



¿Qué es la computación cuántica y por qué es importante?

Los recientes avances tecnológicos han suscitado un renovado interés por una forma futurista de computación. Los investigadores de Microsoft develaron el miércoles un método de computación cuántica que, según la empresa, implica la creación de un nuevo estado de la materia. En diciembre, Google anunció su propio avance en el diseño de chips cuánticos.

Asa Fitch /
THE WALL STREET JOURNAL

Un par de llamativos anuncios recientes de Microsoft y Google han inyectado nuevo entusiasmo en la búsqueda durante décadas de la ultrapotente computación cuántica.

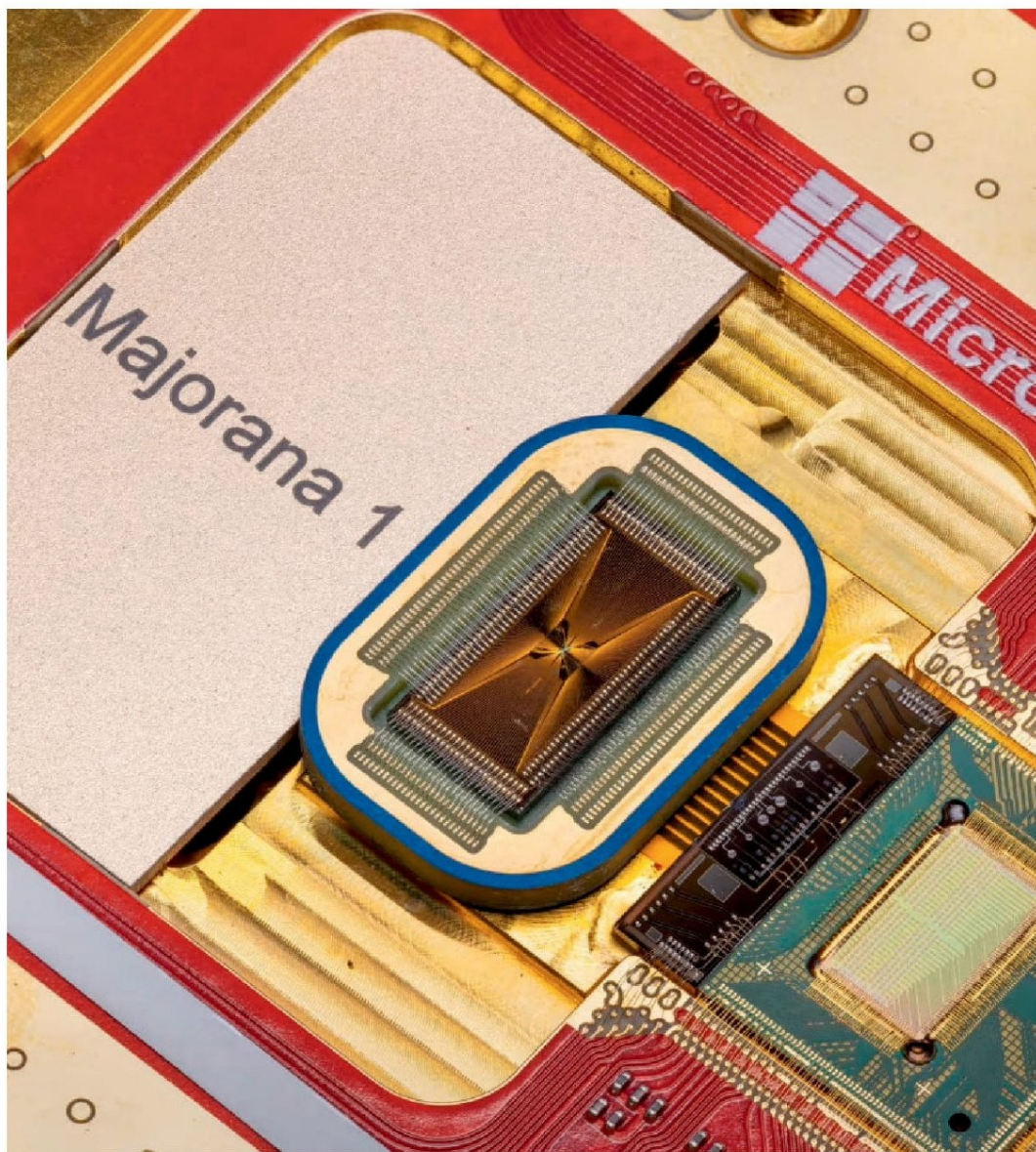
Los investigadores de Microsoft revelaron el miércoles un método de computación cuántica que, según la empresa, implica la creación de un nuevo estado de la materia. En diciembre, Google anunció su propio avance en el diseño de chips cuánticos.

Ambos avances fueron seguidos de una subida de los precios de las acciones relacionadas con la cuántica, ya que los inversores apostaron a que podrían acelerar el desarrollo de una nueva categoría de computadores que podrían ayudar en el descubrimiento de fármacos, entre otras aplicaciones.

Sin embargo, la computación cuántica sigue estando relativamente en pañales. Un puñado de nuevas empresas y grandes compañías tecnológicas están trabajando en ella, pero los expertos del sector afirman que pasarán años antes de que los computadores cuánticos prácticos y potentes estén ampliamente disponibles.

¿Qué es la informática cuántica?

Los computadores normales realizan cálculos mediante interruptores de encendido y apagado. Las distintas disposiciones de



estos interruptores, llamados "bits", representan valores diferentes. Indican al computador o al teléfono lo que debe aparecer en la pantalla o cuál es el resultado correcto de un problema matemático.

El número de bits con los que trabajan los computadores, y por tanto su potencia de cálculo, ha crecido sustancialmente en los últimos cincuenta años. Pero los computadores cuánticos, cuando lleguen, prometen aumentar esa potencia para ciertos

tipos de cálculos hasta niveles que ningún dispositivo basado en binarios podría alcanzar.

Los computadores cuánticos utilizan un tipo diferente de bit, el llamado "qubit", que puede estar encendido, apagado o en algún punto intermedio, una combinación de ambos. Esto permite que un qubit contenga más información que un bit normal - y que los computadores con muchos qubits aumenten exponencialmente esa informa-

ción-, lo que abre un abanico de nuevas posibilidades de cálculo.

"Imagine un chip que cabe en la palma de la mano y que es capaz de resolver problemas que ni siquiera todos los ordenadores de la Tierra juntos podrían resolver hoy", dijo Satya Nadella, director ejecutivo de Microsoft, en una publicación en las redes so-

ciales el miércoles.

¿Por qué es tan importante?

Si los sueños de la industria de la computación cuántica se hacen realidad, los computadores cuánticos realizarían rápidamente cálculos que a los computadores tradicionales les habrían llevado años. Cuando Google presentó su propio chip cuántico en diciembre, dijo que realizaba en cinco minutos un cálculo que habría llevado a uno de los mejores supercomputadores actuales 10 septillones de años (un 10 seguido de 24 ceros).

Un computador cuántico superpotente podría realizar complejas simulaciones del mundo físico con una precisión y velocidad nunca vistas. Sus promotores afirman que podría dar lugar a baterías más eficaces, una producción química más eficiente y nuevos fármacos. En teoría, un computador cuántico potente también podría descifrar muchas de las técnicas actuales de encriptación de datos.

¿Los computadores cuánticos van a descifrar mis contraseñas?

Puede que sí. El campo ha progresado lo suficiente como para que algunas empresas ya se estén preparando para el día en que la computación cuántica pueda romper los métodos clásicos de cifrado. Incluso Apple ha preparado iMessage para un mundo poscuántico. Parte de esto se basa en la expectativa de que los datos cifrados puedan almacenarse con el fin de utilizar la computación cuántica para descifrarlos en el futuro.

El gobierno ha trabajado en la sustitución de las formas actuales de cifrado por algoritmos poscuánticos, algo que podría ser vital para la seguridad nacional. A pesar de los preparativos, esto no es algo que vaya a ocurrir pronto. Por ejemplo, los investigadores afirman que un dispositivo cuántico lo bastante potente como para descifrar bitcoin está probablemente a una década o más de distancia.

¿Cuáles son los retos?

Las empresas llevan décadas trabajando en el reto de la computación cuántica. El entusiasmo actual es una combinación de nuevos avances genuinos y un entorno en el que la gente espera un momento repentino, como el del ChatGPT, que podría catalizar un auge cuántico del mismo modo que lo ha hecho la IA en los últimos dos años.

Sin embargo, el hecho de que los expertos no estén seguros de si estos avances significan que los computadores cuánticos comercialmente viables están a años vista o todavía faltan una década o más, demuestra que la tecnología cuántica aún tiene elementos teóricos.

Las dificultades de la computación cuántica son innumerables. Para empezar, en muchos computadores cuánticos los qubits deben funcionar a temperaturas cercanas al cero absoluto, es decir, por debajo de los

400 grados Fahrenheit negativos.

Ampliar un computador cuántico también puede ser muy complicado.

Todos los chips de computador cometen errores que hay que comprobar y corregir, pero corregir errores con muchos qubits ha sido un reto especialmente espinoso. Algunos avances recientes, como el de Google, han pretendido solucionar el problema, pero sigue siendo quizá el más desalentador para la industria. Microsoft afirmó que su chip cuántico tenía una baja probabilidad de error y que había "identificado caminos claros" para reducirla aún más.

¿Qué es un topoconductor?

Para crear su chip cuántico, Microsoft dijo que sus investigadores crearon el primer "topoconductor" del mundo. El topoconductor explota un estado de la materia llamado "superconductividad topológica" que hasta ahora sólo existía en teoría, según Microsoft.

Los detalles técnicos son complejos e implican cables superdiminutos enfriados hasta casi el cero absoluto y sintonizados con campos magnéticos. Pero Microsoft afirma que su chip cuántico, llamado Majorana 1, está diseñado para albergar hasta un millón de qubits en un solo chip. Es una cifra enorme: Los computadores cuánticos más avanzados sólo tienen miles de qubits.

¿Qué empresas exploran la computación cuántica?

Entre las empresas tecnológicas que exploran la computación cuántica se encuentran Google, Microsoft e IBM, que ayudaron a crear el sector hace aproximadamente una década. Los esfuerzos de inversión e investigación de estas empresas abarcan décadas y numerosos directores ejecutivos, una rareza relativa para una tecnología que no tiene rendimientos previsibles. Hay varias empresas más pequeñas que desarrollan este tipo de computadores o tecnologías adyacentes, como software y algoritmos relacionados.

Hay un puñado de empresas relacionadas con la informática cuántica que cotizan en bolsa: IonQ (IONQ), Quantum Computing (QUBT), D-Wave Quantum (QBTS) y Rigetti Computing (RGTI). Muchas de sus acciones subieron tras el anuncio de Microsoft. D-Wave subió más de un 7% a mediados del jueves, y Rigetti casi un 4%.

Sin embargo, las acciones de estas empresas pueden ser volátiles. El mes pasado cayeron bruscamente cuando el CEO de Nvidia, Jensen Huang, restó importancia a la utilidad de la tecnología a corto plazo.

"Si dijéramos que los computadores cuánticos serán muy útiles en 15 años, probablemente sería demasiado pronto. Si dijéramos 30, probablemente sería tarde", aseguró Huang. **WSJ**