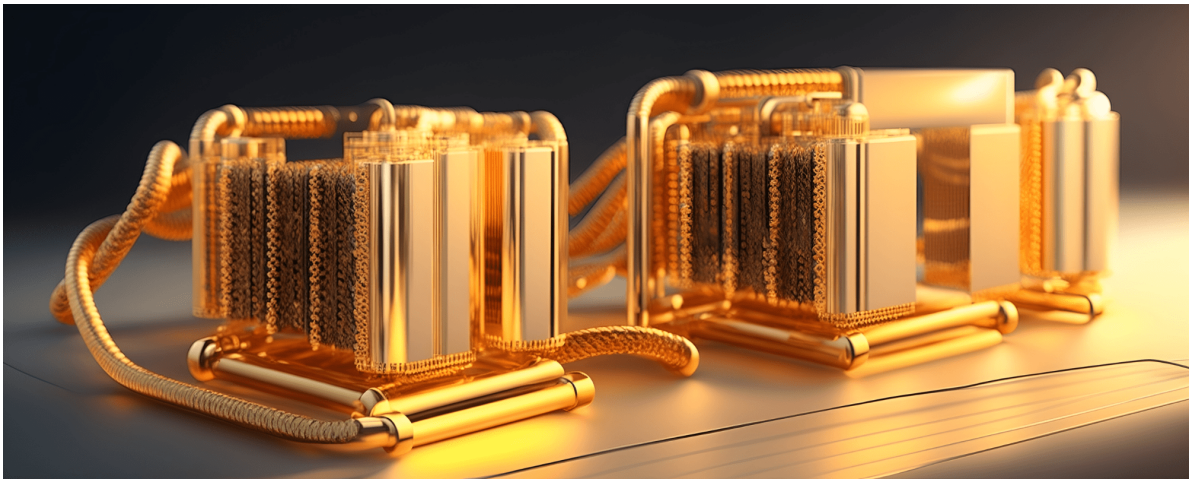
APROXIMACIÓN REGIONAL: GEOPOLÍTICA Y GOBERNANZA

# L’ordinador quàntic: un camí de ciència, tecnologia i sobirania

Alba Cervera Lierta



Luz, espacio y ordenadores cuánticos. Conceptualización: Luisa Quiroga

“Esta es, en el mejor de los sentidos, la idea más absurda que he oído nunca. [1] Esta fue la observación que el Premio Nobel de Física Richard Feynman soltó a Daniel Hillis cuando Hillis le explicó que quería fundar una empresa para construir un ordenador con un millón de procesadores trabajando en paralelo. La fascinación de Feynman por trabajar en las ideas más “absurdas” que se le presentaban lo llevó a hacer una estancia en el MIT con el equipo de Hillis el verano de 1983 para construir el prototipo de la Connection Machine, uno de los primeros superordenadores. No todas las empresas tienen la suerte de tener un Nobel de Física diseñando sus algoritmos y procesadores. Y es que Feynman no tuvo ningún problema a aprender desde cero y especializarse en un campo, el de la computación en paralelo, donde todo estaba por hacer.

El primer algoritmo que se ejecutó en la Connection Machine fue el del cálculo de logaritmos, desarrollado por el mismo Feynman cuarenta años antes durante el proyecto Manhattan. Inmediatamente después, Feynman utilizó este primer superordenador para hacer cálculos de física de partículas de forma mucho más eficiente que en los ordenadores existentes de la época. Y es que el interés de este físico por las máquinas de computar era claro. Descifrar los mecanismos de la naturaleza es cada vez más costoso matemáticamente, y se requiere una potencia de cálculo creciente a medida que bajamos más al detalle. De hecho, la computación tradicional, llamada “clásica”, encuentra uno de sus topes en el hecho de querer simular la física de los engranajes más pequeños de la naturaleza: la física cuántica. Este hecho empezaba a ser bien conocido por la comunidad científica en los años ochenta, y sobre todo por Feynman, que justo un par de años antes de

su “estancia de verano” impartió un seminario magistral sobre los límites de la computación clásica y la necesidad de la computación cuántica.

## La primera revolución cuántica

Hace más de un siglo nacía la física cuántica. Esta teoría física fue capaz de describir fenómenos y experimentos que la conocida como física clásica no podía explicar. Las consecuencias que se fueron desprendiendo de esta teoría eran sorprendentes y, en muchos casos, anti-intuitivas, pero también nos permitieron entender fenómenos como las reacciones nucleares de nuestro Sol o las propiedades de los elementos químicos y sus reacciones. Esta teoría física es la más precisa de todas y, por increíble que nos parezcan sus predicciones, es la que más se ha testeado y validado durante los últimos cien años.

Tan pronto como los humanos descubrimos el funcionamiento de fenómenos naturales, nuestro instinto nos impulsa a crear herramientas que los exploten. La física cuántica no fue una excepción. Enseguida empezaron a aparecer las primeras aplicaciones y dispositivos que se pudieron diseñar gracias a entender la mecánica cuántica: el láser, las placas solares, el GPS, la resonancia magnética, el transistor… Todos fueron surgiendo a mediados del siglo XX y constituyen un periodo que se conoce como *primera revolución cuántica*. Estos inventos, y muchos otros, fueron posibles gracias al hecho de entender fenómenos cuánticos colectivos.

Durante aquellos años, se estaban produciendo otras revoluciones tecnológicas en paralelo. En concreto, gracias a entender la física de los semiconductores, surgió el transistor (1947) y, posteriormente, sus sucesores, los microprocesadores. Con ellos, los humanos empezamos a ser capaces de hacer cálculos automatizados más y más complejos, con más precisión y sin errores. Poco a poco aprendimos formas cada vez más sofisticadas de procesar información codificada en sus unidades mínimas, los bits: los famosos 0 y 1 en que se basa toda la computación clásica.

> Hace más de un siglo nacía la física cuántica, que fue capaz de describir fenómenos y experimentos que la física clásica no podía explicar. Por increíble que nos parezcan sus predicciones, es la teoría que más se ha testeado y validado durante los últimos cien años

Algunos físicos se empezaron a preguntar también qué pasaría si la información se codificara en bits con propiedades cuánticas, denominados “qubits”. El campo de la información cuántica también surgió en aquellos años, aunque, en comparación con su hermana, la información clásica, se desarrolló prácticamente por completo en el terreno teórico, al no existir dispositivos capaces de contener y de controlar qubits.

La computación tradicional fue avanzando a un ritmo frenético y los cálculos se fueron intensificando a medida que los ordenadores eran más y más potentes. Los humanos también tenemos el instinto de poner todos nuestros inventos al límite y, en el caso de los computadores clásicos, uno de estos límites se encuentra en la cuántica.

Llegamos pues al año 1981, cuando Feynman se puso manos a la obra. En una de sus ponencias, manifestó la importancia de construir ordenadores con una capacidad de computación que aumentara a la vez que el tamaño de los sistemas que queremos simular con ellos. Eso significa que si, por ejemplo, queremos utilizar un ordenador para sumar dos números, necesitamos que sus recursos (memoria o número de operaciones por segundo) sean tan grandes como el tamaño de los números que queremos sumar. En cambio, si queremos multiplicarlos, necesitamos que este ordenador tenga unos recursos que crecen como el cuadrado de del tamaño de los números que queremos multiplicar. En el caso de la simulación de los sistemas cuánticos, los recursos necesarios crecen exponencialmente. Este tipo de crecimiento hace que para sistemas cuánticos pequeños podamos utilizar un ordenador estándar sin problemas, pero a medida que los sistemas se hacen grandes, ni siquiera un superordenador tiene bastantes recursos para almacenar tanta información (no hay que decir para hacer operaciones). El motivo es que los ordenadores clásicos codifican la información en bits, y para codificar información de un estado cuántico en una cadena de bits, necesitamos un número exponencial. La observación de Feynman consistió en remarcar que si en lugar de bits clásicos utilizáramos bits cuánticos, no tendríamos este problema de crecimiento exponencial de recursos computacionales. En otras palabras, hay que utilizar ordenadores cuánticos para simular y estudiar sistemas cuánticos.

¿Significa eso que los ordenadores clásicos son inservibles para estudiar la física cuántica? La respuesta es que no. Por un lado, este crecimiento exponencial de recursos que intentamos evitar se da en el peor de los casos: no todos los fenómenos o sistemas cuánticos tienen unas necesidades computacionales tan grandes. Por el otro, podemos (y hacemos) aproximaciones en nuestros cálculos que nos permiten obtener buenos resultados. Hace años que utilizamos superordenadores para estudiar sistemas cuánticos como la química, la ciencia de materiales o la física de partículas, y eso nos ha permitido avanzar en infinidad de campos y de aplicaciones. Todo ello nos da más motivos para perseguir la invención de ordenadores cuánticos que nos abran la puerta a entender mejor la física del mundo microscópico y, en consecuencia, nos aporten también más aplicaciones.

## La computación en la era de la segunda revolución cuántica

Aparte de Feynman, otros físicos de la época habían estado trabajando en las posibilidades de la computación cuántica. Yuri Manin llegó a la misma conclusión que Feynman prácticamente al mismo tiempo. Paul Beniorff hizo un análisis sobre el modelo matemático en que se podía basar la computación cuántica: la máquina de Turing cuántica. Durante los años ochenta, muchos físicos y matemáticos empezaron a proponer algoritmos cuánticos y a estudiar la complejidad computacional. La computación cuántica demostró que ciertos algoritmos se pueden acelerar sustancialmente con el uso de qubits.

El campo experimentó una gran sacudida cuando el físico Peter Shor propuso un algoritmo capaz de factorizar números de forma eficiente con un ordenador cuántico. Una aplicación matemática más si no fuera porque toda la criptografía que utilizamos hoy día se basa precisamente en el hecho de que factorizar no sea nada fácil. El algoritmo de Shor permite a un ordenador cuántico ideal romper toda la criptografía actual, y supone un gran riesgo para toda la ciberseguridad. Este descubrimiento puso la computación cuántica en el foco de la industria y los gobiernos al demostrar que un ordenador cuántico podía ser usado para mucho más que para simular sistemas físicos complejos.

Llega el nuevo milenio y, con él, las primeras puertas lógicas cuánticas experimentales. Cirac, Zoller, Mølmer y Sørensen, entre otros, desarrollan la teoría que casi inmediatamente se aplica experimentalmente y que permite hacer de la computación cuántica una realidad. Con las puertas lógicas, llegan también los qubits. Surgen cada vez más y más propuestas sobre cómo construir chips cuánticos. A diferencia de la computación tradicional, basada en el silicio, hay muchas tecnologías posibles para poder hacer qubits: iones atrapados, fotones, superconductores… Todas ellas se siguen construyendo y mejorando en paralelo, ya que tienen características muy diferentes entre sí.

> El algoritmo de Shor permite a un ordenador cuántico ideal romper toda la criptografía actual, y supone un gran riesgo para la ciberseguridad

En definitiva, la tecnología ya ha avanzado lo suficiente para hacer de la computación cuántica una realidad. Y, con eso, las empresas y los gobiernos empiezan a invertir seriamente en esta segunda revolución cuántica que, a diferencia de la primera, ya no se basa en fenómenos cuánticos colectivos: ahora somos capaces de controlar sistemas cuánticos individuales. Esta revolución tecnológica abarca las comunicaciones, los sensores y, por descontado, la computación.

## Ciencia, tecnología, soberanía

Nos encontramos en un momento histórico y privilegiado. Los prototipos de ordenadores cuánticos son ya una realidad y cada año nos encontramos con algún hito tecnológico. Universidades de todo el mundo tienen grupos diseñando, construyendo y mejorando ordenadores cuánticos hechos de varias tecnologías. Las empresas y las *start-ups* que construyen estos dispositivos empiezan a ofrecer sus servicios. La inversión pública y privada no para de crecer y cada vez surgen más aplicaciones potenciales.

Aun así, no todo es tan ideal como nos gustaría. Sí, tenemos ordenadores cuánticos, pero todavía son pequeños e imperfectos. Para poder implementar los algoritmos cuánticos más potentes que conocemos, necesitamos millones de qubits que sean prácticamente perfectos, es decir, que los posibles errores que puedan surgir durante la computación cuántica se

puedan corregir automáticamente. Desgraciadamente, la computación cuántica todavía no está tan avanzada como para que eso sea posible. Los ordenadores cuánticos actuales están formados por un puñado de qubits “ruidosos” (sin corrección de errores). Nos encontramos delante de lo que se conoce como “Noisy Intermediate-Scale Quantum Computation” (NISQ). Aun así, seguimos adelante y, a la vez que la tecnología mejora año tras año, también lo hacen los algoritmos y las aplicaciones. Muchas personas nos dedicamos a buscar cómo sacar el máximo provecho de los ordenadores cuánticos actuales y a prepararnos para los ordenadores cuánticos del futuro.

Y es que en este punto tenemos dos caminos: quedarnos parados y esperar que la tecnología mejore y que en el futuro alguien nos la ofrezca, o tomar la iniciativa y ser nosotros quienes desarrollemos este ordenador cuántico del futuro.

Europa está adoptando el segundo camino. Desde el 2018 tenemos iniciativas como Quantum Flagship (buque insignia cuántico): mil millones de euros de inversión en tecnologías cuánticas que se distribuyen en cinco grandes pilares: comunicación, sensores, simulación, computación y ciencia básica. En estos momentos, el programa Quantum Flagship está empezando la segunda fase de transferencia tecnológica, que intenta construir los prototipos de aplicaciones cuánticas estudiadas durante la primera fase del proyecto. Gracias a este proyecto están surgiendo muchas *start-ups* europeas especializadas en la fabricación de ordenadores cuánticos y sus componentes. También Europa ha incluido la computación cuántica en la reciente Ley europea de chips (European Chips Act). El mensaje es explícito: Europa no quiere depender en un futuro de tecnología extranjera de chips clásicos y cuánticos, queremos ser los proveedores, y el apoyo a la industria y la ciencia europea claro está.

¿En este punto, en el que tenemos universidades y centros de investigación estudiando y desarrollando la tecnología básica y en el que se está creando el tejido industrial necesario para explotar esta tecnología y construir los ordenadores cuánticos, dónde quedan los usuarios? Al fin y al cabo, alguien tendrá que utilizar esta computación para descubrir aplicaciones.

La computación cuántica ha llegado a un nivel de desarrollo suficiente para que salga de los laboratorios y se pueda ofrecer a los usuarios que quieran explotarla. Desde hace casi 10 años, algunas empresas como IBM, Google, Alibaba y *start-ups* como Rigetti Computing, D-WAVE Systems o IonQ ofrecen acceso remoto a sus ordenadores cuánticos. De hecho, proveedores de la nube como Amazon Web Services aglutinan muchos de estos ordenadores cuánticos y ofrecen un entorno único de acceso a estas máquinas. Aunque el acceso a algunos dispositivos pequeños puede llegar a ser gratuito, lo cierto es que los precios para acceder a los ordenadores cuánticos más avanzados están aumentando de manera significativa, hasta el punto que pueden ser prohibitivos para la mayoría de usuarios potenciales. En una tecnología como la computación cuántica, que promete ser tan disruptiva, garantizar el acceso a los investigadores e investigadoras y a las pequeñas empresas que quieren estudiar posibles aplicaciones pasa a ser fundamental. A esta situación hay que añadir la vertiente política: ¿quién tendrá los conocimientos y la industria capaces de construir y de utilizar la computación cuántica? ¿Estará únicamente en manos

privadas? ¿Qué países y regiones tendrán estas infraestructuras cuánticas?

En este punto es donde los centros de supercomputación dan un paso adelante y ofrecen su experiencia en mantener y dar servicios de supercomputación para hacerlo también en la computación cuántica. De la misma manera que el proyecto Quantum Flagship está financiando el desarrollo científico y tecnológico de las tecnologías cuánticas (entre ellas, la computación), EuroHPC —la rama de la Unión Europea que coordina los proyectos de computación de altas prestaciones— ha empezado a financiar proyectos de adquisición, instalación y operación de ordenadores cuánticos en entornos de supercomputación. Por una parte, el objetivo de la iniciativa EuroHPC es garantizar un acceso público a ordenadores cuánticos, de la misma manera que ya hace años que se garantiza para superordenadores clásicos. De la otra, se pretende fomentar el tejido tecnológico europeo adquiriendo tecnología desarrollada en la Unión Europea.

> La tecnología ya ha avanzado lo suficiente para hacer de la computación cuántica una realidad; las empresas y los gobiernos empiezan a invertir seriamente en esta segunda revolución cuántica. Pero los ordenadores cuánticos todavía son pequeños e imperfectos

Además, no se tiene que olvidar la dimensión científica, y es que todos los algoritmos cuánticos necesitan un componente de computación clásica. Para culminar cualquier algoritmo cuántico, hace falta preparar y procesar gran parte del problema utilizando computación tradicional. La idea principal es que sólo se ejecuta parte del algoritmo (la más costosa) en el chip cuántico, mientras que el resto es computación tradicional. Además, el mismo diseño y control de los ordenadores cuánticos se puede beneficiar sustancialmente de los avances en la computación clásica. Por lo tanto, los ordenadores cuánticos no competirán contra los superordenadores, sino que formarán parte de ellos. Un superordenador no es nada más que muchos ordenadores conectados y trabajando en paralelo. De la misma manera que los superordenadores actuales pueden contener diferentes tipos de procesadores (CPU, GPU, TPU…), también pueden contener procesadores cuánticos, que se utilizarán únicamente para las aplicaciones en que la computación tradicional se pueda quedar corta por la naturaleza del problema que se tiene que resolver.

## Despliegue de ordenadores cuánticos en Europa y en España

En estos momentos podemos encontrar varios prototipos de ordenadores cuánticos distribuidos por universidades, centros de investigación y empresas en territorio europeo. La gran mayoría están en un entorno de desarrollo, es decir, tienen el acceso restringido a los científicos y científicas que los construyen y estudian. De manera natural surgen iniciativas para ampliar este acceso a otros usuarios para los prototipos más avanzados.

Países como Francia, Finlandia, Alemania, Italia, Países Bajos o España han empezado proyectos que persiguen dar acceso a ordenadores cuánticos. El EuroHPC también está impulsando la Infraestructura Europea de Computación Cuántica y Simulación (EuroQCS) instalando ordenadores cuánticos de diferentes tecnologías y de fabricación europea en centros de supercomputación.

En concreto, en España tenemos el proyecto Quantum Spain, dirigido a la Red Española de Supercomputación (NADA) y coordinado por el Centro Nacional de Supercomputación, la Barcelona Supercomputing Center (BSC). El objetivo de este proyecto es instalar un ordenador cuántico en el BSC, el acceso al cual se dará a través de la Red Española de Supercomputación de forma gratuita, siguiendo los mismos protocolos que con el acceso a los superordenadores de la red. La empresa encargada de construir este ordenador cuántico será la start-up española Qilimanjaro, junto con la gran empresa de telecomunicaciones GMV. Esta unión de empresas va de la mano de proveedores tecnológicos europeos, cumpliendo así los objetivos que nos marca la Unión Europea de apostar por la soberanía tecnológica. Además de tener este ordenador cuántico, la Red Española de Supercomputación también desarrollará emuladores cuánticos que permiten simular el comportamiento de ordenadores cuánticos hasta cierto tamaño en un entorno controlado, para así estudiar los algoritmos cuánticos sin necesidad de utilizar un ordenador real. Quantum Spain también persigue desarrollar nuevos algoritmos y aplicaciones, y por eso la red colabora con multitud de universidades y centros de investigación españoles expertos en este campo. Finalmente, una pieza fundamental en cualquier desarrollo tecnológico es la formación de la nueva generación de expertos y expertas en esta tecnología. También forma parte de los objetivos de este proyecto impulsar todas las actividades e iniciativas que contribuyan a la atracción de talento hacia la computación cuántica.

Gracias al proyecto Quantum Spain y a la experiencia demostrada en supercomputación, Europa ha seleccionado España como uno de los primeros nodos del EuroQCS. El BSC tendrá un segundo ordenador cuántico financiado por la Unión Europea a través de la Empresa Común de Informática de Alto Rendimiento Europea (EuroHPC JU). Los dos ordenadores cuánticos se integrarán en el superordenador MareNostrum5, uno de los más potentes de Europa. Así, España tendrá una infraestructura de computación pionera y heterogénea, con procesadores con diferentes características. Los dos proyectos españoles, Quantum Spain y EuroQCS-Spain, han sido posibles gracias a la financiación de la Secretaría de Estado de Digitalización e Inteligencia Artificial con los fondos del Plan de recuperación, transformación y resiliencia (PRTR).

## Una mirada al futuro

La lucha europea para alcanzar la soberanía tecnológica se abandonó durante muchos años en favor de los supuestos beneficios de la globalización. Las tensiones geopolíticas constantes, agravadas por la pandemia global del coronavirus, han puesto de manifiesto todas las carencias industriales de los países de la UE y han reactivado los esfuerzos por convertir Europa en proveedor y no sólo en cliente.

Aunque la soberanía tecnológica debe ser un objetivo claro en la política europea, no hay que olvidar que la ciencia y el conocimiento no entienden de fronteras, y que las políticas de investigación tienen que ser capaces de alcanzar un equilibrio entre la protección de la propiedad intelectual y la colaboración científica e industrial. Países como Estados Unidos, Canadá o China poseen tecnología más avanzada que la europea. Al mismo tiempo, Europa es un gran generador de descubrimientos y de conocimiento y, en consecuencia, también es en muchos casos una gran exportadora de talento. Los ordenadores cuánticos todavía son inmaduros y su verdadero potencial todavía está por descubrir. Para enfrentarnos a un reto tecnológico tan grande, hace falta que todos y todas buscamos la mejor manera de colaborar, sin olvidar tampoco todo el talento que puede quedar escondido en otros países tradicionalmente menos enfocados a este campo científico.

> Todos los algoritmos cuánticos necesitan un componente de computación clásica. Los ordenadores cuánticos no competirán contra los superordenadores, sino que formarán parte de ellos

La computación cuántica no deja de ser un ejemplo más de los frutos que se pueden obtener cuando un grupo obstinado de científicos y científicas deciden hacerse preguntas sobre cómo funcionan los engranajes de la naturaleza y "qué pasaría si…?», sin poner necesariamente el foco en futuras aplicaciones o inventos (que tardarían años en llegar), sólo por el placer y la misión de expandir las fronteras del conocimiento, y deciden trabajar muchas veces en las ideas más absurdas que han oído nunca. Gracias a ellos y a ellas hoy recogemos los frutos de la ciencia del pasado, a la vez que plantamos las semillas de la ciencia y la tecnología del futuro.

NOTES

1 — La citación original es: "That is positively the dopiest idea I ever heard." Hillis, D. (1989) "Richard Feynman and the Connection Machine". *Physics Today*, núm. 42(2), p. 78.

REFERENCIAS BIBLIOGRÁFICAS


- Benioff, P. (1980) "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by turing machines". *Journal of Statistical Physics*, núm. 22(5), p. 563-591.

- Binosi, D. Calarco, T. Colin de Verdière, G. Corni, S. Garcia-Saez, A. Johansson, M. P. Kannan, V. Katz, N. Kerenidis, I. Latorre, J. I. Lippert, Th. Mengoni, R. Michielsen, K. Nominé, J. P. Omar, Y. Öster, P. Ottaviani, D. Schulz, M. Tarruell, L. (2022). "EuroQCS: European Quantum Computing & Simulation Infrastructure". Quantum Flaghship. Disponible en línea.

- Comissión Europea. “European Chips Act” (Ley europea de chips). Disponible en línea.

- EuroHPC – Joint Undertaking (2022). “Selection of six sites to host the first European quantum computers”. Nota de prensa de octubre de 2022 sobre la Empresa Común de Informática de Alto Rendimiento Europea. Disponible en línea.

- Feynman, R. P. (1982). “Simulating physics with computers”. *International Journal of Theoretical Physics*, núm. 21, p. 467-488.

- Manin, Y. (1980). *Computable and Uncomputable*. Moscou: Sovetskoye Radio, p. 128.

- Preskill, J. (2021). “Quantum computing 40 years later”. *Feynman Lectures on Computation*. Segunda edición, publicado por Taylor & Francis Group, editat per Anthony J. G. Hey.



**Alba Cervera Lierta**

Alba Cervera Lierta es investigadora del Barcelona Supercomputing Center – Centro Nacional de Supercomputación (BSC-CNS). Es doctora en computación e información cuántica por la Universidad de Barcelona y posee un máster en Física de Partículas. Tras su doctorado, se trasladó a la Universidad de Toronto como investigadora posdoctoral en el grupo Alán Aspuru-Guizik. Sus ámbitos de estudio tratan de la computación cuántica y sus aplicaciones a corto plazo, así como de las sinergias entre la física cuántica y la inteligencia artificial. Desde octubre de 2021, es coordinadora del proyecto Quantum Spain, una iniciativa de impulso del ecosistema de computación cuántica cuyo objetivo es operar un ordenador cuántico en el BSC-CNS.