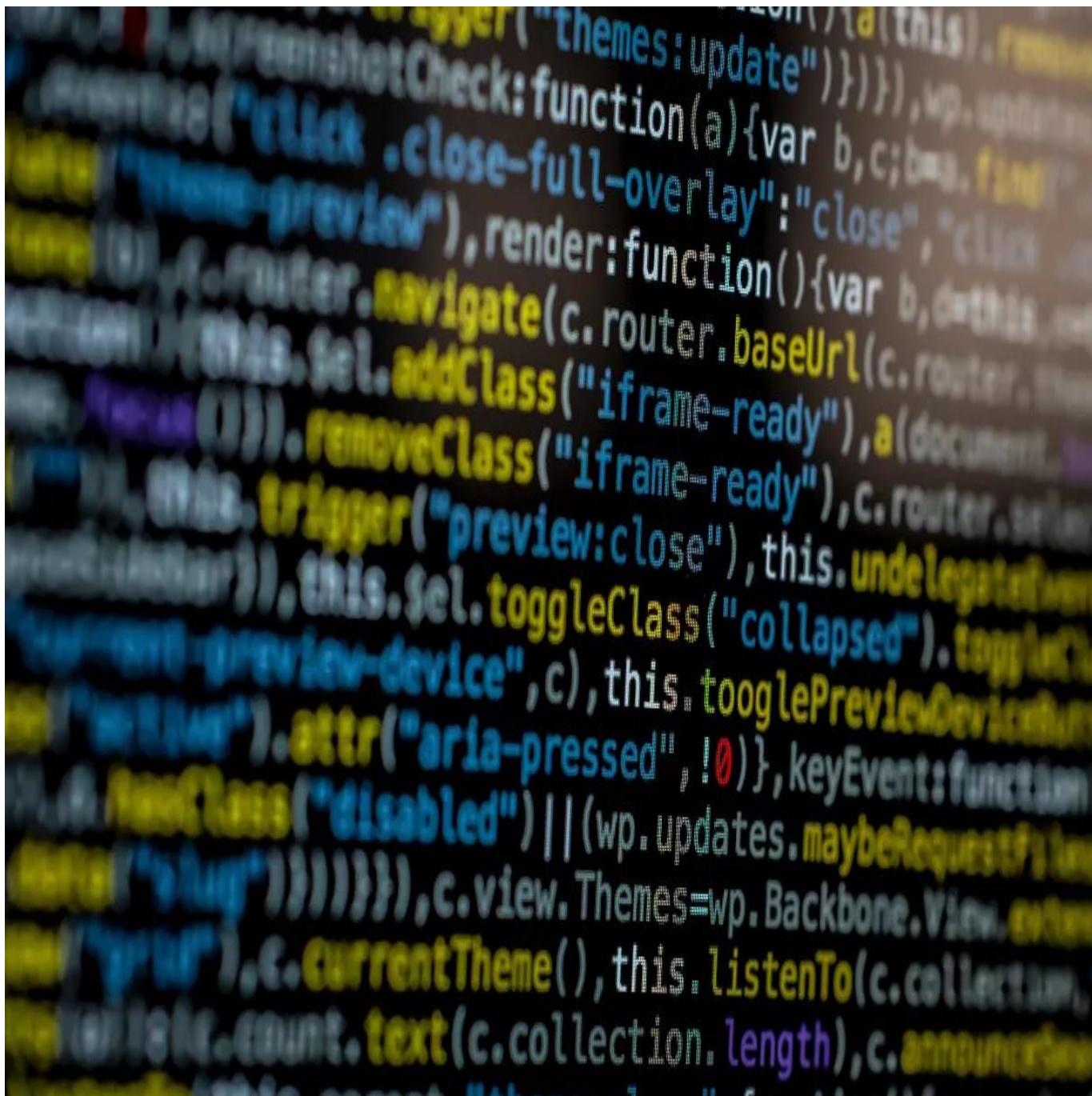


Ordenadores cuánticos, la próxima frontera de la informática



La próxima generación de superordenadores ya no basará su capacidad computacional en transistores, sino en la física cuántica. A lo largo de las próximas décadas asistiremos a una verdadera revolución en el campo de la informática, que traerá consigo máquinas cuya potencia aún solo podemos imaginar.

Imaginemos -sin necesidad de hacer mucho esfuerzo- el caos que produce el tráfico rodado en las grandes ciudades. Atascos, embotellamientos y retrasos en los desplazamientos, debidos al exceso de vehículos en las calles. Supongamos que nos proponemos optimizar la circulación por la urbe, intentando encontrar el mejor trayecto para cada vehículo. Incluso para un ordenador actual, por potente que sea, resultaría una tarea casi imposible de realizar, dado el inmenso número de variables a tener en cuenta y la ingente cantidad de información que debe alimentar el algoritmo para que este resulte eficaz. Sin embargo, se trata de un reto que, en teoría, estaría al alcance de la computación cuántica, la próxima gran revolución de la ciencia

informática.

Resulta que el ejemplo anterior no es una mera invención, sino un experimento real, llevado a cabo en la sobre poblada aglomeración urbana de Pekín, por el gigante automovilístico Volkswagen, en colaboración con Google y D-Wave Systems. De acuerdo con la empresa alemana, el algoritmo utilizado fue capaz de reducir el tráfico optimizando el recorrido a realizar por los vehículos.¹

Los ordenadores cuánticos prometen llevar la computación hasta límites inimaginables actualmente, basando su funcionamiento en la física de partículas. Todavía no es más que eso, una promesa, cuyo despliegue durará décadas, pero ya hoy en día podemos anticipar, a través de experiencias y pruebas, la transformación que traerá consigo esta nueva generación de máquinas.

Aunque es pronto para predecir todo su impacto, la llegada de la computación cuántica implicará importantes ganancias en productividad, que Boston Consulting Group valora en 450.000 millones de dólares anuales. Los pioneros en su utilización serán aquellos sectores cuya actividad reposa sobre unas necesidades de simulación y optimización de sistemas altamente complejas, como pueden ser, entre otros, el diseño de materiales o la creación de nuevos fármacos. A medio plazo, la consultora prevé la generación de un valor para los usuarios finales en cantidades todavía modestas, entre los 2.000 millones de dólares y los 5.000 en 2024.

No nos engañemos, los ordenadores cuánticos no van a borrar del mapa a los ordenadores convencionales, por lo menos en mucho tiempo. Todo problema que pueda ser eficientemente abordado y resuelto por las máquinas de que disponemos en la actualidad seguirán siendo de su competencia. Para la mayoría de las situaciones se mantendrán como la solución más fácil y barata de aplicar. Pero la computación cuántica abrirá nuevas fronteras científicas y tecnológicas, al permitir realizar en poco tiempo tareas en exceso complejas, de otra forma irrealizables o de muy lenta resolución con medios informáticos tradicionales.

Del bit al qubit

En los ordenadores convencionales la información adquiere la forma de bit, un impulso óptico o eléctrico que toma la forma de 1 o 0, como si fuese un interruptor que se enciende o se apaga. Los bits, las unidades básicas de información, se almacenan en transistores dentro de microchips, de forma que cuanto más contengan, más rápido pueden procesar los impulsos eléctricos, y, en consecuencia, más veloz resulta el ordenador al que pertenecen.

En la computación cuántica ya no hablamos de bits, sino de *qubits*. Se trata de ordenadores cuyo funcionamiento no reposa sobre transistores, sino sobre partículas subatómicas, que pueden adquirir los valores 1 y 0. Hasta aquí parece que se comportan como los bits, sin embargo, existen dos propiedades de la mecánica cuántica que los hace distintos: la superposición y el entrelazamiento.

Por una parte, la superposición implica que los qubits pueden adoptar el valor 1 o el valor 0, pero también simultáneamente propiedades de ambos. Esto amplía de forma exponencial la capacidad computacional, pues un ordenador con varios qubits en superposición puede cotejar simultáneamente un elevado número de resultados posibles, y, solamente cuando el estado cuántico de los qubits colapsa a 1 o 0, es el momento en que aparece el resultado final.

La otra propiedad es la posibilidad de entrelazar pares de qubits, de forma que ambos existan en un mismo estado cuántico, lo que implica que, si es alterado el estado de uno de ellos, el del otro cambia instantáneamente de una forma predecible. El entrelazamiento funciona incluso si están separados por grandes distancias. Mientras que en la informática convencional al doblar el número de bits se dobla la capacidad de procesado de información, en el ordenador cuántico el entrelazamiento permite que, al añadir

nuevos qubits, la potencia computacional se dispare exponencialmente.

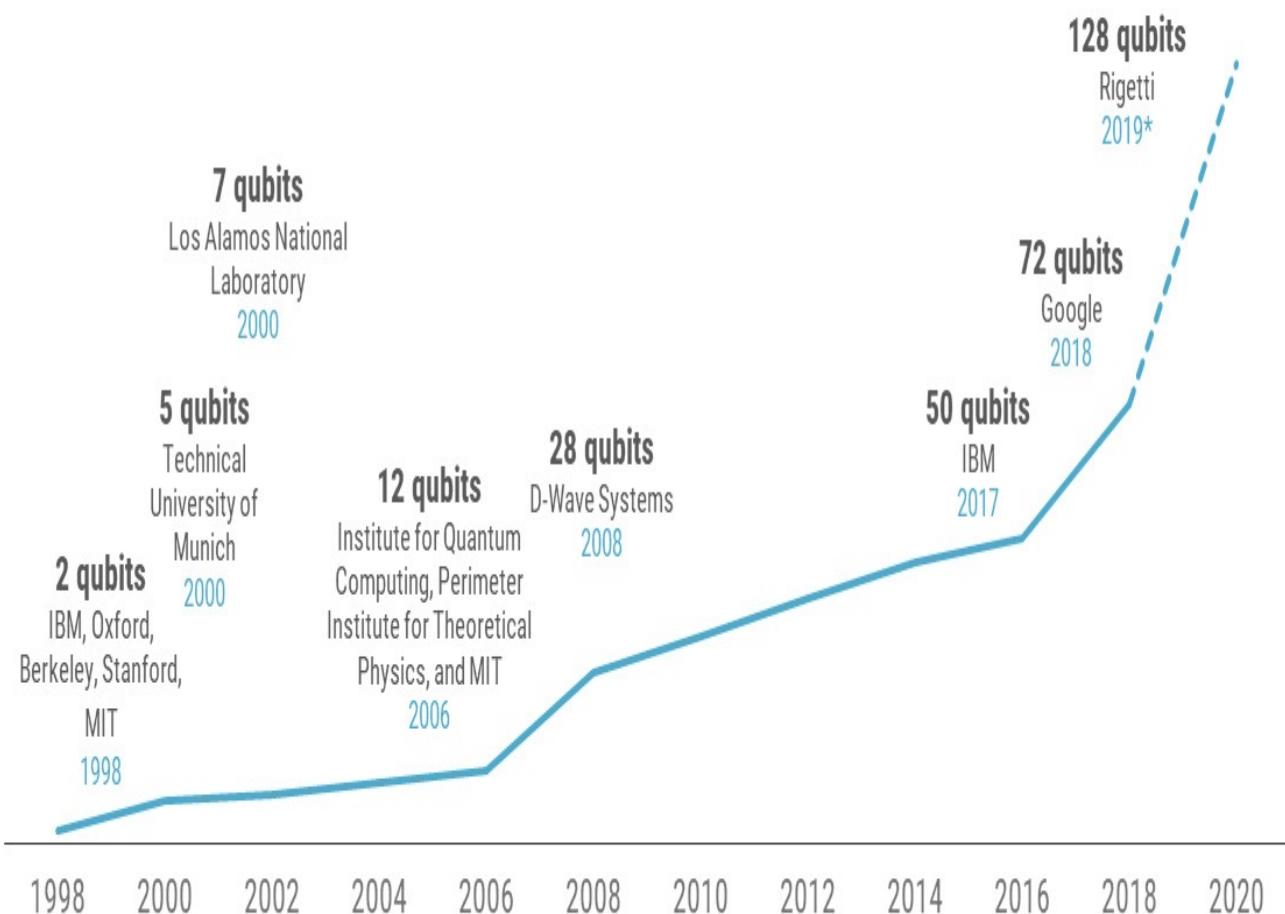
Una larga evolución

El desarrollo de ordenadores cuánticos es harto complejo. Manejar y manipular partículas subatómicas es un reto científico de primer orden. En algunos casos se requiere crear circuitos superconductores y enfriarlos a temperaturas menores que las que hay en el espacio exterior; otras veces se intenta atrapar átomos individuales en campos electromagnéticos dentro de cámaras de vacío. El objetivo en ambos casos es conseguir aislar a los qubits en un espacio cuántico controlado.

Aunque gradualmente surgen nuevos hitos en este campo de investigación, su evolución avanza despacio. El gráfico siguiente -realizado por CBInsights con datos de MIT- muestra las principales experiencias en computación cuántica llevadas a cabo desde finales de la década de los 90, con el número de qubits utilizados en cada caso.

Quantum computers are getting more powerful

Number of qubits achieved by date and organization 1998 – 2020*



Source: MIT, Qubit Counter. *Rigetti quantum computer expected by late 2019.

 CB INSIGHTS

Tras veinte años de investigación, nos encontramos en la actualidad con prototipos que superan los 100 qubits. El anuncio de IBM en 2017 de haber alcanzado los 50 qubits supuso un crecimiento de 25 veces la experiencia de la misma empresa de 1998. Sin embargo, todo parece indicar que a partir de ahora la potencia computacional cuántica acelerará su crecimiento. Google presentó el pasado año un procesador de 72 qubits, mientras que Rigetti quiere disponer de un microchip de 128 qubits antes del fin de 2019.

Las oleadas de la computación cuántica

La llegada de los ordenadores cuánticos se prevé en varias oleadas, que la consultora Boston Consulting Group ha clasificado de la manera siguiente:

La era NISQ. Caracterizada por dispositivos cuánticos ruidosos de escala intermedia (*Noisy Intermediate-Scale Quantum*: NISQ). Tendrá lugar entre los próximos tres a cinco años, y en ella aparecerán máquinas cuánticas cada vez más capaces de realizar funciones específicas, pero que presentarán unas tasas de error demasiado elevadas para resultar funcionales. La precisión en el cálculo todavía supone una ventaja de los ordenadores digitales convencionales frente a los de nueva generación.

Amplia ventaja cuántica. Esta fase llegará dentro de entre diez y veinte años, cuando los ordenadores cuánticos empiecen a realizar tareas significativas con utilidad real en distintos sectores económicos. Comenzarán a presentar ventajas sobre las máquinas digitales en términos de velocidad a la hora de realizar la misma tarea, así como del coste implicado.

Tolerancia a fallas a gran escala. Dentro de más de veinte años la tecnología cuántica habrá superado las limitaciones técnicas y los problemas de estabilidad de las partículas subatómicas, así como de escalabilidad de la potencia computacional. Los ordenadores serán capaces de reducir significativamente sus propios errores y contribuirán a automatizar tareas en muchos sectores de actividad económica.

Qué actividades se benefician

La gran ventaja que ofrece la computación cuántica es poder resolver problemas que llevan procesar una gran densidad de información. En este sentido, destaca como especialmente útil en las siguientes aplicaciones:

Optimización combinatoria. Maximizar o minimizar una función objetivo, como, por ejemplo, calcular las distancias más cortas entre puntos o distribuir eficientemente recursos disponibles. Entre las aplicaciones prácticas, se pueden mencionar la gestión de redes (líneas aéreas, flotas de taxis, energía...), la optimización de cadenas de suministro y de sistemas logísticos, y la administración de carteras de activos financieros.

Ecuaciones diferenciales. Crear modelos de sistemas complejos. Es un campo muy útil, por ejemplo, para la simulación de dinámica de fluidos (diseño de materiales, aeronáutica y automoción) y para la simulación molecular (creación de fármacos y nuevos materiales).

Álgebra lineal. Disciplina muy asociada con la inteligencia artificial y el aprendizaje automático en temas como la identificación de patrones, que puede ser aplicada para la gestión del riesgo financiero, la clasificación de secuencias de ADN o la segmentación de mercados de consumo, por mencionar tres aplicaciones de distintas áreas.

Factorización. Criptografía y ciberseguridad, como descifrar claves o romper códigos.

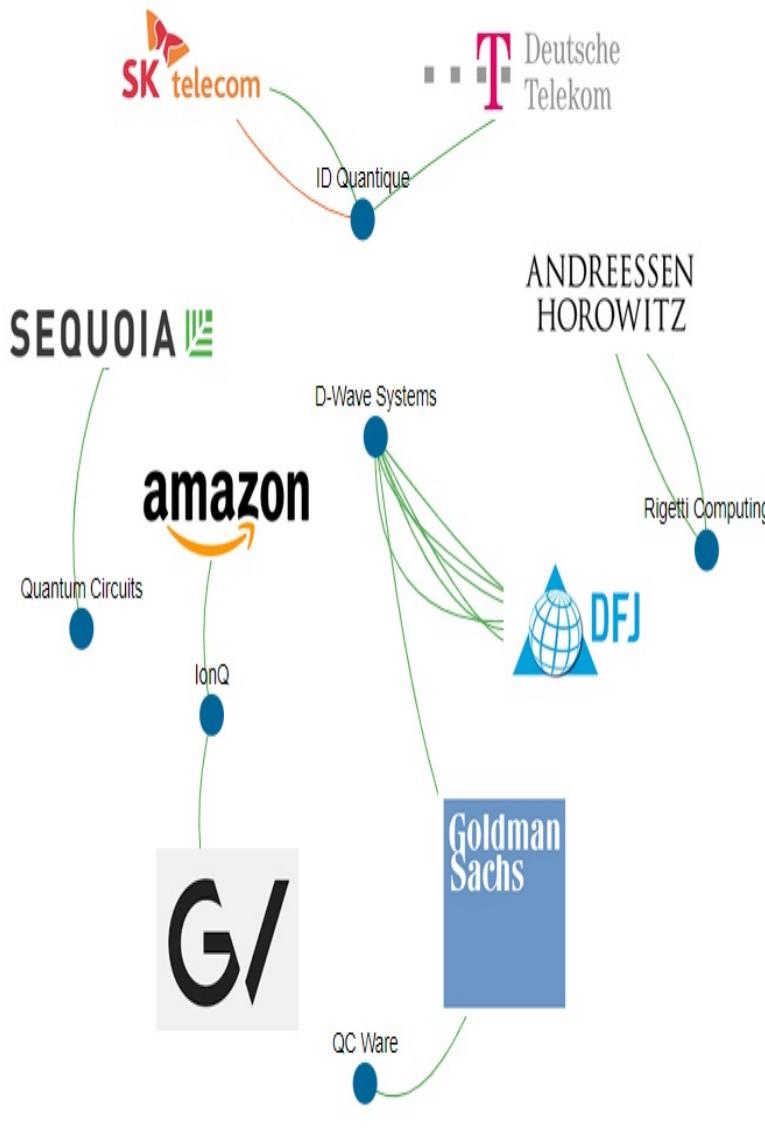
El ecosistema de empresas

Actualmente hay muy pocas *startups* dedicadas a la computación cuántica que hayan conseguido levantar más de 50 millones de dólares. Un informe de CBInsights identifica un total de cuatro, encabezadas por la canadiense D-Wave, que financieramente es la más potente. Le siguen la estadounidense Rigetti Computing, la australiana Silicon Quantum Computing y, finalmente, la británica Cambridge Quantum Computing.

Por otro lado, las inversiones en empresas dedicadas a la tecnología cuántica han ido aumentando desde 2013 hasta superar los 200 millones de dólares en 2017, si bien la cifra del año siguiente fue notablemente menor. En la figura siguiente CBInsights refleja las principales inversiones en las compañías del sector.

Select investors betting on quantum computing startups

2010 – 2019 YTD (1/7/2019)



Source: cbinsights.com

 CB INSIGHTS

green lines = investments

orange lines = acquisitions

Amazon y Google Ventures han centrado su apoyo en IonQ, mientras que las operadoras de telecomunicaciones SK Telecom de Corea y la alemana Deutsche Telekom han invertido en ID Quantique, empresa especializada en un protocolo de encriptación de red basado en tecnología cuántica.

Las firmas de capital riesgo Andreessen Horowitz y Sequoia también han hecho acto de presencia en el sector, la primera participando de Rigetti Computing y la segunda en el fabricante de hardware Quantum Circuits. Igualmente, Draper Fisher Jurvetson (DFJ) ha invertido en D-Wave, al igual que la banca Goldman Sachs.

Llegan los ordenadores cuánticos

Aunque la informática cuántica todavía está dando sus primeros pasos de forma experimental, a principios de 2019 IBM presentó en el marco de CES 2019, la feria de tecnología de Las Vegas, la primera versión comercial de su ordenador cuántico. Bautizado como Q System One, llega hasta los 20 qubits -30 menos que el prototipo que la compañía presentó en 2017-, y está destinado a apoyar actividades científicas y de negocios. El sistema tiene la forma de un gran cubo de cristal de casi tres metros, al que se accede a través de una puerta. La estructura está diseñada para mantener el chip cuántico a una temperatura de 10 milikelvin o una fracción por encima del cero.

Por otro lado, la Unión Europea ha materializado su apoyo al desarrollo de la tecnología cuántica a través del programa Flagship, dotado de 1.000 millones de euros para financiar iniciativas en este campo. Precisamente, uno de los primeros proyectos seleccionados ha sido el presentado por el grupo Quantum Technologies for Information Science (QUTIS) de la Universidad del País Vasco, para construir un ordenador cuántico europeo de libre acceso para investigadores y científicos. El OpenSuperQ estará basado en circuitos superconductores y albergará entre 50 y 100 qubits, muy por encima de los 20 que ostenta la versión comercial de IBM. Si todo va bien, el primer ordenador cuántico de Europa tendrá origen vasco.

Fotografía de [Markus Spiske](#) en Pexels

CBInsights (2019) "What Is Quantum Computing?"

Díaz, E. (2019) "¿Cómo será el ordenador cuántico más evolucionado de Europa?" en *Think Big*. Disponible en: <https://blogthinkbig.com/ordenador-cuantico-europa>

Giles, M. (2019) "Explainer: What is a quantum computer?" en *Harvard Business Review*. Disponible en: <https://www.technologyreview.com/s/612844/what-is-quantum-computing>

Langjone, M., Tillemann-Dick, C., Kumar, A. y Taneja, V. (2019) "Where Will Quantum Computers Create Value—and When?". Boston Consulting Group. Disponible en: <https://www.bcg.com/publications/2019/quantum-computers-create-value-when.aspx>

Pinedo, E. (2019) "IBM presenta la versión comercial de su computadora cuántica" en *Hipertextual*. Disponible en: https://hipertextual.com/2019/01/ibm-version-comercial-computadora-cuantica?utm_medium=feed&utm_source=feedpress.me&utm_campaign=Feed%3A+hipertextual