

El fin de la era del silicio

Se acerca una revolución.

En 2019 y 2020, dos bombas informativas sacudieron el mundo de la ciencia. Dos grupos anunciaron que habían logrado la supremacía cuántica, el legendario punto en el que un tipo de ordenador radicalmente nuevo, llamado «ordenador cuántico», podría superar de manera decisiva a un superordenador digital ordinario en tareas específicas. Era el anuncio de una conmoción capaz de modificar el panorama informático por entero y todos los aspectos de nuestra vida cotidiana.

En primer lugar, Google reveló que su ordenador cuántico, Sycamore, podía resolver en doscientos segundos un problema matemático que llevaría diez mil años en el superordenador más rápido del mundo. Según el boletín *Technology Review* del MIT, Google lo calificó de avance decisivo. Lo compararon con el lanzamiento del Sputnik o el primer vuelo de los hermanos Wright. Era «el umbral de una nueva era de máquinas que harían que el ordenador más potente de la actualidad pareciera un ábaco».

El Instituto de Innovación Cuántica de la Academia China de las Ciencias fue aún más lejos. Afirmaron que su ordenador cuántico era cien billones de veces más rápido que un superordenador normal.

Bob Sutor, vicepresidente de IBM, al comentar el meteórico ascenso de los ordenadores cuánticos, afirmó rotundamente: «Creo que va a ser la tecnología informática más importante de este siglo».

Estas computadoras se han llamado «el ordenador definitivo», un salto tecnológico decisivo con profundas implicaciones en todo el mundo. En lugar de calcular en diminutos transistores, lo hacen mediante el menor de los objetos posibles, los propios átomos, y por ello pueden superar fácilmente la potencia del mejor superordenador. Los ordenadores cuánticos podrían marcar el comienzo de una era del todo nueva para la economía, la sociedad y nuestro modo de vida.

Pero también son algo más que otro potente sistema. Son un nuevo tipo de ordenador capaz de abordar problemas que los equipos digitales nunca podrán resolver, ni siquiera con una cantidad infinita de tiempo. Por ejemplo, estos últimos nunca podrán calcular con precisión cómo se combinan los átomos para crear reacciones químicas esenciales, en especial las que hacen posible la vida. Los ordenadores digitales solo pueden calcular en series digitales, formadas por un conjunto de 0 y 1, que son demasiado burdos para describir las delicadas ondas de electrones que bailan en el interior de una molécula. Por ejemplo, al realizar el tedioso cálculo de los caminos que sigue un ratón en un laberinto, un ordenador digital tiene que pasar por un penoso análisis de cada camino posible, uno tras otro. Un ordenador cuántico, sin embargo, analiza simultáneamente todos los caminos posibles, a la velocidad del rayo.

Esto, a su vez, ha acentuado la rivalidad entre los gigantes de la informática, que compiten por crear el ordenador cuántico más potente del mundo. En 2021, IBM presentó su propio ordenador cuántico, llamado Eagle, que ha tomado la delantera, al poseer más potencia de cálculo que todos los modelos anteriores.

Pero estos récords son como la cubierta de una tarta: están hechos para romperlos.

Dadas las profundas implicaciones de esta revolución, no es de extrañar que muchas de las principales empresas del mundo hayan invertido grandes sumas en esta nueva tecnología. Google, Microsoft, Intel, IBM, Rigetti y Honeywell están construyendo prototipos de ordenadores cuánticos. Los líderes de Silicon Valley son conscientes de que deben seguir el ritmo de esta nueva revolución o quedarse tirados en la cuneta.

IBM, Honeywell y Rigetti Computing han puesto su primera generación de ordenadores cuánticos en internet para despertar el apetito de un público curioso, de modo que la sociedad pueda tener su primera exposición directa a la computación cuántica. Se puede experimentar de primera mano esta nueva revolución conectándose a un ordenador cuántico en internet. Por ejemplo, la plataforma IBM Q Experience, lanzada en 2016, pone a disposición del público quince ordenadores cuánticos a través de internet de manera gratuita. Entre sus usuarios se hallan Samsung y JPMorgan Chase. Ya los utilizan cada mes dos mil personas, desde escolares hasta profesores.

Wall Street se ha interesado mucho por esta tecnología. IonQ se convirtió en la primera empresa importante de computación cuántica en salir a bolsa, y recaudó seiscientos millones de dólares en su OPV de 2021. Y lo que es aún más sorprendente, la rivalidad es tan intensa que una nueva empresa emergente, PsiQuantum, sin ningún prototipo comercial en el mercado ni historial alguno de productos anteriores, despuntó de repente en el mercado de Wall Street hasta alcanzar una valoración de tres mil cien millones de dólares, con la capacidad de captar seiscientos sesenta y cinco millones de dólares en financiación casi de la noche a la mañana. Los analistas empresariales escribieron que rara vez habían visto una situación así, una nueva empresa que se subiera a la ola de la especulación febril y los titulares sensacionalistas hasta alcanzar tales alturas.

La empresa de consultoría y contabilidad Deloitte calcula que el mercado de los ordenadores cuánticos alcanzará los cientos de millones de dólares en la década de 2020 y las decenas de miles de millones de dólares en la de 2030. Nadie sabe cuándo entrarán en el mercado y alterarán el panorama económico, pero las predicciones se revisan constantemente para adaptarse a la inaudita velocidad de los descubrimientos científicos en este campo. Christopher Savoie, consejero delegado de Zapata Computing, dijo acerca del meteórico ascenso de los ordenadores cuánticos: «Ya no es cuestión de si ocurrirá, sino de cuándo».

Incluso el Congreso de Estados Unidos ha expresado un gran interés en ayudar a poner en marcha esta nueva tecnología. Al darse cuenta de que otras naciones ya han financiado generosamente la investigación en ordenadores cuánticos, el Congreso aprobó, en diciembre de 2018, la Ley de Iniciativa Cuántica Nacional para proporcionar el capital inicial con que ayudar a poner en marcha nuevos estudios. La comisión ordenó la creación de entre dos y cinco nuevos Centros Nacionales de Investigación en Ciencias de la Información Cuántica, dotados con ochenta millones de dólares anuales.

En 2021, el Gobierno de Estados Unidos también anunció una inversión de seiscientos veinticinco millones de dólares en tecnologías cuánticas, que supervisará el Departamento de Energía. A su vez, gigantescas corporaciones como Microsoft, IBM y Lockheed Martin aportaron trescientos cuarenta millones de dólares adicionales a este proyecto.

China y Estados Unidos no son los únicos que utilizan fondos públicos para acelerar esta tecnología. El Gobierno del Reino Unido está construyendo el Centro Nacional de Computación Cuántica, que servirá para centralizar la investigación en este campo, en el laboratorio Harwell del Consejo de Instalaciones Científicas y Tecnológicas de Oxfordshire. Espoleadas por el Gobierno, a finales de 2019 se habían fundado en el Reino Unido treinta nuevas empresas dedicadas a la computación cuántica.

Los analistas del sector reconocen que es una apuesta de un billón de dólares. No hay garantías en un campo tan competitivo. A pesar de los impresionantes logros técnicos conseguidos por Google y otras empresas en los últimos años, un ordenador cuántico viable que pueda resolver problemas del mundo real está todavía a muchos años vista. Aún nos queda por delante una enormidad de trabajo duro. Algunos críticos incluso afirman que podría ser una quimera. Pero las empresas informáticas son conscientes de que, a menos que den sus primeros pasos en el sector cuántico, podrían quedarse fuera de golpe.

Ivan Ostojic, socio de la consultora McKinsey, afirmó: «Las empresas de los sectores en los que la computación cuántica tendrá el mayor potencial de impacto deberían implicarse ya». Ámbitos como la química, la medicina, el petróleo y el gas, el transporte, la logística, la banca, los productos farmacéuticos y la ciberseguridad están listos para los grandes cambios. Y añade: «En principio, la computación cuántica será relevante para todos los directores de sistemas de información, ya que acelerará las soluciones a una gran variedad de problemas. Esas empresas tienen que poseer la capacidad cuántica».

Vern Brownell, ex director general de D-Wave Systems, una empresa canadiense de computación cuántica, señaló: «Creemos que estamos a punto de poder ofrecer funcionalidades que no se consiguen con la informática clásica».

Muchos científicos creen que estamos entrando en una era completamente nueva, con perturbaciones comparables a las que crearon la introducción del transistor y la del microchip. Empresas sin vínculos directos con la producción informática, como el gigante de la automoción Daimler, propietario de Mercedes-Benz, ya están invirtiendo en esta nueva tecnología, al intuir que los ordenadores cuánticos pueden allanar el camino a nuevos desarrollos en sus propios sectores. Julius Marcea, directivo de la rival BMW, ha escrito: «Estamos entusiasmados por investigar el potencial transformador de la computación cuántica en el sector automovilístico, y estamos decididos a ampliar los límites de la capacidad técnica». Otras grandes empresas, como Volkswagen y Airbus, han creado sus propias divisiones de computación cuántica para explorar de qué modo puede esta revolucionar su negocio.

Las empresas farmacéuticas también observan atentamente los avances en este campo, conscientes de que los ordenadores cuánticos pueden ser capaces de simular procesos químicos y biológicos complejos, para lo cual los ordenadores digitales se quedan muy cortos. Las enormes instalaciones dedicadas a hacer ensayos con millones de fármacos podrían ser sustituidas algún día por «laboratorios virtuales» que los prueben

en el ciberespacio. Algunos temen que, llegado el momento, esto pueda sustituir a los químicos. Pero Derek Lowe, que lleva un blog sobre descubrimiento de fármacos, afirma: «No es que las máquinas vayan a sustituir a los químicos. Es que los químicos que utilicen máquinas sustituirán a los que no lo hagan».

Incluso el Gran Colisionador de Hadrones (LHC, por sus siglas en inglés), a las afueras de Ginebra (Suiza), la mayor máquina científica del mundo, que hace chocar protones a catorce billones de electronvoltios para recrear las condiciones del universo primitivo, utiliza ahora ordenadores cuánticos para ayudar en la criba de enormes masas de datos. En un segundo, pueden analizar hasta un billón de bytes generados por unos mil millones de colisiones de partículas. Quizá algún día los ordenadores cuánticos desentrañen los secretos de la creación del universo.

Supremacía cuántica

En 2012, cuando el físico John Preskill, del Instituto de Tecnología de California, acuñó el término «supremacía cuántica», muchos científicos negaron la idea. Pensaban que pasarían décadas, si no siglos, antes de que los ordenadores cuánticos pudieran superar a los digitales. Al fin y al cabo, la computación en átomos individuales, en lugar de en las placas de silicio de los chips, se consideraba endemoniadamente difícil. La más mínima vibración o ruido puede perturbar la delicada danza de los átomos en un ordenador cuántico. Pero, hasta hoy, los asombrosos anuncios de supremacía cuántica han echado por tierra las sombrías predicciones de los detractores. Ahora el interés se centra en la rapidez de desarrollo de este campo.

Las convulsiones causadas por estos notables logros también han sacudido las salas de juntas y las agencias de inteligencia secretas de todo el mundo. Documentos filtrados por denunciantes han demostrado que la CIA y la Agencia de Seguridad Nacional siguen de cerca los avances en este campo. Esto se debe a que los ordenadores cuánticos son tan potentes que, en principio, podrían descifrar todos los cibercódigos conocidos. Esto significa que los secretos cuidadosamente protegidos por los gobiernos, que son sus joyas de la corona y contienen su información más confidencial, son vulnerables a los ataques, al igual que lo son los secretos mejor guardados de las empresas e incluso de los particulares. La situación es tan urgente que incluso el Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST, por sus siglas en inglés), que establece la política y los estándares nacionales, ha publicado recientemente unas directrices para ayudar a las grandes empresas y organismos a planificar la inevitable transición a esta nueva era. El NIST ya ha anunciado que espera que para 2029 los ordenadores cuánticos sean capaces de romper el cifrado AES de 128 bits, el código utilizado por muchas empresas.

En la revista *Forbes*, Ali El Kaafarani señalaba: «Es una perspectiva bastante aterradora para cualquier organización que tenga información confidencial que proteger».

China ha empleado diez mil millones de dólares en su Laboratorio Nacional para las Ciencias de la Información Cuántica, porque están decididos a ser líderes en este fundamental campo en rápida evolución. Los países invierten decenas de miles de

millones en proteger celosamente sus códigos. Armado con un ordenador cuántico, un pirata informático podría entrar en cualquier ordenador digital del planeta, perturbando así las industrias e incluso el ejército. Toda la información protegida quedaría entonces disponible para el mejor postor. La irrupción de los ordenadores cuánticos en el santuario de Wall Street podría, asimismo, desestabilizar los mercados financieros. Estos sistemas también podrían desintegrar la cadena de bloques tecnológica, causando así estragos en el mercado del bitcoin. Deloitte ha calculado que alrededor del 25 por ciento de los bitcoins son potencialmente vulnerables al pirateo por parte de un ordenador cuántico.

«Los responsables de proyectos de cadena de bloques probablemente estarán muy atentos a los avances de la computación cuántica», concluye un informe de CB Insights, una empresa dedicada al software de datos.

Así, lo que está en juego es nada menos que la economía mundial, fuertemente vinculada a la tecnología digital. Los bancos de Wall Street utilizan ordenadores para registrar transacciones de muchos miles de millones. Los ingenieros utilizan ordenadores para diseñar rascacielos, puentes y cohetes. Los artistas dependen de los ordenadores para animar las superproducciones de Hollywood. Las empresas farmacéuticas utilizan ordenadores para desarrollar su próximo fármaco milagroso. Los niños necesitan los ordenadores para jugar al último videojuego con sus amigos. Y nosotros dependemos esencialmente de los teléfonos móviles para recibir noticias instantáneas de nuestros amigos, socios y parientes. A todos nos ha entrado alguna vez el pánico cuando no encontramos el móvil. De hecho, es muy difícil nombrar cualquier actividad humana que no haya sido puesta patas arriba por los ordenadores. Dependemos tanto de ellos que si, de repente, todos ellos dejaran de funcionar en el mundo entero, la civilización se sumiría en el caos. Por eso los científicos siguen con tanta atención el desarrollo de los ordenadores cuánticos.

Fin de la ley de Moore

¿A qué se debe todo este revuelo y controversia?

El auge de los ordenadores cuánticos es señal de que la era del silicio está llegando gradualmente a su fin. Durante el último medio siglo, la explosión de la potencia informática se ha descrito mediante la ley de Moore, llamada así por el fundador de Intel, Gordon Moore. Esta hipótesis establece que la potencia de los ordenadores se duplica cada dieciocho meses. A pesar de ser engañosamente simple, esta ley ha acertado con el notable aumento exponencial que predice, el cual no tiene precedentes en la historia de la humanidad. No hay ningún otro invento que haya tenido un impacto tan generalizado en un periodo de tiempo tan breve.

Los ordenadores han pasado por muchas etapas a lo largo de su historia, y en cada una han aumentado extraordinariamente su potencia y provocado importantes cambios sociales. De hecho, la ley de Moore se puede extender hasta el siglo XIX, a la era de los ordenadores mecánicos. Por aquel entonces, los ingenieros utilizaban cilindros giratorios, engranajes y ruedas para realizar operaciones aritméticas sencillas. A principios del siglo

pasado, estas computadoras empezaron a utilizar la electricidad, sustituyendo los engranajes por relés y cables. Durante la Segunda Guerra Mundial, los ordenadores utilizaban una gran cantidad de válvulas de vacío para descifrar los códigos secretos de los gobiernos. En la posguerra, se pasó a los transistores, que podían miniaturizarse hasta un tamaño microscópico, lo que facilitó continuos avances en velocidad y potencia.

En la década de 1950, los ordenadores centrales solo podían ser adquiridos por grandes empresas y organismos públicos, como el Pentágono y los bancos internacionales. Aunque eran potentes (por ejemplo, el ENIAC podía hacer en treinta segundos lo que a un ser humano le llevaría veinte horas), eran caros y voluminosos, pues a menudo ocupaban toda una planta de un edificio de oficinas. El microchip revolucionó todo este proceso, reduciendo su tamaño a lo largo de las décadas, de modo que un chip típico, tan grande como una uña, puede contener ahora unos mil millones de transistores. Los teléfonos móviles que ahora utilizan los niños para jugar a videojuegos son más potentes que una habitación llena de aquellos torpes dinosaurios que en su día utilizó el Pentágono. Damos por sentado que el ordenador que llevamos en el bolsillo supera con creces la potencia de los utilizados durante la Guerra Fría.

Todo acaba por ser superado. Cada transición en el desarrollo del ordenador ha dejado obsoleta la tecnología anterior en un proceso de destrucción creativa. La ley de Moore ya se está ralentizando y puede llegar a detenerse. Esto se debe a que los microchips son tan compactos que la capa más fina de transistores tiene unos veinte átomos de espesor. Cuando se alcanzan los cinco átomos aproximadamente, la ubicación de los electrones se vuelve incierta, por lo que pueden escaparse y provocar un cortocircuito en el chip, o bien generar tanto calor que los chips se fundan. En otras palabras, según las leyes de la física, la ley de Moore acabará por colapsar si seguimos utilizando principalmente silicio. Podríamos estar asistiendo al final de la era del silicio. El siguiente salto podría ser la era postsilicio o cuántica.

Como ha dicho Sanjay Natarajan, de Intel: «Creemos que hemos exprimido todo lo que se puede exprimir de esa arquitectura».

Silicon Valley puede acabar convirtiéndose en el próximo Cinturón del Óxido.

Aunque ahora las cosas parecen tranquilas, tarde o temprano este nuevo futuro hará acto de presencia. Como dice Hartmut Neven, director del Laboratorio de Inteligencia Artificial de Google: «Parece que no está pasando nada, y entonces, de repente, estás en un mundo diferente».

¿Por qué son tan potentes?

¿Qué hace que los ordenadores cuánticos sean tan potentes que las naciones del mundo tengan prisa por dominar esta nueva tecnología?

Básicamente, todos los ordenadores modernos se basan en información digital, que puede codificarse en una serie de 0 y 1. La unidad de información más pequeña, un solo dígito, se denomina bit. Esta secuencia de 0 y 1 se introduce en un procesador digital,

que realiza el cálculo y produce un resultado. Por ejemplo, su conexión a internet se mide en términos de bits por segundo o bps, lo que significa que cada segundo se envían mil millones de bits a su ordenador, y esto le permite acceder al instante a películas, correos electrónicos, documentos, etc.

Sin embargo, en 1959, el premio Nobel Richard Feynman adoptó una manera distinta de ver la información digital. En un profético y pionero artículo titulado «There's Plenty of Room at the Bottom» («Hay mucho espacio en el fondo») y en artículos posteriores, se preguntaba: ¿por qué no sustituir esta secuencia de 0 y 1 por estados de átomos, creando así un ordenador atómico? ¿Por qué no sustituir los transistores por el objeto más pequeño posible, el átomo?

Los átomos son como peonzas. En un campo magnético, pueden alinearse hacia arriba o hacia abajo con respecto al campo magnético, lo que puede corresponder a un 0 o a un 1. La potencia de un ordenador digital está relacionada con el número de estados (los 0 o los 1) que contiene la máquina.

No obstante, debido a las extrañas reglas del mundo subatómico, los átomos también pueden girar en cualquier combinación de ambos estados. Por ejemplo, podría haber un estado en el que la partícula gire hacia arriba el 10 por ciento del tiempo y hacia abajo el 90 por ciento, o bien que gire hacia arriba el 65 por ciento del tiempo y hacia abajo el 35 por ciento. De hecho, hay un número infinito de formas en las que un átomo puede girar. Esto aumenta extraordinariamente el número de estados posibles. Así, el átomo es capaz de transportar mucha más información, no solo en un bit, sino en un cúbit, es decir, una mezcla simultánea de los estados arriba y abajo. Los bits digitales solo pueden transportar un bit de información cada vez, lo que limita su potencia, pero los cúbits, o bits cuánticos, tienen una potencia casi ilimitada. El hecho de que, a nivel atómico, los objetos puedan existir simultáneamente en múltiples estados se denomina «superposición» (esto también significa que las leyes habituales del sentido común se violan con regularidad a nivel atómico. A esa escala, los electrones pueden estar en dos lugares al mismo tiempo, lo que no ocurre con los objetos grandes).

Además, los cúbits pueden interactuar entre sí, lo que no es posible en el caso de los bits ordinarios; es lo que se denomina «entrelazamiento». Mientras que los bits digitales tienen estados independientes, cada vez que se añade un nuevo cúbit, este interactúa con todos los cúbits anteriores, por lo que se duplica el número de interacciones posibles. Por tanto, los ordenadores cuánticos son, de forma intrínseca, exponencialmente más potentes que los digitales, porque se duplica el número de interacciones cada vez que se añade un cúbit adicional.

Por ejemplo, hoy en día los ordenadores cuánticos pueden tener más de cien cúbits. Esto significa que son 2100 veces más potentes que un superordenador con un solo cúbit.

El ordenador cuántico Sycamore, de Google, el primero en alcanzar la supremacía cuántica, es capaz de procesar setenta y dos trillones de bytes de memoria con sus cincuenta y tres cúbits. Así, un ordenador cuántico como Sycamore eclipsa a cualquier ordenador convencional.

Las implicaciones comerciales y científicas son enormes. En la transición de una economía mundial digital a una economía cuántica, hay mucho en juego.

Obstáculos para los ordenadores cuánticos

La siguiente pregunta clave es: ¿qué nos impide comercializar hoy mismo potentes ordenadores cuánticos? ¿Por qué algún emprendedor no desvela haber inventado un ordenador cuántico capaz de descifrar cualquier código conocido?

El problema al que se enfrentan los ordenadores cuánticos también fue previsto por Richard Feynman cuando propuso por primera vez el concepto. Para que estos sistemas funcionen, los átomos tienen que estar dispuestos con precisión para vibrar al unísono; es lo que se denomina «coherencia». Pero estas partículas son objetos increíblemente pequeños y sensibles. La más mínima impureza o perturbación del mundo externo puede hacer que este grupo de átomos pierda la coherencia, echando así a perder todo el cálculo. Esta fragilidad es el principal problema al que se enfrentan los ordenadores cuánticos. Así, la pregunta del billón de dólares es: ¿podemos controlar la decoherencia?

Para minimizar la contaminación procedente del mundo exterior, los científicos utilizan equipos especiales para hacer descender la temperatura hasta casi el cero absoluto, donde las vibraciones no deseadas son mínimas. Pero esto exige unas bombas y conductores especiales y muy caros.

Sin embargo, nos enfrentamos a un misterio. La madre naturaleza utiliza la mecánica cuántica a temperatura ambiente sin ningún problema. Por ejemplo, el milagro de la fotosíntesis, uno de los mecanismos más importantes que se desarrollan en la Tierra, es un proceso cuántico que tiene lugar a temperaturas normales. Para realizar la fotosíntesis, la madre naturaleza no utiliza una sala llena de exóticos aparatos que funcionan cerca del cero absoluto. Por razones que no se comprenden bien, en el mundo natural se puede mantener la coherencia incluso en un día cálido y soleado, cuando las perturbaciones del mundo exterior deberían generar el caos a nivel atómico. Si lográramos averiguar cómo la madre naturaleza hace su magia a temperatura ambiente, podríamos dominar el mundo cuántico e incluso la propia vida.

Revolucionar la economía

Aunque los ordenadores cuánticos suponen una amenaza para la ciberseguridad de las naciones a corto plazo, también tienen enormes implicaciones prácticas a largo plazo: el poder de revolucionar la economía mundial, crear un futuro más sostenible y marcar el comienzo de una era de medicina cuántica que ayude a curar enfermedades hasta ahora incurables.

Son muchas las áreas en las que los ordenadores cuánticos pueden superar a los ordenadores digitales convencionales:

1. Motores de búsqueda

En el pasado, la riqueza podía medirse en términos de petróleo u oro.

En la actualidad se mide, cada vez más, en datos. Las empresas solían desechar sus propios datos financieros, pero ahora admiten que esta información es más valiosa que los metales preciosos. Aun así, la criba de montañas de datos puede abrumar a un ordenador digital convencional. Aquí es donde entran en juego los ordenadores cuánticos, capaces de encontrar la aguja en el pajar. Estos sistemas pueden analizar las finanzas de una empresa para aislar el puñado de factores que le impiden crecer.

De hecho, JPMorgan Chase se ha asociado recientemente con IBM y Honeywell para analizar sus datos con el fin de hacer mejores predicciones del riesgo y la incertidumbre financieros y aumentar la eficiencia de sus operaciones.

2. Optimización

Una vez que los ordenadores cuánticos han utilizado motores de búsqueda para identificar los aspectos clave de los datos, la siguiente cuestión es cómo ajustarlos para maximizar determinados factores, como el beneficio. Como mínimo, las grandes empresas, universidades y organismos públicos utilizarán los ordenadores cuánticos para minimizar los gastos y maximizar su eficiencia y beneficios. Por ejemplo, el rendimiento neto de una empresa depende de centenares de factores, como salarios, ventas, gastos, etc., que cambian rápidamente con el tiempo. Un ordenador digital tradicional podría verse superado al tratar de hallar la combinación adecuada de esta miríada de factores para maximizar el margen de beneficio. En cambio, una empresa financiera podría querer utilizar ordenadores cuánticos para predecir el futuro de ciertos mercados financieros que manejan miles de millones de dólares en transacciones diarias. Aquí es donde ayudarían los ordenadores cuánticos, proporcionando la potencia computacional necesaria para optimizar su balance final.

3. Simulación

Los ordenadores cuánticos también podrían resolver ecuaciones complejas que se hallan más allá de la capacidad de los ordenadores digitales. Por ejemplo, las empresas de ingeniería podrían utilizarlos para calcular la aerodinámica de reactores, aviones y coches, con el fin de encontrar la forma ideal que reduzca la fricción, minimice los costes y maximice la eficiencia. O los gobiernos podrían utilizar ordenadores cuánticos para predecir el tiempo, desde determinar la trayectoria de un gigantesco huracán hasta calcular cómo afectará el calentamiento global a la economía y a nuestro modo de vida en las próximas décadas. O bien, los científicos podrían utilizar los ordenadores cuánticos para hallar la configuración óptima de los imanes en máquinas gigantes de fusión nuclear con el fin de aprovechar la potencia de la fusión de hidrógeno y «meter el Sol en una botella».

Pero quizá la mayor de las ventajas esté en el uso de ordenadores cuánticos para simular cientos de procesos químicos fundamentales. La situación ideal sería poder predecir el resultado de cualquier reacción química a nivel atómico sin utilizar ningún

producto en absoluto, solo ordenadores cuánticos. Esta nueva rama de la ciencia, la química computacional, determina las propiedades químicas no mediante experimentos, sino simulándolas en un ordenador cuántico, lo que podría, a la larga, eliminar la necesidad de costosos y prolongados ensayos. Toda la biología, la medicina y la química se reducirían a mecánica cuántica. Esto implica crear un «laboratorio virtual» en el que podamos probar rápidamente nuevos fármacos y tratamientos dentro de la memoria de un ordenador cuántico, evitando décadas de ensayo y error, así como lentos y tediosos experimentos de laboratorio. En lugar de realizar miles de ensayos químicos complejos, caros y pausados, bastaría con pulsar el botón de un ordenador cuántico.

4. Fusión de IA y ordenadores cuánticos

La inteligencia artificial (IA) destaca por su capacidad para aprender de los errores, a fin de realizar tareas cada vez más difíciles. Ya ha demostrado su eficacia en la industria y la medicina. Sin embargo, una de las limitaciones de la IA es que la enorme cantidad de datos que debe procesar puede sobrepasar fácilmente las posibilidades de un ordenador digital convencional. Pero la capacidad de cribar montañas de datos es uno de los puntos fuertes de los ordenadores cuánticos. Por tanto, la combinación de IA y ordenadores cuánticos puede incrementar significativamente la capacidad de estos para resolver problemas de todo tipo.