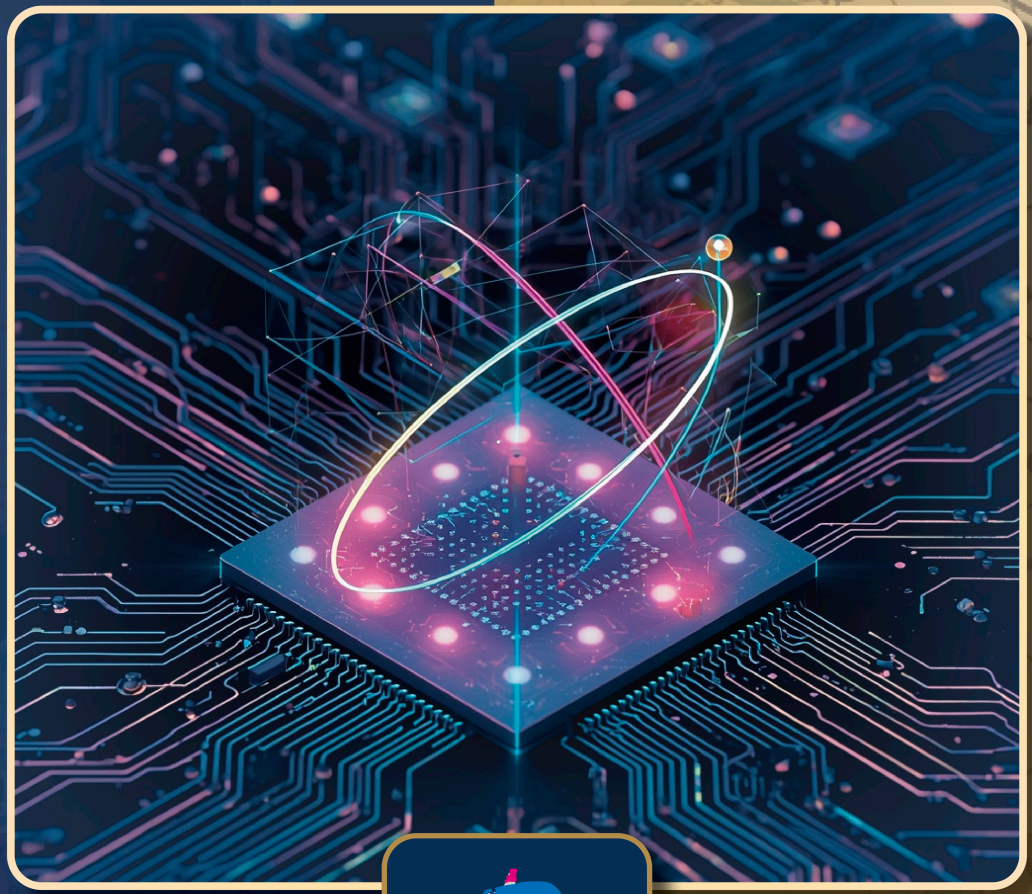
JACINTO VELASCO REBOLLEDO

COMPUTACIÓN CUÁNTICA

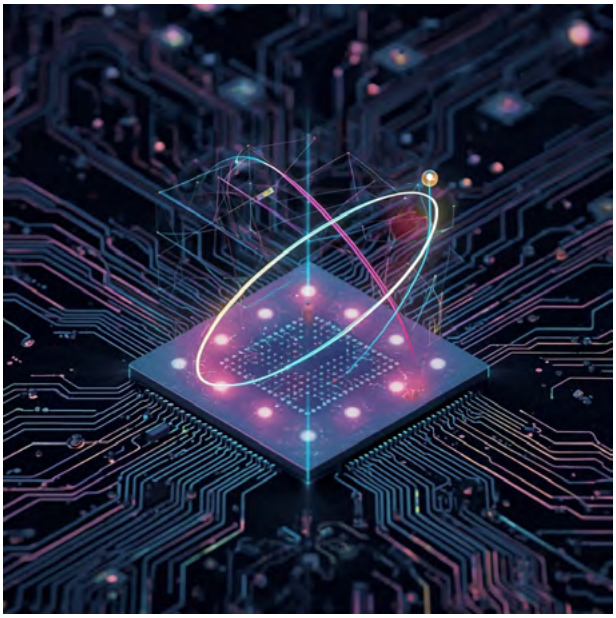
Circuitos, algoritmos y aplicaciones reales



DIAZ DE SANTOS

COMPUTACIÓN CUÁNTICA

Circuitos, algoritmos
y aplicaciones reales



JACINTO VELASCO REBOLLEDO

DIAZ DE SANTOS

Madrid • Buenos Aires • México • Bogotá

Ediciones Díaz de Santos
Internet: http//www.editdiazdesantos.com
E-mail: ediciones@editdiazdesantos.com

ISBN: 978-84-9052-592-0 (edición papel)
e-ISBN: 978-84-593-7 (edición digital)
Depósito Legal: M-10381-2026

Diseño de cubierta y Fotocomposición: P55 Servicios Culturales

Índice

Prólogo

La computación está cambiando de forma irreversible. Durante décadas, los ordenadores cuánticos habitaron exclusivamente el terreno de la especulación teórica o la ciencia ficción. Hoy, constituyen una realidad tangible que redefine los cimientos mismos del procesamiento de información. La transición de lo cuántico desde los laboratorios académicos hacia los centros de datos empresariales ha dejado de ser promesa para convertirse en fenómeno industrial. Gobiernos, universidades, corporaciones globales y startups tecnológicas están invirtiendo miles de millones no por curiosidad intelectual, sino porque han comprendido que se abre una nueva dimensión en la forma de interactuar con la información, el conocimiento y la materia.

Este libro nace en ese contexto: no como un ejercicio abstracto, sino como un puente entre dos mundos. Por un lado, la física cuántica, con su estructura matemática rigurosa y sus principios contraintuitivos —superposición, entrelazamiento, interferencia— que desafían las nociones clásicas de causalidad y determinismo. Por otro, la ingeniería, la industria, la economía del dato, que buscan soluciones concretas a problemas reales. En estas páginas, propongo un recorrido que parte desde los postulados fundamentales de la mecánica cuántica hasta los algoritmos de vanguardia que ya se ejecutan en hardware disponible. No se trata de especulación, sino de análisis y aplicación.

Nos encontramos en plena era NISQ (Noisy Intermediate-Scale Quantum), procesadores con decenas e incluso cientos de cúbits, todavía ruidosos, imperfectos, pero funcionales. Esta etapa de transición ha catalizado enfoques creativos, como el aprendizaje automático cuántico, los modelos híbridos que combinan redes neuronales clásicas con circuitos parametrizables, y las estrategias de mitigación de ruido. Este libro ofrece una visión estructurada de estas sinergias emergentes, abordando tanto la teoría como su implementación práctica. Cada capítulo está pensado no solo para informar, sino para inspirar: mediante circuitos explicativos, visualizaciones accesibles y aplicaciones reales, se invita al lector a explorar activamente este nuevo paradigma.

Sin embargo, más allá del contenido técnico, el propósito de esta obra es más profundo: formar criterio. La computación cuántica no es únicamente

una oportunidad tecnológica, es una apuesta estratégica global. Firmas como McKinsey proyectan que este mercado podría superar el billón de dólares hacia 2035. Pero la magnitud de su impacto no será únicamente económica, sino civilizacional. El poder de simular moléculas con precisión cuántica acelerará la farmacología y la medicina personalizada. La optimización combinatoria redefinirá la logística, la energía y las finanzas. Y la criptografía post cuántica determinará el estándar de seguridad en la era de los datos.

Quien domine estos conceptos adquirirá una ventaja profesional diferencial. Para el ingeniero o científico, se trata de pasar de implementador a creador, de consumidor de herramientas a arquitecto de soluciones. Para el decisor estratégico o gestor de innovación, comprender el funcionamiento real de los algoritmos cuánticos permitirá discernir entre ruido de mercado y oportunidades legítimas. Esta obra está escrita con ambos perfiles en mente. Es técnica, sí, pero también formativa. Porque el futuro no lo determinarán las tecnologías disponibles, sino las mentes que sepan interpretarlas y dirigirlas.

Publicar este libro no responde a un entusiasmo pasajero. Representa el fruto de años de trabajo, reflexión y colaboración con instituciones de investigación y centros de innovación. Mi compromiso como autor es ofrecer una guía clara, crítica y útil. Una brújula para navegar el mar cuántico que se avecina. No pretendo dar respuestas definitivas, pero sí proporcionar el lenguaje, las herramientas y la perspectiva necesaria para que cada lector construya las suyas con fundamento.

Si has llegado hasta aquí, ya formas parte de esta transformación. Bienvenido a la era cuántica. Que este libro sea tu punto de partida para comprenderla, aprovecharla y, por qué no, liderarla.

Dr. Jacinto Velasco Rebolledo

¿A quién va dirigido este libro?

Este libro nace con el propósito de servir como una guía académica, técnica y estratégica para navegar con solvencia la revolución tecnológica que representa la computación cuántica. Está dirigido a todas aquellas personas que no solo desean conocer esta nueva forma de procesar información, sino comprenderla con profundidad y aplicarla con sentido crítico. La obra está diseñada para acompañar tanto al lector que se inicia con formación técnica sólida como al profesional experimentado que busca tomar decisiones fundamentadas en torno a esta tecnología emergente.

Estudiantes universitarios y de posgrado

Dirigido a quienes cursan programas en física, ingeniería, matemáticas, informática o ciencias de datos, este libro proporciona una formación teórico-práctica completa que permite abordar algoritmos cuánticos reales, entender su arquitectura, modelado y simulación, y entrenar circuitos variacionales sobre hardware actual. Es ideal como texto de estudio, material de cátedra o preparación para investigación.

Investigadores y docentes universitarios

Para académicos que trabajan en computación cuántica, física aplicada, química computacional o aprendizaje automático cuántico, este libro actúa como una herramienta de consulta rigurosa y didáctica, con estructura formal, fundamentos matemáticos desarrollados, y casos de uso actuales. Su nivel técnico permite ser usado como base para cursos avanzados o para orientar trabajos de tesis y desarrollo experimental.

Ingenieros y profesionales del sector tecnológico

Ingenieros en software, desarrolladores de algoritmos, científicos de datos y arquitectos de sistemas que deseen integrar componentes cuánticos en sus flujos de trabajo encontrarán en este libro una hoja de ruta clara y sin simplificaciones. Desde la codificación de datos hasta la optimización

híbrida y el análisis de resultados mediante *bitstrings*, cada tema está acompañado por esquemas operativos y explicaciones aplicadas.

Directivos, líderes de innovación y tomadores de decisiones

En un entorno tecnológico cada vez más complejo, este libro está especialmente pensado para ayudar a ejecutivos, gestores de I+D, CTOs, responsables de inversión y estrategia tecnológica a comprender qué es realmente la computación cuántica, qué puede y no puede hacer en la actualidad, y cómo evaluar oportunidades reales sin caer en falsas promesas o discursos inflados. Comprender lo cuántico es hoy una ventaja competitiva, y este libro proporciona los fundamentos necesarios para tomar decisiones con criterio y visión.

Autodidactas avanzados y tecnólogos curiosos

Profesionales y entusiastas con bases en álgebra, lógica computacional o física moderna que desean profundizar en lo cuántico encontrarán aquí un texto desafiante pero claro, sin tecnicismos innecesarios, estructurado para guiar paso a paso desde los principios físicos hasta la ejecución de algoritmos en hardware actual.

Recursos del autor y repositorio de código

Con el objetivo de facilitar el aprendizaje activo, promover la reproducibilidad científica y extender el contenido más allá del texto impreso, este libro se complementa con un repositorio público de código fuente alojado en GitHub. Este recurso digital ha sido cuidadosamente diseñado para acompañar al lector en su recorrido, permitiéndole experimentar directamente con los algoritmos, circuitos y arquitecturas descritas en los distintos capítulos.

El repositorio organiza su contenido en correspondencia directa con la estructura del libro. Cada capítulo teórico cuenta con una carpeta específica que incluye los scripts, bloques de código y archivos auxiliares necesarios para ejecutar los ejemplos allí presentados. De este modo, se garantiza una experiencia didáctica coherente y alineada con la narrativa técnica de la obra.

Contenido del repositorio

El lector encontrará implementaciones completas de:

- Circuitos variacionales y modelos híbridos, tales como VQE, QAOA, clasificadores cuánticos y codificadores de datos.
- Simulaciones cuánticas reproducibles, que replican exactamente los resultados numéricos, visuales y esquemáticos del libro.
- Scripts en Python, desarrollados sobre bibliotecas de uso profesional como Qiskit, PennyLane, NumPy, Matplotlib y otras herramientas auxiliares relevantes.
- Ejemplos de ejecución en hardware real, configurados para ser ejecutados directamente en plataformas como IBM Quantum Experience y compatibles con simuladores locales.
- Plantillas de entrenamiento híbrido, que integran circuitos cuánticos parametrizables con optimizadores clásicos, tal como

se describe en las secciones de aprendizaje automático cuántico.

- Visualizaciones interactivas, figuras dinámicas y herramientas de análisis de estados, fidelidades y métricas cuánticas relevantes.

Accesibilidad y documentación

Cada módulo de código está acompañado por documentación explicativa en formato README.md, así como instrucciones paso a paso para su ejecución, requisitos de entorno, ejemplos de uso y recomendaciones de hardware. Se ha procurado mantener un estilo limpio, modular y extensible, de modo que el lector pueda modificar, adaptar o ampliar los scripts a sus propias investigaciones o prácticas educativas.

Finalidad pedagógica y científica

Este entorno de trabajo no es una simple colección de ejemplos, sino una herramienta pedagógica pensada para aprender haciendo. La computación cuántica, al igual que otras disciplinas emergentes, requiere experiencia directa con código, datos, entrenamiento de modelos y experimentación sobre hardware real. El repositorio permite precisamente eso: convertir la teoría en práctica, y el conocimiento en experiencia tangible.

El acceso completo al material se encuentra disponible en el github del autor.

También está disponible para la descarga en la siguiente dirección:

https://www.editdiazdesantos.com/libros/9788490525920

jvelareb/QC

1 Fundamentos de la computación cuántica

1.1 Introducción y motivación histórica

Para entender la computación cuántica hay que entender una crisis. Durante el siglo XX, confiamos en que podíamos simular el mundo usando ordenadores clásicos. Y funcionó para calcular trayectorias balísticas o gestionar bases de datos bancarias. Pero cuando los físicos intentaron simular la naturaleza a escala atómica, se toparon con un muro: las leyes de Newton no aplican allí. Átomos y electrones se rigen por principios que la lógica binaria (ceros y unos) no puede digerir eficientemente.

La chispa saltó en 1981, cuando el Nobel Richard Feynman planteó una provocación: si la naturaleza es cuántica, nuestros simuladores también deberían serlo. Feynman notó que la complejidad de un sistema cuántico crece brutalmente. Un sistema de N partículas no tiene un solo estado, sino una combinación de 2^n posibilidades simultáneas. Con apenas 300 partículas, el número de parámetros necesarios para definirlas supera al número de átomos en el universo observable. Ningún superordenador clásico, ni presente ni futuro, podría jamás manejar esa cantidad de datos a la fuerza bruta. Hacía falta un nuevo tipo de máquina.

Lo que empezó como una curiosidad teórica cobró forma en 1985, cuando David Deutsch definió el modelo del ordenador cuántico universal, demostrando que no era una fantasía física. Pero la verdadera sacudida llegó en los 90. Peter Shor demostró que estas máquinas hipotéticas podrían romper la criptografía moderna (factorizando números enteros a velocidades imposibles para un PC clásico), y Lov Grover probó que podrían buscar en bases de datos desordenadas con una eficiencia inaudita.

De pronto, la computación cuántica dejó de ser filosofía para convertirse en una carrera tecnológica. No se trata solo de hacer cálculos más rápido, se trata de calcular de otra forma. Como dijo Seth Lloyd: "el universo es, en esencia, un ordenador cuántico". El objetivo ahora es construir máquinas que hablen ese mismo idioma fundamental para dejar de simular la realidad y empezar a replicarla.

1.2 La computación cuántica... ¿realidad o ficción?

1.2.1 Argumentos a favor

Esta es una de las preguntas más fascinantes y controvertidas de la ciencia contemporánea en torno a la computación cuántica. Después de décadas de desarrollo teórico y experimental, la comunidad científica se encuentra dividida entre optimistas convencidos, escépticos fundamentados y quienes adoptan posturas intermedias. Conviene analizar con rigor los argumentos de cada lado, apoyándonos en los logros documentados y reconociendo los desafíos pendientes.

La teoría de la computación cuántica se basa en principios físicos bien establecidos de la mecánica cuántica, lo que ya es un sólido punto de partida. Además, existen logros experimentales recientes que respaldan el optimismo. Por ejemplo, el teorema del umbral de tolerancia a fallos demuestra teóricamente que la corrección de errores cuánticos es posible si las tasas de error de las puertas se mantienen por debajo de cierto umbral crítico. Esto implica que, en principio, una computadora cuántica a gran escala y libre de errores es alcanzable con suficiente refinamiento tecnológico.

El 23 de octubre de 2019 se informó públicamente que el procesador cuántico Sycamore, desarrollado por Google, habría alcanzado lo que se conoce como supremacía cuántica. Esta afirmación se fundamentó en la ejecución de un circuito cuántico aleatorio compuesto por 53 cúbits, cuya resolución se completó en aproximadamente 200 segundos. Según estimaciones preliminares, dicha tarea habría requerido, en su equivalente clásico, un tiempo computacional del orden de 10.000 años, incluso para los superordenadores más potentes disponibles en esa época. No obstante, esta aseveración fue objeto de cuestionamiento. Investigadores de IBM argumentaron que, mediante una optimización sustancial de algoritmos clásicos y el aprovechamiento de la arquitectura Summit, el mismo cálculo podría completarse en un intervalo considerablemente menor, estimado en aproximadamente dos días y medio.

A pesar del debate técnico generado, el evento marcó un punto de inflexión en el desarrollo del hardware cuántico y permitió evidenciar una ventaja computacional concreta, aunque restringida a un tipo de problema artificialmente estructurado. A partir de ese momento se ha observado una

intensificación sustancial en los esfuerzos industriales orientados a extender dicha ventaja. Compañías como IBM, IonQ y Rigetti han presentado procesadores operativos con decenas e incluso centenas de cúbits físicos. Sin embargo, debe señalarse que el número de cúbits lógicos funcionales, entendidos como aquellos capaces de participar en cómputos tolerantes a fallos, permanece limitado por restricciones prácticas vinculadas con la fidelidad, el acoplamiento y la corrección de errores.

IBM ha delineado una hoja de ruta tecnológica en la que se proyecta la integración de más de 1.000 cúbits físicos en un solo chip en un horizonte temporal breve. Asimismo, se ha planteado como objetivo el desarrollo de sistemas con 100.000 cúbits para el año 2030. Esta expansión contempla el uso de arquitecturas modulares que emplean enlaces cuánticos coherentes para interconectar múltiples unidades, lo cual introduce retos adicionales relacionados con la sincronización entre nodos, la latencia de comunicación y la implementación de códigos de corrección de errores distribuidos.

Desde la perspectiva económica, la inversión privada en computación cuántica ha adquirido una magnitud que refleja una convicción creciente en su viabilidad técnica y en su potencial transformador para diversas industrias. Grandes corporaciones tecnológicas como Microsoft, Amazon, Google e IBM mantienen divisiones especializadas dedicadas a esta área del conocimiento. Además, numerosas startups han logrado captar financiamiento de riesgo por montos que ascienden a cientos de millones de dólares. Las proyecciones elaboradas por analistas del sector sugieren que el mercado cuántico global podría alcanzar un volumen estimado en 1,3 billones de dólares estadounidenses hacia el año 2035. Dicho crecimiento abarcaría aplicaciones en dominios como optimización industrial, simulación molecular, servicios financieros, inteligencia artificial y seguridad criptográfica.

Los argumentos que sustentan la legitimidad del progreso cuántico no se restringen a expectativas de largo plazo. Se dispone actualmente de resultados experimentales concretos que ratifican la solidez física del enfoque. Entre estos se encuentran fidelidades superiores al 99.9 por ciento en la ejecución de puertas lógicas elementales, validación empírica de correlaciones cuánticas multipartitas en sistemas de escala intermedia, e implementación inicial de esquemas de corrección de errores basados en códigos como el de superficie y el de Shor. Asimismo, el formalismo matemático que sustenta la teoría cuántica, articulado mediante operadores lineales en espacios de

Hilbert, permanece coherente internamente y en consonancia con todos los principios físicos confirmados experimentalmente.

En consecuencia, el estado actual del arte en computación cuántica permite identificar una confluencia entre la viabilidad conceptual, la validación empírica y el compromiso sostenido del sector industrial. Aunque persisten desafíos técnicos de notable complejidad, tales como la escalabilidad efectiva, la mitigación de la decoherencia y la implementación robusta de códigos de corrección de errores, los avances acumulados en los últimos años constituyen evidencia sustancial de que se está transitando hacia la consolidación de computadores cuánticos de utilidad práctica.

1.2.2 Argumentos en contra

Muchos físicos e ingenieros, por otro lado, mantienen un escepticismo saludable sobre los plazos y alcances de la computación cuántica, señalando desafíos que podrían ser insuperables o al menos demorarlo todo varias décadas. Existen limitaciones técnicas fundamentales que hoy por hoy no tienen solución clara. Por ejemplo, los mejores cúbits superconductores actuales mantienen coherencia durante apenas decenas de microsegundos bajo condiciones de laboratorio extremadamente controladas. Cada cúbit adicional y cada operación realizada multiplican las oportunidades de error. Las estimaciones sugieren que un solo cúbit lógico (es decir, completamente corregido de errores) podría requerir del orden de 1.000 cúbits físicos de alta calidad trabajando en conjunto. El Dr. Mark Horowitz, quien presidió un panel de las Academias Nacionales de EE. UU. sobre el tema, señalaba que harían falta aproximadamente 100.000 veces más cúbits de los que tenemos hoy, y tasas de error 100 veces menores para construir un computador cuántico de propósito general plenamente funcional. Estas cifras dan una idea de la enorme brecha que aún existe entre los prototipos actuales y una máquina escalable y útil.

Algunos expertos argumentan que controlar los enormes números de parámetros continuos en un sistema de muchos cúbits podría estar más allá de la realidad física. Para una computadora cuántica ideal de 1.000 cúbits (sin errores), el número de parámetros cuánticos a calibrar y mantener coherentes excedería astronómicamente el número de átomos en el universo. Además, el matemático Gil Kalai ha sostenido que las distribuciones de

probabilidad obtenidas de dispositivos cuánticos NISQ (de escala intermedia y ruidosos) serían en la práctica combinaciones de distribuciones clásicas sensibles al ruido, sin capacidad real de superar a los algoritmos clásicos. Su argumento, basado en una teoría matemática de sensibilidad al ruido desarrollada en los años 90, sugiere que el propio ruido cuántico podría imposibilitar ventajas significativas a gran escala.

Los escépticos plantean desafíos fundamentales: la decoherencia rápida, la corrección de errores masiva necesaria, la complejidad de calibración, e incluso la posibilidad de que la propia naturaleza cuántica sea demasiado sensible al entorno para ofrecer ventajas robustas. Estas objeciones no deben ser ignoradas, porque delinean con precisión los obstáculos que cualquier arquitectura cuántica deberá superar.

1.2.3 Posiciones intermedias y matizadas

Entre el optimismo y el escepticismo extremos, muchos expertos adoptan una posición intermedia. Reconocen que los dispositivos cuánticos actuales de tipo NISQ pueden tener una utilidad limitada en problemas específicos, sin representar todavía una revolución computacional general. La evidencia reciente sugiere una realidad más matizada. Por ejemplo, un informe de Forrester Research de 2024 concluía que, aunque la computación cuántica había logrado avances importantes, permanece experimental, con aplicaciones a gran escala probablemente aún a una década de distancia. En esta línea, se espera que en el corto y mediano plazo las ventajas cuánticas se circunscriban a dominios muy concretos (como la simulación química o ciertos problemas de optimización), mientras que la informática clásica seguirá dominando la computación de propósito general durante años.

Un hecho ilustrativo es que ya existen algunos resultados prácticos acotados en la era NISQ. La empresa D-Wave Systems, por ejemplo, ha reportado éxitos con su enfoque de computación cuántica de reconocido (*quantum annealing*), en colaboración con otros clientes lograron optimizar recursos de red móvil en 40 segundos, cuando un método clásico requería 27 horas para el mismo problema, y con Pattison Food Group redujeron un problema de planificación de 80 horas clásicas a solo 15 horas, ahorrando un 80% de tiempo. Si bien estas aplicaciones no implican una supremacía general, muestran que la computación cuántica no es ni pura ficción ni realidad

completamente madura. Es una tecnología emergente con logros verificables, pero también con limitaciones significativas.

Lo importante, coinciden muchos, es que el debate ha resultado productivo, el escepticismo informado actúa como una herramienta para exigir rigor en las afirmaciones y refinar la narrativa, separando la publicidad exagerada del progreso real. Así, mientras los argumentos escépticos plantean desafíos legítimos que la comunidad debe resolver, los avances técnicos documentados demuestran un progreso constante.

La pregunta no es entonces simplemente ¿realidad o ficción?, sino más bien para qué problemas específicos será útil la computación cuántica, en qué horizonte temporal, y con qué limitaciones. La respuesta probablemente sea que esta tecnología encontrará aplicaciones prácticas en dominios puntuales mucho antes de convertirse (si es que lo hace alguna vez) en una sustituta general de las computadoras clásicas. En cualquier caso, el diálogo entre expectativas y cautela está guiando la investigación hacia metas concretas y alcanzables

1.3 El mercado de la computación cuántica

La historia de la computación cuántica ha alcanzado un capítulo decisivo en 2024 y 2025. Lejos de ser ya una mera curiosidad científica confinada a los laboratorios de física teórica, la tecnología ha cruzado el umbral hacia la utilidad práctica. Las Naciones Unidas han designado el año 2025 como el Año Internacional de la Ciencia y la Tecnología Cuántica, conmemorando un siglo desde el desarrollo inicial de la mecánica cuántica, pero más importante aún, marcando el momento en que la industria global ha comenzado a validar esta tecnología como un componente futuro de la infraestructura crítica.

El cambio más profundo que define el estatus actual de la computación cuántica es filosófico y técnico: la industria ha dejado de obsesionarse únicamente con aumentar el número de cúbits (la unidad básica de información cuántica) para centrarse en estabilizar los cúbits. Este giro de hacer crecer los cúbits a estabilizar los cúbits es la señal definitiva para las industrias de misión crítica de que la tecnología pronto será lo suficientemente segura y fiable como para integrarse en sus operaciones. Nos encontramos en la transición de la era experimental a una fase de despliegue temprano,

donde la prioridad es la fidelidad del cálculo y la corrección de errores sobre la potencia bruta inestable.

Esta maduración se refleja en las valoraciones del mercado, que muestran una trayectoria de crecimiento fenomenal. Aunque las estimaciones varían, el consenso es de una expansión explosiva. Se calcula que el mercado de tecnologías cuánticas (que abarca computación, comunicación y detección) podría alcanzar un valor total de hasta 198.000 millones de dólares para el año 2040. Específicamente, el segmento de la computación cuántica, que partía de una valoración de aproximadamente 1.420 millones de dólares en 2024, se proyecta que crezca a una tasa compuesta anual (CAGR) de más del 30% en los próximos años, con algunas previsiones situando su valor entre 90.000 y 170.000 millones de dólares para 2040. Este crecimiento no es lineal y se espera que sea disruptivo, con un efecto multiplicador de 158 veces sobre el periodo actual, lo que indica una demanda tremenda y una transformación industrial inminente.

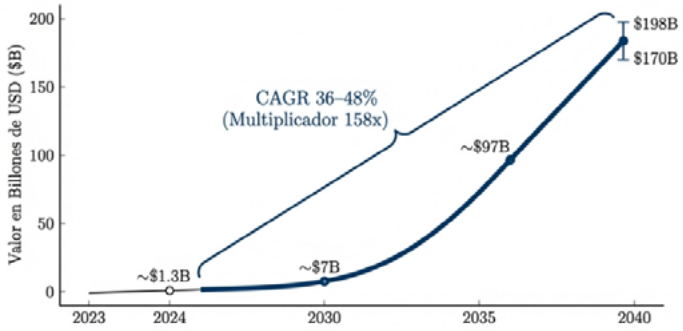


Figura 1.1. Volumen de negocio de la computación cuántica.

En el corazón de esta revolución se encuentra una batalla feroz por la supremacía del hardware. Los gigantes tecnológicos y los startups más avanzados han logrado hitos que redefinen lo posible. Google, por ejemplo, ha sacudido la industria con su chip cuántico Willow. Este procesador ha demostrado una capacidad asombrosa para la corrección de errores, realizando en menos de cinco minutos un cálculo que a una supercomputadora clásica le tomaría 10 septillones de años. Este logro no es solo una demostración de velocidad, sino una prueba de concepto vital de que los errores cuánticos pueden ser gestionados a escala.

Paralelamente, IBM ha continuado su marcha hacia la escalabilidad con la presentación del Quantum System Two, un sistema modular diseñado para integrar la computación cuántica con sistemas clásicos, facilitando el camino hacia la supercomputación centrada en lo cuántico. No se trata solo de chips superconductores, Microsoft ha introducido el chip *Majorana 1*, basado en una arquitectura topológica que promete resolver problemas de escala industrial en años en lugar de las décadas que se preveían anteriormente.

Sin embargo, el acceso a estas máquinas prodigiosas no implica necesariamente que cada empresa tenga un ordenador cuántico en su sótano. El modelo dominante que ha emergido es la Computación Cuántica como Servicio (QCaaS). Dado el costo prohibitivo y la complejidad de mantener el hardware (que a menudo requiere temperaturas cercanas al cero absoluto), la mayoría de las organizaciones accederán a esta potencia a través de la nube. Se proyecta que el mercado de QCaaS alcance los 48.300 millones de dólares para 2033, democratizando el acceso a la tecnología y permitiendo a investigadores y empresas probar algoritmos sin inversiones de capital masivas.

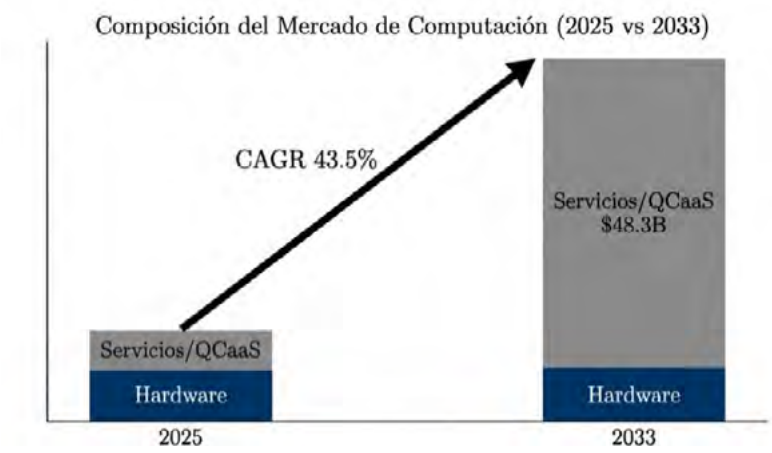


Figura 1.2. Mercado estimado con visión 2033 de la computación cuántica.

La computación cuántica ha dejado de ser un asunto puramente comercial para convertirse en una cuestión de seguridad nacional de primer orden. El mapa geopolítico de la inversión está cambiando drásticamente. Históricamente, América del Norte, liderada por Estados Unidos, ha mantenido una posición dominante, controlando alrededor del 38% al 43% del

mercado global en años recientes. Sin embargo, su hegemonía se está erosionando frente al avance agresivo de Asia y la consolidación de Europa.

Figura 1.3. Mapa de países más influyente en 2025 en computación cuántica.

En 2024, se observó un fenómeno revelador: mientras que la financiación privada (capital de riesgo) disminuyó un 19%, la financiación pública y gubernamental se disparó, representando el 34% de toda la inversión total en startups cuánticas. Los gobiernos están interviniendo con urgencia, reconociendo que quedarse atrás en esta carrera implica vulnerabilidad estratégica.

El desarrollo de la computación cuántica presenta una dinámica claramente diferenciada a nivel geográfico, con Asia emergiendo como una de las regiones que avanza con mayor rapidez. Japón ha adoptado una estrategia particularmente ambiciosa, anunciando en 2025 una inversión del orden de 7.400 millones de dólares, equivalente a más de un billón de yenes, destinada al fortalecimiento del ecosistema nacional de tecnologías cuánticas. Esta iniciativa responde al objetivo explícito de recuperar terreno frente a otros actores globales y de establecer una infraestructura sólida que permita al país desempeñar un papel de liderazgo tecnológico durante la próxima década.

China, por su parte, continúa consolidando su posición dominante en términos de propiedad intelectual. El país lidera de forma sostenida el número de solicitudes de patentes relacionadas con computación cuántica, lo que refleja un enfoque estratégico de largo plazo orientado al control de tecnologías clave y a la construcción de ventajas competitivas estructurales. Esta acumulación sistemática de patentes sugiere una política deliberada de

consolidación de capacidades tanto científicas como industriales en el ámbito cuántico.

Europa mantiene igualmente una posición relevante en el panorama internacional. En 2024, la región capturó más del 33 por ciento de la cuota de mercado global de tecnologías cuánticas según diversas métricas sectoriales, resultado de una colaboración estrecha y sostenida entre instituciones académicas, centros de investigación y actores industriales. Este modelo de cooperación ha permitido una transferencia eficiente de conocimiento desde la investigación fundamental hacia aplicaciones tecnológicas concretas.

Dentro del contexto europeo, varios países han intensificado de manera notable sus compromisos financieros. España anunció en 2025 inversiones del orden de 900 millones de dólares destinadas al desarrollo de capacidades en computación cuántica, mientras que Alemania y el Reino Unido continúan financiando de forma significativa programas de investigación en semiconductores avanzados y tecnologías cuánticas. Estas iniciativas reflejan una comprensión compartida de que la computación cuántica constituye un eje estratégico para la competitividad científica, tecnológica y económica a medio y largo plazo.

1.4 Bits, cúbits y principios cuánticos

1.4.1 Del bit clásico al cúbit

Toda la tecnología digital contemporánea se fundamenta en una idea extremadamente simple y, al mismo tiempo, extraordinariamente poderosa: el bit. El bit constituye la unidad básica de información en la computación clásica y solo puede adoptar dos estados posibles, convencionalmente representados como 0 y 1. Esta dicotomía se ha interpretado históricamente de múltiples maneras equivalentes, tales como apagado y encendido o falso y verdadero. Resulta notable que un concepto tan elemental haya sido suficiente para sustentar el desarrollo completo del ecosistema computacional moderno, desde dispositivos personales hasta infraestructuras de cálculo a escala planetaria.

En las primeras computadoras de mediados del siglo XX, los bits físicos se implementaban mediante tubos de vacío de tamaño macroscópico, con elevados consumos energéticos y limitaciones severas de fiabilidad. Con el

avance de la microelectrónica, estos elementos fueron reemplazados progresivamente por transistores cada vez más pequeños, hasta alcanzar en la actualidad dimensiones del orden de pocos nanómetros. A pesar de esta evolución tecnológica, el principio lógico subyacente ha permanecido inalterado. Un bit clásico se encuentra siempre en un estado bien definido en cada instante del tiempo, ya sea 0 o 1, sin posibilidad de adoptar valores intermedios o superposiciones.

La física cuántica, en contraste, describe el comportamiento de la materia y la radiación a escalas subatómicas de una manera radicalmente distinta. En este régimen, los sistemas físicos no se caracterizan por estados bien definidos antes de la observación, sino por funciones de onda que codifican distribuciones de probabilidad sobre múltiples configuraciones posibles. Electrones, fotones y átomos pueden encontrarse en superposiciones coherentes de estados, una propiedad que carece de análogo directo en la experiencia macroscópica cotidiana.

Esta característica fundamental del mundo cuántico es precisamente la que se explota en la computación cuántica mediante el concepto de cúbit, abreviatura de bit cuántico. El cúbit no constituye una simple extensión del bit clásico, sino una entidad física cuya descripción requiere el formalismo completo de la mecánica cuántica. A diferencia del bit clásico, que solo puede adoptar uno de sus dos valores posibles en cada instante, un cúbit puede encontrarse en una superposición coherente de los estados básicos asociados a 0 y 1 hasta el momento en que se realiza una medición. Es esta capacidad de coexistencia de estados, junto con otros fenómenos estrictamente cuánticos como el entrelazamiento, la que proporciona a la computación cuántica su potencial para abordar problemas que resultan intratables en el paradigma clásico.

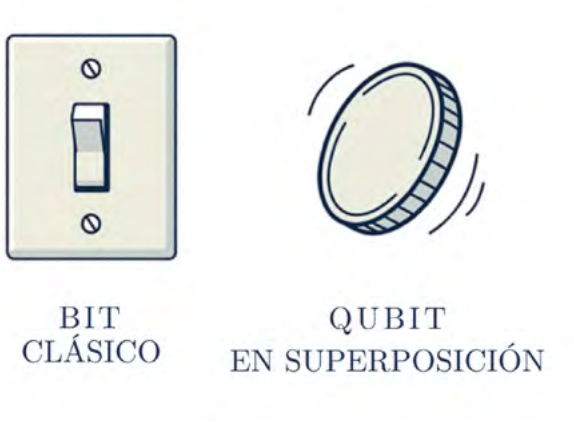


Figura 1.4. Ejemplo práctico entre computación clásica y cuántica.

Como analogía intuitiva para introducir el concepto de superposición cuántica puede considerarse el lanzamiento de una moneda al aire. Mientras la moneda se encuentra girando, no muestra de manera observable ni cara ni cruz, y solo cuando es detenida y observada se manifiesta un resultado concreto. Esta imagen resulta útil para ilustrar el comportamiento de un cúbit, el cual puede evolucionar en una superposición coherente de los estados básicos asociados a $|0\rangle$ y $|1\rangle$ hasta el momento de la medición. No obstante, es fundamental subrayar una diferencia esencial entre ambos casos. En el experimento clásico de la moneda, la incertidumbre es de carácter epistemológico, ya que el sistema posee en todo momento un estado bien definido, aunque sea desconocido para el observador. En contraste, en el caso cuántico no existe un valor definido previo a la medición, sino que el cúbit se describe genuinamente como una superposición de estados conforme a los postulados de la mecánica cuántica.

Esta naturaleza cuántica es la que confiere a los cúbits capacidades computacionales que no tienen análogo en la computación clásica. Mientras que un sistema compuesto por n bits clásicos solo puede representar uno de los 2^n estados posibles en un instante dado, un sistema de n cúbits puede existir en una superposición coherente de todos los 2^n estados simultáneamente. Esta diferencia implica un crecimiento exponencial del espacio de estados accesible al sistema cuántico. En términos puramente informativos, un número moderado de cúbits es suficiente para describir espacios de

dimensión extraordinariamente grande, superando con rapidez cualquier capacidad de representación clásica directa.

La consecuencia de esta propiedad es la posibilidad de diseñar algoritmos cuánticos que exploten la superposición y el entrelazamiento para explorar de manera simultánea un número exponencial de configuraciones. Esta capacidad no debe interpretarse como una evaluación directa y paralela de todas las soluciones posibles, sino como una evolución coherente del sistema cuántico en la que las amplitudes de probabilidad asociadas a distintas configuraciones interfieren entre sí. Mediante una secuencia cuidadosamente diseñada de operaciones unitarias, las amplitudes correspondientes a soluciones incorrectas pueden cancelarse, mientras que las asociadas a soluciones correctas se refuerzan. Este mecanismo de interferencia constituye el núcleo de la ventaja cuántica en algoritmos como los de búsqueda, factorización o simulación de sistemas físicos.

Una analogía útil para visualizar este proceso es la de un laberinto con un gran número de rutas posibles. Un ordenador clásico debe explorar estas rutas de forma secuencial, descartando caminos uno a uno hasta encontrar una salida. En contraste, un ordenador cuántico puede describirse como un sistema cuyo estado representa una superposición de encontrarse en múltiples rutas de manera simultánea. A través de la interferencia cuántica, las trayectorias que no conducen a la solución pueden suprimirse progresivamente, de modo que al realizar la medición final el sistema colapsa con alta probabilidad en el estado que codifica la solución buscada.

La superposición cuántica no es una construcción puramente abstracta, sino un fenómeno experimentalmente verificado. Un ejemplo paradigmático es el experimento de la doble rendija, en el cual un electrón individual produce un patrón de interferencia característico de una onda, lo que indica que el sistema se comporta como si hubiese atravesado simultáneamente ambas rendijas. En computación cuántica, esta misma propiedad se utiliza para manipular amplitudes de probabilidad de manera controlada, lo que permite diseñar algoritmos que aprovechan la estructura del problema para obtener ventajas computacionales específicas.

Esta riqueza de posibilidades viene acompañada, sin embargo, de una notable fragilidad física. Los cúbits son sistemas extremadamente sensibles a su entorno, y cualquier interacción no controlada puede provocar la pérdida de coherencia cuántica, proceso conocido como decoherencia. Esta

fragilidad constituye uno de los principales desafíos tecnológicos en el desarrollo de ordenadores cuánticos prácticos. A pesar de ello, el potencial del paradigma cuántico es evidente. El cúbit no representa una versión más eficiente del bit clásico, sino una unidad fundamentalmente distinta de información, capaz de explorar un espacio continuo de estados y de obedecer reglas que no tienen equivalente en la computación tradicional.

Comprender en profundidad qué distingue a un cúbit de un bit clásico y cómo esta diferencia se traduce en nuevas formas de procesamiento de la información resulta esencial para apreciar por qué la computación cuántica no constituye una mejora incremental del paradigma clásico, sino una transformación conceptual profunda en la forma de abordar el cálculo y la simulación de sistemas complejos.

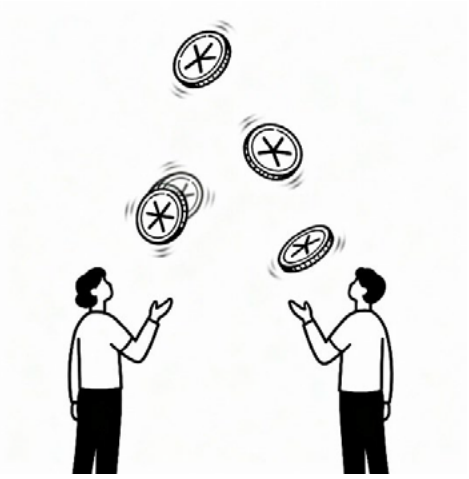


Figura 1.5. Una moneda en el aire, antes de caer, puede ser una analogía imperfecta de la superposición de un cúbit.

La diferencia, sin embargo, es que, en el caso cuántico, esta combinación no se debe a nuestra ignorancia o a la velocidad con la que se mueven, es esencial para la naturaleza de las cosas.

1.4.2 Entrelazamiento: correlaciones más allá del sentido común

Si la superposición cuántica obliga a admitir que un sistema físico puede describirse como una combinación coherente de múltiples estados

simultáneamente, el fenómeno del entrelazamiento cuántico lleva esta idea un paso más allá. En presencia de entrelazamiento, dos o más partículas pueden compartir un estado cuántico común de tal manera que el comportamiento de cada subsistema individual no puede describirse de forma independiente. En estos casos, el estado del sistema completo no admite una factorización en estados individuales asociados a cada partícula, lo que da lugar a correlaciones que carecen de análogo en la física clásica.

El entrelazamiento introduce correlaciones no locales entre los subsistemas, en el sentido de que las propiedades observables de una partícula están intrínsecamente ligadas a las de otra, independientemente de la distancia espacial que las separe. Como consecuencia, la medición realizada sobre una parte del sistema determina instantáneamente las estadísticas de medición de las demás partes, aun cuando estas se encuentren separadas por grandes distancias. Este comportamiento resulta profundamente contraintuitivo desde la perspectiva clásica, en la cual se asume que los sistemas físicos poseen propiedades bien definidas y localizadas.

Desde un punto de vista experimental, el entrelazamiento puede generarse de manera controlada en laboratorio y mantenerse incluso cuando las partículas entrelazadas se separan a escalas macroscópicas. Este fenómeno motivó una de las críticas más conocidas a la mecánica cuántica, formulada por Albert Einstein, quien lo describió como una acción fantasmal a distancia, al considerar inaceptable que una partícula pudiera verse afectada instantáneamente por lo que ocurre a otra sin mediación causal local. No obstante, a partir de la década de 1980, una amplia serie de experimentos, iniciados por Alain Aspect y posteriormente extendidos por Anton Zeilinger y otros investigadores, ha confirmado de manera concluyente la realidad física del entrelazamiento.

Estos experimentos han demostrado la violación sistemática de las desigualdades de Bell, descartando cualquier teoría basada en variables ocultas locales como explicación del fenómeno. Los resultados indican que las correlaciones observadas no pueden reproducirse mediante modelos clásicos que respeten simultáneamente localidad y realismo. En este sentido, la información cuántica no se encuentra asociada a partículas individuales, sino distribuida en las correlaciones que existen entre ellas. Esta no localización de la información constituye uno de los rasgos más profundos y conceptualmente disruptivos de la mecánica cuántica y desempeña un papel central en

aplicaciones de la computación cuántica, la comunicación y la criptografía cuánticas.

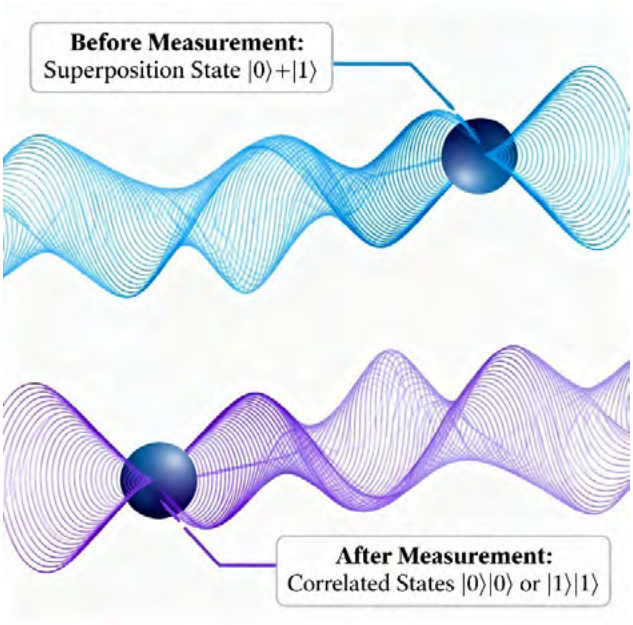


Figura 1.6. Dos cúbits entrelazados. La medición de uno afecta instantáneamente al otro, sin importar la distancia.

El entrelazamiento cuántico habilita una serie de fenómenos que no tienen equivalente en la física clásica y que constituyen la base de múltiples aplicaciones cuánticas avanzadas. Entre estos fenómenos se encuentra la teleportación cuántica de estados, un protocolo mediante el cual el estado completo de un cúbit puede transferirse de un sistema a otro distante utilizando un par de partículas entrelazadas y un canal de comunicación clásica. En este proceso no se transmite materia ni energía de forma superlumínica, sino información cuántica, cuya reconstrucción en el destino depende de las correlaciones no locales establecidas previamente.

Otro ejemplo destacado es la criptografía cuántica, en la cual el entrelazamiento se utiliza para generar claves criptográficas cuya seguridad está garantizada por los principios fundamentales de la mecánica cuántica. En estos protocolos, cualquier intento de interceptar o medir los cúbits entrelazados introduce perturbaciones inevitables en las correlaciones del

sistema, perturbaciones que pueden ser detectadas por los usuarios legítimos. De este modo, la seguridad de la comunicación no se basa en supuestos computacionales, sino en leyes físicas fundamentales.

En la actualidad, el entrelazamiento se genera, manipula y mide de manera rutinaria en diversos sistemas experimentales, incluyendo plataformas de óptica cuántica basadas en fotones y dispositivos superconductores empleados en computación cuántica. No obstante, la preservación del entrelazamiento a gran escala y durante tiempos prolongados continúa siendo uno de los principales retos tecnológicos, debido a la sensibilidad extrema de los sistemas cuánticos frente a interacciones no controladas con el entorno.

Desde una perspectiva computacional, el entrelazamiento constituye un recurso esencial para la obtención de ventajas cuánticas. Numerosos algoritmos cuánticos requieren la creación y manipulación de estados entrelazados para procesar información de formas que no pueden ser reproducidas por ningún sistema clásico eficiente. En este sentido, el entrelazamiento no debe entenderse como un fenómeno accesorio, sino como uno de los pilares fundamentales sobre los que se construye la computación cuántica moderna.

Figura 1.7. El entrelazamiento crea correlaciones que desafían la localidad clásica, un recurso clave para la computación y comunicación cuántica.

1.4.3 Unitariedad y reversibilidad

En la computación clásica existen operaciones (por ejemplo, una puerta AND) que no son reversibles: si obtenemos un resultado 1 de una compuerta AND, no podemos saber con seguridad cuáles fueron las entradas (varias combinaciones de bits de entrada podrían producir la salida 1, lo que implica pérdida de información). En el mundo cuántico, en cambio, las

operaciones válidas deben ser unitarias y por tanto reversibles. La unitariedad es una propiedad matemática de las transformaciones cuánticas que garantiza que la información no se pierde ni se crea de la nada. Cada operación cuántica U tiene una inversa U† tal que: UU† = I, donde I es la matriz identidad. Esta condición implica que U conserva la norma de los vectores de estado (es decir, la suma total de probabilidades sigue siendo 1) y que toda transformación puede deshacerse aplicando la operación inversa adecuada. En otras palabras, una puerta lógica cuántica siempre tiene un modo de deshacer, ninguna información se descarta irreversiblemente en el proceso.

La unitariedad también asegura que las probabilidades se preserven y evolucionen de forma coherente. Un efecto crucial de esto es que las operaciones cuánticas no pueden aumentar ni disminuir la incertidumbre global de un estado: simplemente la trasladan entre diferentes componentes del sistema. En última instancia, la unitariedad garantiza que la evolución cuántica sea una especie de danza perfectamente controlada y predecible (a nivel de amplitudes), aunque el resultado final, tras la medición, se manifieste de forma probabilística. Esta reversibilidad intrínseca tiene profundas implicaciones: por ejemplo, significa que no existe en mecánica cuántica un operador que actúe como la función borrar clásica (no podemos eliminar información cuántica arbitrariamente sin dejar rastro, lo que se relaciona con la naturaleza de la medición y la termodinámica de la información).

1.4.4 La medición y el colapso de la función de onda

En la computación clásica, muchas de las operaciones lógicas fundamentales no son reversibles. Un ejemplo paradigmático es la compuerta AND, cuyo resultado no permite reconstruir de manera unívoca las entradas originales. Si la salida de una compuerta AND es igual a 1, existen múltiples combinaciones posibles de bits de entrada que conducen a ese mismo resultado, lo que implica una pérdida irreversible de información. Esta irreversibilidad es una característica intrínseca del modelo clásico de computación y está íntimamente relacionada con la disipación de energía y con la termodinámica de la información.

En contraste, en el marco de la computación cuántica, todas las transformaciones físicas válidas que describen la evolución de un sistema aislado

deben ser unitarias y, por tanto, reversibles. La unitariedad constituye una propiedad matemática fundamental de las transformaciones cuánticas y garantiza que la información no se crea ni se destruye durante la evolución del sistema. De manera formal, una operación cuántica se describe mediante un operador unitario U que satisface la condición $UU^{\dagger} = U^{\dagger}U = I$ donde $U^{\dagger}$ denota el adjunto hermítico de U e I es el operador identidad. Esta condición implica que la norma del vector de estado se conserva bajo la evolución, lo que asegura que la suma total de las probabilidades de medición permanece igual a uno. Asimismo, toda transformación unitaria admite una operación inversa bien definida, dada precisamente por $U^{\dagger}$, lo que significa que cualquier puerta lógica cuántica puede deshacerse aplicando la transformación inversa correspondiente.

La reversibilidad inherente a la unitariedad tiene consecuencias profundas para el procesamiento de la información cuántica. En particular, las operaciones cuánticas no pueden eliminar información de manera arbitraria, ni aumentar o disminuir la incertidumbre global asociada a un estado. En su lugar, la evolución unitaria redistribuye coherentemente las amplitudes de probabilidad entre las distintas componentes del sistema. Desde este punto de vista, la dinámica cuántica puede interpretarse como una evolución determinista y perfectamente controlada a nivel de amplitudes complejas, aun cuando los resultados observables tras la medición se manifiesten de manera probabilística.

Una implicación directa de este principio es la inexistencia de un operador cuántico que desempeñe el papel de una operación de borrado clásica. No es posible eliminar información cuántica de forma irreversible sin que el entorno registre alguna huella del proceso. Este hecho se encuentra estrechamente relacionado con el problema de la medición en mecánica cuántica y con los fundamentos de la termodinámica de la información, incluyendo resultados como el principio de Landauer. La medición cuántica, a diferencia de la evolución unitaria, introduce un elemento intrínsecamente no reversible, ya que proyecta el estado del sistema sobre un subespacio asociado a un resultado observable específico.

En este sentido, la distinción entre evolución unitaria y medición resulta central para la computación cuántica. Mientras que los circuitos cuánticos se construyen exclusivamente a partir de operaciones unitarias

reversibles, la obtención de resultados clásicos requiere inevitablemente un proceso de medición que rompe la reversibilidad y convierte la información cuántica en información clásica accesible. Esta dualidad entre evolución coherente y medición irreversible constituye uno de los rasgos conceptuales más profundos y distintivos de la computación cuántica frente al paradigma clásico.

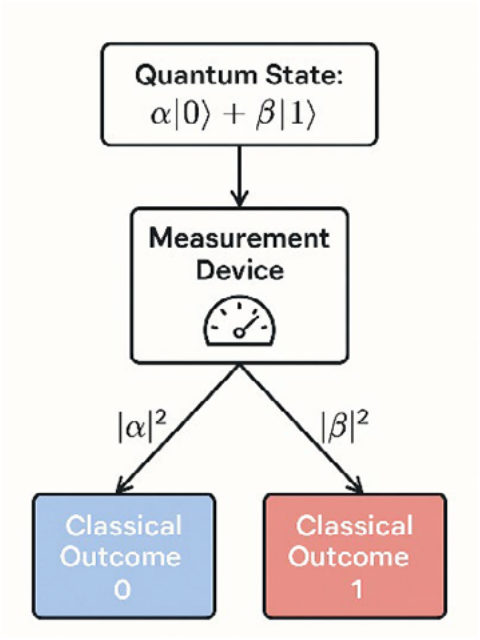


Figura 1.8. La medición es un proceso irreversible que extrae información clásica de un sistema cuántico, colapsando su estado.

Este comportamiento resulta conceptualmente desconcertante, ya que contradice la lógica determinista que caracteriza a la física clásica. En el marco clásico se asume que, si se conocieran con precisión todas las condiciones iniciales de un sistema, su evolución futura podría predecirse de manera exacta. La mecánica cuántica, en contraste, establece un límite fundamental a esta aspiración predictiva, al afirmar que solo pueden conocerse las probabilidades asociadas a los posibles resultados de una medición.

La incertidumbre cuántica no constituye una limitación tecnológica ni una manifestación de ignorancia epistemológica, sino una propiedad intrínseca de la naturaleza. El proceso de medición desempeña un papel central en esta descripción, al revelar que la realidad cuántica no se manifiesta

plenamente hasta que se produce una interacción con un sistema de medida. Durante la evolución previa a la observación, el estado cuántico codifica simultáneamente múltiples posibilidades, las cuales se actualizan en un resultado concreto únicamente en el acto de medición.

El colapso del estado cuántico transforma esta superposición de posibilidades en una experiencia definida, pero lo hace de acuerdo con leyes probabilísticas estrictamente determinadas por la función de onda. Este hecho pone de manifiesto el carácter profundo e ineludible del azar en la descripción cuántica de la naturaleza y subraya una diferencia conceptual fundamental entre la mecánica cuántica y las teorías físicas clásicas deterministas.

1.4.5 El principio de no-clonación

Uno de los resultados teóricos más profundos y conceptualmente reveladores de la mecánica cuántica es el denominado teorema de no clonación, formulado a comienzos de la década de 1980. Este teorema establece que no es posible clonar de manera exacta un estado cuántico arbitrario y desconocido. Este resultado marca una diferencia estructural fundamental entre la información clásica y la información cuántica. En el ámbito clásico, la información puede copiarse y replicarse sin restricciones fundamentales, mientras que en el dominio cuántico dicha operación se encuentra prohibida por los propios principios de la teoría.

De manera más precisa, el teorema de no clonación afirma que no existe ningún operador cuántico universal capaz de tomar como entrada un cúbit preparado en un estado arbitrario, junto con un segundo cúbit en un estado de referencia fijo, y producir como salida dos copias idénticas del estado original. En otras palabras, no existe una transformación cuántica válida que realice la operación $|\psi\rangle|0\rangle \rightarrow |\psi\rangle|\psi\rangle$ para todo estado cuántico $|\psi\rangle$. Dado que toda evolución de un sistema cuántico aislado debe describirse mediante operadores unitarios, el resultado implica que ninguna operación unitaria puede llevar a cabo una clonación perfecta de estados cuánticos desconocidos.

Este límite no tiene un origen tecnológico ni experimental, ni se debe a una perturbación accidental introducida durante el proceso de copia. Se trata, por el contrario, de una consecuencia matemática directa de la

linealidad de la mecánica cuántica. Intuitivamente, la clonación exacta requeriría disponer de información completa sobre el estado a copiar. Sin embargo, la única forma de obtener dicha información sería mediante una medición, y el proceso de medición altera de manera irreversible el estado cuántico general, destruyendo la coherencia necesaria para reproducirlo fielmente.

Desde un punto de vista conceptual, el principio de no clonación pone de manifiesto que la información cuántica posee una naturaleza intrínsecamente distinta de la información clásica. Aunque es posible copiar información clásica extraída de sistemas cuánticos, por ejemplo, mediante la repetición estadística de mediciones sobre un conjunto de sistemas preparados de forma idéntica, no es posible generar copias adicionales perfectas de un estado cuántico individual sin conocer exactamente su preparación. La imposibilidad de clonar estados individuales desconocidos subraya el carácter no clásico y no replicable de la información cuántica.

Una consecuencia práctica particularmente relevante del teorema de no clonación se manifiesta en el ámbito de la comunicación cuántica. En protocolos de distribución cuántica de claves criptográficas, este principio garantiza que un posible intruso no puede interceptar y duplicar los cúbits transmitidos sin introducir perturbaciones detectables. Cualquier intento de copia imperfecta altera inevitablemente el estado cuántico y modifica las correlaciones esperadas, permitiendo a los usuarios legítimos detectar la presencia de un ataque.

En un sentido más amplio, el teorema de no clonación impone restricciones fundamentales sobre el procesamiento y la transmisión de información cuántica, pero al mismo tiempo habilita nuevas posibilidades que no existen en la computación clásica. Este principio constituye uno de los pilares conceptuales de la información cuántica moderna y desempeña un papel central tanto en la seguridad de las comunicaciones cuánticas como en la comprensión profunda de las diferencias entre los paradigmas clásico y cuántico de procesamiento de la información.

1.4.6 El ordenador cuántico

La concepción del computador cuántico surge directamente de los principios fundamentales de la mecánica cuántica. El desarrollo de la física

del siglo XX puso de manifiesto que, a escala atómica y subatómica, la materia y la energía no obedecen las leyes deterministas de la física clásica, sino que se describen mediante estados caracterizados por superposición, indeterminación y probabilidades de medición. Este cambio profundo en la comprensión de la naturaleza condujo de manera natural a la pregunta de por qué los dispositivos de cómputo continúan basándose exclusivamente en principios clásicos, cuando el universo físico en su nivel más fundamental se rige por leyes cuánticas.

Un computador cuántico no debe entenderse como una simple extensión más rápida de un ordenador convencional, sino como un dispositivo basado en un conjunto de principios físicos radicalmente distintos. Mientras que el computador clásico codifica la información en bits que solo pueden adoptar valores discretos de 0 o 1, el computador cuántico emplea cúbits como unidades básicas de información. Estos cúbits pueden encontrarse en superposiciones coherentes de los estados básicos asociados a 0 y 1, manteniendo esta coexistencia de posibilidades hasta el momento en que se realiza una medición. De este modo, la información cuántica no se limita a valores discretos, sino que se describe mediante amplitudes complejas que evolucionan de forma continua en el espacio de estados.

Gracias a esta propiedad, un registro compuesto por n cúbits no representa una única configuración entre las 2^n posibles, sino que puede describirse como una superposición coherente de todas ellas. Esta capacidad no implica que el sistema evalúe secuencialmente todas las configuraciones, sino que la evolución unitaria del estado cuántico permite manipular simultáneamente las amplitudes asociadas a un número exponencial de configuraciones. La ventaja potencial del cómputo cuántico surge precisamente de la capacidad de diseñar evoluciones en las que la interferencia cuántica refuerza las amplitudes correspondientes a soluciones relevantes y suprime las asociadas a configuraciones incorrectas.

Para comprender esta diferencia conceptual resulta necesario abandonar la analogía directa con los computadores digitales clásicos. En la computación convencional, muchas de las operaciones lógicas fundamentales son irreversibles y conllevan una pérdida de información, como ocurre en puertas lógicas tales como AND, OR o XOR. En contraste, la computación cuántica se basa exclusivamente en transformaciones unitarias, lo que implica que toda operación es, en principio, perfectamente reversible. Cada puerta

cuántica, ya sea una rotación, una operación de fase o una compuerta de entrelazamiento, se describe mediante una matriz unitaria U que actúa sobre el vector de estado del sistema de cúbits.

La unitariedad garantiza que la información cuántica no se destruye ni se crea durante la evolución del sistema, sino que se redistribuye coherentemente dentro del espacio de Hilbert asociado. Desde un punto de vista físico, el computador cuántico transforma de manera controlada la estructura de las amplitudes de probabilidad del estado cuántico, preservando la normalización y la coherencia del sistema. Esta característica distingue de forma fundamental al cómputo cuántico del paradigma clásico y constituye la base sobre la cual se construyen los algoritmos cuánticos capaces de ofrecer ventajas computacionales en problemas específicos.

1.5 Algoritmos NISQ

Los algoritmos NISQ, siglas de Noisy Intermediate Scale Quantum, constituyen la primera generación de algoritmos cuánticos diseñados específicamente para su ejecución en dispositivos cuánticos actuales, caracterizados por un número intermedio de cúbits y por la presencia inevitable de ruido y errores operacionales. Típicamente, estos dispositivos disponen de entre 50 y varios cientos de cúbits, con tasas de error por compuerta que impiden la implementación práctica de esquemas completos de corrección de errores. El término NISQ fue introducido por John Preskill en 2018 para describir esta etapa transitoria entre los prototipos de laboratorio y los futuros computadores cuánticos tolerantes a fallos.

En el contexto del aprendizaje automático cuántico, los algoritmos NISQ desempeñan un papel central, ya que permiten explorar modelos entrenables que aprovechan propiedades genuinamente cuánticas de la información, como la superposición y el entrelazamiento, sin requerir infraestructuras de corrección de errores a gran escala. Estos algoritmos constituyen, por tanto, el marco operativo más relevante para las aplicaciones cuánticas a corto y medio plazo.

Una característica fundamental de los algoritmos NISQ es la necesidad de minimizar la profundidad de los circuitos cuánticos, con el fin de reducir la acumulación de errores debidos a la decoherencia y a la imperfección de las compuertas. Para compensar estas limitaciones físicas, se adopta un

paradigma híbrido cuántico clásico, en el cual el procesador cuántico se utiliza como un recurso especializado dentro de un bucle de optimización controlado clásicamente. En este esquema, cada ejecución del circuito cuántico actúa como una evaluación de un oráculo físico, del cual se extraen valores esperados de ciertos observables mediante mediciones repetidas.

Los resultados de estas mediciones se emplean para construir una función de coste clásica, que cuantifica el desempeño del modelo cuántico parametrizado. A continuación, un optimizador clásico ajusta los parámetros del circuito con el objetivo de minimizar o maximizar dicha función. Entre los métodos de optimización más utilizados se encuentran técnicas de descenso de gradiente, así como algoritmos estocásticos robustos al ruido, como el método de Simultaneous Perturbation Stochastic Approximation. Este procedimiento se repite de manera iterativa hasta alcanzar un criterio de convergencia o hasta agotar un presupuesto computacional predefinido.

Este enfoque híbrido constituye el núcleo de numerosos algoritmos NISQ contemporáneos, incluyendo los clasificadores cuánticos variacionales, los circuitos cuánticos parametrizados para aprendizaje supervisado y no supervisado, así como algoritmos de optimización y simulación cuántica variacional. Aunque las limitaciones del hardware actual restringen el tamaño y la complejidad de los problemas abordables, los algoritmos NISQ representan un paso esencial hacia la explotación práctica de la computación cuántica y proporcionan un marco experimental y teórico clave para el desarrollo de aplicaciones cuánticas futuras.

Entre los algoritmos NISQ aplicables al aprendizaje automático destacan diversos enfoques híbridos que combinan procesamiento cuántico con optimización clásica, diseñados específicamente para explotar las capacidades y limitaciones del hardware cuántico actual. Estos algoritmos se fundamentan en el uso de circuitos cuánticos parametrizados de profundidad reducida, junto con bucles de optimización clásicos que permiten mitigar el impacto del ruido y de los errores por compuerta característicos de los dispositivos NISQ.

El algoritmo Variational Quantum Eigensolver fue concebido originalmente para la estimación de energías de estados fundamentales en sistemas cuánticos moleculares. No obstante, su estructura general lo hace directamente adaptable a tareas de regresión y ajuste de modelos en aprendizaje automático. El método se basa en la minimización del valor esperado de un

observable, interpretado como una función de coste, mediante la optimización de un conjunto de parámetros clásicos que controlan un circuito cuántico variacional. Esta formulación convierte al VQE en uno de los pilares conceptuales de los métodos híbridos cuántico-clásicos y en un caso prototípico de algoritmo NISQ.

El algoritmo Quantum Approximate Optimization Algorithm se orienta a la resolución de problemas de optimización combinatoria y discreta. Su funcionamiento se basa en la aplicación alternada de operadores asociados al coste del problema y de operadores de mezcla, ambos controlados por parámetros continuos que se ajustan de forma iterativa. Esta estructura ha permitido su adaptación a contextos de aprendizaje profundo, donde puede emplearse como núcleo de arquitecturas cuántico clásicas destinadas a la exploración eficiente de paisajes de optimización de alta dimensionalidad. Estudios recientes han puesto de manifiesto que este enfoque puede mejorar la búsqueda de mínimos globales en problemas caracterizados por múltiples óptimos locales.

Las redes neuronales cuánticas extienden el concepto de red neuronal clásica al dominio cuántico, reemplazando los pesos sinápticos por ángulos de rotación asociados a puertas cuánticas parametrizadas. En este modelo, el entrenamiento no se basa en derivadas analíticas convencionales, sino en técnicas específicas del marco cuántico, como la regla de desplazamiento de parámetros. Este método permite estimar gradientes a partir de la evaluación del circuito con parámetros desplazados, haciendo viable el entrenamiento de redes cuánticas en hardware real. De este modo, las redes neuronales cuánticas permiten implementar esquemas de aprendizaje supervisado y no supervisado que conservan una analogía formal con el aprendizaje profundo clásico, pero operan dentro del formalismo de la mecánica cuántica.

Otro enfoque relevante es la Quantum Support Vector Machine, que representa una adaptación del método de máquinas de soporte vectorial al entorno cuántico. Este algoritmo explota la capacidad de los procesadores cuánticos para evaluar kernels definidos como productos de fidelidad entre estados cuánticos. La posibilidad de calcular estos kernels en espacios de Hilbert de gran dimensión permite construir fronteras de decisión altamente no lineales, cuya evaluación eficiente resulta inalcanzable mediante técnicas clásicas convencionales. En este sentido, la QSVM proporciona un marco

alternativo para el aprendizaje supervisado, particularmente adecuado para problemas con estructuras de separación complejas entre clases.

El paradigma generativo adversarial también ha sido trasladado al dominio cuántico mediante las Quantum Generative Adversarial Networks. En este enfoque, dos circuitos cuánticos parametrizados desempeñan los roles de generador y discriminador, respectivamente, y se entrenan de manera competitiva siguiendo un esquema análogo al de las redes generativas adversariales clásicas. En el contexto NISQ, estos modelos se han adaptado mediante la reducción de la profundidad de los circuitos y la aplicación de técnicas de mitigación del ruido, lo que permite su ejecución práctica en dispositivos cuánticos ruidosos. Las QGAN abren nuevas posibilidades para la síntesis de datos y la modelización probabilística desde una perspectiva cuántica.

Desde un punto de vista formal, todos estos algoritmos híbridos pueden describirse como problemas de minimización de valores esperados de observables. Si $\hat{C}$ representa un operador de coste, como un observable de energía o una medida de error, el objetivo del entrenamiento puede expresarse como

$$\min\langle\psi(\theta) \mid \hat{C} \mid \psi(\theta)\rangle$$

Cada ejecución del circuito cuántico proporciona una estimación estadística de este valor esperado mediante el promedio de los resultados de medición. La sensibilidad del coste con respecto a un parámetro θ_i se obtiene utilizando la regla de desplazamiento de parámetros, cuya forma básica es

$$\frac{\partial}{\partial\theta_i}\langle\hat{C}\rangle = \frac{1}{2}\left[\langle\hat{C}\rangle_{\theta_i+\frac{\pi}{2}} - \langle\hat{C}\rangle_{\theta_i-\frac{\pi}{2}}\right]$$

Este método evita el uso de derivadas numéricas inestables y permite el cálculo de gradientes directamente en hardware cuántico real.

En la práctica, los algoritmos NISQ aplicados al aprendizaje automático se utilizan como marcos adaptativos flexibles. Versiones modificadas del VQE han sido empleadas para tareas de regresión cuántica y aproximación de funciones, mientras que formulaciones variacionales del QAOA pueden reinterpretarse como clasificadores binarios mediante el ajuste de los

parámetros de mezcla para minimizar el error de clasificación. Un ansatz típico de dos cúbits empleado en tareas de clasificación simple puede escribirse como

$$U(\theta) = CNOT \cdot R_y^{(1)}(\theta_2) \cdot R_y^{(0)}(\theta_1)$$

Resultados teóricos recientes indican que muchos modelos NISQ pueden aproximar de manera eficiente distribuciones de probabilidad clásicas de alta complejidad, siempre que la profundidad del circuito y la topología del ansatz se seleccionen de forma apropiada. De manera complementaria, se ha demostrado que técnicas de inteligencia artificial pueden emplearse para optimizar los propios circuitos cuánticos, identificando secuencias equivalentes con menor profundidad y menor coste en recursos físicos. Esta interacción bidireccional entre aprendizaje clásico y computación cuántica refuerza el carácter híbrido de los enfoques NISQ y subraya su relevancia como puente hacia futuras arquitecturas cuánticas tolerantes a fallos.

1.6 Aplicaciones actuales de la computación cuántica

La computación cuántica, concebida inicialmente como una propuesta teórica que desafiaba los límites establecidos de la física y la informática, ha evolucionado de manera sostenida durante las últimas décadas hasta consolidarse como una disciplina experimental madura, orientada progresivamente hacia aplicaciones prácticas. A diferencia de otras tecnologías emergentes, su potencial transformador no se fundamenta en una mejora incremental del rendimiento computacional, sino en la posibilidad de abordar clases de problemas que se consideran intratables dentro del paradigma clásico. Esta capacidad no se deriva de un simple aumento en la velocidad de cálculo, sino de un cambio profundo en la forma en que la información se representa y se manipula, apoyándose en cúbits, entrelazamiento y evolución unitaria.

A pesar de los retos técnicos que aún deben superarse, se identifican ya dominios de aplicación claramente definidos, tanto en el ámbito industrial como en la investigación científica, y se anticipan transformaciones de gran alcance que afectarán a múltiples sectores estratégicos de la economía y de la ciencia. En este sentido, la computación cuántica ha comenzado a trascender

el entorno puramente académico para integrarse, de forma incipiente pero tangible, en procesos industriales reales.

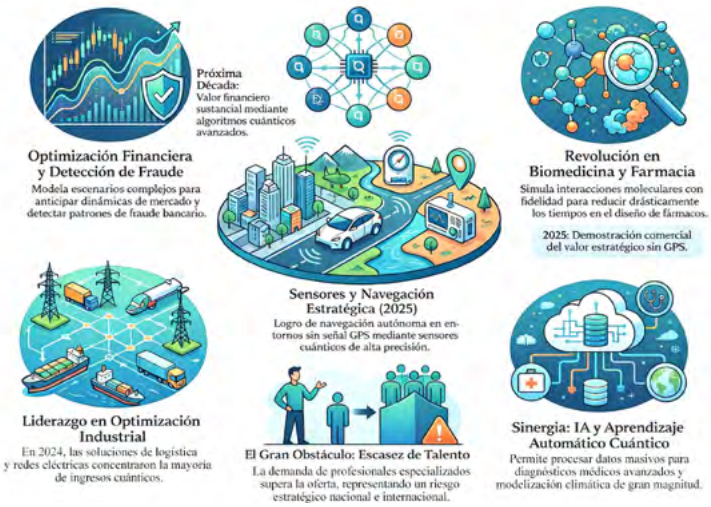


Figura 1.9. Aplicaciones estratégicas y sectores de impacto potencial de la computación cuántica.

El sector financiero constituye actualmente uno de los principales motores de adopción de esta tecnología. Instituciones bancarias y entidades de servicios financieros están explorando el uso de algoritmos cuánticos para la optimización de carteras, el análisis avanzado de riesgos y la detección de patrones asociados al fraude. La capacidad de los sistemas cuánticos para modelar escenarios complejos y analizar grandes volúmenes de datos permite anticipar dinámicas de mercado con un nivel de sofisticación que resulta difícil de alcanzar mediante métodos clásicos, abriendo la posibilidad de generar un valor económico sustancial en el horizonte de la próxima década.

En 2025 se produjo un hito relevante con la demostración de ventaja cuántica en el ámbito de los sensores por parte de la empresa Q CTRL. Mediante el uso de técnicas de detección cuántica, se logró una mejora significativa en sistemas de navegación en entornos carentes de señal GPS, superando el rendimiento de alternativas clásicas y dando lugar a aplicaciones comerciales de alto valor estratégico.

En el ámbito biomédico y farmacológico, la computación cuántica se perfila como una herramienta de especial relevancia. El descubrimiento y diseño de nuevos fármacos depende de la simulación precisa de interacciones

moleculares complejas, un problema que desafía severamente las capacidades de la computación clásica. Dado que los sistemas cuánticos obedecen las mismas leyes físicas que gobiernan la dinámica molecular, la computación cuántica ofrece un marco natural para modelar estas interacciones con mayor fidelidad. Esta capacidad promete reducir de manera drástica los tiempos de investigación, acelerando el desarrollo y la validación de nuevos tratamientos.

La optimización constituye otro de los dominios donde la computación cuántica ha mostrado un impacto significativo. En 2024, este segmento concentró una parte sustancial de los ingresos del mercado cuántico. Aplicaciones que abarcan desde la planificación de rutas de transporte global hasta la optimización de cadenas de suministro y redes eléctricas se benefician de la capacidad de los algoritmos cuánticos para explorar espacios de soluciones de dimensionalidad extremadamente alta, imposibles de tratar de forma exhaustiva mediante enfoques clásicos.

La convergencia entre inteligencia artificial y computación cuántica, conocida como aprendizaje automático cuántico, emerge como uno de los campos más prometedores. Este enfoque permite procesar datos de alta dimensionalidad y detectar estructuras y patrones que escapan a los métodos clásicos convencionales. Se prevé que esta sinergia dé lugar a herramientas avanzadas aplicables en ámbitos como el diagnóstico médico, la modelización climática y la toma de decisiones complejas, con un impacto económico potencial de gran magnitud en las próximas décadas.

No obstante, el camino hacia una adopción amplia de la computación cuántica se enfrenta a obstáculos significativos. Uno de los más inmediatos es la escasez de personal altamente cualificado. La demanda de profesionales con formación especializada en tecnologías cuánticas supera de forma considerable la oferta actual, lo que ha sido identificado como un factor de riesgo estratégico a nivel nacional e internacional.

A este desafío se suma la preocupación asociada al denominado Día Q, entendido como el momento hipotético en el que un computador cuántico suficientemente potente pueda comprometer los esquemas criptográficos clásicos actualmente en uso. Este escenario plantea implicaciones profundas para la seguridad de la información digital a escala global, desde infraestructuras críticas hasta transacciones financieras y comunicaciones gubernamentales.

Como respuesta a estas amenazas han surgido dos líneas de desarrollo complementarias. La criptografía post cuántica se centra en el diseño de algoritmos clásicos resistentes a ataques cuánticos y se perfila como una solución pragmática a corto plazo debido a su facilidad de despliegue mediante actualizaciones de software. Por otro lado, la distribución cuántica de claves emplea principios fundamentales de la mecánica cuántica para establecer canales de comunicación con garantías de seguridad teórica, aunque requiere infraestructuras de hardware específicas. Sectores estratégicos, como el gubernamental y el de telecomunicaciones, han comenzado a invertir de manera significativa en estas tecnologías.

En conjunto, la situación actual de la computación cuántica puede caracterizarse como una fase de madurez acelerada y consolidación estratégica. La cuestión central ya no reside en determinar si la tecnología es viable, sino en establecer cuándo y cómo podrá escalarse de manera sostenible. Con una inversión pública creciente y una competencia geopolítica que actúa como catalizador de la innovación, la computación cuántica se integra progresivamente en el tejido industrial, configurándose como uno de los pilares tecnológicos del futuro próximo.

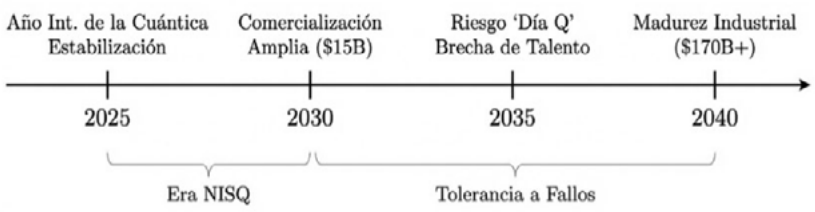


Figura 1.10. Línea temporal prevista con los hitos más importantes.

Las empresas que actúen ahora, invirtiendo en talento y experimentando con servicios en la nube (QCaaS), estarán posicionadas para capturar un valor inmenso. Sin embargo, deben navegar simultáneamente los riesgos de seguridad que la misma tecnología introduce. El año 2025 marca el comienzo de una carrera en la que la ventaja del primer movimiento será decisiva, y donde la capacidad de estabilizar los cúbits determinará quién lidera la economía del futuro

1.7 Usos avanzados y perspectivas futuras

Además de las aplicaciones ya consolidadas, se están explorando activamente usos avanzados de la computación cuántica en dominios como la metrología de alta precisión, los sensores cuánticos, las redes cuánticas, la inteligencia artificial distribuida y los esquemas de computación cuántica federada. En el ámbito de la metrología, dispositivos basados en estados cuánticos coherentes, como los relojes atómicos de última generación, permiten definir unidades fundamentales de medida con niveles de precisión sin precedentes, superando ampliamente las capacidades de los estándares clásicos. Estos avances resultan esenciales para la sincronización global, la navegación de alta precisión y la verificación de teorías físicas fundamentales.

En el campo de los sensores cuánticos, la extrema sensibilidad de ciertos estados cuánticos frente a perturbaciones externas se explota para detectar variaciones diminutas en campos eléctricos, magnéticos y gravitacionales. Esta capacidad habilita aplicaciones de alto impacto en áreas como la medicina, mediante técnicas de imagen más precisas, la navegación inercial en entornos donde las señales satelitales no están disponibles, la exploración geológica de alta resolución y la detección temprana de fenómenos naturales como terremotos. La posibilidad de medir magnitudes físicas con una resolución cercana a los límites impuestos por la mecánica cuántica constituye uno de los avances tecnológicos más significativos de este paradigma.

Las redes cuánticas se perfilan como la base de una futura infraestructura de comunicación con garantías de seguridad fundamental. En este contexto, estados cuánticos entrelazados se distribuyen entre nodos espacialmente separados con el objetivo de compartir información cuántica de manera robusta. El desarrollo de repetidores cuánticos, memorias cuánticas y protocolos avanzados de mitigación de errores en el canal de comunicación representa uno de los principales desafíos tecnológicos actuales, aunque los progresos recientes indican un avance sostenido. Estas redes podrían dar lugar a una futura Internet cuántica, capaz de integrar computación distribuida, sincronización temporal de alta precisión y servicios criptográficos de nueva generación.

De forma complementaria, la computación híbrida cuántico clásica emerge como un enfoque particularmente prometedor. Este paradigma busca combinar la estabilidad y escalabilidad de los algoritmos clásicos con la