50% de probabilidades de pasar. Si anotamos un 1 cada vez que un fotón pasa y un 0 cada vez que se refleja, tenemos una clave 100% aleatoria.
 6. Lo más frecuente es utilizar como estados cuánticos la polarización de partículas de luz que, si pensamos en los fotones como flechas, puede verse como la dirección de estas, de manera que un 0 puede ser un fotón con polarización vertical y un 1 un fotón con polarización horizontal. Si alguien observa la clave en su transmisión, la dirección del fotón cambia y con ella la clave. Cuando se intercambia -sacrificándola- un pedazo de esa clave para ver si ambos tienen la misma es cuando se detecta a posibles espías. Solo en caso de no haberlos se procede a utilizar el resto de la clave.

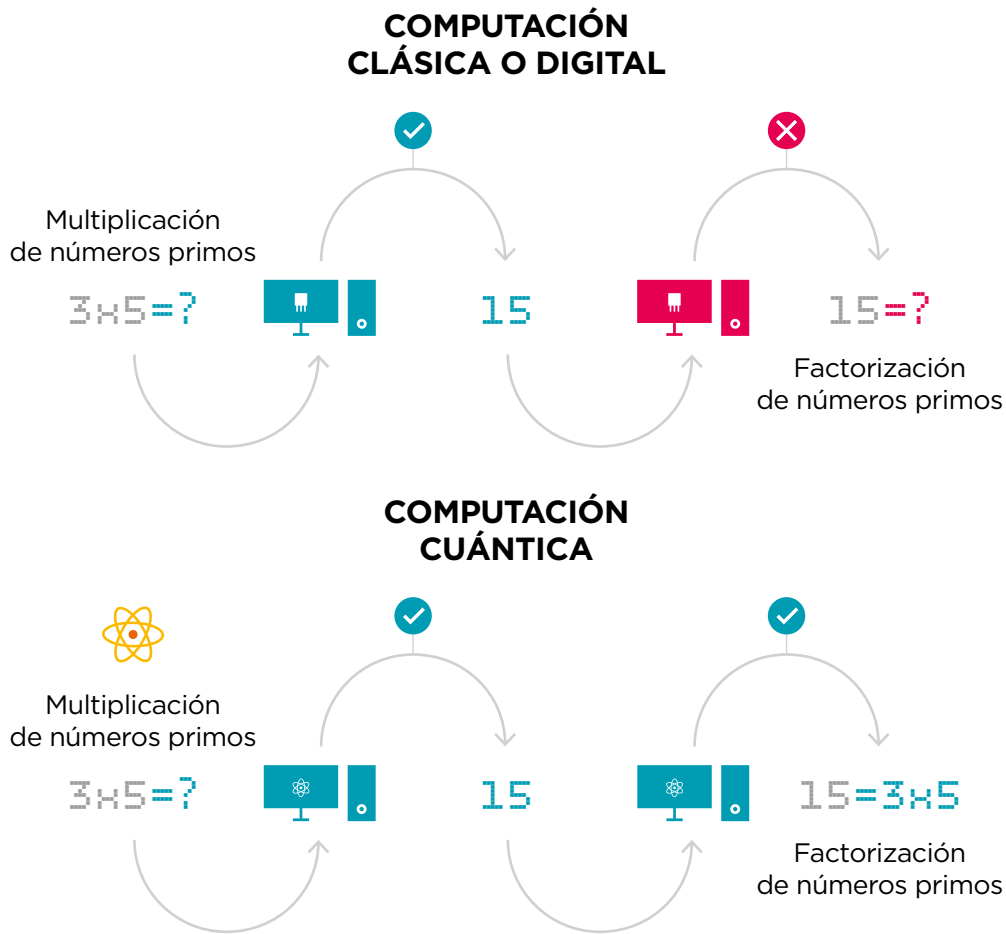


FIGURA 4. Ejemplo del problema de factorización, base de muchos de los protocolos de encriptación actuales. Para números suficientemente grandes, ni siquiera toda la capacidad computacional actual trabajando de manera conjunta sería capaz de factorizarlos. Cuando la computación cuántica esté madura, un solo computador será capaz de hacerlo.

dimensiones de unos pocos milímetros [18]. En cuanto al intercambio de claves, los primeros protocolos de QKD empezaron a idearse y publicarse en los años 80. El más utilizado es el BB84, propuesto por C. Bennett y G. Brassard en 1984 [19] -descrito en el anexo B-. El segundo más relevante es el E91 propuesto por A. Eckert en 1991 [20].

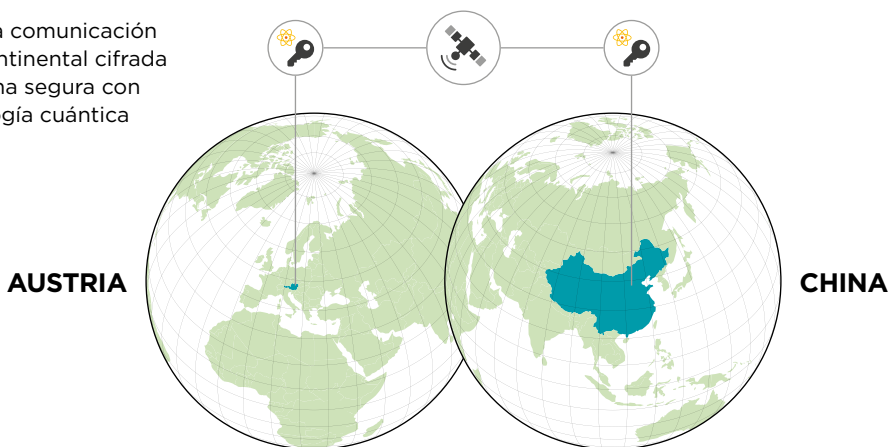
Para la implementación de estos protocolos mediante los cuales, insistimos, se intercambian claves que cambian si alguien las observa, se necesita escoger unos sistemas cuánticos en los que codificar los ceros y unos generados aleatoriamente. Por cuestiones prácticas, se utilizan mayoritariamente fotones. Los fotones o partículas de luz pueden viajar, entre otros medios, por fibra óptica y por el espacio libre. Sin embargo, la atenuación que presenta la fibra óptica es mucho mayor que la que presenta el espacio libre una vez superamos una cierta altura y evitamos las capas atmosféricas más densas.

Actualmente, la limitación experimental al transferir estas claves a través de un canal de fibra óptica de nodo a nodo es de unos pocos cientos de kilómetros. **La primera implementación documentada consistió una red de 6 nodos y 29 km de longitud operando entre las Universidades de Harvard y Boston en 2004** [21,22]. Recientemente se ha conseguido, en condiciones muy favorables, un intercambio de claves por fibra óptica entre nodos a más de 400 km de distancia [23]. La escalabilidad de estas redes está condicionada al desarrollo de repetidores cuánticos [24] -los repetidores tradicionales actúan como un espía perturbando la clave, de forma que no son válidos-, lo que requiere de tecnología muy sofisticada que permita la creación de memorias cuánticas que están aún en desarrollo [25,26]. China es dueña de la red de mayor longitud hasta la fecha, con 32 nodos y más de 2000 km de distancia uniendo las ciudades de Beijing y Shanghai [27].

Para las comunicaciones por el espacio libre se utilizan telescopios actuando como nodos. El primero en colocar satélites en órbita para realizar telecomunicaciones cuánticas Tierra-espacio y espacio-Tierra fue, de nuevo, China. En 2016, la misión espacial bajo el nombre de QUESS (*Quantum Experiments at Space Scale*) puso en órbita un satélite de unos 600 kg de peso, conocido como MICIUS, con un costo total de la misión de unos \$100 millones [28,29]. **En comunicación con tres estaciones terrestres ubicadas en Delingha, Nanshan y Lijiang, se consiguió generar y compartir claves cuánticas por primera vez a largas distancias, superando los 1200 km** [30,31].

Gracias al uso de este satélite, el 17 de septiembre de 2017 se realizó el mayor hito hasta la fecha en el campo de la información cuántica; **una videollamada de hora y media entre China y Austria encriptada cuánticamente a una distancia de 7.600 km**, pasando a ser la primera comunicación intercontinental cifrada de forma segura con tecnología cuántica -al menos de carácter público-. La videollamada “viajó” por un cable de fibra óptica fue encriptada y desencriptada en China y Austria con una clave cuántica que fue generada y compartida previamente haciendo uso del satélite [32].

Primera comunicación intercontinental cifrada de forma segura con tecnología cuántica



Todo apunta a que, en unos pocos años, todos los dispositivos conectados a internet -e incluso algunos que no lo estén- se comunicarán cifrando la información con claves cuánticas que previamente hayan generado de manera aleatoria y compartido de forma segura. Cuando los computadores cuánticos sean suficientemente potentes y confiables, todas las comunicaciones que no incorporen la tecnología necesaria para la generación y el intercambio de claves cuánticas no serán suficientemente seguras con la llegada de la computación cuántica. Por tanto, no solo será inseguro tener documentos cifrados con claves clásicas en el futuro sino que **cualquier archivo o información sensible o confidencial que pueda ser descargada o interceptada hoy en día, puede ser custodiada hasta que un computador cuántico pueda descifrarla**, lo que se enuncia ya popularmente como *“Hack today, crack tomorrow”*. Es por este motivo que gobiernos y empresas privadas están sumándose de forma cada vez más generalizada a esta carrera por volver a ser capaces de garantizar la seguridad de sus datos.

En el anexo C se presenta un resumen detallado de las iniciativas documentadas más relevantes hasta la fecha.



TECNOLOGÍAS CUÁNTICAS

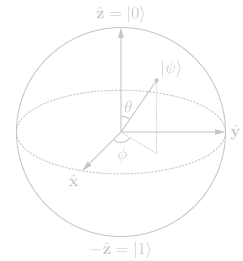
Una oportunidad transversal e interdisciplinar
para la transformación digital y el impacto social

IMPACTO EN TECNOLOGÍAS EMERGENTES



IMPACTO EN TECNOLOGÍAS EMERGENTES

Estamos en un momento de transformación digital en el que distintas tecnologías emergentes como blockchain, inteligencia artificial, drones, internet de las cosas (IoT por su nombre en inglés), realidad virtual, 5G, impresoras 3D, robots o vehículos autónomos tienen cada vez más presencia en múltiples ámbitos y sectores. Estas tecnologías, llamadas a mejorar la calidad de vida del ser humano acelerando el desarrollo y generando impacto social, avanzan hoy en día de manera paralela. Solo en contadas ocasiones vemos compañías desarrollando productos que exploten combinaciones de dos o más de estas tecnologías, como blockchain y IoT o drones e inteligencia artificial. Si bien están destinadas a converger generando así un impacto exponencialmente mayor, la etapa inicial de desarrollo en que se encuentran y la escasez de desarrolladores y personas con perfiles técnicos hacen que las convergencias sean aún una tarea pendiente.



De las tecnologías cuánticas, por su potencial disruptivo, se espera que no solo converjan con todas estas nuevas tecnologías sino que tengan una influencia transversal en prácticamente la totalidad de ellas. La computación cuántica amenazará la autenticación, intercambio y almacenamiento seguro de datos, teniendo un impacto mayor en aquellas tecnologías en las que la criptografía tiene un rol más relevante, como ciberseguridad o blockchain, y un impacto negativo menor pero también a considerar en tecnologías como 5G, IoT o drones. Por otro lado, la capacidad computacional que ofrecerá la computación cuántica unida a las otras ventajas que aportan el resto de tecnologías cuánticas emergentes permitirá acelerar la evolución de la mayoría de las tecnologías digitales, lo que resulta especialmente prometedor para la inteligencia artificial.



CIBERSEGURIDAD

¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad se puede entender como el campo que estudia **cómo proteger información digital durante su procesamiento, almacenamiento e intercambio**.

Con el nacimiento y la adopción en los años 80 y 90 de internet, que no es otra cosa que una red global de dispositivos interconectados, fue necesario desarrollar estándares que posibilitasen operar en ella desde cualquier lado del planeta, utilizando diferentes sistemas y hablando diferentes lenguas. Con este propósito, la Organización Internacional de Normalización (ISO por sus siglas en inglés) creó y publicó como estándar en 1984 el denominado modelo OSI (por su nombre en inglés *Open Systems Interconnection*), que de manera teórica define 7 capas [34], como se recoge en la figura 5.



FIGURA 5. Modelo OSI

	Capa	Tipo	Función	Riesgos de seguridad principales
Software	7 Aplicación	Datos	APIs de alto nivel, servicios de acceso a red para aplicaciones	Virus y troyanos
	6 Presentación	Datos	Codificación de caracteres, compresión de datos, criptografía	Robo de información personal y ataques a la BIOS
	5 Sesión	Datos	Intercambio continuo de datos entre dos nodos	
	4 Transporte	Segmentos	Segmentación y reconiliación de datos	Falseado de IP, autenticación, desenscriptación de información, ataques de reinyección
Hardware	3 Red	Paquetes	Direccionamiento, enrutamiento y control de tráfico	
	2 Enlace de datos	Infraestructura	Direccionamiento físico	Escuchas indebidas, ataques de saturación de las tablas, envenenamiento ARP, ...
	1 Física	Bits	Bits de datos lógicos	Acceso indebido a la capa física con robo y modificación de datos

Cada una de estas capas presenta riesgos diferentes que desde el campo de la ciberseguridad han venido siendo estudiados durante décadas, y que con la llegada de la computación y la criptografía cuántica cambiarán radicalmente.

EL FUTURO DE LA CIBERSEGURIDAD EN LA ERA CUÁNTICA

Los riesgos de seguridad al utilizar dispositivos conectados a internet son variados como se puede ver en la figura 5, donde se presentan algunos de los más relevantes en el marco del modelo OSI. Muchas de las brechas de seguridad se corresponden con comportamientos y actitudes inadecuadas o inseguras por parte de los usuarios, lo que no es objeto de análisis en este documento. Si bien las amenazas de seguridad son de distinta índole, en esencia todo se puede reducir a criptografía y autenticación, tal y como comentábamos en la sección de Información Cuántica. Si el acceso a la red de los usuarios no es suplantado ni robado y la información es almacenada y compartida con una criptografía completamente segura, de manera que no permita a nadie no autorizado acceder a ella, entonces la mayoría de las posibles brechas de seguridad desaparecen. Es por este motivo que en esta sección nos hemos centrado en ver qué va a cambiar en criptografía y autenticación en la era cuántica.

Estos cambios serán grandes y necesarios y es que, con la llegada de la computación cuántica, la ciberseguridad actual está bajo grave amenaza. **Los computadores cuánticos, cuando sean suficientemente robustos, serán capaces de romper todos los protocolos utilizados en la actualidad para criptografía y autenticación que de una forma u otra descansan incondicionalmente en algoritmos de criptografía asimétrica⁷.** Dada la gravedad de la afirmación, no está de más citar a dos de las agencias de estándares de mayor reputación a nivel global como son NIST (por su nombre en inglés *National Institute for Standards in Technology*) y NSA (por su nombre en inglés *National Security Agency*):

“Si se llegasen a construir computadoras cuánticas suficientemente potentes, serían capaces de romper muchos de los sistemas de encriptación pública actualmente utilizados” - NIST [36]

“Un computador cuántico suficientemente potente, si se llegase a construir, sería capaz de socavar todos los algoritmos de clave pública ampliamente utilizados para el establecimiento de claves y firmas digitales.” - NSA [37]

Ambas agencias destacan el problema que la computación cuántica supone para la criptografía y la autenticación actuales y también plantean soluciones similares consistentes en **no dar el salto aún a la criptografía cuántica descrita en la sección de Información Cuántica -posiblemente por la renovación masiva de hardware que eso requeriría- sino centrarse en lo que se denomina *Post-Quantum Cryptography* (PQC)**, que plantea la utilización de nuevos algoritmos matemáticos que sean más difíciles de invertir que los actuales. Dos posibles razones por las cuales adoptan esta postura son el estado prematuro

7. En el año 1994, P. Shor [17] publicó un algoritmo cuántico para invertir de forma eficiente los protocolos de ciberseguridad basados en logaritmos discretos y factorización de números primos. Este algoritmo ya ha sido implementado en computadores cuánticos con éxito, y en el momento en que estos tengan un número suficientemente grande de *qubits* podrán utilizarse para romper la criptografía actual de manera eficiente.

de la tecnología y la renovación masiva de hardware que requeriría instaurar una red de telecomunicaciones con criptografía asimétrica.

En el documento citado [36], NIST propone como ejemplos de algoritmos a investigar aquellos clasificados como *lattice-based cryptography*, *code-based cryptography*, *multivariate polynomial cryptography* y *hash-based signature* entre otras, y destaca las iniciativas europeas PQCrypto [38], SAFEcrypto [39] y la iniciativa japonesa CREST Crypto Math [40] que ya están trabajando en ellos.

Adicionalmente, esta agencia abrió en 2017 un proceso para recibir propuestas públicas de PQC con fecha límite el 30 de noviembre [41]. Su intención es involucrar a la comunidad y jugar un papel líder en la búsqueda de un consenso internacional para la estandarización de metodologías seguras de encriptación tras la llegada de la computación cuántica.

Por su parte, PQCrypto ya ha realizado la recomendación específica de utilizar los nuevos algoritmos de encriptación simétrica conocidos como SPHINCS y XMSS [42].

El problema que presentan este tipo de algoritmos es que nunca serán completamente seguros ya que su seguridad depende de la alta dificultad matemática que se presenta para invertirlos con la insuficiente capacidad computacional actual, pero que puede cambiar de un día para otro. Así es que ya hay algoritmos cuánticos listos para romper la criptografía actual en cuanto un ordenador cuántico con un número de *qubits* suficientemente grande sea suficientemente robusto como para correrlos [17].

Criptografía

Este problema no existe en criptografía cuántica. Los protocolos cuánticos de criptografía no utilizan algoritmos matemáticos, sino que se consisten en procesos físicos cuya violabilidad iría en contra de las leyes de la naturaleza.

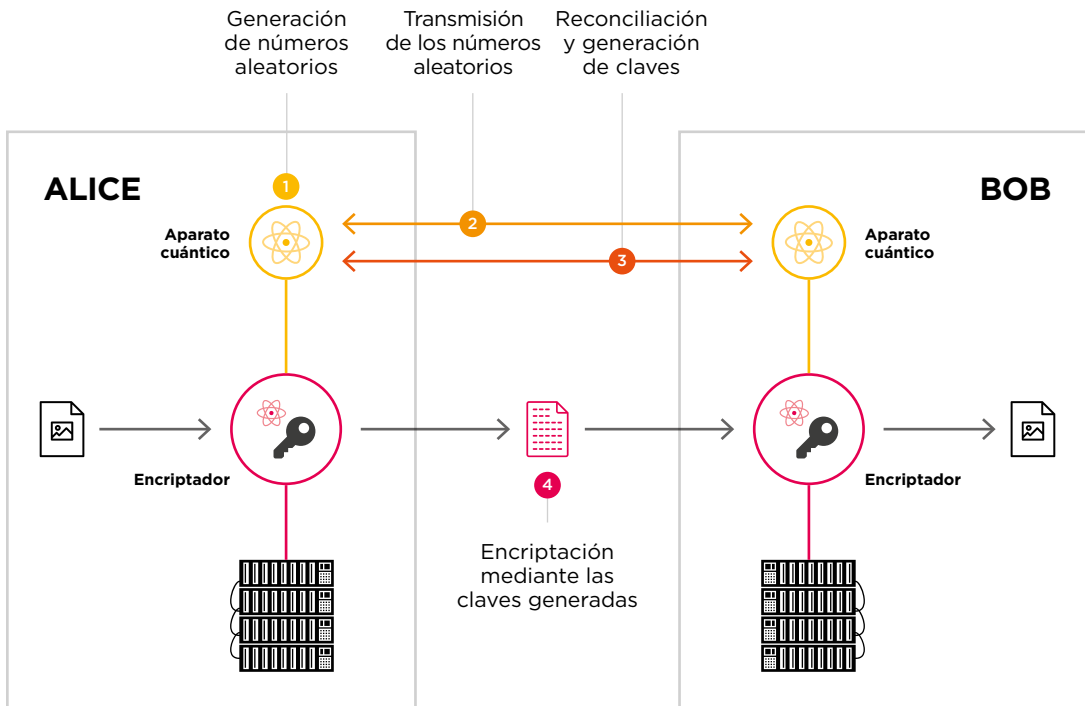
“La seguridad que proporciona QKD está garantizada por las leyes de la física. [...] Esto implica que incluso si un adversario tuviese capacidad computacional ilimitada, clásica y cuántica, QKD es seguro y siempre lo será.” - ETSI [43]

El Instituto Europeo de Estándares en Telecomunicaciones (ETSI por su nombre en inglés), en un documento mucho más amplio que los de NSA y NIST publicado en 2015, **considera la criptografía cuántica como la única alternativa segura de encriptación a largo plazo y analiza su funcionamiento, ventajas y desafíos.** Asimismo, describe casos de uso de QKD como encriptación y autenticación, infraestructura de redes, almacenamiento en la nube o inteligencia artificial, y campos de aplicación como medicina y salud, servicios financieros o aplicaciones móviles. [43]

El hecho de que la seguridad dependa de las leyes de la física se debe a que, como comentábamos en la sección de Información Cuántica, la criptografía cuántica tiene lugar a nivel de hardware y no de software, lo que en el modelo OSI se corresponde con la capa 2. **Esto tiene la ventaja de permitir utilizar procesos cuánticos que la hacen completamente**



FIGURA 6. Alice y Bob utilizando generadores de números aleatorios y QKD para generar y compartir claves seguras.



segura puesto que (i) la generación de claves es completamente aleatoria y (ii) no pueden ser espiadas en su intercambio sin ser detectado. Si bien es cierto que para implementar criptografía cuántica es necesario hacer una renovación completa de hardware, también lo es que los equipos son sustituidos y mejorados continuamente, por lo que no debería ser un gran impedimento, teniendo en cuenta que está en juego la seguridad de todas las telecomunicaciones.

Actualmente, las opciones comerciales de este equipamiento consisten típicamente en dispositivos capaces de conectarse entre ellos para:

- Generar claves aleatorias cuánticamente utilizando generadores cuánticos de números aleatorios (QRNG por su nombre en inglés).
- Intercambiar las claves codificadas en estados cuánticos como la polarización de fotones.
- Realizar un proceso de reconciliación para detectar posibles observadores y depurar la clave.
- Transmitir la clave localmente a un encriptador tradicional que se conecta con el dispositivo electrónico en cuestión que quiere transmitir información, como se ilustra en la figura 6.

En el presente, de nuevo el líder mundial en la provisión comercial de esta tecnología es IDQuantique, si bien otras compañías como MagiQ, SeQureNet o QuintessenceLabs también tienen productos, y entidades como Toshiba, NEC, Mitsubishi o IBM cuentan con programas de investigación.

En el anexo C se presentan algunas de las técnicas más conocidas de encriptación asimétrica y se compara la dificultad de romperlas o invertirlas con computadoras clásicas y cuánticas, que pasará de ser de miles o millones de años a días, horas o minutos.

Autenticación

Si bien la criptografía cuántica ofrece la seguridad ante la computación cuántica que no es posible conseguir con criptografía clásica, la amenaza a la autenticación no tiene aún una solución clara. Al igual que para encriptar información, para autenticarse y firmar digitalmente se utiliza criptografía asimétrica. Concretamente, **una firma digital no es otra cosa que una pareja de claves público-privada, de manera que para firmar los mensajes se nos solicita la clave privada y al destinatario le llegan con nuestra clave pública**, permitiéndole verificar que es nuestro ya que:

- Nadie que no tenga nuestra clave privada puede generar nuestra clave pública.
- Una entidad tercera de confianza ha verificado previamente que esa pareja de claves nos corresponde a nosotros y ha emitido un certificado que así lo manifiesta y que nosotros podemos enviar también al receptor junto con el mensaje.

El problema es que la computación cuántica sí permite descubrir la clave privada a partir de la pública y por tanto toda la seguridad del proceso desaparece. La razón por la cual no es tan sencillo dar una solución cuántica a esto se debe a que la autenticación de servidores, que ocurre a nivel de red -en capa 3 del modelo OSI- y la autenticación de usuarios que ocurre a nivel de aplicación -en capa 7 del modelo OSI- no son fácilmente trasladables a la capa física -capa 2 del modelo OSI-.

Para entender esta dificultad hay que tener presente que **la autenticación implica (i) generación de identidad, (ii) validación de identidad (por un tercero de confianza), (iii) posibilidad de verificación de identidad (verificar la validación del tercero de confianza), (iv) posibilidad de repudiación de identidad, (v) reutilización de identidad y (vi) recuperación de identidad, entre otros**. Esto requiere de la utilización de registros o memorias, lo que cuánticamente es muy complejo y aún está en desarrollo, ya que la naturaleza del mundo microscópico prohíbe clonar estados cuánticos [14], y por tanto dificulta almacenarlos. La mayoría de las memorias cuánticas desarrolladas hasta la fecha son capaces de almacenar simultáneamente estados de unas pocas decenas de fotones; el récord actual lo ostenta desde 2017 un grupo de investigación de la Universidad de Warsaw, que llegó a almacenar 665 estados simultáneos [44]. Las memorias cuánticas tendrán también un gran impacto en el almacenamiento de datos cuando estén listas, para lo que todavía queda un largo camino por recorrer.

Sin embargo, esto no ha evitado el desarrollo, aunque lento, de esquemas de firmas digitales cuánticas (QDS por sus siglas en inglés). En 2001, D. Gottesman de la Universidad de Berkeley y I. L. Chuang del MIT Media Lab [45], propusieron el **primer modelo teórico**

de firmas digitales cuánticas⁸. Las realizaciones experimentales más exitosas de estas se han llevado a cabo sin utilizar memorias ni repetidores cuánticas, lo que dificulta el proceso y obliga a modificarlo de manera ingeniosa. La primera fue capaz, en 2015, de transmitir firmas digitales cuánticas a más de 2 km de distancia [46]. Un año después, en 2016, se realizó una transmisión por vía aérea a una distancia de 1.6 km [47,48]. Ese mismo año se pasaba por primera vez la barrera de los 100 km utilizando una fibra óptica de 102 km, máxima distancia hasta la fecha [49]. El problema que presentan estas firmas es que, pese a ser completamente seguras, no son reusables ya que al utilizarlas se desvela una parte de la clave privada. Esto hace que, incluso una vez superada la complejidad de su implementación a nivel de infraestructura, no sean tan prácticas como se desearía. Para más información sobre el avance experimental de las QDS se recomienda la lectura de la publicación *Progress in experimental quantum digital signatures* [50].

Una idea muy interesante que sería igualmente válida para criptografía y ofrecería nuevos horizontes para la autenticación cuántica es la del internet cuántico. Algunos, como QuTech, están trabajando en hojas de rutas para la consecución de redes de computadores cuánticos interconectados que incorporen todos los beneficios de las tecnologías cuánticas como criptografía simétrica segura o sincronización mediante relojes atómicos. El grupo de trabajo ha publicado ya un artículo en el que define seis etapas para el desarrollo de un internet cuántico [51].

El desarrollo de redes de computadores cuánticos requerirá del desarrollo de arquitecturas óptimas y viables para los mismos que les permitan utilizar las propiedades cuánticas mencionadas a lo largo de este documento para garantizar la seguridad a todos los niveles. En el año 2000, D. DiVincenzo identificaba cinco criterios para el desarrollo de computadores cuánticos robustos, a saber, (i) un sistema físico escalable con *qubits* bien caracterizados, (ii) la habilidad de inicializar *qubits* a placer, como por ejemplo en el estado $|000\dots\rangle$, (iii) tiempos de coherencia suficientemente largos, mucho mayores que el tiempo operacional de las puertas lógicas, (iv) un conjunto de puertas lógicas universales y (v) capacidad de medida sobre *qubits* específicos [52]. En 2017, M.F. Brandl publicaba lo que denominó una arquitectura cuántica de Von Neumann, donde combinaban la arquitectura clásica de Von Neumann con los cinco criterios de DiVincenzo [53].

En definitiva, **es un hecho que la ciberseguridad cambiará radicalmente en los próximos años para resistir ataques con computadores cuánticos.** Para mejorar los algoritmos de criptografía asimétrica ampliamente utilizados en la actualidad se plantea o bien la ideación de nuevos algoritmos asimétricos conocidos como *post-quantum cryptography* o bien criptografía cuántica simétrica consistente en generación de números aleatorios cuánticamente -QRNG- y distribución cuántica de claves -QKD-. Tenemos entonces que la segunda técnica es cien por cien segura aunque por el momento solo nos sirva en materia de criptografía y requiera modificaciones de infraestructura, y la primera solo ofrece garantías a corto plazo pero por el momento parece la solución más viable en materia

8. Sin entrar en detalles técnicos, estas firmas funcionan de manera similar a las firmas Lamport y los árboles de Merkle pero (i) utilizando generadores de números aleatorios para las claves privadas y (ii) utilizando mapeos cuánticos en lugar de funciones hash para la generación de claves públicas a partir de las privadas.

de autenticación. **A largo plazo, es posible que veamos nacer un nuevo concepto de internet como una red diferente de computadores, esta vez cuánticos o híbridos, conectados, que a su vez incorpore una nueva criptografía.**

Como discutiremos en la cuarta sección de este documento, las grandes potencias mundiales son conscientes de esta amenaza y están llevando a cabo programas billonarios para dominarla y combatirla, al mismo tiempo que universidades, *start-ups* y grandes empresas tecnológicas buscan cada vez con más frecuencia jugar un papel importante en esta era cuántica naciente.



BLOCKCHAIN

¿QUÉ ES BLOCKCHAIN?

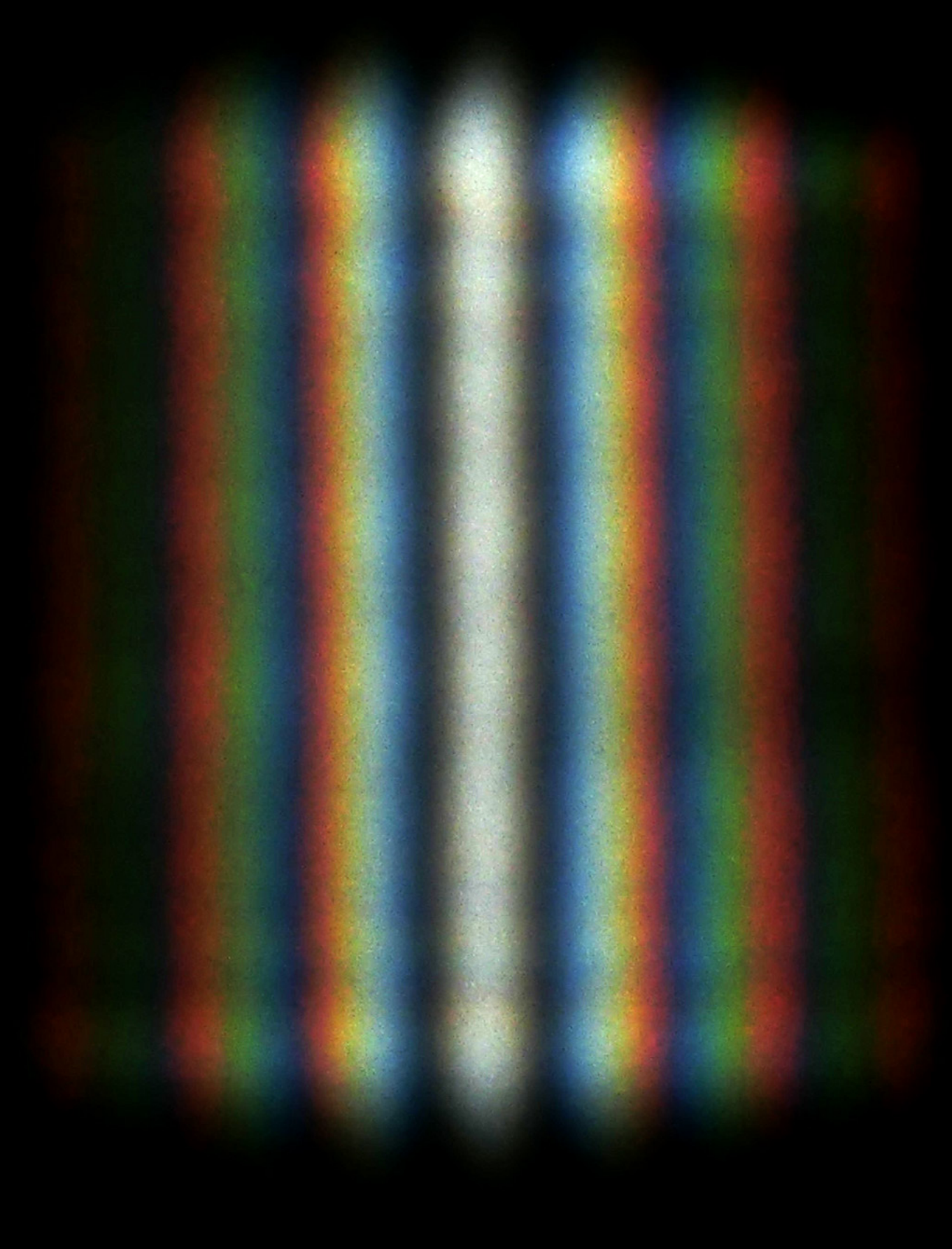
Blockchain es una tecnología inicialmente propuesta en 1991 por los físicos S. Haber y W.S. Stornetta, con la idea de tener un registro digital, inmutable y descentralizado de archivos de audio, imagen, video o texto ordenado cronológicamente [54].

En 2008 dio el salto a la fama con el nacimiento de Bitcoin [55], una criptomoneda cuya seguridad y funcionamiento son garantizados gracias a blockchain, y desde entonces ha ofrecido soporte tecnológico de más de 2000 criptomonedas así como de muchas otras soluciones digitales que nada tienen que ver con dinero no fiduciario. Algunos ejemplos de las múltiples aplicaciones de esta tecnología pueden encontrarse en cadenas de suministro, sistemas de votaciones transparentes, trazabilidad del suministro energético, inclusión financiera, remesas, identidad digital, ayuda humanitaria, registros médicos y de propiedad, certificaciones académicas, etc.

La tecnología blockchain es útil porque permite tener un registro de transacciones inmutable, descentralizado y consensuado. Por transacción se entiende todo aquello que se realice en la solución digital, desde la creación de un usuario o la actualización de un documento hasta la venta de un activo. En la implementación ideal de la tecnología, todos los participantes tienen una copia de la cadena sincronizada con las demás y cualquier información que se desee añadir debe ser previamente validada por los participantes según las reglas definidas en lo que se conoce como protocolo de consenso.⁹

Para más información sobre esta tecnología, recomendamos la lectura del documento que publicamos desde el ITE Tech Lab detallando el funcionamiento de la misma desde un punto de vista que intenta ser no técnico pero sí riguroso, y que responde a las preguntas acerca de cuándo la tecnología es útil y cómo comenzar a construir una solución [56]. Para lecturas más livianas, recomendamos también los dos artículos relacionados publicados en Abierto al Público [57,58].

9. En la práctica, muchos blockchain, generalmente clasificados como permissionadas (federadas o privadas), cuentan con una o varias entidades que controlan la red y deciden sobre quién puede acceder y qué permisos tiene sobre la misma para ver y modificar información.



Patrón de interferencia resultante de luz solar pasando a través de dos rendijas con una anchura de 1 cm y una separación de 0.5 mm. En las partes superior e inferior de la imagen, la interferencia al borde de la rendija produce una variación notable de la intensidad.

¿EN QUÉ BASA BLOCKCHAIN SU SEGURIDAD?

Hay dos elementos a destacar sobre la seguridad de blockchain. El primero tiene que ver con las claves de los participantes y el segundo con la encriptación de las transacciones y bloques; una vez más, vemos que de nuevo la seguridad se concentra en torno a autenticación y criptografía.

Claves de los participantes

En blockchain a los participantes se les genera una pareja de claves, conocidas como **clave pública** o **wallet** y **clave privada**, que definen y caracterizan su identificación y autenticación.¹⁰

La **clave pública** o **wallet** es la clave con la que cada participante se muestra a los demás; ya sea para firmar transacciones, enviar información, recibirla o realizar cualquier interacción con la blockchain. Por el otro lado, la **clave privada** es la clave con la que cada participante se autentica en el sistema. Solo el poseedor de la **clave privada** puede emitir firmas con la **clave pública**.

Esta pareja de claves es generada por la blockchain para cada participante utilizando algoritmos de clave asimétrica. Como explicábamos cuando hablamos de ciberseguridad, las computadoras cuánticas podrán correr algoritmos cuánticos, concretamente el algoritmo de Shor [17], capaces de realizar ingeniería inversa que permita encontrar la clave privada de un usuario a partir de su clave pública de manera eficiente.

Minado de bloques, protocolos de consenso y reversibilidad de las funciones hash

El otro gran punto fuerte de seguridad de la tecnología blockchain es el proceso mediante el cual, según las reglas que determina el protocolo de consenso que se utilice en cada blockchain, se agrupan **transacciones** formando un **bloque** y este se **encripta** utilizando una función *hash*. A este proceso que se conoce como **minado**.

La blockchain o cadena de bloques será segura siempre y cuando la función *hash* utilizada para encriptar satisfaga dos condiciones conocidas como ser **resistente a pre-imágenes y a colisiones**.

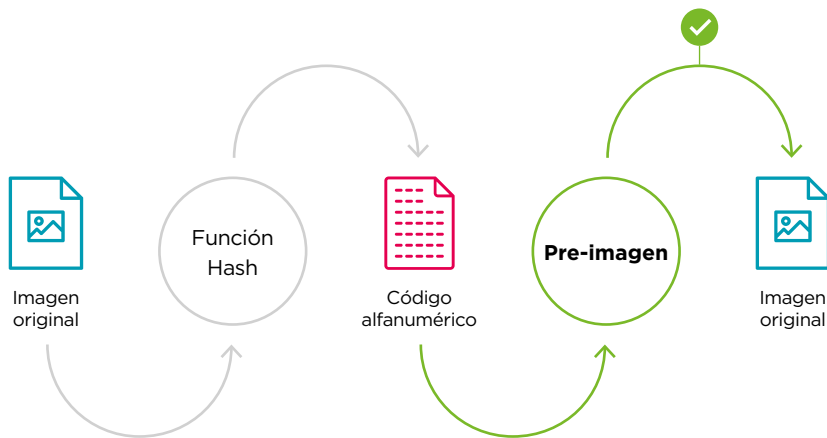
10. Para ser precisos, no siempre la clave pública y el wallet son lo mismo y de hecho es importante resaltar la diferencia, sobre la que ahondaremos en el siguiente epígrafe. En las redes más importantes la clave pública se genera con criptografía asimétrica a partir de la privada y luego se “hashea” para dar lugar al *wallet* -actualmente por cuestiones de espacio, no de seguridad-, de forma que el *wallet* es la clave pública “hasheada”.

Resistencia a pre-imágenes

Dado el código alfanumérico *hash* resultado de minar un bloque, ha de ser imposible encontrar en un tiempo razonable -entendiendo por tiempo razonable el suficiente como para que no ocurra mientras el *hash* siga siendo utilizado- el contenido de ese bloque que dio lugar a ese código. Es decir, romper la criptografía.

Con este propósito, se busca que la técnica utilizada para “hashear” no posibilite que haya un algoritmo que permita tener una estrategia mejor para invertirlo que la fuerza bruta.

 **FIGURA 7.** Concepto de pre-imagen.



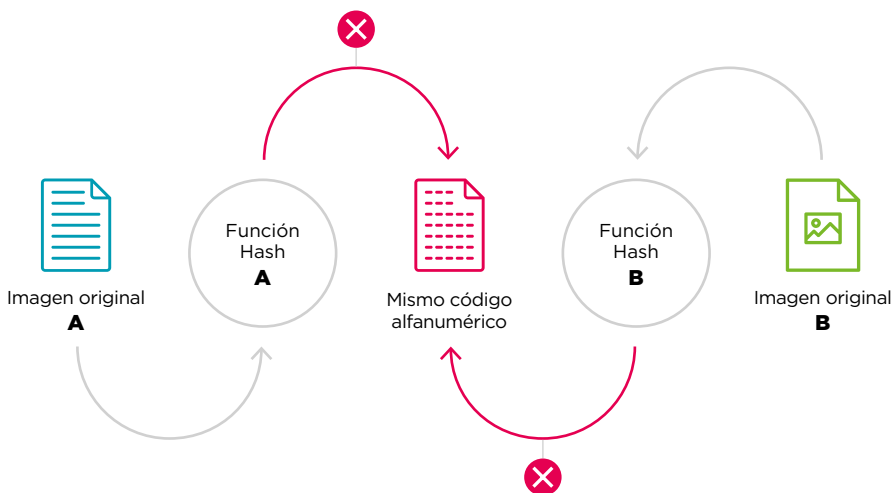
Resistencia a colisiones

Dados dos bloques diferentes -es decir, que contienen transacciones diferentes- ha de ser muy difícil -entendiendo por muy difícil que no ocurra en un tiempo razonable- que les corresponda el mismo *hash*.

Cabe apuntar que el número de posibles combinaciones de transacciones diferentes que definen el contenido de un bloque son infinitas, mientras que el número de posibles hashes resultado de encriptar los bloques es finito, puesto que son códigos alfanuméricos de una determinada longitud que además, en general, están restringidos a comenzar por un número determinado de ceros. Es por eso que no se puede exigir que sea imposible que dos mensajes tengan el mismo *hash* al encriptarlos pero se pide que, pese a poder darse el caso, nunca ocurra.



FIGURA 8. Concepto de colisión.



EL FUTURO DE BLOCKCHAIN EN LA ERA CUÁNTICA

Pueden identificarse al menos **cuatro situaciones en las que las tecnologías cuánticas afectarán a la tecnología blockchain**, que tienen que ver con los dos estándares de seguridad de estas cadenas de bloques descritos en el epígrafe anterior, con la criptografía y con el hecho de que blockchain hace uso de internet y de servidores o computadoras tradicionales. Estas cuatro situaciones son **(i) la autenticación, (ii) el minado de bloques, (iii) la reversibilidad de funciones hash y (iii) el uso de internet y sus protocolos para la comunicación entre nodos y wallets.**

Tecnologías cuánticas y autenticación en blockchain

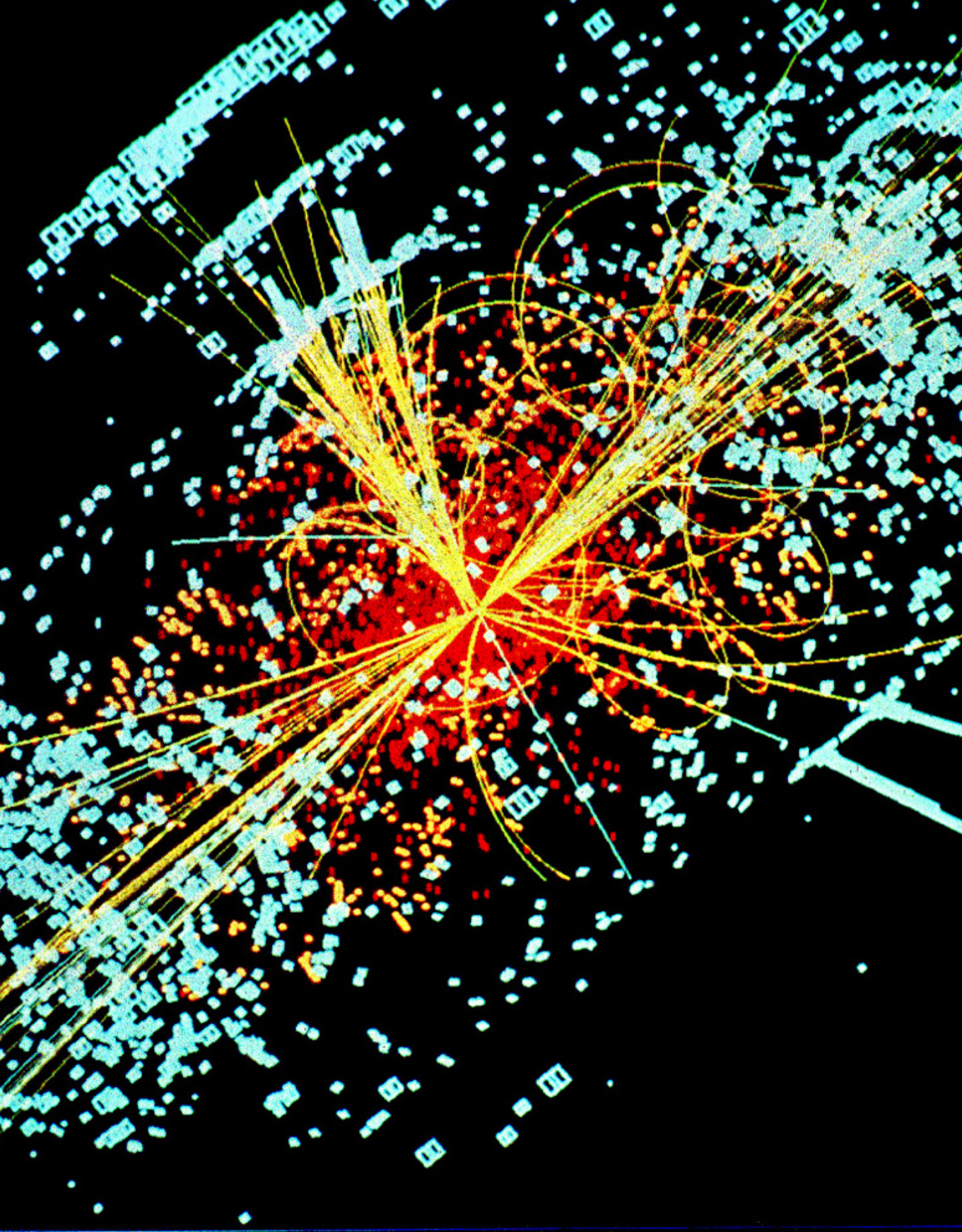
La tecnología blockchain utiliza criptografía asimétrica para generar las parejas de **clave pública - clave privada** de los participantes. En general, se utiliza criptografía de curvas elípticas o más concretamente *Elliptic Curve Digital Signature Algorithm* (ECDSA)¹¹. Como ya hemos remarcado varias veces en este documento, la computación cuántica será capaz de romper este tipo de criptografía de manera eficiente gracias al algoritmo de Shor [17], lo que traerá consecuencias de mayor y menor relevancia. La autenticación en blockchain a nivel de usuario final -los dueños de *wallets* donde se almacenan todo tipo de *assets*- es segura en la medida en que las claves privadas de dichos usuarios estén a salvo de hackers.

Gracias a que, como explicábamos en el epígrafe previo, los *wallets* no son las claves públicas en sí sino que son el resultado de aplicarles una función *hash* -o “hashearlas”-, y teniendo en cuenta que aún no se conoce forma de invertir funciones *hash* con algoritmos cuánticos, conocer un *wallet* no permite a un hacker con un computador cuántico encontrar la **clave privada** del usuario de blockchain al que el *wallet* corresponde, ya que tendría que invertir la función *hash* para encontrar la clave pública y luego invertir el algoritmo de criptografía asimétrica para encontrar la clave privada, y la computación cuántica solo presenta grandes ventajas en lo segundo.

Sin embargo, las claves públicas son reveladas a la red cuando el usuario realiza una transacción. En ese momento, **un computador cuántico suficientemente potente puede hacer ingeniería inversa gracias al algoritmo de Shor [17] y encontrar la clave privada de un usuario en un plazo de minutos.** En el momento en que esto ocurra, la identidad de ese usuario en la blockchain puede ser usurpada y todos los bienes y activos de los que sea propietario en la red pueden serle robados y enviados a otra cuenta, sin ninguna posibilidad ni derecho a reclamarlos.

Una forma de minimizar la amenaza que esto supone consiste en regenerar las parejas de claves tras cada transacción. Suponiendo que esta práctica se adoptase siempre y en todos los casos, la amenaza aún persiste en las transacciones pendientes de procesar. Para que una

11. Concretamente, las dos redes públicas más importantes, a saber, Bitcoin y Ethereum, utilizan los parámetros de la curva secp256k1 ECDSA propuesta por Certicom [60,61,62] y Hyperledger, el software más utilizado para redes privadas y federadas -con el permiso de Ethereum- utiliza la curva prime256v1 [63].



Un ejemplo de simulación a partir de los datos de la desintegración dos protones de muy alta energía generando un Bosón de Higgs en el decaimiento en dos haces de hadrones y dos electrones en el detector CMS del LHC en el CERN. Las líneas representan las posibles vías de desintegración, mientras que la zona en azul claro representa la energía obtenida en la desintegración de las partículas en el detector. Lucas Taylor / CERN. Octubre 1997.

transacción se considere aceptada en la blockchain, ha de ser incorporada en un bloque y este ha de ser secundado por la red, de forma que se añadan más bloques a continuación. En algunas ocasiones hay bloques que no son secundados y las transacciones, pese a haber conseguido entrar en un bloque, no han llegado a la versión más larga de la cadena y por tanto no son aceptadas. En la red Bitcoin se publica un bloque cada 10 minutos en promedio, y se considera suficiente esperar hasta que otros seis bloques hayan sido añadidos posteriormente para estar seguros de que el bloque y sus transacciones han sido aceptados por la red. Esto supone en torno a una hora. Durante ese periodo de tiempo, la **clave pública** es revelada a la red y un computador cuántico suficientemente rápido y potente podría descubrir la **clave privada** a partir de la misma, acceder a la cuenta y robar los bienes -incluso los que se están transfiriendo en esa misma transacción- antes de que la transacción se consolide en el blockchain y la clave sea modificada y por tanto segura de nuevo.

Dos estudios realizados por profesores de la Universidad de Waterloo y el centro de investigación de Microsoft en Estados Unidos **estiman el número de *qubits* lógicos necesarios para poder implementar algoritmos cuánticos capaces de romper firmas digitales de 256 bits de longitud generadas con criptografía de curvas elípticas -las utilizadas actualmente en estas redes- en 1500 [12] y 2330 [13]**, respectivamente. Aún es incierto a cuántos *qubits* físicos equivaldría esto, pero diferentes expertos estiman que un *qubit* lógico podría llegar a requerir de más de 1000 *qubits* físicos. Un tercer estudio realizado por investigadores de Singapur, Australia y Francia afirma en varias ocasiones que, según sus extrapolaciones, **en 2027 ya contaremos con computadores cuánticos suficientemente potentes como para romper estas claves en menos de 10 minutos [64]**.

Es por tanto una necesidad imperiosa el modificar los algoritmos de generación de claves en blockchain. Hay tres vías para hacer esto, tal y como discutíamos en la sección de Ciberseguridad:

- **La utilización de algoritmos para generación de claves asimétricas más sofisticados**, lo que se conoce como *post-quantum cryptography* y cuya seguridad ante la computación cuántica es, en el mejor de los casos, temporal -eventualmente se conseguirá romperlos-. Como comentábamos en la sección anterior, el NIST está en el proceso de evaluación de una convocatoria pública de propuestas [41] y la iniciativa europea PQCrypto ha identificado los algoritmos basados en hashes SPHINCS [65] y XMSS [66] como los mejores candidatos hasta el momento [42].
- **La utilización de criptografía simétrica cuántica.** La tecnología cuántica actual permite (i) generar claves simétricas completamente aleatorias con generadores cuánticos de números aleatorios y (ii) compartirlas de manera totalmente segura al codificarlas en estados cuánticos que cambian si son observados -QKD-. Sin embargo, no está claro aún cómo utilizarla para desarrollar esquemas de criptografía asimétrica como los utilizados hoy en día para autenticación y firmas digitales, ya que todavía se está en una etapa muy temprana en el desarrollo de memorias cuánticas y repetidores cuánticos. Lo mismo ocurre con los esquemas de firmas digitales cuánticas, donde se va avanzando lentamente; la mayor distancia de implementación de uno de estos protocolos hasta el momento fue de 102 km, en 2017. [49].

- **El desarrollo de una nueva metodología de firma digital que pueda aprovechar la criptografía simétrica cuántica ya disponible** para habilitar una autenticación y firma digital totalmente diferente, prescindiendo de parejas de claves **público-privadas**. Esto, si bien aún no se ha planteado, podría ser más complejo inicialmente al suponer un cambio de paradigma y metodología, unido a una renovación de equipos dado que la criptografía cuántica tiene lugar a nivel de hardware, pero también podría ser más sencillo en la práctica al no tener que utilizar criptografía simétrica cuántica para hacer criptografía asimétrica de autenticación y firmas digitales de una manera forzada, como proponen los esquemas de firmas digitales cuánticas actuales.

No ha habido prácticamente ninguna iniciativa documentada hasta el momento que haya explorado alguna de estas tres alternativas, ni ninguna otra, para mejorar la inseguridad de las firmas digitales en blockchain. Quizás la prueba de concepto de mayor repercusión es la realizada por investigadores rusos en julio de 2018, en la que reportan la utilización de firmas digitales cuánticas, lo que corresponde a la segunda solución propuesta [67]. Este mismo grupo publicaba en noviembre de 2018 en *Nature* su análisis de los riesgos de la amenaza de la computación cuántica en blockchain y las posibles soluciones cuánticas a tener en cuenta [68].

En cuanto a las reacciones y movimientos en la comunidad blockchain frente a esta amenaza, la realidad observada es que son mínimos o inexistentes. Gran parte de la comunidad ni siquiera está interesada en entender la amenaza que supone la computación cuántica para blockchain. Prueba de ello es que en Consensus 2018, el mayor evento del año sobre blockchain que congregó a más de 8500 personas en Nueva York, no hubo ninguna presentación ni ningún panel en el que se mencionase el tema, y más de lo mismo en Labitconf 2018, el evento más importante sobre blockchain en Latino América que tuvo lugar en Santiago de Chile.

Algunos líderes de la comunidad blockchain, en cambio, sí han reaccionado. Un ejemplo es Vitalik Buterin, una de las figuras más importantes y respetadas tras haber fundado Ethereum en 2015 [69], que a la vez que reconocía su preocupación ante la llegada de la computación cuántica, mostraba su agrado sobre el esquema *hash-based* conocido como firmas Lamport [70] y su intención de incorporarlo para sus firmas digitales cuando los computadores cuánticos sean una amenaza [71,72].

Cualquiera de las alternativas presentadas planteará desafíos extra como la viabilidad de llegar a consensos en las redes públicas para hacer estas grandes modificaciones o la viabilidad para actualizar todas las firmas digitales de todas las cuentas activas. Sin embargo, es de gran importancia que estos debates empiecen a ser una realidad lo antes posible puesto que **toda aquella información o datos que hoy en día esté encriptada con criptografía asimétrica tradicional y pueda ser descargada, será vulnerable de ser descryptada con la llegada de la computación cuántica.**

Tecnologías cuánticas y reversibilidad de las funciones hash

Una buena noticia para blockchain es que no se conocen ni se prevé que se desarrollen algoritmos cuánticos para invertir las funciones *hash* de manera eficiente, aunque no

hay prueba matemática de que las funciones *hash* no puedan ser invertidas [73,74], de forma que **la resistencia a pre-imágenes está a salvo por el momento pero no se puede garantizar que vaya a estarlo por siempre**. El día que eso ocurra, la tecnología blockchain tal y como la conocemos hoy en día quedará obsoleta.

En cuanto a la **resistencia a colisiones**, que es el otro punto importante relativo a las funciones *hash*, **depende exclusivamente de la “calidad” de estas funciones por lo que no cambiará con la llegada de la computación cuántica**. Si las funciones son suficientemente buenas y no se aplican sobre una cantidad de datos extremadamente grande, será altamente improbable que dos cadenas de datos diferentes obtengan el mismo *hash*.

Tecnologías cuánticas y minado de bloques

Lo que si cambiará es el minado de bloques, ya que los computadores cuánticos podrán correr el algoritmo cuántico de Grover [75], que permite encontrar un elemento determinado en una lista desordenada de N elementos en un número de pasos \sqrt{N} , mientras que la computación clásica necesita en promedio $N/2$ pasos.

Encontrar un elemento determinado en una lista es en cierto modo lo que se hace al minar bloques en blockchain; minar es buscar cuál es la pieza aleatoria denominada *nonce* que, concatenada al resto de elementos del bloque (número de bloque, transacciones, ...), da un *hash* válido¹². Por tanto, **los computadores cuánticos podrán minar bloques realizando un número menor de pruebas o pasos para encontrar el *hash***.

En Bitcoin, la red pública más utilizada hasta la fecha y que permitió a la tecnología blockchain dar el salto a la fama, el número de *hashes* a probar en promedio para encontrar el válido y ser el ganador del protocolo de consenso conocido como *proof of work* es $2^{256}/t$, siendo t un parámetro que se recalcula cada 2016 bloques, de forma que la dificultad se mantiene acorde a la pauta de que la comunidad de mineros tarde, en promedio, 10 minutos en validarlo. Se define también la dificultad $D=2^{224}/t$, que es la cantidad anterior dividida por el número de *nonces* disponibles, que es 2^{32} [23]. Actualmente, en enero de 2019, la dificultad es $D=5 \cdot 10^{12}$ [76], lo que utilizando las fórmulas anteriores supone tener que probar del orden de $4.19 \cdot 10^{29}$ *hashes* con un computador clásico. Teóricamente, en un computador cuántico sería necesario realizar únicamente un número de pasos o iteraciones del proceso del orden de $6.48 \cdot 10^{14}$.

12. En redes públicas como Bitcoin o Ethereum tiene lugar una competición para encontrar el hash de cada bloque, ya que conlleva una recompensa en forma de criptomoneda que en Bitcoin es actualmente de 12.5 Bitcoins, lo que corresponde actualmente -a marzo de 2019- unos \$50.500 y llegó a equivaler a \$237.500 en enero de 2018, cuando Bitcoin alcanzó su mayor precio. Esta recompensa es la que motiva el conocido gasto computacional y energético asumido por parte de estos mineros.

Fijando el número de *qubits* lógicos¹³ en 2024, lo que se espera sea una realidad entre 2025 y 2030, el estudio realizado por distintas instituciones de Singapur, Australia y Francia determinó que la computación cuántica no será capaz en la próxima década de minar bloques con mayor rapidez que los actuales dispositivos ASIC [77] tan eficientemente diseñados para este propósito, si bien en el futuro puedan llegar a hacerlo hasta 100 veces más rápido [64].

Aun cuando esto ocurra, el problema no es crítico y la solución para salvaguardar la seguridad de blockchain sigue siendo simple. En caso de mantener los protocolos de consenso actuales, **siempre se puede aumentar la dificultad para compensar el aumento de velocidad ofrecido por la computación cuántica**. Por otro lado, también se han comenzado a **proponer nuevos protocolos de consenso como Cuckoo Cycle [78], Momentum [79] o Equihash [80]** que presentan mayor resistencia a la computación cuántica ya que, pese a consistir igualmente en la aplicación de funciones *hash* a la información de los bloques, ahora las condiciones de validez del mismo aplican no solo al *nonce* sino también al *header* [81], de forma que no es suficiente con iterar sobre una sucesión de elementos hasta encontrar el *hash* válido.

Tecnologías cuánticas y utilización de internet

En la sección de Ciberseguridad analizábamos algunas de las amenazas de seguridad que se cernirán sobre internet con la llegada de la computación cuántica, lo que afecta indirectamente a blockchain al hacer uso del mismo. Dos de las consecuencias adversas que tendrían lugar para blockchain en un internet inseguro son:

- La usurpación de identidad de nodos y *wallets*, permitiendo suplantar a otros usuarios o participantes del blockchain.
- Las prácticas conocidas como *man in the middle* (MITM), que consisten en una tercera persona no autorizada interceptando y modificando información que viajaría, en este caso, entre un *wallet* y un nodo o entre dos nodos.

Los detalles acerca de las posibles maneras de conseguir un internet seguro ante la computación cuántica se discutieron en la sección de Ciberseguridad, por lo que no volveremos sobre ellos.

Por último, si bien no procede entrar en detalle por cuestiones de complejidad, cabe mencionar que ya están surgiendo propuestas para construir blockchain enteramente cuánticos, basándose en el fenómeno del entrelazamiento y en la imposibilidad de copiar estados cuánticos [82] -al observar un sistema cuántico, como describimos en la sección dedicada a las tecnologías cuánticas, este cambia, de ahí que sea imposible clonarlo- [14].

13. Los *qubits* lógicos son aquellos que se utilizan para realizar el procesamiento. Sin embargo, para la corrección de errores, cada uno de estos *qubits* va acompañando de varios *qubits* más, conocidos como *qubits* físicos.

Esta tecnología, que sería completamente distinta a la tecnología blockchain actual, si algún día se desarrollase ofrecería una seguridad completa al estar basada en procesos físicos y no en la dificultad matemática de invertir *hashes* o firmas digitales, de forma análoga a cómo la criptografía cuántica es segura por naturaleza frente a la seguridad limitada que ofrece la criptografía clásica. En el caso de que algún día la computación cuántica sea capaz de invertir las funciones *hash* de manera eficiente, este tipo de soluciones parecen ser las únicas viables para blockchain.



INTELIGENCIA ARTIFICIAL

¿QUÉ ES LA INTELIGENCIA ARTIFICIAL?

Inteligencia artificial, si bien es entendida y definida de muchas maneras, puede verse como la habilidad que pueden desarrollar las máquinas para mostrar comportamientos inherentes a los seres humanos como razonar, aprender, percibir, planificar, ser creativo o resolver problemas.

Hay distintas disciplinas dentro de la inteligencia artificial como *machine learning*, redes neuronales, procesamiento de lenguajes, reconocimiento de imágenes, reconocimiento de voz, etc. que en conjunto proveen a la máquina con la capacidad para mostrar comportamientos humanos. Cada vez más frecuentemente, los algoritmos que hay tras estas subcategorías están diseñados para aprender de forma autónoma a medida que son alimentados con datos.

Dentro de la inteligencia artificial es común distinguir cuatro niveles en función del grado sofisticación de los comportamientos de la máquina:

- Reactiva: Capacidad para responder a estímulos o *inputs* en tiempo real sin tener en cuenta experiencias pasadas o memorizar procesos.
- Memoria limitada: Capacidad para responder a estímulos o *inputs* tomando decisiones que tienen en cuenta experiencias pasadas retenidas en una memoria.
- Teoría de la mente: Capacidad para tener pensamientos y emociones propios que condicionen sus decisiones y su interacción con el mundo.
- Conciencia propia: Capacidad para ser conscientes de su propia conciencia y existencia y entenderse a sí mismos, más allá de entender a los seres humanos.

La última de las cuatro etapas es la que se asocia idealmente al concepto de inteligencia artificial, en el que las máquinas son capaces de simular plenamente una inteligencia similar a la que reconocemos en los seres humanos. Sin embargo, hasta el momento solo se ha podido desarrollar tecnología en las dos primeras categorías, dando lugar en ocasiones a frustración entre sus desarrolladores.

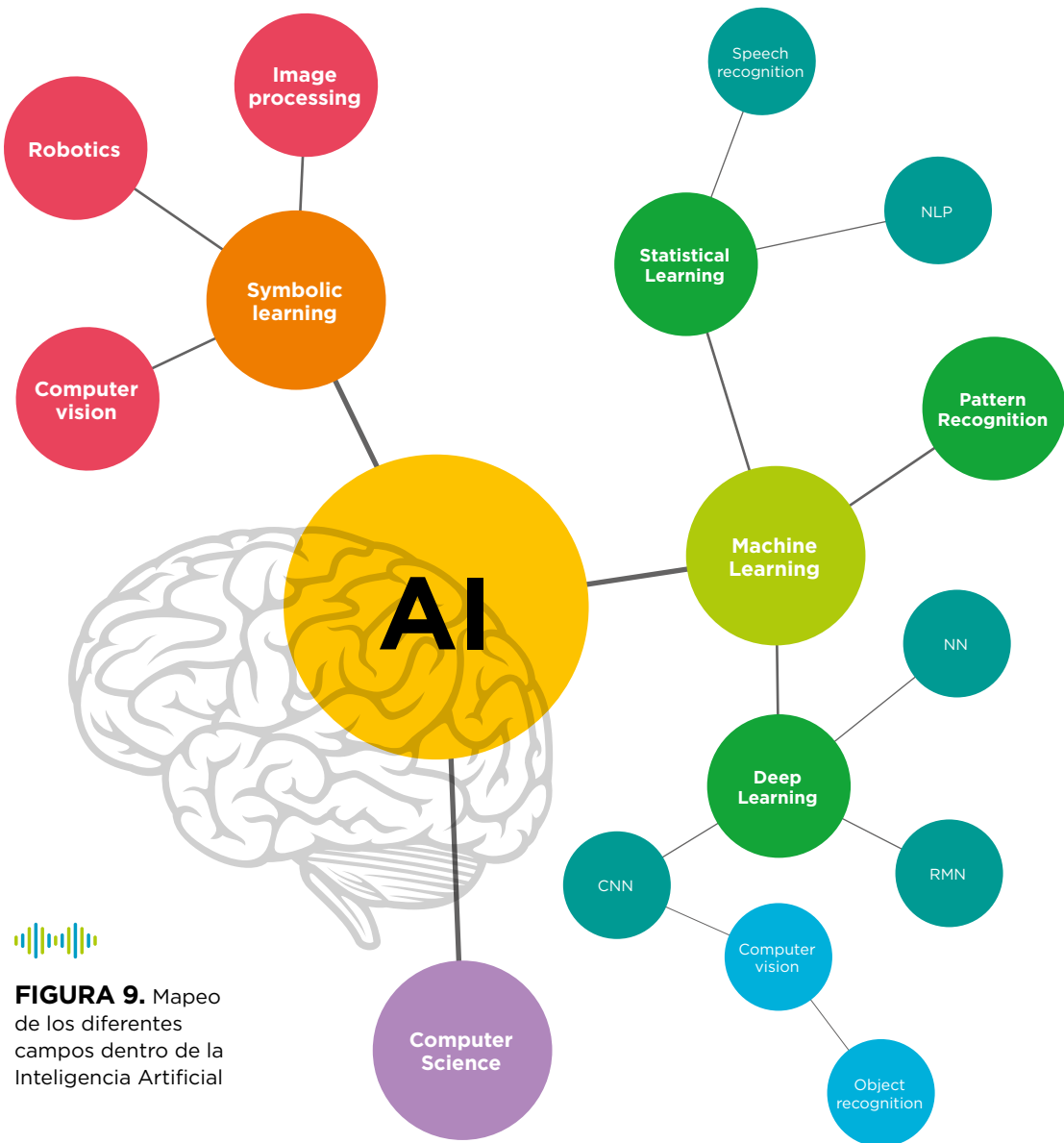


FIGURA 9. Mapeo de los diferentes campos dentro de la Inteligencia Artificial

EL FUTURO DE LA INTELIGENCIA ARTIFICIAL EN LA ERA CUÁNTICA

Es posible que la computación cuántica sea lo que necesita la inteligencia artificial para llegar a alcanzar esos dos estadios más avanzados, para los que fue inicialmente pensada [83-85]. Actualmente hay un campo activo de investigación creciente en inteligencia artificial cuántica y *machine learning* cuántica.

Desde el año 2000, han comenzado a publicarse investigaciones sobre cómo la computación cuántica puede aplicarse en el mapeo de las expresiones del lenguaje [86], teoría de juegos [87], clasificación de imágenes [88], problemas de coordinación [89], procesamiento de lenguajes naturales [90], estrategias económicas el contexto de los juegos de

bienes públicos [91] -donde un número de participantes se distribuyen en grupos que han de tomar decisiones de inversión de capital cuya rentabilidad depende del resultado del resto de jugadores- y hasta vida artificial cuántica [92].

Un estudio realizado en instituciones inglesas y americanas concluye que las principales áreas en las que la computación cuántica podría tener aplicaciones a corto plazo dentro de la inteligencia artificial con un procesador de en torno a 1000 *qubits* son **(i) la resolución de problemas que son muy difíciles de tratar o intratables con las técnicas actuales de *machine learning*, como el encontrar patrones y correlaciones en conjuntos de datos no estructurados -fotos, imágenes, videos, etc- que permitan clasificarlos utilizando algoritmos no supervisados, (ii) el análisis de conjuntos de datos susceptibles de tener correlaciones intrínsecas de tipo cuánticas, como en las ciencias cognitivas, y (iii) el desarrollo de algoritmos híbridos donde se incorporan rutinas cuánticas allí en donde el algoritmo clásico se vuelve ineficiente o inservible [93].**

La capacidad de tratar problemas exponencialmente complejos radica en la promesa que la computación cuántica podrá realizar operaciones matemáticas que hoy no son tratables. Por ejemplo, plataformas sociales como las que utilizamos hoy en día captan ingentes cantidades de datos por segundo que no pueden utilizar en tiempo real para realizar recomendaciones porque no está disponible la capacidad computacional necesaria. Esto aplica también en el sector de transporte, para regulación de tráfico, o en el sector finanzas, para predicción de crisis financieras, como discutiremos más adelante.

En 2014, cuatro investigadores chinos implementaron el primer algoritmo cuántico de *machine learning* en un procesador de cuatro *qubits* [94]. El algoritmo implementado fue la versión cuántica de la técnica denominada *support vector machine* (SVM), que es un algoritmo supervisado capaz de, a partir de datos pre-divididos en grupos, clasificar datos nuevos. La técnica implementada se conoce por tanto como *quantum support vector machine* (QSVM) y fue aplicada al problema conocido como reconocimiento óptico de caracteres (ROC), que consiste en la digitalización de textos. El objeto del experimento consistía en que el procesador cuántico fuese capaz de identificar correctamente la escritura de los números 6 y 9. Para ello, se entrenó a la máquina con imágenes que le permitieron aprender qué era un 6 y qué era un 9, y a continuación se le pasaron muestras escritas de estos números que fue capaz de clasificar satisfactoriamente.

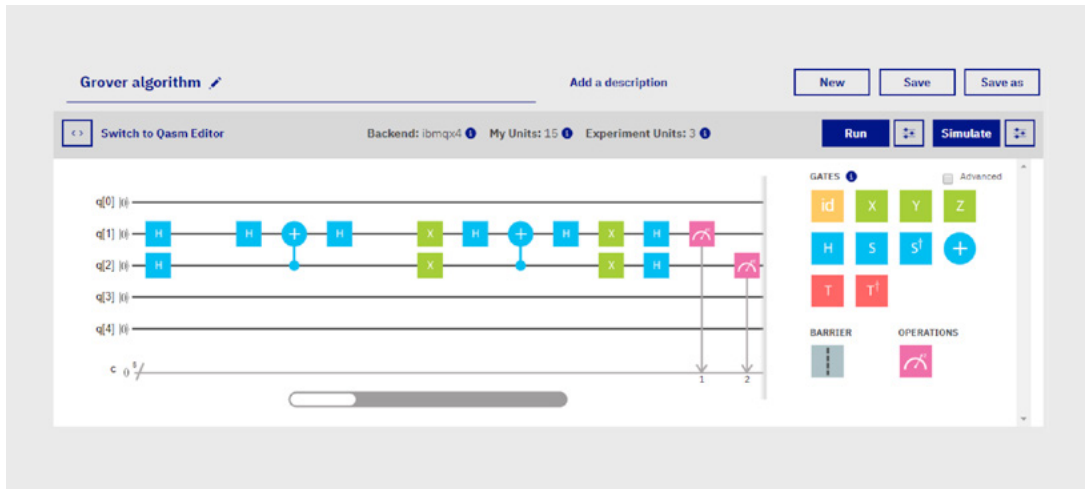
Hay varios estudios teóricos que discuten las convergencias y dificultades de la combinación de inteligencia artificial con la computación cuántica y proponen algoritmos en los campos de *deep learning* y *neural networks* entre otros [95-107].

Para comenzar a probar este tipo de algoritmos, en la red hay ya disponibles decenas de simuladores de computadores cuánticos con diferentes lenguajes de programación ya existentes como C, C++, Java, Matlab, Maxima, Python o Octave, y también nuevos como Q# [108]. De entre las plataformas más populares para jugar con una máquina cuántica virtual podemos destacar Rigetti Forest [109] y IBM QISKit [110].

Un estudio muy interesante [111] simula lo que denominan vida artificial cuántica [92], consistente en emular los procesos de reproducción, mutación, interacción y muerte. Para ello, parejas de *qubits* hacen la función de individuos, siendo un *qubit* la representación del genotipo y el otro la del fenotipo. La información se codifica en el genotipo y se transmite de generación en generación.



FIGURA 10. Algoritmo de Grover sobre 2 qubits corriendo en el simulador cuántico de IBM.



Para cerrar esta sección decir que, si bien este es un campo muy nuevo como se deduce del hecho de que casi todas las referencias corresponden a publicaciones del año 2018, hay una comunidad creciente de investigadores generando conocimiento. A medida que las máquinas virtuales y los computadores cuánticos reales vayan introduciendo más *qubits* y ganando robustez, la inteligencia artificial cuántica se volverá una realidad y quizás, gracias a ello -o por culpa de ello-, las máquinas consigan llegar a poder tener emociones y ser conscientes de su propia existencia, como inicialmente se pensó.



OTRAS TECNOLOGÍAS

INTERNET DE LAS COSAS (IOT) Y DRONES

Una de las tecnologías emergentes que está creciendo más rápido es el internet de las cosas o IoT (por su nombre en inglés), consistente en la red de dispositivos conectados a través de internet que según Ericsson superará los 25 billones en 2020 [112] y según Bain generará más de 300 billones de dólares anuales [113] principalmente en agricultura, en la industria automovilística y en infraestructura [114].

Un ejemplo interesante que combina IoT, drones y tecnologías cuánticas es el sensor cuántico desarrollado por la compañía QLM Technology, que va montado sobre un dron y es capaz de detectar fugas de gas natural a una distancia de hasta 150 metros desplazándose a una velocidad de hasta 48 km/h. Esto, en palabras de su fundador, les permite “una sensibilidad 10 veces superior a la de su competidor más cercano para detectar estas fugas, que ocasionan entre 6 y 35 billones de dólares en pérdidas al año en la industria del gas natural” [115].

En un artículo publicado por Telefónica en 2017, se destacaba el gran impacto esperado de las tecnologías cuánticas en el internet de las cosas, donde señalaban la necesidad de utilizar la información cuántica para crear canales cuánticos de telecomunicaciones que conecten estos dispositivos de manera segura y la computación cuántica para hacerlos más inteligentes y eficientes [116]. Además, coincidían con GrowthEnabler en que el de las Ciudades Inteligentes (más conocidas por su nombre en inglés *Smart Cities*) será uno de los sub-sectores de IoT más beneficiado [117]. Para más información, se recomienda el artículo de Forbes [118] y la publicación de IDQuantique [119].

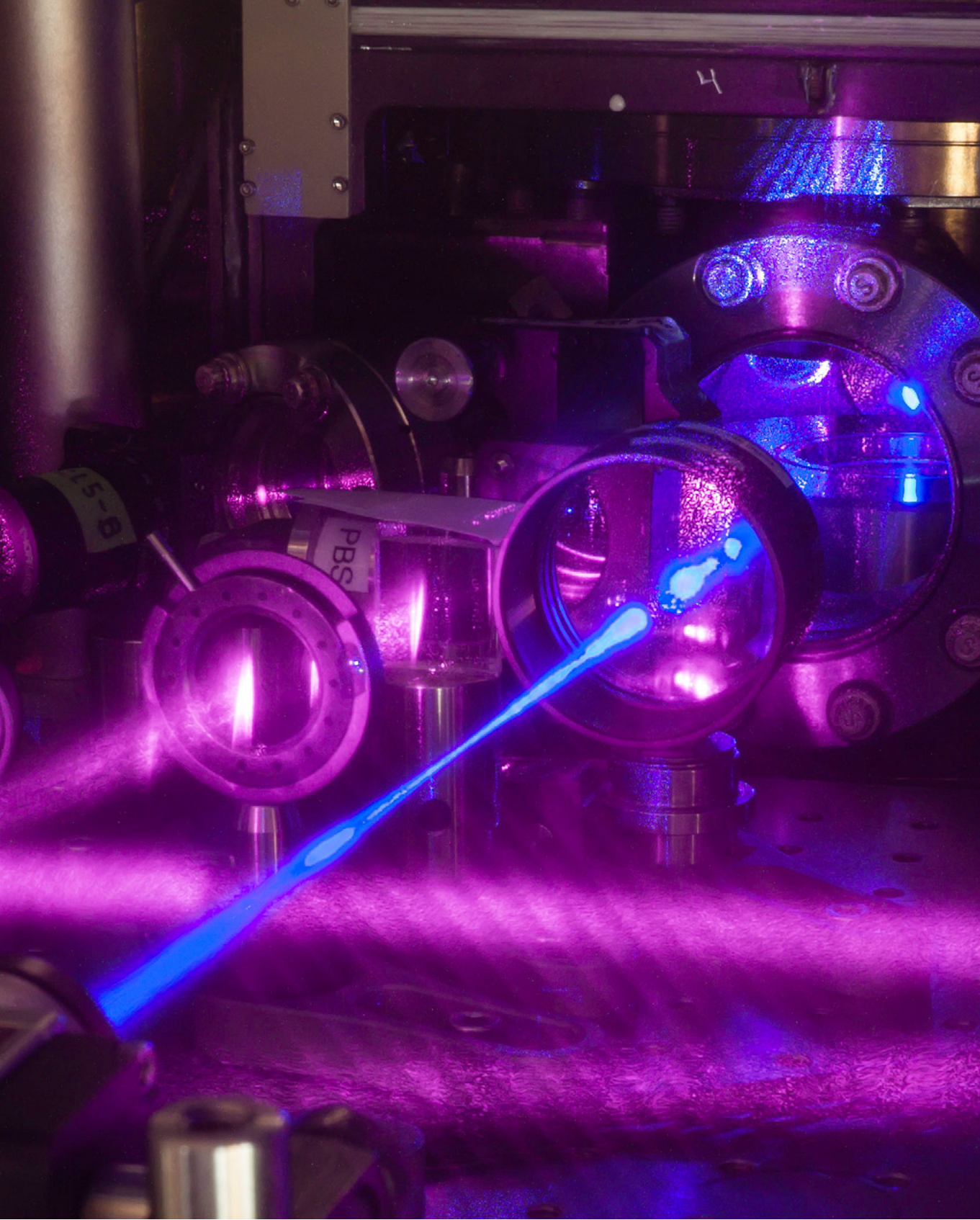
5G

Este gran aumento del número de dispositivos conectados a internet apremia el desarrollo del 5G, la quinta generación de comunicaciones móviles, que ofrecerá una mayor velocidad y una menor latencia en la subida, tráfico y descarga de datos.

Un estudio publicado por Deloitte en 2018 reconocía los esfuerzos realizados por países como Estados Unidos, Corea del Sur, Japón o Alemania pero consideraba que China, por la inversión realizada en infraestructura y torres, está a la cabeza del desarrollo y adopción de redes 5G. Este estudio también revela que, desde 2015, China Tower, la mayor compañía de torres de telecomunicaciones del mundo, ha invertido 17,7 billones de dólares en capital y añadido más de 350.000 puntos de infraestructura en China [120].

Muchos de los actores trabajando en el desarrollo de redes 5G ya se están enfocando en hacerlas *quantum-safe*, es decir, resistente a la computación cuántica y su capacidad de *hacking* de las telecomunicaciones actuales. Entre ellos, cabe destacar el trabajo de la compañía surcoreana SK Telecom. Ya en 2017, en el Mobile World Congress en Barcelona firmaron un acuerdo con la compañía alemana Deutsche Telekom para “garantizar telecomunicaciones seguras en la era cuántica” [121] y otro acuerdo con Nokia para “trabajar conjuntamente en criptografía cuántica” [122]. En el mismo congreso un año después, en febrero de 2018, se anunciaba una inversión de 65 millones de dólares por parte de SK Telecom en la compañía suiza líder en manufacturación de tecnología cuántica para criptografía IDQuantique [123].

Estas alianzas han dado ya sus frutos; en junio de 2018 se anunció [124] la realización de pruebas que incorporaban sistemas de criptografía cuántica -generadores cuánticos de números aleatorios y protocolos de criptografía simétrica cuántica- sobre la red de pruebas de Deutsche Telekom en Alemania [125,126]. Unos meses después, en septiembre de 2018, se reportó la realización de pruebas satisfactorias de interoperabilidad entre los sistemas de criptografía asimétrica de IDQuantique y la solución de Transporte



Reloj atómico tridimensional (3D) cuántico de gas perteneciente a JILA consistente en una rejilla de luz formada por tres pares de haces de luz. Se han utilizado dos tablas para configurar los componentes ópticos alrededor de una cámara de vacío. Aquí se muestra la tabla superior, donde están montados lentes y otros elementos ópticos. Un haz láser azul excita una nube de átomos de estroncio con forma cúbica localizados detrás de la ventana circular en medio de la tabla. Los átomos de estroncio tienen una fluorescencia fuerte cuando son excitados con luz azul. Crédito: G.E. Marti/JILA.

Óptico Seguro de Nokia [127] sobre la red comercial de telecomunicaciones de SK Telecom en Seúl, para conectar datos reales en producción en Corea, entre los distritos de Bundang y Jung-gu [128].

En Corea del Sur, además, SK Telecom, KT y LG Uplus han acordado trabajar de forma colaborativa y no competitiva en el desarrollo de una infraestructura 5G para el país [129]. De manera paralela, estos tres grandes de las telecomunicaciones están asesorando a la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), la agencia de las Naciones Unidas responsable de las tecnologías de información y comunicación, en la redacción de borradores [130] que establezcan estándares para poder construir redes de telecomunicaciones que incorporen 5G y criptografía cuántica que sean interoperables a nivel mundial. Este tipo de estándares son fundamentales para que las distintas iniciativas alrededor del mundo sean escalables e interoperables.

Cambiando de continente, la nueva compañía estadounidense Quantum Xchange está desarrollando la primera red comercial con criptografía cuántica de Estados Unidos [131] que “conectará los mercados financieros de Wall Street con centros de respaldo en Nueva Jersey, permitiendo mantener información confidencial segura” [132]. Esta compañía de telecomunicaciones llegaba este año a un acuerdo con SK Telecom por valor de 8.9 millones de dólares [133] para que le proveyese sus sistemas de criptografía cuántica.

IMPRESIÓN 3D

La fabricación de sensores cuánticos está a su vez relacionada con la impresión 3D, consistente en la construcción de objetos tridimensionales mediante la deposición de material en capas. En los últimos años se han realizado grandes avances en la preparación, el control y la medida de gases atómicos permitiendo desarrollar sensibilidades metrológicas sin precedentes que posibilitan la medición de campos gravitatorios y magnéticos con mucha más precisión. Esto tiene aplicaciones como escáneres biomédicos, mapeo subterrestre no invasivo o navegación GPS [134,135].

Para la fabricación de sensores cuánticos portables que ofrezcan estas posibilidades es necesaria la producción eficiente y robusta de los mismos. Distintos grupos de trabajo han venido utilizando la técnica de manufacturación aditiva -conocida también como impresión 3D- para la fabricación de trampas atómicas, cámaras de vacío y apantalladores magnéticos [136,137] que son de enorme utilidad en campos como la metrología y los sensores cuánticos.



TECNOLOGÍAS CUÁNTICAS

Una oportunidad transversal e interdisciplinar
para la transformación digital y el impacto social

IMPACTO SOCIAL POR SECTORES



IMPACTO SOCIAL POR SECTORES

A lo largo del documento hemos hablado con detalle de la información cuántica y de la computación cuántica, pero ya en la introducción mencionábamos que estos dos campos, si bien quizás los más disruptivos, no eran los únicos dentro de las nuevas tecnologías cuánticas, entre los que también se encuentran los simuladores cuánticos, la óptica cuántica, la metrología cuántica, los relojes atómicos o los sensores cuánticos. El conjunto de estas nuevas tecnologías, que serán la base de la era cuántica que está a la vuelta de la esquina, cambiarán notablemente la vida de las personas tanto directa como indirectamente. Sectores y ramas como medicina, biología, genética, educación y trabajo, economía y finanzas, agricultura, transporte o meteorología dispondrán de una nueva generación de herramientas tecnológicas cuánticas altamente disruptivas.



COMPUTACIÓN CUÁNTICA

La computación cuántica es la tecnología cuántica más conocida popularmente por su potencial para pulverizar la capacidad computacional disponible en el presente, con aplicaciones en prácticamente todos los campos imaginables. Desde el año 2000, universidades y grandes compañías tecnológicas como IBM, Google, Microsoft o Rigetti han ido batiendo el récord del computador cuántico con un mayor número de qubits, que actualmente -a principios de 2019- ostenta Google con 72. Si bien se han resuelto pequeños problemas a modo de prueba, aún ninguno ha sido con ventaja frente a la computación digital o clásica, lo que se conoce como supremacía cuántica y se espera que ocurra inminentemente. Distintos expertos consideran que en el plazo de 10 años se tendrán computadores cuánticos suficientemente robustos para realizar hitos como romper todos los algoritmos de criptografía -asimétrica- actuales de manera eficiente.



INFORMACIÓN CUÁNTICA

La información cuántica es el campo encargado de estudiar la cuantificación, almacenamiento y transferencia de información cuánticamente. En este campo se encuentra la criptografía cuántica, que ofrecerá una manera completamente segura de proteger información y datos incluso ante la computación cuántica, y fue testeada con éxito en producción hace ya más de 10 años. En Suiza, por ejemplo, llevan desde 2007 encriptando cuánticamente la información de las votaciones nacionales entre el centro de recuento y el de almacenamiento. China, a la cabeza en este campo, lanzó en 2016 el primer satélite que posibilitaba telecomunicaciones intercontinentales cuánticamente encriptadas, como demostraron con una videollamada de una hora y media de duración con Austria en 2017, y alberga una red comercial terrestre cuántica de más de 2000 km de longitud. Se espera que a principios de la próxima década haya una red de telecomunicaciones cuánticas entre Asia y Europa, y que para 2030 sea global.



SIMULADORES CUÁNTICOS

Un simulador cuántico es un sistema físico cuántico que puede ser preparado o manipulado de manera que permita estudiar propiedades de un sistema complejo clásico o cuántico, bien porque lo reproduce a menor escala y de manera controlada o bien porque puede trabajar de manera eficiente con la función matemática que describe su dinámica. Hay distintos tipos y permiten resolver problemas inabordables con computación clásica. A diferencia de un computador cuántico, no son universales, esto es, no pueden resolver “cualquier problema resoluble”. Están programados para abordar problemas o situaciones específicas.



RELOJES ATÓMICOS

Los relojes atómicos miden el tiempo a partir de procesos microscópicos que ocurren en la naturaleza con una periodicidad extremadamente alta, en contraste con los relojes clásicos, que se basan en la periodicidad de procesos mecánicos mucho menos precisos. Desde 1967 se define un segundo como el tiempo que transcurre durante 9.192.631.770 oscilaciones de un átomo de ¹³³Ce. La frecuencia de resonancia de átomos iguales, en este caso de átomos de Cesio, es siempre la misma y no depende del entorno. Gracias a este fenómeno, ya se han construido relojes atómicos con precisiones tales que si dos relojes hubiesen sido creados en el *Big Bang*, hoy en día no habrían llegado a desfasar ni un segundo entre ellos.



METROLOGÍA CUÁNTICA

La metrología cuántica consiste en el estudio del uso de sistemas físicos con propiedades cuánticas, como el entrelazamiento, que permitan realizar medidas de gran precisión y sensibilidad. De nuevo, este campo tiene gran importancia para la información, comunicación y criptografía cuántica.



ÓPTICA CUÁNTICA

La óptica cuántica es el campo que trata los procesos y fenómenos cuánticos que ocurren a nivel microscópico en la interacción de fotones con materia. Es esencial para los campos de la información, comunicación y criptografía cuántica pues sienta la base del trabajo con fotones. También permite la fabricación de todo tipo de sensores de luz de gran precisión, más manipulables, de menor tamaño y menor coste que son de gran utilidad en diversos procesos industriales.



SENSORES CUÁNTICOS

Los sensores cuánticos son aquellos que explotan propiedades cuánticas en sistemas físicos para conseguir alta sensibilidad y resolución. Como ahora discutiremos, tienen grandes aplicaciones en medicina. En este grupo se encuentra el campo conocido como *quantum imaging* consistente en el procesamiento cuántico de imágenes, que tiene entre sus productos cámaras de muy alta sensibilidad de gran utilidad por ejemplo para vehículos autónomos.



IMPACTO EN MEDICINA, BIOLOGÍA Y GENÉTICA

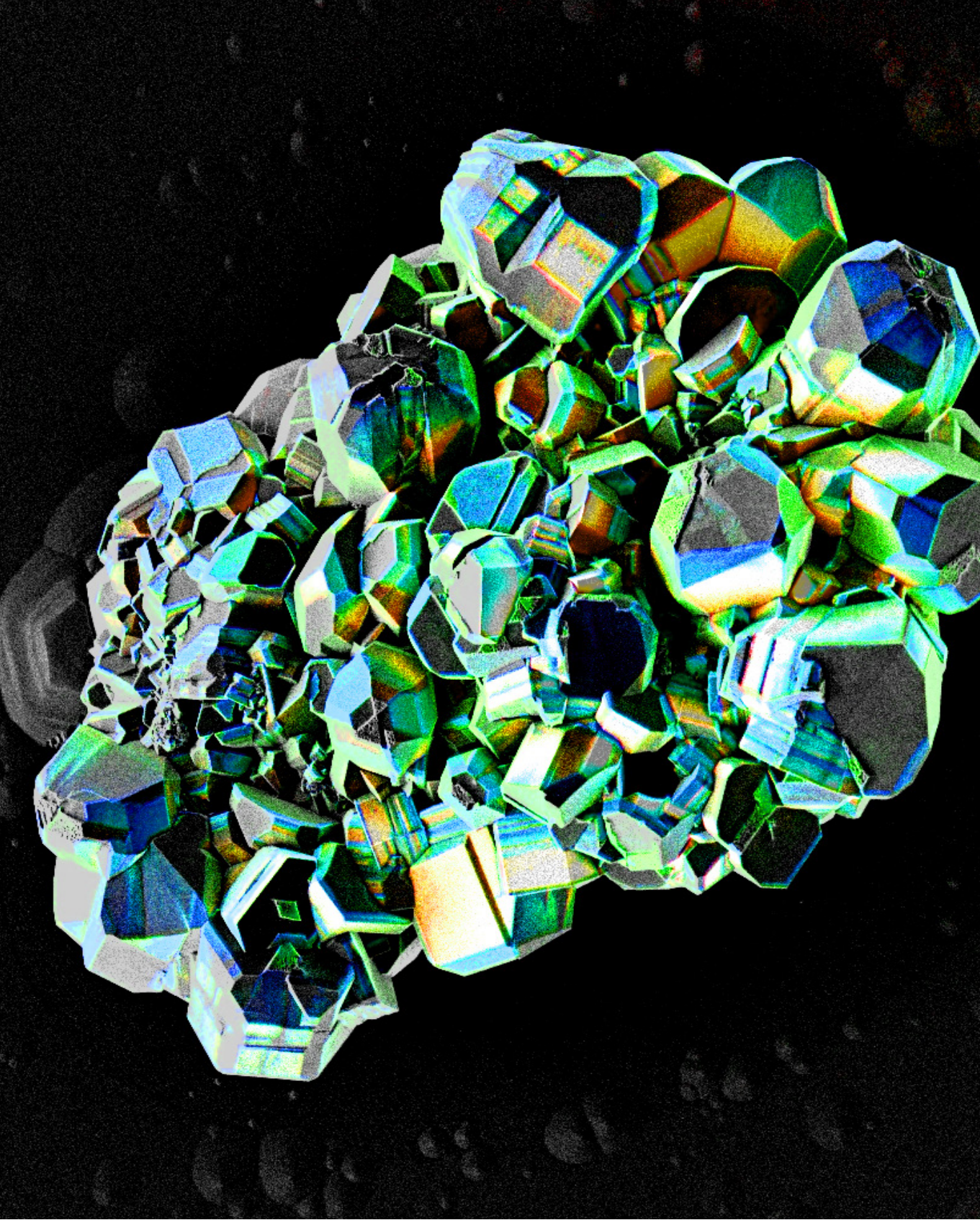
La sanidad, la medicina y la biología ya saben lo que es beneficiarse de tecnologías cuánticas. Las imágenes por resonancia magnética, que permiten detectar tumores y otras patologías de manera no invasiva, o el láser, utilizado en múltiples tipos de cirugías de gran precisión, son dos ejemplos de tecnologías cuánticas que llevan décadas utilizándose de manera exitosa [138,139]. Con las nuevas tecnologías cuánticas, en los próximos años se abrirá la puerta a técnicas y procesos que con la tecnología actual son inalcanzables.

La **simulación y la computación cuántica** tienen potencial para poder **reproducir la interacción y el efecto de una medicina sobre un determinado organismo**, suponiendo un salto disruptivo en el diseño de medicamentos; hoy en día es imposible simular con computadores clásicos la dinámica de un sistema molecular simple¹⁴, por lo que el testeo de medicamentos supone en la mayoría de los casos años de pruebas en animales y seres humanos a lo largo de las fases de descubrimiento, clínica y pre-clínica [140].

Por su parte, **la óptica cuántica** ofrecerá grandes aplicaciones biomédicas. La rama de la óptica cuántica de plasmones -cuasipartículas correspondientes a excitaciones de plasma- permite realizar estudios y mediciones muy precisas de la dinámica de células vivas. Esto no solo posibilita la realización de nano-espectroscopias no invasivas sino que también permite **perturbar, manipular y, por tanto, controlar organismos vivos a nivel molecular**. Las aplicaciones en diagnóstico molecular, medicina de precisión y nano-biología son incontables [141-143]. En el instituto de investigación nacional japonés *Quantum and Radiological Science and Technology* (QST) **ya están utilizando técnicas no invasivas que les permiten detectar un tumor sólido en media hora**, y son capaces de mapear la zona a nivel molecular determinando el tamaño y propiedades de las nano-plataformas que han de ser enviadas para conseguir el mejor tratamiento posible, así como predecir su eficacia terapéutica". [144]

En 2017, la consultora internacional Accenture, la compañía de software cuántico 1Qbit y la firma de biotecnología Biogen iniciaron una colaboración para **“diseñar la primera aplicación cuántica de comparación molecular** con potencial para mejorar de manera

14. A la hora de simular procesos microscópicos como por ejemplo la interacción de un medicamento con un organismo, los computadores actuales no son capaces de procesar eficientemente las interacciones entre átomos y moléculas que tienen lugar. Esto hace que la dificultad para realizar simulaciones en la actualidad sea exponencial con respecto al número de moléculas -si aumentamos el número de moléculas, el número de pasos a procesar por la computadora aumenta exponencialmente-, causando que se tarde varios años en simular sistemas de pocas moléculas, y haciendo inviable la simulación de procesos complejos para realizar avances médicos. En cambio, con la computación cuántica la dificultad se reduce a polinómica -es decir, al aumentar el número de moléculas, el número de pasos a realizar aumenta a un ritmo similar-, permitiendo que estas simulaciones sean realizables.



El nitruro de indio-galio es una aleación semiconductora que emite luz cuando se irradia con partículas energéticas. Durante los procesos MOVPE ha crecido accidentalmente. El brillo corresponde a su imagen SEM estándar, mientras el color entre capas aparece debido a la luz emitida bajo el haz de electrones. Los canales azul y verde son, de manera aproximada colores naturales, mientras el rojo se corresponde con la emisión ultravioleta. La imagen demuestra que las estructuras InGaN/GaN son altamente anisotrópicas al igual que sus propiedades de cátodoluminiscencia.

significativa el diseño molecular avanzado con el objetivo de **acelerar el desarrollo de medicinas para problemas neurológicos complejos como esclerosis múltiple, Alzheimer, Parkinson o la enfermedad de Lou Gehrig** [145].

Otra aplicación tangencial es la utilización de criptografía cuántica para asegurar datos médicos. Según IDQuantique, líder mundial de manufacturación para venta de hardware para criptografía cuántica, en la primera mitad de 2016 fueron robados los registros médicos de más de 30 millones de pacientes en un total de 263 brechas de seguridad ante ciberataques, que tomaron 233 días en promedio en ser descubiertas y otros 111 en ser comunicadas [146].

En definitiva, las tecnologías cuánticas están llamadas a permitir un descubrimiento y producción de medicamentos mucho más rápido y eficaz, encontrar la cura a enfermedades hoy en día incurables, un mayor entendimiento de la biología y el genoma de los seres vivos, y una mayor protección ante ciberataques para robar datos de pacientes, entre otras muchas aplicaciones.



IMPACTO EN EDUCACIÓN Y TRABAJO

Como mencionábamos antes, estamos en una era de rápida digitalización, lo que genera una gran demanda de muchos perfiles tecnológicos en todos los sectores. Dado que en la mayoría de las regiones del mundo, especialmente en América Latina y el Caribe, las carreras científicas o técnicas son vistas en muchas ocasiones como muy complicadas, que no hay una buena formación -o simplemente una formación- tecnológica o computacional de base en las escuelas, que la oferta diversa de programas de estudios de grado o máster en carreras con potencial tecnológico evoluciona mucho más lentamente de lo que el mercado demanda y que desde las instituciones no se realiza una labor concienciadora adecuada, hay un número alarmante de vacantes de trabajo relacionadas con tecnología en todo el planeta. Datos de la consultora Allen & York revelan que solo en Reino Unido habrá 800.000 en 2020 [147]. Un estudio del Banco Mundial titulado *Los trabajos del mañana* destaca la necesidad de apostar por la formación y creación de puestos de trabajo en tecnología en la región para poder mantener los niveles de productividad y prosperidad crecientes y los niveles de pobreza decrecientes en América Latina y el Caribe [148].

Con respecto a las tecnologías cuánticas en particular, el “problema” es aún mucho mayor. Si bien es posible acceder a distintos puestos de trabajo tecnológicos habiendo estudiado diferentes carreras, **las tecnologías cuánticas requieren un entendimiento de la física que raramente se puede adquirir sin haber estudiado Física**. Es por eso que esta demanda ya existente y no cubierta de personal con conocimientos de física cuántica solicitado en ciberseguridad, empresas de software y hardware o consultoras, entre otros, será aún más difícil de satisfacer que el promedio en tecnología. Según un reporte publicado en 2018 por BBCReport, el mercado comercial en tecnologías cuánticas presentará una tasa anual compuesta de crecimiento (CAGR por sus siglas en inglés) del 37,3% hasta 2022, alcanzando un valor de 161 millones de dólares, y **un CAGR del 53% entre 2022 y 2027, alcanzando un valor de 1,3 billones de dólares** [149].



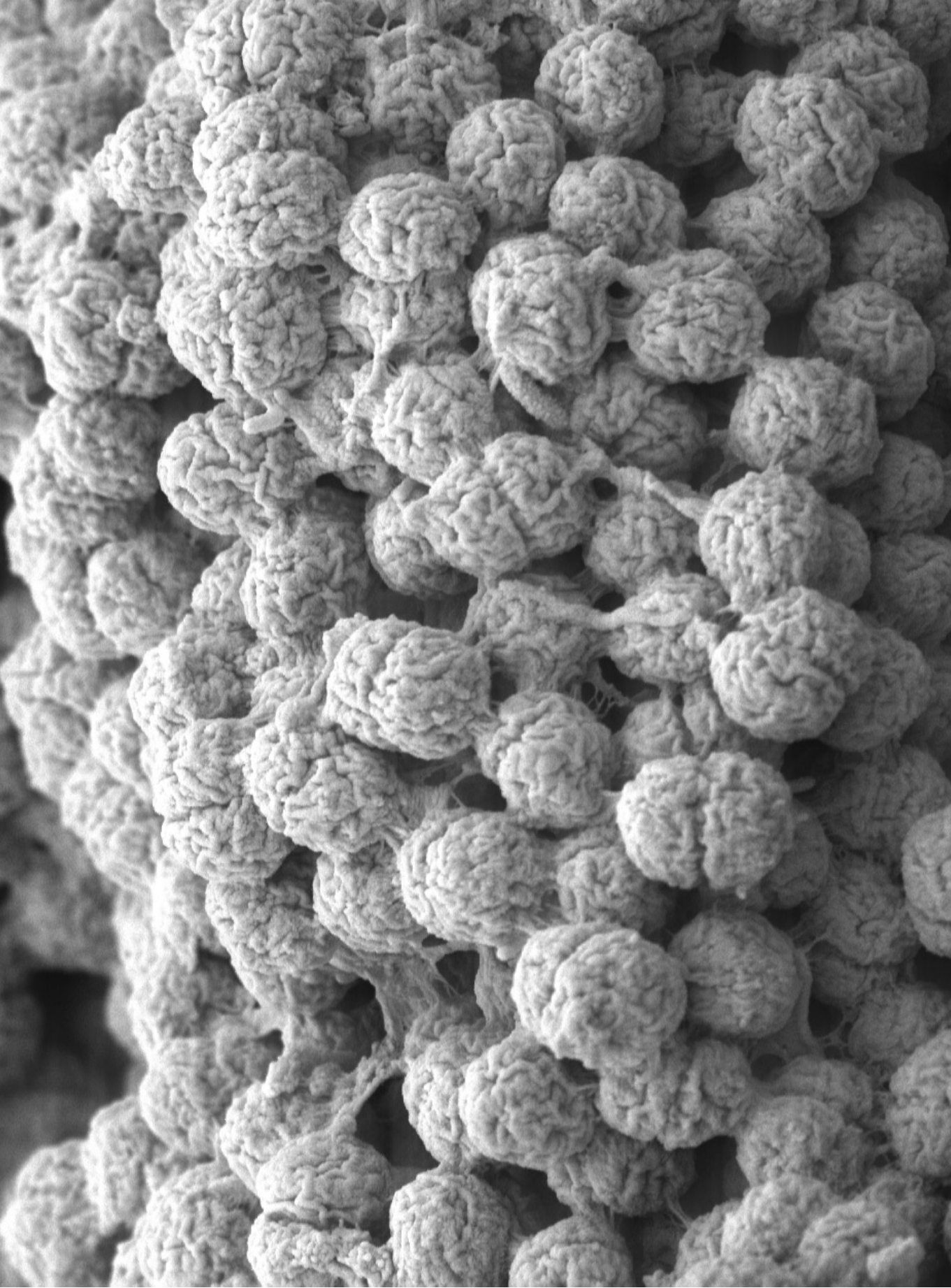
IMPACTO EN ECONOMÍA Y FINANZAS

Otra área en la que la era cuántica provocará cambios es la de la economía y las finanzas. **La capacidad de los computadores y los simuladores cuánticos para resolver problemas complejos y procesar números enormes de posibilidades con rapidez y eficiencia permitirá construir, simular y mejorar modelos financieros utilizando algoritmos cuánticos.** Tal y como comentábamos en la sección en la que hablamos de esta tecnología, la computación cuántica no evalúa distintas opciones una a una como la computación actual o clásica, sino que las evalúa todas a la vez, ofreciendo una reducción exponencial, en muchos casos, del tiempo y los recursos de procesamiento. **Adicionalmente, ofrece la posibilidad de introducir aleatoriedad verdadera cuando así se requiera para la construcción de dichos modelos.**

Simuladores como los *quantum annealers* ya están operando en el mercado y permiten tratar de manera eficiente problemas reales con un gran número de variables. En términos generales, su desempeño consiste en encontrar la función que describe matemáticamente ese problema real -modelizarlo- y minimizarla, encontrando los valores óptimos de las variables.

Un ejemplo de la aplicabilidad de los *quantum annealers* consiste en la predicción de crisis financieras. Un estudio publicado en 2017 prueba matemáticamente que predecir una crisis financiera es un problema intratable computacionalmente, ya que pertenece a la clase de complejidad NP completo [150]. Concretamente, prueban que incluso en redes financieras simples en las que “el regulador tiene toda la información sobre la entera estructura de la red y la única incertidumbre es acerca de qué activos financieros perderán valor, calcular el número de instituciones que pueden quebrar en una red es NP-completo”. Este año, los investigadores R. Orús y E. Lizaso, socios de Entanglement Partners, y S. Mugel, los tres miembros de la Quantum World Association (QWA), demostraron que “los valores de mercado de equilibrio de los activos de entidades financieras después de una crisis espontánea pueden ser calculados por *quantum annealers* [...], proveyendo así una nueva vía con potencial para predecir crisis financieras” [151].

Otra aplicación cuántica en este campo la ofrecen los relojes atómicos. Actualmente, la marca de tiempo de las transacciones económicas, cuya precisión y sincronización es fundamental sobre todo en las de alta frecuencia, depende del sistema global de navegación por satélite (GNSS por sus siglas en inglés), de redes computacionales y también ya de relojes atómicos locales, según un reporte de la Unión Europea [152], que además encuentra esencial regular y utilizar más ampliamente en este y otros ámbitos por la gran precisión que ofrecen.





IMPACTO EN ENERGÍA Y AGRICULTURA SOSTENIBLE

El ejemplo más relevante de los beneficios de las tecnologías cuánticas en energía y agricultura lo encontramos en la fabricación de amoníaco, una sustancia esencial para la fabricación de fertilizantes cuya producción consume el 2% de la energía mundial al año [153]. Según el informe anual de la Asociación Internacional de Fabricantes de Fertilizantes (IFA por sus siglas en inglés), en 2018 el consumo de fertilizantes alcanzó los 187 millones de toneladas, cuya demanda creciente motivará la inversión de 98.000 millones de dólares entre 2018 y 2022 para construir 60 nuevas unidades de producción que permitirán producir 78 millones de toneladas más al año [154]. En América Latina y el Caribe, la industria petroquímica está liderada por Brasil, México, Venezuela, Trinidad y Tobago, y Argentina [155,156].

El amoníaco es esencial para la producción de fertilizantes. El proceso de producción del mismo, conocido como Haber-Bosch en honor a sus inventores a principios del siglo XX, consiste en la reacción de combinación de hidrógeno y nitrógeno y requiere de la disociación del nitrógeno, que solo se consigue en **condiciones extremas de presión y temperatura, lo que consume del orden del 2% de la energía mundial** [157].

Ya es conocida una nueva forma de conseguir amoníaco a temperatura ambiente a partir de la encima nitrogenasa [153]. Para ello, se necesita primero entender a nivel molecular cómo se produce la síntesis de amoníaco, lo que es imposible con computadores clásicos pero se vuelve viable con computadores cuánticos. **Esto permitiría ahorrar un 2% de la energía mundial, reducir el impacto medioambiental negativo de estos procesos y abaratar el precio de multitud de alimentos.**

El sector energético se verá también directamente beneficiado por la capacidad de computadores y simuladores cuánticos para procesar volúmenes enormes de datos e información, lo que permitirá una distribución mucho más eficiente de los recursos energéticos, abaratando el precio de la electricidad.



OTROS IMPACTOS

Los anteriores no serán los únicos sectores que se verán beneficiados con la llegada de las tecnologías cuánticas.

En transporte, por ejemplo, se podrá modelizar en tiempo real la circulación tanto de vehículos como de ciudadanos haciendo uso de las cantidades enormes de datos que hoy en día ya están captando aplicaciones como Waze o Google Maps. Los simuladores cuánticos serán capaces, mediante la búsqueda de mínimos en estos modelos matemáticos,

de proponer la ruta óptima con mayor precisión, **coordinar los semáforos para habilitar una vía de emergencia en caso necesario, simular catástrofes y analizar las mejoras necesarias para evitarlas o minimizar sus consecuencias**, y un largo etcétera. Con la llegada de los vehículos autónomos que son solo el aperitivo de la industria del transporte del futuro, sin duda disponer de esta capacidad cuántica de procesamiento será esencial.

Presenciaremos también grandes cambios en meteorología, donde la simulación cuántica permitirá abordar la complejidad del clima de forma mucho más precisa, con potencial para predecir catástrofes naturales.



TRADING CUANTITATIVO

Mejora del entendimiento de variables y fenómenos correlacionados y su impacto en los mercados financieros



MACHINE LEARNING

Mejora en los procesos de aprendizaje de la máquina y capacidad para calcular escenarios, alternativas y matemáticas más complejas



OPTIMIZACIÓN DE RUTAS

Gracias a la capacidad de evaluar múltiples escenarios mediante paralelismo cuántico



PERSONALIZACIÓN DE DROGAS

Habilidad de desarrollar mejores drogas en base a un mejor entendimiento de la formación de las moléculas y la genómica



SEGURIDAD POST-CUÁNTICA

Resistencia criptográfica a la computación cuántica gracias a la habilitación de aleatoriedad verdadera y a la modificación de las claves al ser observadas por espías, permitiendo detectar a los mismos



SÍNTESIS DE NUEVAS MOLÉCULAS

Basado en la mejora en la capacidad para entender reacciones químicas y simular interacciones atómicas



PREDICCIONES METEOROLÓGICAS

Capacidad de entender fenómenos atmosféricos gracias al aumento de la capacidad computacional



NUEVOS MATERIALES

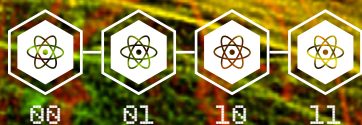
Desarrollo de nuevos materiales gracias a la capacidad para simular interacciones moleculares y propiedades físicas



TECNOLOGÍAS CUÁNTICAS

Una oportunidad transversal e interdisciplinar
para la transformación digital y el impacto social

PROGRAMAS Y ESTRATEGIAS POR PAÍS



PROGRAMAS Y ESTRATEGIAS POR PAÍS

El potencial que tienen las tecnologías cuánticas y la nueva revolución que está al llegar no son desconocidos para las primeras potencias mundiales y las principales empresas tecnológicas, que en los últimos años han comenzado a realizar inversiones billonarias en el entendimiento, la exploración y el control de las mismas para situarse en la cabeza de su adopción y explotación.



CHINA

China es reconocida internacionalmente como la primera potencia a nivel de gobierno en la investigación y el desarrollo de tecnologías cuánticas. No en vano, ha dispuesto un presupuesto 10 veces mayor que sus competidores más cercanos -Estados Unidos y la Unión Europea-.



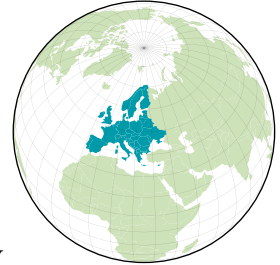
Como comentábamos en el bloque de Información Cuántica y detallamos en el Anexo C, China ha estado a la cabeza en el desarrollo de redes de telecomunicación cuántica tanto terrestres como espaciales. El lanzamiento en 2016 del satélite MICIUS para la realización de telecomunicaciones Tierra-espacio y espacio-Tierra en el marco del programa QUESS (*Quantum Experiments at Space Scale*) supuso un hito histórico a nivel mundial, y permitió realizar el 17 de septiembre de 2017 la primera videollamada intercontinental cuánticamente encriptada, entre las Academias de Ciencia de China y Austria [30]. También en 2017 se realizó QKD a una distancia de hasta 719 km entre el laboratorio espacial Tiangong-2 y la estación en tierra Nanshan [158]. China prevé lanzar otros 10 satélites que permitan tener en 2020 una red de comunicaciones intercontinental entre Europa y Asia, que se expanda hasta ser una red mundial en 2030 [48]. Según la revista del MIT, esta clarividencia responde al liderazgo de Jian-Wei Pan, el físico cuántico que denominan el “Padre de la Cuántica en China” [159].

En cuanto a redes terrestres, de entre las distintas iniciativas recogidas en el Anexo C cabe destacar la liderada por la Universidad de Ciencia y Tecnología, que conecta cuánticamente cuatro ciudades con una fibra óptica de 2000 km desde Beijing hasta Shanghái, siendo la mayor red cuántica terrestre conocida de telecomunicaciones cuánticas [60].

Adicionalmente, en 2017 se anunciaba la construcción del Laboratorio Nacional para Ciencias de la Información Cuántica, que ocuparía 37 hectáreas -370.000 metros cuadrados- y estaría ubicado en Hefei. El presupuesto para el mismo, cuya construcción se demoraría unos 2 años y medio estando por tanto operativa en 2020, es de 76 billones de yuan, equivalente a 11.5 billones de dólares [161,162].



UNIÓN EUROPEA



A nivel de la Unión Europea, la concienciación sobre la necesidad de invertir en el estudio, desarrollo y adopción de tecnologías cuánticas queda establecida con la publicación del *Quantum Manifesto* [163] en mayo de 2016, un documento breve apoyado por más de 3.400 representantes de la academia y la industria de prácticamente la totalidad de los países europeos. Los objetivos de esta iniciativa eran (i) promover una industria cuántica europea competitiva para posicionar a Europa como líder a nivel global (ii) expandir el liderazgo y la excelencia científica europea en investigación cuántica (iii) convertir a Europa en una región dinámica y atractiva para negocios innovadores en tecnologías cuánticas y (iv) beneficiarse de los avances en tecnologías cuánticas para proveer mejores soluciones en campos como energía, salud, seguridad y medioambiente. Con este propósito, el Manifiesto sugiere un conjunto de 6 actividades clave:

- Apoyar el desarrollo de actividades científicas relacionadas con tecnologías cuánticas.
- Crear un ecosistema favorable de innovación y negocio para tecnologías cuánticas.
- Facilitar un nuevo nivel de coordinación entre academia e industria para llevar productos del laboratorio al mercado.
- Crear una nueva generación de profesionales europeos en tecnologías cuánticas enfocando la educación en la intersección de ciencia, ingeniería y negocio.
- Coordinar inversiones públicas y estrategias en tecnologías cuánticas a nivel europeo.
- Promover el involucramiento de regiones miembro que no tienen actualmente programas fuertes de investigación en tecnologías cuánticas.

El documento recalca la “importancia de las tecnologías cuánticas y la necesidad de lanzar una iniciativa europea ambiciosa para asegurarse de que Europa permanezca en la vanguardia de estas tecnologías y asuma un rol de liderazgo en la futura explotación comercial”.

A raíz del Manifiesto comenzó a crearse el tercer programa *flagship* de la Unión Europea, tras el Graphene Flagship y el Human Brain Program, esta vez para tecnologías cuánticas y bajo el nombre Quantum Flagship. El programa fue inaugurado finalmente en octubre de 2018 en Viena [164] y cuenta con un presupuesto de 1 billón de euros -equivalente a 1.15 billones de dólares- a invertir durante 10 años. Actualmente se puede encontrar en su portal información concerniente a llamados a propuestas e información sobre conferencias, además de material divulgativo donde se desmitifican algunas ideas



erróneas sobre las tecnologías cuánticas y se promociona lo que ellos denominan la Segunda Revolución Cuántica.¹⁵

Por su parte, la Agencia Estatal Europea (ESA, por su nombre en inglés), cuenta con distintas iniciativas. Una es la conocida como Space-QUEST (*Quantum Entanglement for Space Experiments*), que propone situar un transmisor en el ala externa del módulo Columbus en la Estación Espacial Internacional (ISS por sus siglas en inglés) [165,166]. Otra es Eutelsat Quantum, “una misión pionera que influenciará como serán los satélites de telecomunicaciones en Europa”, en el marco de la cual se pondrá en órbita un satélite para la realización de telecomunicaciones cuánticas Tierra-espacio y espacio-Tierra en la segunda mitad de 2019 [167].



ESTADOS UNIDOS



En los últimos años han sido varias las voces que urgían el establecimiento de un programa para coordinar el estudio y desarrollo de tecnologías cuánticas a nivel gubernamental en los Estados Unidos, al estilo de los que hemos estado discutiendo en China y Europa. Entre ellas destacaba la visión, por ejemplo, del reelegido representante por Texas en el Congreso, William Hurd, que ostenta también el cargo de Director del Subcomité de Tecnologías de la Información [168], que ha venido manteniendo la posición de que “aquel que consiga el primer computador cuántico robusto será capaz de anular toda la criptografía de los demás, y por eso China y Rusia están acumulando textos cifrados que eventualmente podrán descifrar” [169]. La revista del MIT publicaba en 2014 un artículo relativo a la carrera espacial para las telecomunicaciones cuánticas destacando el liderazgo de China y manifestando que “Los planes de Estados Unidos son mucho menos claros. Esto puede deberse a que el trabajo se está haciendo de manera privada. En caso contrario, están siendo muy lentos” [170].

A finales del año 2018 este movimiento demandado tuvo lugar [171,172], con la publicación de un documento resumiendo una estrategia nacional en Ciencias de Información Cuánticas [173] y el lanzamiento de la iniciativa *National Quantum Initiative Act* [174] que, tras ser aprobada por el senado, fue firmada por el Presidente D. Trump el día 21 de diciembre convirtiéndose en la Ley Pública 115-368 [175]. Esta legislación propone

15. La segunda revolución cuántica se refiere a esta era naciente en la que existe un número importante de tecnologías cuánticas nacientes de gran impacto esperado. La Primera Revolución Cuántica corresponde o bien a la etapa entre 1900 y 1930 en la que nace la Mecánica Cuántica y se comprende su valor y utilidad para describir el mundo microscópico, o bien al nacimiento de las primeras tecnologías cuánticas como los láseres, dependiendo del autor. En este documento nos mostramos en desacuerdo con el uso de esta denominación por la falta de consenso con respecto a cuál es la Primera Revolución Cuántica y por su falta de relación con la mal denominada Segunda, sea cual sea la que se considere la primera.

dedicar 1.3 billones de dólares para financiar investigación en tecnologías cuánticas en un esfuerzo en el que participarán el Departamento de Energía, el NIST, la Fundación Nacional de Ciencia, o la NASA, entre otros. Según Science, actualmente el gobierno invertía en torno a 250 millones de dólares al año en el campo cuántico que iban destinados principalmente a la Oficina de Investigación de la Armada, y este nuevo presupuesto irá a parar por primera vez a laboratorios, principalmente [176].

Esta ley establece el mandato de la “implementación de un Programa Nacional Cuántico por parte del Presidente para, entre otras tareas, establecer los objetivos y prioridades para un plan de 10 años que acelere el desarrollo de la ciencia de información cuántica -que definen como el almacenamiento, transmisión, manipulación o medida de información codificada en sistemas que pueden solamente ser descritos por las leyes de la Física Cuántica- y aplicaciones tecnológicas” [175].

Inicialmente el NIST ha de llevar a cabo actividades específicas en ciencia cuántica y organizar un taller para discutir el desarrollo de una industria en información y tecnología cuántica; la Fundación Nacional de Ciencia ha de llevar a cabo una investigación básica y un programa de investigación en información cuántica e ingeniería -tarea compartida con el Departamento de Energía-, así como otorgar becas para el establecimiento de Centros Multidisciplinarios para la Investigación y Educación Cuántica; y la Oficina de Ciencia ha de establecer y operar Centros de Investigación Nacionales.

A nivel privado la situación es muy diferente, puesto que distintas compañías estadounidenses han estado en la vanguardia del desarrollo de tecnologías cuánticas desde su inicio, especialmente en la computación cuántica.

IBM, bajo el liderazgo del reputado físico I. Chuang, conseguía allá por el año 2000 correr por primera vez el algoritmo cuántico de Grover [75] en un computador cuántico con 3 *qubits*, en colaboración con la Universidad de Stanford [8]; desde entonces ha estado aumentando el número de *qubits* de sus procesadores y en 2017 conseguía desarrollar el primer computador cuántico de 50 *qubits* [177]. Adicionalmente, tiene un computador cuántico de 20 *qubits* “abierto al público”, de manera que cualquier persona con acceso a internet puede enviarles un algoritmo y lo corren por tí, y un kit de desarrollo de software (SDK por sus siglas en inglés) denominado QISKit [178]. El 2019 ha empezado también con novedades, puesto que IBM ha sacado el primer computador cuántico comercial de 20 *qubits* bajo el nombre *Q System One* [179]; pese a tener una capacidad muy limitada, supone un gran paso en la carrera de la computación cuántica [180].

Otra gran multinacional estadounidense que ha apostado fuerte por la computación cuántica es Google, que finalizaba el 2018 siendo la compañía con el computador cuántico más potente en su poder; hito que conseguía en marzo al alcanzar los 72 *qubits* [181], desbancando así al computador de IBM de 50 *qubits*. También tiene un acuerdo con NASA para la exploración conjunta de los procesadores cuánticos que Google está desarrollando [182] y es miembro de una alianza con NASA y D-Wave en el marco de la cual en 2017 instalaban en uno de los centros de Google el *quantum annealer* de D-Wave de 2000 *qubits*, conocido como D-Wave 2000Q [183].

Rigetti, por su parte, ha venido desarrollando y dando acceso en su plataforma online a procesadores de 8 y 19 *qubits*, y en agosto de 2018 se comprometía al desarrollo de un computador cuántico de 128 *qubits* en los siguientes 12 meses [184,11]. En su plataforma ofrecen la posibilidad de “desarrollar y ejecutar programas cuántico-clásicos en un entorno virtual clásico conectado con su hardware cuántico” [185].

Intel también ha venido jugando un papel destacado colaborando con el instituto de investigación holandés QuTech, logrando desarrollar un procesador de 17 *qubit* en 2017 y uno de 49 en 2018 [186].

Un quinto actor que no puede dejar de mencionarse es Microsoft, que también va en busca del primer computador cuántico robusto pero con una arquitectura diferente, renunciando a los *qubits* superconductores que utilizan IBM, Google, Intel o Rigetti y que son más difíciles de escalar, y optando por un computador cuántico topológico. En su página web podemos encontrar también un Quantum Development Kit para empezar a programar algoritmos cuánticos, y la promesa de la provisión de servicios cuánticos en su plataforma de Azure [187,188].

Cabe también mencionar que la compañía estadounidense Quantum Xchange está desarrollando la primera red comercial con criptografía cuántica de Estados Unidos, según la propia compañía, que “conectará los mercados financieros de Wall Street con centros de respaldo en Nueva Jersey, permitiendo mantener información sensible segura” [189].

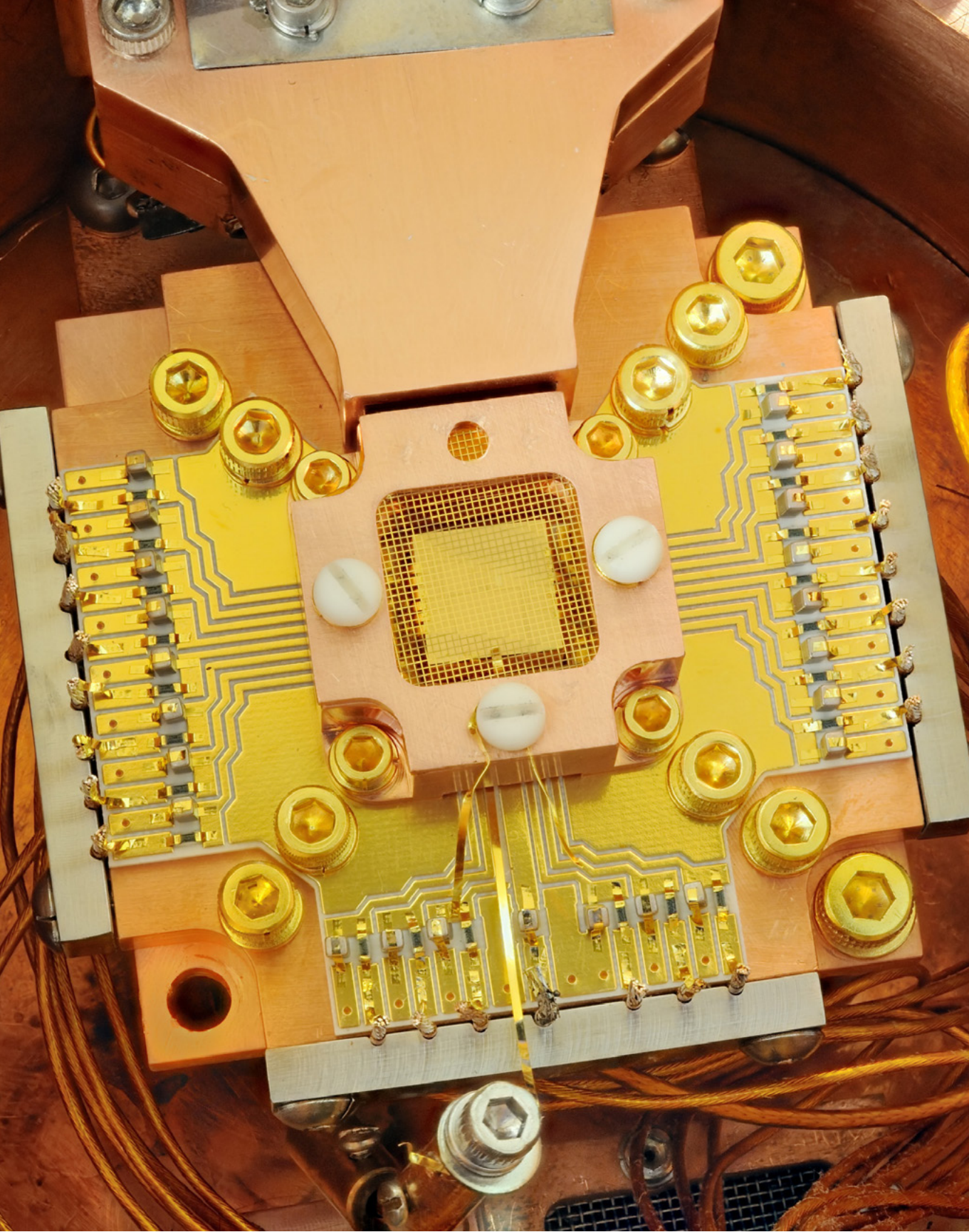


JAPÓN

Diferentes medios se hacían eco en 2017 del anuncio por parte del gobierno japonés del lanzamiento de un programa para unirse a la carrera de la computación cuántica, para el que dispondrían 30 billones de yenes, equivalente a unos 332 millones de dólares, en un plan de 10 años a comenzar en abril de 2018 [190].



Paralelamente, Japón ha mostrado un interés particular y el desarrollo de una red neuronal cuántica de gran interés (QNN por sus siglas en inglés). Un año después del anuncio oficial en octubre de 2016 por parte de la Agencia de Ciencia y Tecnología de Japón (JSP por sus siglas en inglés) [191], se revelaba el apoyo a NTT en el desarrollo de una QNN capaz de resolver problemas de optimización combinatoria, con aplicaciones sociales y médicas, entre otras. El prototipo consiste en una fibra óptica circular cerrada, un amplificador óptico especial (PSA por su nombre inglés) y un circuito electrónico (FPGA por su nombre en inglés). Un ejemplo de su capacidad puede verse en la resolución del problema conocido como *Max Cut* consistente en dividir personas en dos grupos evitando de la manera más eficiente posible las incompatibilidades entre parejas de ellos, dando lugar a dos grupos lo más compatibles posible. La red neuronal cuántica es capaz de resolver este problema para 2.000 personas con 20.000 incompatibilidades en 5 milisegundos con un coste energético de 1kW, en contraste con los 10KW que consumiría un computador cuántico [192-194].



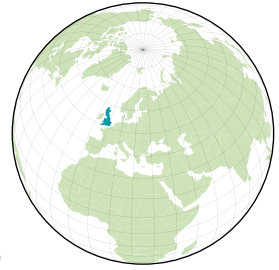
Físicos del NIST utilizaron este aparato para forzar dos iones de berilio (átomos eléctricamente cargados) a intercambiar las unidades de energía medibles más pequeñas en ambas direcciones, una técnica que puede simplificar el procesamiento de información en un computador cuántico. Los iones están atrapados con una separación de unos 40 micrómetros por encima de el chip cuadrado dorado en el medio. El chip está rodeado por un cable de cobre y oro para prevenir la acumulación carga estática. Crédito: Y. Colombo/NIST.

Japón también ha realizado grandes avances en el campo de las telecomunicaciones cuánticas, como se detalla en el Anexo C. Han desarrollado una red terrestre con seis nodos entre las ciudades de Koganei, Otemachi, Hakuson y Hongo con conexiones de hasta 90 km [195], y en 2017 realizaron telecomunicaciones Tierra-espacio utilizando un micro satélite conocido como *Small Optical Transponder* (SOTA) orbitando a una altitud de 600 km [196].



REINO UNIDO

Reino unido anunció en 2013 una inversión de 270 millones de libras, equivalente a 350 millones de dólares, para financiar durante sus primeros cinco años el programa *National Quantum Technologies Programme* con el objetivo de “crear una comunidad cuántica en el gobierno, en la industria y en la academia para situar a Reino Unido en una posición de liderazgo en el nuevo mercado multibillonario de las tecnologías cuánticas” [197].



El programa tiene como objetivo comenzar el desarrollo de aplicaciones en campos como defensa, comunicaciones seguras, tecnologías de la información, petróleo y gas, para después evolucionar a aplicaciones de mercado más generales, y ve aplicaciones en distintas industrias, mercados y sectores, entre las que destaca dispositivos cuánticos para medir el tiempo, sensores cuánticos de gravedad, sistemas cuánticos de posicionamiento, comunicaciones seguras cuánticas, dispositivos de detección de luz cuánticos y computadores cuánticos [198].

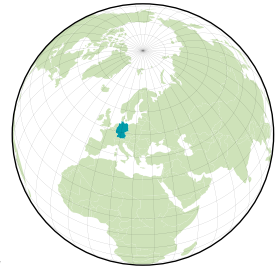
Actualmente están co-liderando el programa EPSRC, Innovate UK, BEIS, NPL, GCHQ, Dstl y KTN, y su visión tiene un importante enfoque académico. Ya se han invertido 120 millones de libras en 4 grupos de trabajo en, a saber, sensores y metrología [199], procesamiento cuántico de imágenes [200], tecnologías de la información cuánticas [201] y tecnologías de telecomunicaciones cuánticas [202] operativos desde 2014 y que cuentan con 17 universidades y 132 compañías bajo el liderazgo, en este caso, de las universidades de Birmingham, Glasgow, Oxford y York, respectivamente.

En un reporte publicado en 2015 por el *Quantum technologies Strategic Advisory Board* del programa, liderado por el profesor David Delpy, estimaban el desarrollo de prototipos comerciales como microscopios biológicos, aplicaciones espaciales para monitorización ambiental y predicción de terremotos o diagnóstico médica entre 2015 y 2025, y predecían la construcción de computadores cuánticos robustos a partir de 2025 [203].

Otra publicación de gran interés que debe su crédito al director de asesoría científica del gobierno, el profesor Sir M. Walport, estima que a largo plazo la industria de tecnologías cuánticas será comparable a la de componentes electrónicos, valorada en 240 billones de dólares [204].



ALEMANIA



Alemania se convertía en septiembre de 2018 en el país de la Unión Europea con la mayor inversión en tecnologías cuánticas, al aprobar para su iniciativa nacional QUTEGA [205] una financiación de 650 millones de dólares para un programa de 5 años entre 2018 y 2022 que buscará (i) expandir la cartera de investigación en tecnologías cuánticas, (ii) crear redes de investigación para nuevas aplicaciones, (iii) establecer proyectos emblemáticos para industrias competitivas, (iv) asegurar seguridad y soberanía tecnológica, (v) conformar la cooperación internacional e (vi) involucrar a la ciudadanía alemana [206].

De esta iniciativa han salido ya dos documentos estandarte en alemán, *Tecnologías Cuánticas: Fundamentos y Aplicaciones* [207] y *Tecnologías Cuánticas: Desde los fundamentos hacia el mercado* [208].

Paralelamente, distintos organismos alemanes, entre los que se encuentra el Instituto Max Planck y el Centro Aeroespacial Alemán (DLR por sus siglas en alemán) han cooperado para la realización en 2016 de su propio estudio experimental, en el que han testeado la transmisión de señales de fotones a 38.600 km de distancia entre la estación espacial transportable localizada para esta prueba en el Observatorio del Teide, Tenerife, y el satélite estacionario Alphasat I-XL [209].



AMÉRICA LATINA Y EL CARIBE



En América Latina y el Caribe ningún país ha apostado aún por la inversión directa en programas nacionales para la exploración y el desarrollo de tecnologías cuánticas.

S. Venegas, doctor en Física Teórica por la Universidad de Oxford y uno de los padres del área de la computación cuántica en México, tras haber fundado el grupo de investigación en procesamiento cuántico de imágenes del Instituto Tecnológico de Monterrey y haber impartido multitud de cursos gratuitos a estudiantes, considera que Brasil y México son los países más avanzados en la región en número de investigadores y publicaciones. También resalta que, pese a no haber programas a nivel nacional con fondos específicamente dedicados, sí hay universidades y centros de investigación en los que cursar másteres y doctorados en materias relacionadas con las tecnologías cuánticas, como por ejemplo el programa de doctorado en nanotecnología del Tecnológico de Monterrey.

En cuanto a Brasil, la entidad de referencia es el Grupo de Computación Cuántica en el Laboratorio Nacional para Computación Científica, cuya misión es “desarrollar investigaciones originales en computación e información cuántica, supervisar estudiantes de

doctorado y máster, impulsar colaboraciones nacionales e internacionales y, en la medida de lo posible, participar en el desarrollo de hardware cuántico” [210].

Según un estudio, en 2015 Brasil contó con una inversión anual estimada de 11 millones de euros -12.6 millones de dólares- y 104 autores diferentes de publicaciones entre 2013 y 2015 en tecnologías cuánticas [211].



RESTO DEL MUNDO

Los anteriores no son los únicos países que han hecho movimientos para posicionarse en la carrera para explorar, desarrollar y adoptar tecnologías cuánticas. Otros muchos también han iniciado programas nacionales y dedicado importantes cantidades económicas. Es este el caso, por ejemplo, de Canadá, con la Universidad de Waterloo destacando a nivel mundial y reconociendo orgullosa haber invertido más de 1.5 billones de dólares durante los últimos 15 años en tecnologías cuánticas [212]; de Rusia, con el *Russian Quantum Center* donde colaboran distintas instituciones y universidades [213]; Francia, con su *Paris Centre for Quantum Computing* (PCQC) [214]; Dinamarca, con su *Quantum Innovation Centre* (Qubiz) [215]; Singapur, con su *Centre for Quantum Technologies* (CQT) [216]; Australia, con su *Centre for Quantum Computation & Communication Technology* [217]; Holanda, guiada por QuTech [218]; Israel con un foco particular en defensa [219] y otros muchos.



INVERSIÓN EN TECNOLOGÍAS CUÁNTICAS ALREDEDOR DEL MUNDO

Gasto estimado reciente basado en
datos públicos (en dólares)

BRASIL
SIN DATOS

ESTADOS UNIDOS

1,3 BILLONES

MÉXICO
SIN DATOS

ALEMANIA

650 M

PAÍSES BAJOS

154 M

REINO UNIDO

456 M

DINAMARCA
12 MILLONES

UNIÓN EUROPEA

1 BILLÓN

ISRAEL
117 M

RUSIA
SIN DATOS

JAPÓN

332 M

COREA DEL SUR
40 M

CHINA

10 BILLONES

AUSTRALIA
26 M

CONCLUSIONES



Con este documento hemos tratado de entender las tecnologías cuánticas y ver sus aplicaciones con impacto social y para el desarrollo. Hemos explicado qué son, cómo funcionan y cómo van a revolucionar campos y tecnologías como ciberseguridad, blockchain, inteligencia artificial, internet de las cosas, 5G, drones o impresoras 3D. Asimismo, hemos analizado y ofrecido ejemplos sobre cuál será el impacto en sectores como medicina, biología, genética, educación, economía y finanzas, energía, agricultura sostenible, transporte o meteorología, y también hemos presentado los distintos programas y estrategias que están adoptando los países para no quedarse atrás.



La computación cuántica abre las puertas al tratamiento computacional de procesos que son sencillamente intratables por los computadores actuales, lo que presenta una amenaza para algunos campos y una gran ventaja para otros. Ejemplos de lo primero los encontramos en ciberseguridad o blockchain, ya que la computación cuántica será capaz de romper de forma eficiente los algoritmos y protocolos en los que se basa la seguridad de internet o las firmas digitales que son imprescindibles en blockchain. Ejemplos de lo segundo los encontramos en medicina, biología o genética, donde se podrá simular la acción de medicamentos renunciando a prácticas en animales y se abrirá la puerta a la búsqueda más eficiente para curar el cáncer o enfermedades como Alzheimer, Parkinson

o esclerosis múltiple; en finanzas, donde se podrán elaborar modelos matemáticos mucho más precisos y procesar datos en tiempo real de manera mucho más ágil y eficiente para toma de decisiones; o en energía y agricultura sostenible, donde hará posible explorar nuevas técnicas de producción de amoníaco con costo energético y económico muy bajo, eliminando los procesos actuales que consumen un 2% de la energía mundial y encarecen los alimentos.



El campo de la información cuántica ofrece una forma completamente segura de almacenar y compartir información, ya que no se basa en problemas matemáticos difíciles de resolver sino en la propia física de la naturaleza, lo que implica que para romper la criptografía tendríamos que violar leyes físicas. En criptografía cuántica todo ocurre a nivel de hardware y no a nivel de software. Diferentes países han desarrollado ya las primeras redes de telecomunicaciones cuánticas en estado de prueba siguiendo un liderazgo marcado por China, primer país en desplegar un satélite para telecomunicaciones espaciales cuánticamente encriptadas en 2016 y que también cuenta con una red terrestre de más de 2000 km entre las ciudades de Beijing y Shanghái. Esto implica que, en el plazo de pocos años, posiblemente todos los dispositivos que utilicemos a diario y que almacenen o compartan datos e información lo hagan utilizando claves cuánticas, y todas las comunicaciones estén aseguradas con esta tecnología. Alineado con ello se encuentran ya propuestas como el internet cuántico.



Las posibilidades que se abren para la inversión pública, para el desarrollo de negocio y emprendimientos en proceso de expansión en el aprovechamiento de estas tecnologías para obtener impactos sociales como los que se detallan en este documento son innegables. Las tecnologías cuánticas emergentes van a ser responsables de una revo-

lución tecnológica que ya está comenzando y que avanzará a pasos agigantados, con un CAGR esperado del 37% hasta 2022 alcanzando como industria un valor de 161 millones de dólares, y un CAGR del 53% entre 2022 y 2028 llegando a 1300 millones de dólares.



Varias potencias mundiales no lo han pasado por alto y están invirtiendo cifras billonarias. China, con su programa de más de 10 billones de dólares, Estados Unidos con su programa de 1,3 billones y la Unión Europea con su programa de 1 billón están actualmente a la cabeza, seguidos de cerca por muchos otros países. En cuanto a América Latina y el Caribe, Brasil y México son los países que lideran en cuanto a número de investigadores y publicaciones. Sin embargo, en ningún país hemos podido saber acerca de programas nacionales financiados con fondos públicos dedicados a la investigación y el desarrollo de estas nuevas tecnologías cuánticas, como sí ocurre en los otros muchos países de los que hemos hablado, principalmente en Europa y Asia.



También ha llamado nuestra atención la importancia que están teniendo las alianzas entre gobiernos y grandes empresas tecnológicas para el desarrollo y la implementación de estas tecnologías, que parece se convertirá en una práctica habitual en los próximos años. Las tecnologías cuánticas están abriendo la puerta a una nueva era y es necesario realizar un esfuerzo desde el sector educativo para formar a futuros profesionales, desde el sector industrial y tecnológico para entender, apoyar y desarrollar nuevos productos con tecnologías cuánticas y desde los gobiernos, para estar protegidos y preparados.



REFERENCIAS

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 y 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): 1648. DOI: <https://doi.org/10.1063/1.476739>.
6. R.J. Hughes et al. *The Los Alamos trapped Ion quantum computer experiment*. Fortschr. Phys. 46 (1998): 329-361.
7. 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.
8. I.L. Chuang. *Experimental realization of a quantum algorithm*. Nature 393 (1998): 143-146.
9. <https://www-03.ibm.com/press/us/en/pressrelease/52403.wss>
10. <https://research.googleblog.com/2018/03/a-preview-of-bristleccone-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 y 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 y 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-ten-gas-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 y 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](https://arxiv.org/abs/quant-ph/0412029v1) (2004).
22. C. Elliott et al. *Current status of DARPA Quantum Network*. [arXiv:quant-ph/0503058v2](https://arxiv.org/abs/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. Brieger, W. Dür, J.L. Cirac y 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. 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 y 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 y 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. Vincenzo. *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 y 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 y V. Colina Unda. *Aprende los tres elementos clave de blockchain con este ejemplo práctico*. IDB Blog: Abierto al público (2018).
58. M. Allende López y 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. D. Aggarwal et al. *Quantum attacks on Bitcoin and how to protect against them*. arXiv:1710.10377v1 [quant-ph].
65. D.J. Bernstein et al. *SPHINCS: Practical stateless hash-based signatures*. Advances in Cryptology -- EUROCRYPT (2015): 368-397.
66. J. Buchmann, E. Dahmen y 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 y 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-eighth annual 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](https://doi.org/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 y 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. *Lenguaje is physical*. Quantum information processing 1, 6 (2002) pp. 495-509. <https://doi.org/10.1023/A:1024074616373>.
87. E.W. Piotrowski y 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 y 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 y B. Coecke. *Quantum algorithms for compositional natural language processing*. SLPCS@QPL (2016). DOI:10.4204/EPTCS.221.8
91. KY. Chen, T. Hogg y R. Beausoleil. *Quantum Information Processing* 1, 449 (2002). <https://doi.org/10.1023/A:1024070415465>.
92. U. Alvarez Rodriguez, M. Sanz, L. Malata y Enrique Solano. *Artificial Life in Quantum Technologies*. Scientific Reports 6, 20956 (2016).
93. Perdomo-Ortiz, M. Benedetti, J. Realpe-Gómez y R. Biswas. *Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers*. Quantum Science and Technology 3, 3 (2018).
94. L. Zhaokai, L. Xiaomei, X. Nanyang y D. Juangeng. *Experimental realization of quantum artificial intelligence*. Phys. Rev. Lett 114, 140504 (2015).
95. V. Dungio y 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 y Michal Broughton. *A universal training algorithm for quantum deep learning*. arXiv:1806.09729v1 [quant-ph].
98. M.V. Altaisky, N.E. Kaputkina y V.A. Krylov. Symmetry and decoherence-free subspaces in quantum neural networks. arXiv:1802.05710v1 [quant-ph].
99. E. Farhi y Harmut Neven. *Classification with quantum neural networks or near term processors*. arXiv:1802.06002v1 [quant-ph].
100. J. Bausch y 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 y 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 y 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/louiscolombus/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/ko-rea_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. <https://www.nature.com/articles/s41598-018-26455-9>
137. J. Vovrosh et al. *Additive manufacturing for quantum technologies*. Scientific Reports 8, 2023 (2018).
138. <https://www.nibib.nih.gov/espanol/temas-cientificos/imagen-por-resonancia-magn%C3%A9tica-irm>
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 al. *Quantized plasmon quenching dips nanospectroscopy via plasmon resonance energy transfer*. Nature Methods 4, 1015–1017 (2017).
143. K. Lee, Y. Cui y 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-healthcare-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 y 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 y S. Khanna. *Sensitivity and computational complexity in financial networks*. Algorithmic Finance 5, 3–4 (2016): 95–110.
151. R. Orús, S. Mugel y 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&c=produccion-de-amoniac-y-urea-en-manos-de-seis-paises
156. <http://www.ssecoconsulting.com/industria-petro-quiacutemica-en-ameacutercalatina.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-computers>
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 y 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. y 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 y 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 y M.E. Hellman. *New directions in cryptography*. IEEE Transactions on information theory 22, 6 (1976).
242. James 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 y 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).

ANEXOS



ANEXO A

EVOLUCIÓN DE LA COMPUTACIÓN CUÁNTICA

A las primeras ideas sobre cómo simular física con computadores, allá por los años 80, firmadas por P. Benioff [1] y R. Feynman [2], les siguieron 20 años de publicaciones que dieron lugar al campo hoy conocido como computación cuántica, proponiendo las primeras formas de construirlos y los primeros algoritmos que podrían correr sobre ellos. En 1998, tres grupos de investigación independientes consiguieron construir los primeros computadores cuánticos de 2 *qubits*. Por un lado, una colaboración entre IBM, el MIT Media Lab y la Universidad de California, Berkeley liderada por el investigador de IBM I. Chuang [3] lo logró en Berkeley [4]; por otro lado, el trabajo de J.A. Jones y M. Mosca hacía lo propio en la Universidad de Oxford [5] y también de forma paralela hacía historia el equipo liderado por R.J. Hughes y D.F.V. James en Los Álamos, California [6,7].

Unos meses después, de nuevo con I. Chuang a la cabeza, se conseguía implementar el algoritmo de Grover en el primer computador cuántico de 3 *qubits* en el centro de investigación de IBM en Almaden, San José [8].

Dos años más tarde, entre los años 2000 y 2001, una colaboración entre IBM y la Universidad de Stanford desarrollaba el primer computador cuántico de 7 *qubits* e implementaba por primera vez el algoritmo de Shor para descomponer números en el producto de sus números primos, consiguiendo factorizar el número 15 en sus factores primos 3 y 5 [221]. Este hito fue conseguido también por la Universidad de los Álamos en el año 2000.

En 2005, en la Universidad de Innsbruck logran implementar el primer *qubyte* -8 *qubits*- [222]. Un año después, en 2006, investigadores del Waterloo y el MIT, consiguen elevar la cifra a 12 *qubits* [223]. De nuevo se tardó un año en volver a batir el récord; en 2007 D-Wave conseguía llegar a los 16 *qubits* [224].

Tras estos avances tan seguidos en el tiempo, sobrevinieron 10 años de cierta frustración hasta que en mayo de 2017 IBM anunciaba un nuevo récord con el primer computador cuántico de 17 *qubits* [9], cifra que era en octubre igualada por Intel [188]. Pocos meses después, de nuevo IBM conseguía llegar a los 50 *qubits* [179] y, al mismo tiempo, ofrecía acceso online a un computador cuántico de 20 para que cualquier usuario pudiese realizar simulaciones y ofrecer retroalimentación [225].

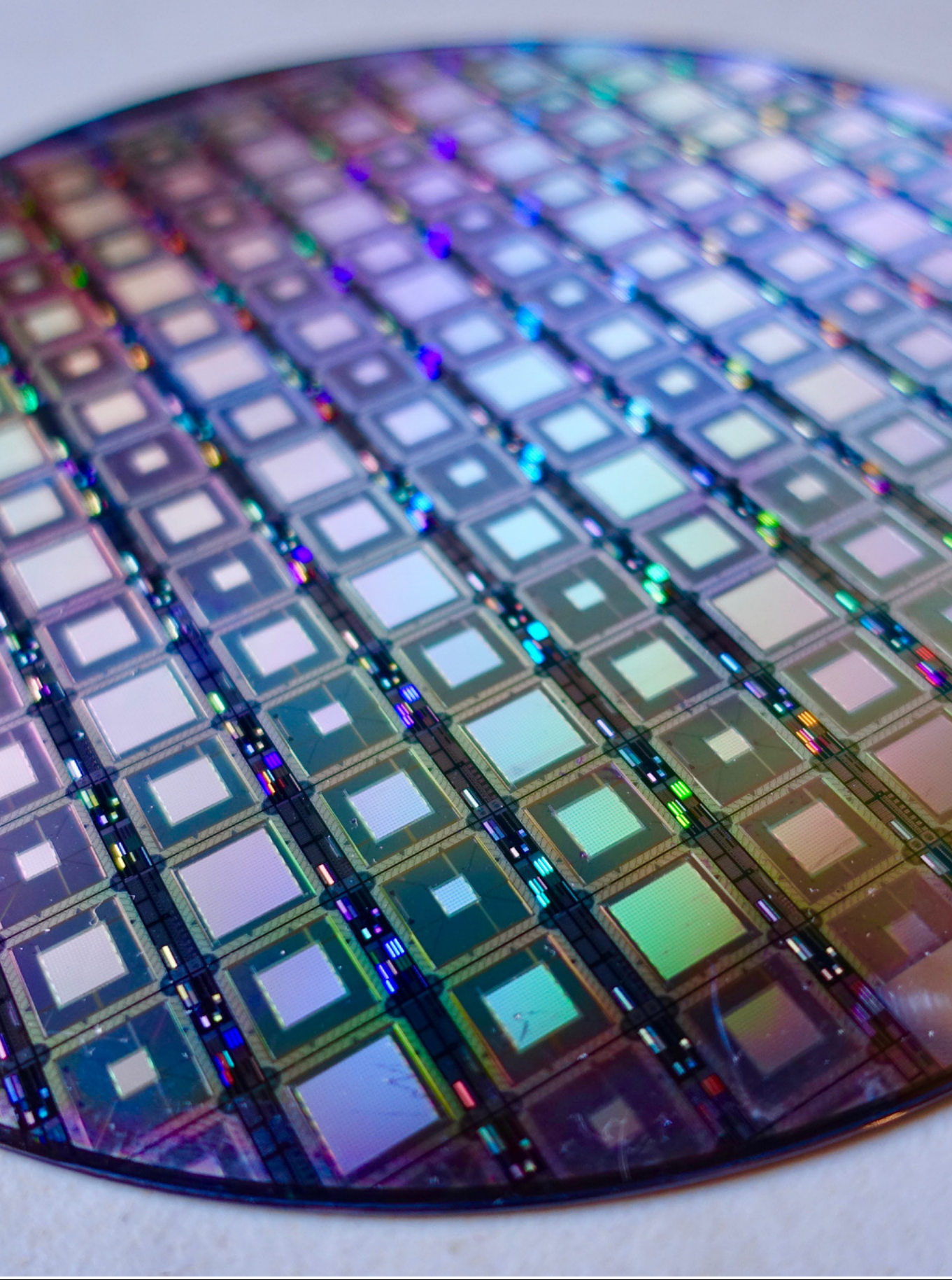
En abril de 2018, Google se colocó líder en esta carrera con un computador cuántico de 72 *qubits* que es el computador cuántico con mayor capacidad hasta la fecha [10].

Los participantes de esta carrera tras la computación cuántica están ahora centrados en conseguir la supremacía cuántica, que consiste en ejecutar un proceso con un computador cuántico más eficientemente que con un computador clásico. El propio Google opina que 50 *qubits* podrían ser suficientes para conseguirlo [226], por lo que se espera que la noticia salte en un futuro cercano.

Desde que en torno al año 2000 empezaron a construirse los primeros procesadores cuánticos, se estimó en torno a 2030 la fecha en la cual esta tecnología estaría lista para ser utilizada con alguno de los propósitos recién mencionados. Como ya apuntamos anteriormente, algunos consideran que computador cuántico de entre 1500 [12] y 2330 [13] *qubits* lógicos sería suficiente para romper, en un tiempo razonable, claves utilizadas en ciberseguridad actualmente, y que **en 2027 será posible romper las firmas digitales utilizadas en blockchain en menos de 10 minutos** [64].

En la figura 3, presentada en la sección I, se puede ver el ritmo exponencial al que está creciendo la tecnología. Una evidencia de ello es el lanzamiento del primer computador cuántico comercial por parte por IBM en enero de 2019, que cuenta con un procesador de 20 *qubits*, bajo el programa *IBM Q System One* [181,182]. Hasta ahora solo se han puesto en venta *quantum annealers*, que son simuladores cuánticos -y no computadores- con aplicaciones específicas, generalmente en problemas de optimización, como por ejemplo los de D-Wave 2000Q de 2000 *qubits* [185].

Lo más probable es que pasen décadas antes de que podamos encontrar computadores cuánticos domésticos y es posible que, cuando esto ocurra, los computadores no sean cuánticos o clásicos sino híbridos, con dos procesadores a los que les sean asignadas unas u otras tareas en función de su complejidad y características. También es de esperar que para el público general el primer contacto con computación cuántica llegue a través de servicios provistos en la nube conocidos como *software as a service*, donde se podrá utilizar recursos de hardware y software cuántico de grandes compañías tecnológicas por un precio que varíe en función del uso.



Una vista aumentada de una oblea perteneciente a un computador cuántico de D-Wave.
Crédito: Steve Jurvetson, Menlo Park, USA. Febrero 2018.

ANEXO B

CRIPTOGRAFÍA CUÁNTICA

Como explicábamos en la sección de Información Cuántica, el gran cambio de paradigma que ofrece la criptografía cuántica consiste en utilizar procesos que ocurren a nivel físico -de hardware- y no de software para garantizar la seguridad de la información. **La criptografía cuántica ofrece ya soluciones comerciales para la generación cuántica de números completamente aleatorios y la encriptación totalmente segura de información.**

Generación de números aleatorios

La generación de números aleatorios clásica se basa en algoritmos que parten de una semilla y son deterministas. Con algoritmos clásicos que tienen lugar a nivel de software no es posible conseguir aleatoriedad verdadera. Sin embargo, sí podemos conseguir aleatoriedad verdadera utilizando procesos físicos que son aleatorios, y gracias al entendimiento del mundo microscópico que la Mecánica Cuántica nos ofrece, conocemos y podemos utilizar varios de ellos. Una forma sencilla de hacerlo es trabajar con partículas de luz, denominadas fotones, y polarizadores o espejos semi-reflectores. Si un fotón incide sobre un espejo que tiene un 50% de probabilidades de reflejarlo y un 50% de dejarlo pasar, podemos establecer el convenio de anotar un 0 cuando el fotón se refleja y un 1 cuando lo atraviesa y por tanto generar una clave 100% aleatoria.

Este tipo de procesos son relativamente sencillos de conseguir hoy en día y compañías como IDQuantique tienen dispositivos comerciales de dimensiones milimétricas [18].

Encriptación cuántica simétrica (QKD)

Todos los procesos y protocolos ampliamente utilizados hoy en día para transmitir información, por ejemplo a través de internet, dependen de criptografía asimétrica para establecer una comunicación segura entre dos usuarios, generalmente denominados Alice y Bob. Esta criptografía permite que Alice le envíe a Bob una **clave pública** con la que encriptar información de manera que solo Alice con su **clave privada** puede desencriptarla. Bob podría enviarle una clave simétrica encriptada con esa **clave pública** de manera que solo Alice y Bob la conociesen y entonces podrían comenzar a utilizarla para encriptar mensajes. Así es como funciona, de manera resumida, el protocolo https de internet. El problema es que la computación cuántica va a ser capaz de, a partir de la **clave pública**, encontrar las **claves privadas** y romper la criptografía [36-37,43].

De nuevo, la criptografía cuántica permite, gracias a un proceso físico, crear y compartir una clave simétrica cien por cien segura. Esto es gracias al principio de incertidumbre y al de no clonación que ocurren en el mundo microscópico, y que imposibilitan observar sin modificar o copiar sin modificar un estado cuántico, y por tanto la información codificada en ese estado. Es decir, si Alice de alguna forma codifica un 0 o un 1 en la polarización de una partícula de luz y se lo envía a Bob, una vez Bob reciba ese fotón, lo mida y hable con Alice, **van a poder saber si alguien observó ese fotón por el medio, lo que**

significa que van a poder estar seguros de si una clave es o no segura antes de usarla, pudiendo renunciar a una criptografía asimétrica insegura. Este proceso se conoce como distribución cuántica de claves (QKD por sus siglas en inglés) y es esencialmente tal y como acabamos de describir. Vamos a explorarlo un poco más a nivel físico.

Es bien conocido que la luz tiene una propiedad denominada polarización, que utilizan nuestras gafas de sol para filtrarla en verano haciendo la vida más fácil a nuestros ojos. Si estudiamos la polarización a nivel de partículas de luz, conocidas como fotones, un modelo simplificado y útil consiste en imaginárselas como flechas con una dirección determinada, que es la dirección de polarización. Para medir, detectar o interactuar con los fotones se utilizan polarizadores, que dejan pasar a las partículas en función de la dirección de polarización de los mismos. Dado que las partículas son sistemas cuánticos, las partículas de luz son susceptibles a fenómenos cuánticos como la superposición o el entrelazamiento.

Esto propicia que, si lanzamos una partícula, digamos con polarización diagonal, a través de un polarizador, puede pasar lo siguiente:

- Si el polarizador es diagonal, el fotón pasa en un 100% de los casos como ocurre en el mundo macroscópico cuando un objeto es del tamaño y forma de un agujero. Por ejemplo, es como si pusiéramos un sofá en diagonal para hacerlo atravesar una puerta que sea diagonal.
- Si el polarizador es vertical, en un 50% de las veces el fotón no lo atravesará y el otro 50% lo hará pero convertido en un fotón con polarización vertical, de forma que alguien que vea el fotón salir del polarizador no sabrá qué dirección de polarización tenía antes. Esto ocurre porque el fotón diagonal es a su vez una combinación -una superposición cuántica- de un fotón vertical y otro horizontal y entonces, cuando llega al polarizador, se le “obliga” a dejar de ser diagonal y decidir si convertirse en su “proyección” horizontal¹⁶ -de forma que no atraviesa el polarizador- u optar por la vertical -de manera que lo atraviesa pero convertido en un fotón polarizado verticalmente-. Esto ocurre siempre que polarizador y fotón tengan una polarización que diste en 45 grados, por lo que si el polarizador es horizontal ocurre lo mismo. Esto no tiene análogo clásico, puesto que un sofá en diagonal nunca atravesará una puerta con forma vertical.
- Si el polarizador está girado 90 grados con respecto a la polarización del fotón, entonces el fotón no lo atraviesa en ningún caso.
- Si la polarización fuese cualquier otra, la probabilidad de que el fotón atravesase el polarizador depende de cuánto disten la dirección del fotón y la del polarizador. La probabilidad aumenta desde un 0% cuando son ortogonales hasta un 100% cuando son paralelos.

Los casos 2 y 4 solo ocurren con sistemas cuánticos y esta fenomenología es la que se utiliza en criptografía cuántica, más conocida como *quantum key distribution* (QKD), para compartir claves de forma segura entre dos individuos, que se suelen conocer como Alice

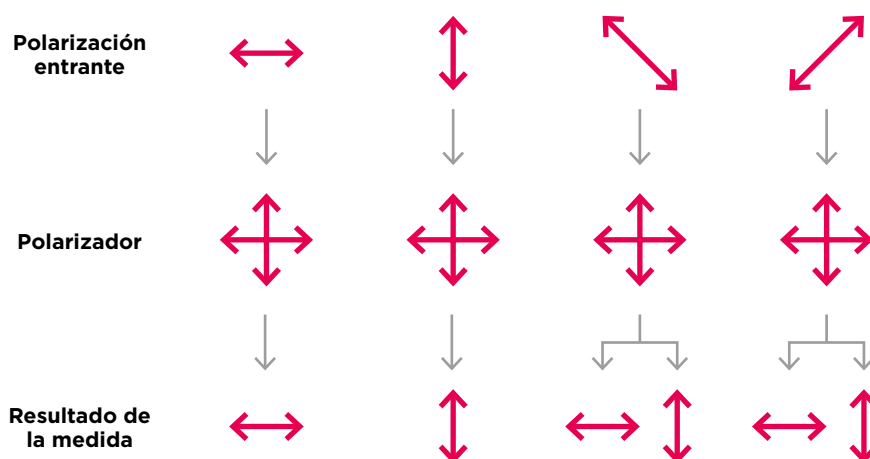
16. No es correcto decir proyecciones porque pareciese que la mitad del fotón corresponde a cada proyección, de manera que solo la mitad del fotón (quizás la mitad de su intensidad) atraviesa el polarizador, pero eso no es lo que ocurre. El fotón realmente convive en una superposición de polarizaciones y si se decanta por la que tiene el polarizador, lo atraviesa como un todo.

y Bob. La seguridad radica en el hecho de que si alguien intercepta la clave y la mide con sus polarizadores, la va a modificar, y esa modificación puede ser detectada por Alice y Bob determinando por tanto que hubo un espionaje. El protocolo más utilizado de QKD es el denominado BB84 [19] y puede describirse en los siguientes pasos:

1. Alice y Bob acuerdan cuál va a ser su código de unos y ceros en términos de la polarización de fotones y qué tipo de polarizadores van a utilizar para medirlos. Por ejemplo, determinan que las flechas a 45 y 90 son ceros y las flechas a 0 y 135 son unos. Esta negociación tiene lugar a través de un canal clásico y no revela ninguna información al espía sobre la futura clave.
2. Alice le envía a Bob fotones aleatoriamente polarizados en una de las 4 direcciones a través de un canal cuántico -que puede ser el mismo que el clásico- y, si el espía la intercepta, es detectado ya que el 50% de las veces elige el polarizador incorrecto y cambia la dirección de polarización del fotón.
3. Bob mide los fotones que Alice le envía cualquiera de los 4 polarizadores, que va seleccionando aleatoriamente, y registra el polarizador utilizado y si la polarización del fotón corresponde a un cero -es decir, está a 45% o 90%- o un uno -a 0 y 135 grados- en función del consenso inicial.



FIGURA 11. Representación esquemática del efecto de polarizadores sobre fotones.



En los dos casos de la izquierda el polarizador deja pasar el fotón en el estado inicial puesto que se escoge la base correcta. En los dos casos de la derecha, al escoger la base incorrecta, el fotón no puede pasar en el estado inicial y hay un 50% de probabilidad de que el fotón pase en cada una de las dos direcciones ilustradas.

4. Alice y Bob vuelven a comunicarse por un canal clásico, y Bob le dice a Alice qué polarizadores utilizó. Por el fenómeno de superposición cuántica explicado anteriormente, si Bob utiliza un polarizador horizontal-vertical y el fotón viene polarizado diagonalmente, Bob va a obtener un fotón vertical o un fotón horizontal con un 50% de probabilidad para cada opción. Es por eso que en ningún caso podrá saber que el fotón que venía era diagonal, de forma que pierde la información del uno o el cero que Alice había codificado en esa polarización diagonal. Por tanto, Alice y Bob descartan de su clave los unos y ceros que corresponden a medidas de Bob con el polarizador equivocado.

- 5. Una vez que Alice y Bob tienen la clave limpia con los unos y ceros correspondientes a medidas adecuadas, utilizan un canal clásico para compartir un pedazo de esa clave. Si la clave que cada uno tiene diverge de la del otro en un porcentaje mayor al que se estima por el error intrínseco del canal, entonces determinan que alguien ha observado la clave en su envío, habiendo introducido un error adicional con su elección aleatoria de polarizadores.
- 6. Si la clave no ha sido espiada, Alice y Bob utilizan la parte que no han sacrificado y que sigue siendo secreta para encriptar y desencriptar información. Si ha sido espiada, pueden o bien desecharla o bien aplicar técnicas para reducir la información que el espía tiene sobre la clave.

La seguridad del proceso radica en que el espía nunca va a poder predecir la clave que manda Alice, ya que es 100% aleatoria -cosa que permiten las tecnologías cuánticas y que no es posible con tecnología clásica-, ni tampoco va a poder adivinar los polarizadores que utilizará Bob para usar los mismos y no introducir un error adicional, ni tampoco es capaz de saber el resultado que obtiene Bob al medir con sus polarizadores aun espiondo la conversación entre Alice y Bob en la que, a posteriori este se lo comunica a ella. Por tanto, el espía nunca tiene nada de información sobre la clave si solo espía las comunicaciones clásicas, y si decide espionar las comunicaciones cuánticas es detectado.

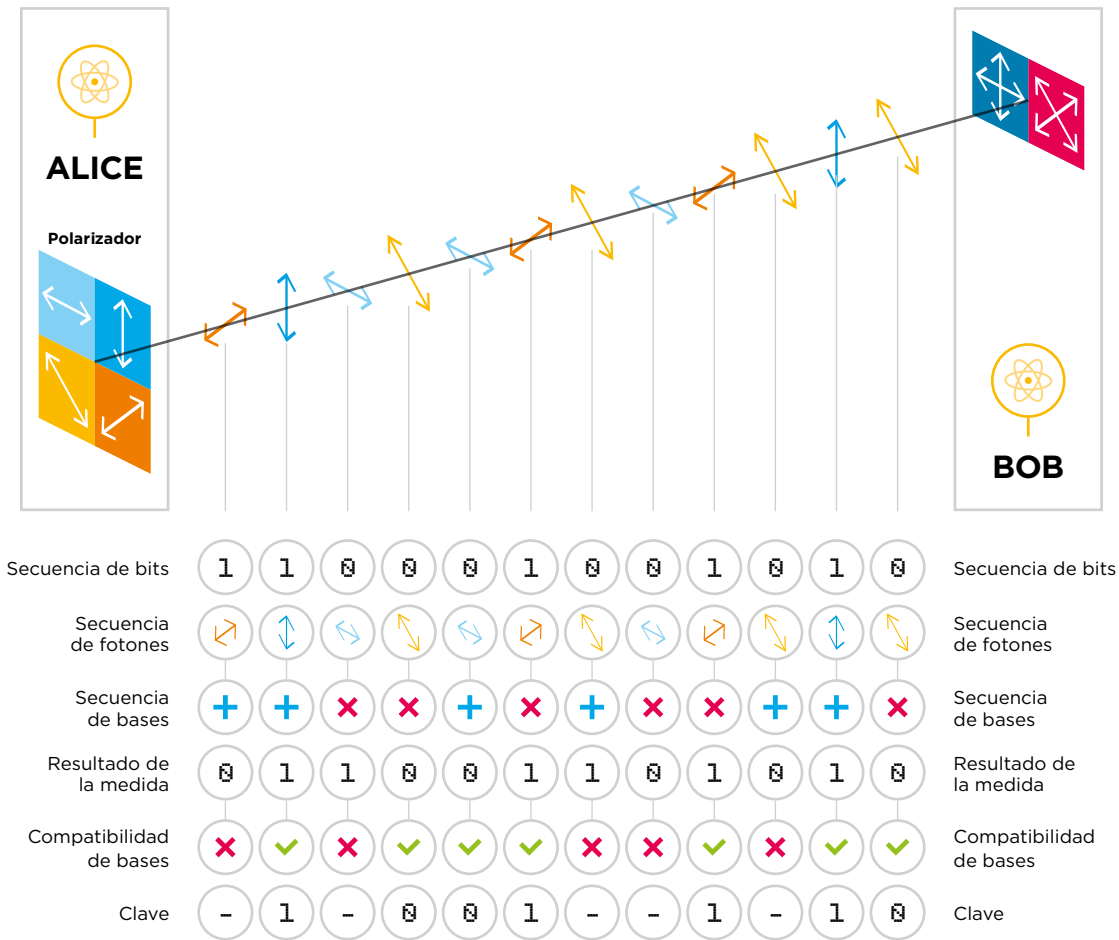


FIGURA 12. Representación a alto nivel del esquema BB84 del protocolo de criptografía cuántica simétrica (QKD por sus siglas en inglés) entre Alice y BOB

ANEXO C

EVOLUCIÓN DE LAS REDES DE COMUNICACIÓN CUÁNTICAMENTE ENCRİPTADAS

QKD por tierra utilizando fibras ópticas

Al igual que la carrera por la computación cuántica, la carrera por las telecomunicaciones cuánticas comenzó a ofrecer los primeros prototipos con la entrada del siglo XXI. La primera red cuántica terrestre conocida fue DARPA (*Defense Advanced Research Projects Agency*) *Quantum Network*, operada entre las Universidades de Harvard y Boston en 2003. Contó con una longitud de unos 29 km que inicialmente servía para conectar seis nodos y que en 2005 incorporó cuatro más [21,22].

La primera red operando para un caso real, según el proveedor IDQuantique, fue instalada en Suiza con el objeto de proteger la información de las votaciones nacionales en su transmisión desde el centro de almacenamiento al de conteo [227,228].

Poco después, en 2008, se desarrolló otra red robusta en Viena con motivo del proyecto europeo SECOQD (*Secure Communication based on Quantum Cryptography*). Fue coordinada por el AIT (*Austrian Institute of Technology*) en 2008 y contó una financiación de 11 millones de euros por parte de la Unión Europea. La red dispuso de seis nodos, cinco de ellos situados en instalaciones de Siemens y el sexto en una estación repetidora, sumando una longitud total de 285 km divididos en fibras ópticas entre nodos de longitudes desde 6 km hasta 85 km [229,230].

Otro proyecto interesante es *QuantumCity* en Sudáfrica, que nace de la colaboración entre el Centro para Tecnologías Cuánticas de la Universidad de KwaZulu-Natal, la Compañía de Innovación de esta misma Universidad, eThekwin Municipality y el Fondo de Innovación. La red cuántica fue desarrollada en 2009 contando, inicialmente, con cuatro nodos distribuidos en varios suburbios del distrito de eThekwin y conectados en forma de estrella, con longitudes de fibra entre nodos desde 2.6 km a 27 km [231].

En China han tenido lugar varias iniciativas. Una de ellas, operativa desde 2007, consistió en una red en el área metropolitana de Beijing, con 4 nodos operando en las áreas de Wangjing, Dongxiaokou, Nanshan y Huangchenggen en forma de estrella, con distancias entre los mismos variando desde 32 km hasta 42.6 km [232]. El siguiente caso a mencionar es la red que comenzó a operar en 2009 en el área metropolitana de Heifei, de nuevo con 4 nodos en forma de estrella y un quinto nodo adicional situados en UTSC, Wan'an, Meilan, Wanxi y Feixi, con capacidad para realizar llamadas telefónicas encriptadas cuánticamente y en tiempo real entre cualquier pareja de entre los cinco nodos, con hasta 60 km de distancia [233]. La tercera red operó durante más de 5000 horas desde diciembre de 2011 hasta julio de 2012 entre las zonas metropolitanas de Heifei, Chaohu y Wuhu. En Heifei estuvieron activos los 5 nodos de la red que recién hemos descrito, en Wuhu se instalaron 3 nodos más y en Chaohu operó un noveno.

La longitud total de la fibra óptica instalada fue de cerca de 200 km [234]. A estas tres iniciativas les han seguido otras, entre las que destaca la liderada por la Universidad de Ciencia y Tecnología China que pretende conectar cuánticamente cuatro ciudades con una fibra óptica de 2000 km desde Beijing hasta Shanghai [27].

La red mejor documentada es quizás la desarrollada por Tokio y se estructura en tres capas [195]. La primera es la capa cuántica, que está constituida por seis nodos distribuidos entre las ciudades de Koganei, Otemachi, Hakuson y Hongo conectados punto a punto y generando claves a través de diferentes protocolos. La segunda es la capa de administración o control donde un agente de administración de claves (KMA por sus siglas en inglés) localizado en cada nodo, que corresponde físicamente a un PC protegido, recibe la clave a través de una interfaz de aplicación (API por sus siglas en inglés) desarrollada por NEC Corporation y el Instituto Nacional de Tecnología de Información y Telecomunicaciones de Japón (NICT por sus siglas en inglés), que hace posible la interoperabilidad entre los distintos sistemas y protocolos que conforman la red. Estos servidores funcionando como KMA se encargan de recoger las claves cuánticas así como información sobre las mismas,

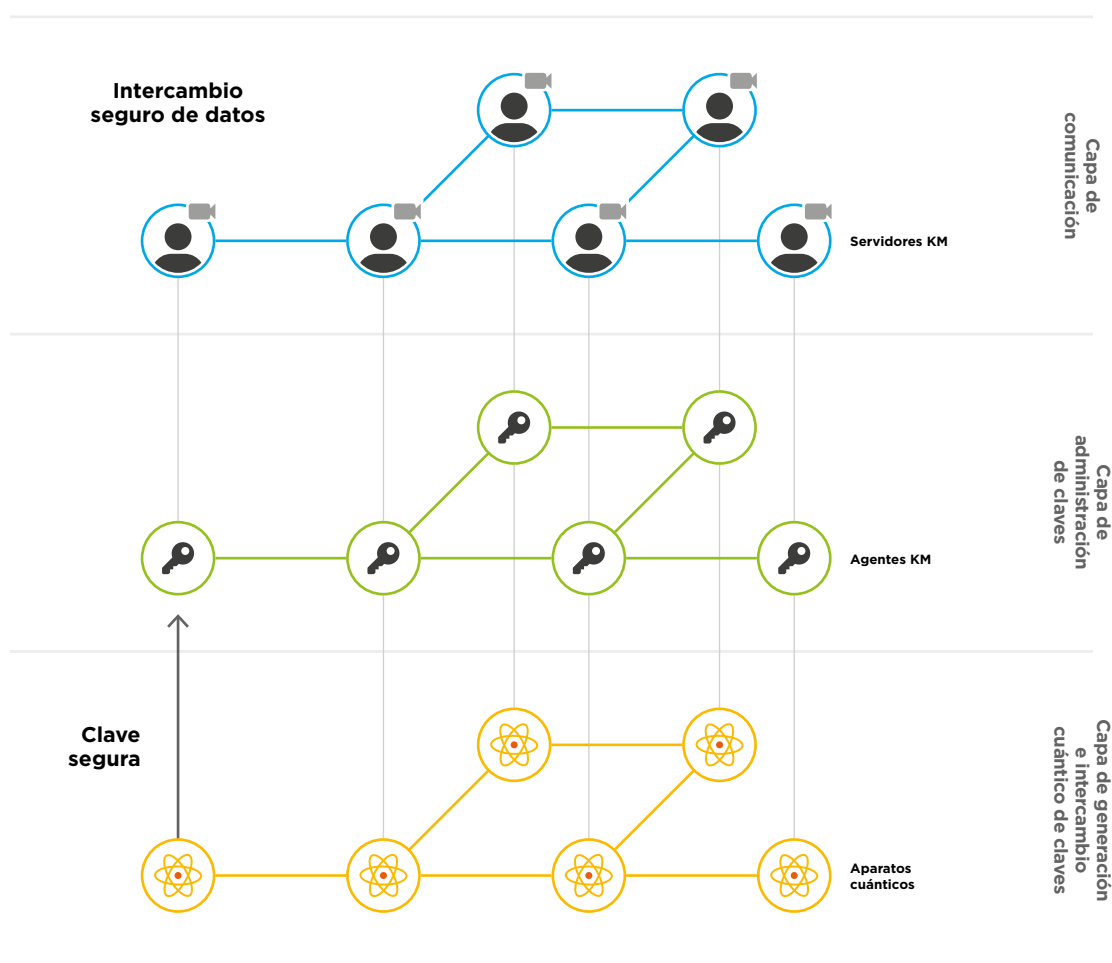


FIGURA 13. Ilustración esquemática de la red cuántica de 6 nodos ubicada en Tokio, estructurada en 3 capas.

como por ejemplo el ratio de error cuántico por *qubit* (QBER), para posteriormente enviarlas a un servidor centralizado de administración de claves (KMS). La tercera capa es la capa de comunicación, en la cual se utilizan las claves cuánticas generadas para, siguiendo el estándar AES-256, encriptar y desencriptar archivos de audio, texto, video u otros datos producidos por diferentes aplicaciones. Las distintas conexiones utilizan cables con longitudes entre 1 km y 90 km.

Estados Unidos comienza ahora, al menos de manera pública, a probar la tecnología. La compañía estadounidense Quantum Xchange está desarrollando la primera red comercial con criptografía cuántica del país [131] que “conectará los mercados financieros de Wall Street con centros de respaldo en Nueva Jersey, permitiendo mantener información sensible segura” [132]. Este gigante de las telecomunicaciones llegaba este año a un acuerdo con SK Telecom por valor de 8.9 millones de dólares [126] para que le supliera con sus sistemas de criptografía cuántica.

QKD por aire utilizando satélites

Las redes por aire, como comentábamos en la sección de Información cuántica, tienen un mayor alcance que las terrestres puesto que las señales se enfrentan a una atenuación mucho menor al pasar la mayor parte del tiempo por encima de la atmósfera. Dada la necesidad de tener satélites en órbita para posibilitar estas comunicaciones, la primera prueba se hizo esperar un poco más.

El primero en colocar satélites en órbita para realizar telecomunicaciones cuánticas Tierra-espacio y espacio-Tierra fue China. En 2016, la misión espacial bajo el nombre de QUESS (*Quantum Experiments at Space Scale*) puso en órbita un satélite de unos 600 kg de peso, conocido como MICIUS, con un costo total de la misión de unos \$100 millones [28,29]. En comunicación con tres estaciones terrestres ubicadas en Delingha, Nanshan y Lijiang, se consiguió generar y compartir claves cuánticas por primera vez a largas distancias, superando los 1200 km [30,31].

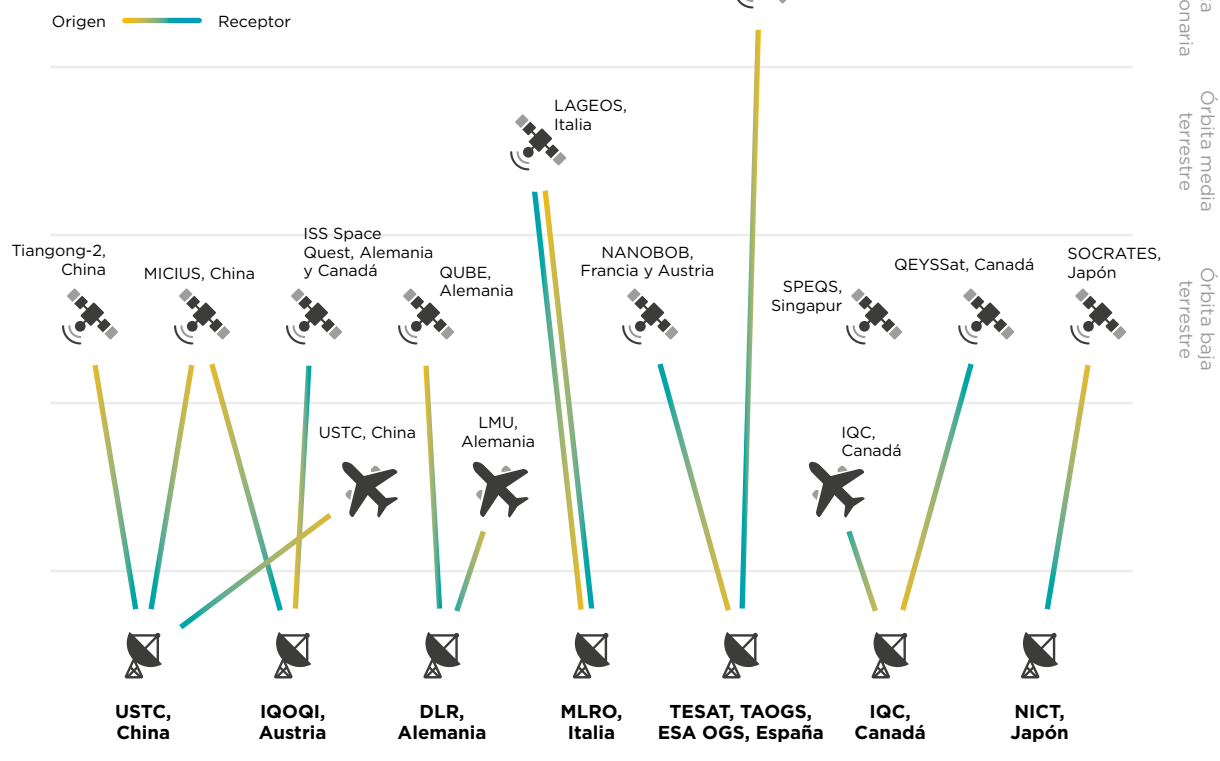
Gracias al uso de este satélite, el 17 de septiembre de 2017 se realizó el mayor hito hasta la fecha en el campo de la información cuántica: una videollamada de hora y media entre China y Austria encriptada cuánticamente a una distancia de 7600 km, pasando a ser la primera comunicación intercontinental cifrada de forma segura con tecnología cuántica. La videollamada viajó por un cable de fibra óptica siendo encriptada y desencriptada en China y Austria con una clave cuántica que fue generada y compartida previamente haciendo uso del satélite- [32].

Además, China prevé lanzar otros 10 satélites que permitan tener en 2020 una red intercontinental de comunicaciones entre Europa y Asia, que se expanda hasta ser una red mundial en 2030 [33].

Otra iniciativa China ha sido el estudio de la viabilidad de realizar este tipo de telecomunicaciones cuánticas Tierra-espacio y espacio-Tierra utilizando dispositivos específicos en estaciones espaciales, con la intención de evitar generar una constelación de satélites.

**FIGURA 14.**

Algunas de las muchas iniciativas llevadas a cabo por distintos países y academias [238].



Con este propósito, en 2017 realizaron QKD a una distancia de hasta 719 km entre el laboratorio espacial Tiangong-2 y la estación en tierra Nanshan [159].

Por su parte, Japón logró en 2017 realizar QKD utilizando un micro-satélite conocido como *Small Optical Transponder* (SOTA) de 6 kg de peso, 17.8 cm de largo, 11.4 cm de ancho y 26.8 cm de alto, orbitando a una altitud de 600 km [196].

En Europa, también en 2016, una colaboración entre instituciones académicas y observatorios italianos clamó haber conseguido realizar transmisiones óptimas de fotones a más 7000 km de distancia, entre el satélite LAGEOS-2, orbitando a 5620 km de altura, y el observatorio Matera Laser Ranging Observatory, lo que abre la puerta a QKD a distancias aún más largas [235].

Esta colaboración publicó en abril de 2018 haber roto la barrera de los 20.000 km en el intercambio de fotones [236]. Para ello, establecieron comunicación entre dos satélites de la constelación GLANOASS -un total de más de 20 de satélites que opera en tres planos orbitales y que fue desarrollada en la segunda mitad del siglo XX para la geo-localización por satélite rusa [237]-.

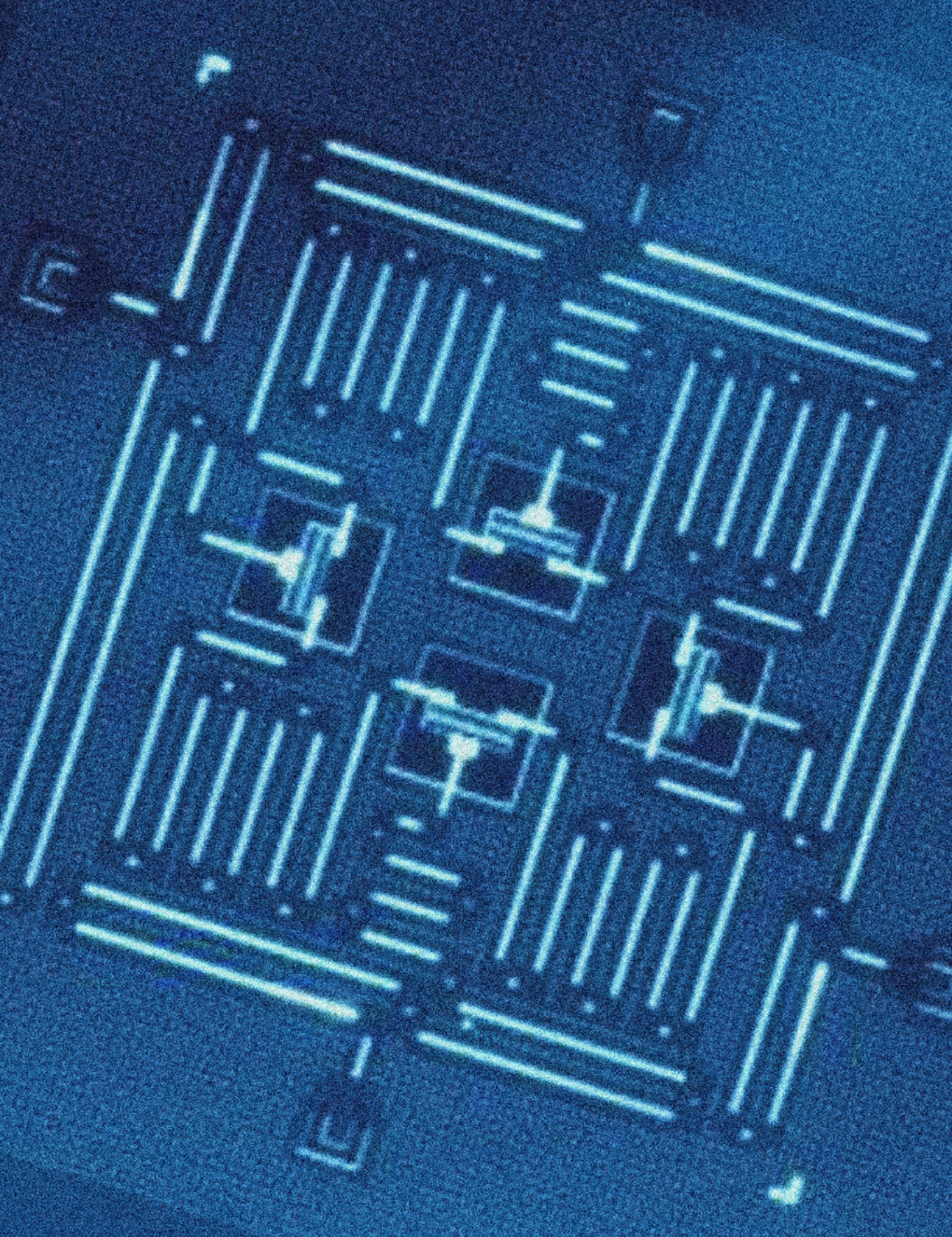
Otra iniciativa interesante, esta vez a nivel europeo, es la conocida como Space-QUEST (*Quantum Entanglement for Space Experiments*) de la Agencia Espacial Europea (ESA por sus siglas en inglés) [53,54], que propone situar un transmisor en el ala externa del módulo Columbus en la Estación Espacial Internacional (ISS por sus siglas en inglés). En la ESA encontramos también la iniciativa Eutelsat Quantum, “una misión pionera que influenciará cómo serán los satélites de telecomunicaciones en Europa”, en el marco de la cual se pondrá en órbita un satélite para la realización de telecomunicaciones cuánticas Tierra-espacio y espacio-Tierra en la segunda mitad de 2019 [166].

Paralelamente, distintos organismos alemanes, entre los que se encuentra el Instituto Max Planck y el Centro Aeroespacial Alemán (DLR por sus siglas en alemán) han cooperado para la realización en 2016 de su propio estudio experimental, en el que han testado la transmisión de señales de fotones a 38600 km de distancia entre la estación espacial transportable localizada para esta prueba en el Observatorio del Teide, Tenerife, y el satélite estacionario Alphasat I-XL [209].

Un poco más hacia el sur y hacia el este encontramos la colaboración entre Francia y Austria denominada NanoBob, que trata de ofrecer datos más precisos sobre la óptima disposición de sistemas para realizar QKD utilizando satélites, y realizar sincronizaciones precisas entre los relojes en la nave y en tierra [238].

Estos son solo algunos de los proyectos que han sido realizados o serán realizados en un futuro cercano [239]. Vemos por tanto que, con China a la cabeza, varios países principalmente asiáticos y europeos están invirtiendo para no quedarse atrás en la carrera por las telecomunicaciones cuánticas. En lo que concierne al resto del mundo no hemos encontrado información sobre otras iniciativas ambiciosas, si bien se tiene conocimiento de diferentes pruebas de concepto tanto a nivel de gobierno como por parte de empresas tecnológicas y entidades financieras.

Con respecto a América Latina y el Caribe, no hemos encontrado información sobre ningún programa similar a los que están llevándose a cabo en Europa y Asia, y no tenemos conocimiento de ningún programa ni ninguna prueba de concepto en la región en el marco de las telecomunicaciones cuánticas.



Un dispositivo consistente en cuatro trasmones, cuatro buses cuánticos y cuatro resonadores de lectura fabricados en IBM y descritos en la publicación *Building logical qubits in a superconducting quantum computer system*. J.M. Gambetta et al. Enero 2017.

ANEXO D

CRİPTOGRAFÍA ASIMÉTRICA

Las primeras ideas sobre criptografía asimétrica, también conocida como encriptación de clave pública, surgieron en la década de los 70. Oficialmente se asocian a los documentos publicado por R. Merkle [240] y W. Diffie y M. Hellman [241] en 1976 pero parece que fue en realidad J. Ellis, criptógrafo al servicio de la inteligencia británica, quien de forma clasificada exploró por primera vez este campo en 1970 [242].

Entre las distintas técnicas de criptografía asimétrica cabe destacar el algoritmo RSA, la criptografía de curvas elípticas y la criptografía de logaritmos discretos [243].

Algoritmo RSA

El algoritmo RSA se basa en la dificultad que supone para los computadores clásicos factorizar números enteros grandes, dado que la dificultad es exponencial -el número de pasos necesarios a realizar crece exponencialmente con el tamaño del entero a factorizar-. Fue propuesto por R. Rivest, A. Shamir y L. Adleman del MIT en 1978 [244], de ahí el nombre con las iniciales de sus apellidos. Sin embargo, en 1997 se desclasificó un documento probando que C. Cocks y M. Williamson del servicio de inteligencia británico habían propuesto un método similar en 1973 [245].

La idea tras el algoritmo es que, dados los números enteros e , d y n tal que para cualquier entero m satisfaciendo $0 \leq m \leq n$ se cumpla:

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

Es extremadamente difícil con algoritmos clásicos encontrar d dados e y n , o incluso dado m . Se conoce entonces m como el mensaje a encriptar, e como la clave pública que se facilita a la persona que envía el mensaje para que lo encripte y d la clave privada necesaria para desencriptarlo que solo el destinatario del mensaje posee.

El algoritmo clásico que resuelve el problema más eficientemente, por ser el más rápido en factorizar números enteros mayores de 10^{100} , se conoce como *general number field sieve* (GNFS). El problema a resolver no es otro que, dado el entero n , encontrar los enteros primos p y q -relacionados con e y d - tal que:

$$n=pq$$

RSA Laboratories tuvo activo entre 1991 y 2007 un desafío mediante el cual premiaban con recompensas económicas a aquellos que consiguiesen factorizar números RSA de distintas longitudes [246]. El número de mayor longitud que ha conseguido factorizar

-que se tenga conocimiento- es el RSA-768, que tiene 768 dígitos binarios y 232 dígitos decimales. El equipo responsable, premiado en 2009 con \$50.000 dólares, tuvo que realizar más de 10^{20} operaciones para encontrar el número haciendo uso del algoritmo GNFS, llevadas a cabo en cientos de ordenadores con procesadores muy potentes durante dos años. Con un único procesador AMD Opteron de 2.2 GHz con 2 GB de RAM les habría tomado del orden de 1500 años [247]. Según sus investigaciones, estimaron que la factorización de un número de 1024-bits tendría una dificultad 1000 veces mayor.

En 2015 la NSA recomendó dejar de utilizar esta técnica de encriptación.

Problema de logaritmos discretos (DLP) y criptografía de curvas elípticas (ECC)

Dado un grupo cíclico finito G y un generador del grupo α , el problema de logaritmos discretos sobre G consiste en encontrar el único $d \in [0, |G| - 1]$ que, dado un elemento cualquiera del grupo $\beta \in G$, satisfaga:

$$\alpha^d = \beta$$

Es decir, encontrar el logaritmo en base α del elemento β :

$$d = \log_{\alpha} \beta$$

Hay ciertos grupos G para los que sus propiedades específicas permiten desarrollar algoritmos que resuelvan este problema en tiempo polinómico, como por ejemplo $G = \mathbb{Z}_N$. Para otros grupos G , en cambio, la dificultad es exponencial o subexponencial, por lo que son más apropiados para desarrollar algoritmos criptográficos.

Algunos algoritmos populares como la encriptación de ElGamal [248] conocida como *Digital Signature Algorithm* (DSA) o el intercambio de claves de Diffie-Hellman proponen el uso del grupo multiplicativo módulo p , $G = (\mathbb{Z}_p)^*$. Otros proponen el uso de grupos abelianos finitos de curvas elípticas $G = \text{GF}(p^n)$, como por ejemplo la versión Diffie-Hellman sobre curvas elípticas (ECDSA por sus siglas en inglés).¹⁷

La primera organización de desarrollo de consenso y estándares que apadrinó el uso de curvas elípticas fue ANSI en 1999 con los estándares ANSI X9.62 [249]. Un año después el NIST en la publicación 186-2 de FIPS daba también su respaldo proponiendo distintas curvas elípticas a utilizar [250].

17. El logaritmo elíptico es la formulación aditiva del logaritmo discreto; esto es, las exponenciaciones y productos del segundo se transforman en productos y sumas del primero.

El proceso es un poco más sofisticado que RSA, y por eso también resulta ser más seguro, de forma que se consigue la misma complejidad con claves más cortas. Para el lector interesado en una comparación más detallada se recomienda el documento de A. I. Ali [251], en donde se puede encontrar información como la de la siguiente tabla:

Longitud clave RSA (bits)	Longitud clave ECDSA (bits)
1024	192
2048	256



TECNOLOGÍAS CUÁNTICAS

Una oportunidad transversal e interdisciplinar
para la transformación digital y el impacto social