Deloitte.
University Press

Señales para estrategas

De la fantasía a la realidad♦

La computación cuántica está llegando al mercado

Por David Schatsky y Ramya Kunnath Puliyakodil

Introducción: Una nueva manera para resolver problemas computacionalmente intensivos

SE acepta, la computación cuántica es difícil de explicar. Pero eso no ha detenido que esa fantástica tecnología atraiga billones de dólares de inversión en I&D, reciba la atención de firmas de capital de riesgo, y estimule programas de investigación en compañías de alta tecnología y empresas. Algunas compañías están empezando a tomar la delantera en la aplicación de la tecnología cuántica a problemas computacionalmente intensivos en finanzas, administración del riesgo, seguridad cibernética, ciencia de materiales, energía, y logística.

Señales

- En los últimos tres años, los inversionistas de capital de riesgo han colocado $147 millones *startups* [empresas que inician] de computación cuántica; globalmente los gobiernos han proporcionado $2.2 billones en apoyo a los investigadores.[1]

- Algunas de las compañías de tecnología líderes en el mundo tienen programas activos de computación cuántica.

- Organizaciones de servicios financieros, aeroespacial y defensa, y del sector público están investigando aplicaciones de la computación cuántica.

♦ Documento original: "***From fantasy to reality.*** *Quantum computing is coming to the marketplace*", Deloitte University Press, April 26, 2017. By David Schatsky and Ramya Kunnath Puliyakodil. https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/quantum-computing-enterprise-applications.html?id=us:2sm:3tw:4dup3456:5awa:6DUPress:20170503:sfs:du_press&linkId=37161437. Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.

- El fabricante de computación cuántica D-Wave Systems anunció la disponibilidad general de su computador de la próxima generación, junto con el primer cliente para el nuevo sistema.[2]

- VC firm Andreessen Horowitz ha señalado su intención de financiar *startups* de computación cuántica.[3]

- Cuerpos emisores de estándares están buscando una transición hacia sistemas criptográficos que puedan soportar computadores cuánticos.[4]

Una forma fantástica de computación

Inspirada por las ideas de un físico carismático, la computación cuántica promete tener un impacto enorme en campos que varían desde finanzas hasta ciencias de la vida y fabricación. Tiene el potencial de crear enorme riqueza mediante hacer posible resolver algunos de los problemas computacionalmente más difíciles. Podría incluso permitir que los científicos creen tipos completamente nuevos de materia.

Los computadores cuánticos, mediante aprovechar las propiedades extrañas de las partículas sub-atómicas, serán capaces de realizar ciertos tipos de cálculos exponencialmente más rápido que los computadores más rápidos actualmente conocidos.[5] Los investigadores dicen que este poder permitirá que los computadores cuánticos rompan los sistemas de encriptado que actualmente mantienen seguras las transacciones en línea en el mundo;[6] descubrir con mayor precisión y velocidad portafolios de inversión óptimos que los modelos más sofisticados que hoy están en uso;[7] y ayudar a diseñar nuevos materiales y procesos industriales mediante predecir de manera precisa los comportamientos de las moléculas.[8]

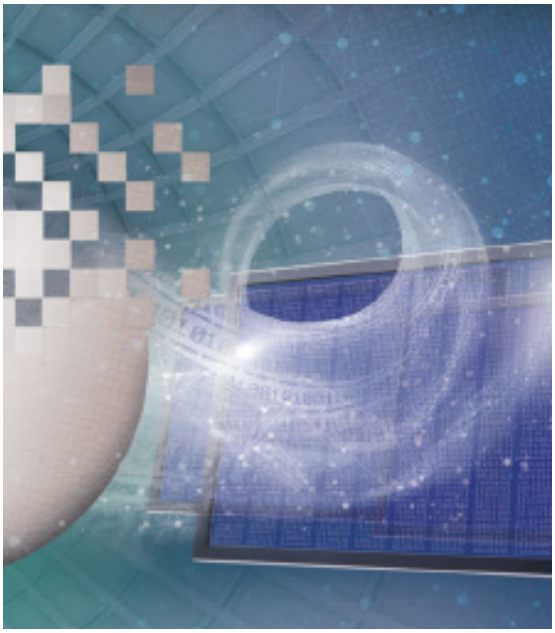
Todo esto puede parecer un sueño distante, pero dinero real está entrando ahora a la computación cuántica. El campo ha atraído $147 millones en capital de riesgo en los últimos tres años y $2.2 billones en financiación del gobierno globalmente. Y el ritmo de la inversión se está incrementando.[9] La actividad no está reducida a los laboratorios académicos de investigación y a las compañías de *startup*: un número creciente de empresas está comprometiendo recursos para explorar cómo aplicar la computación cuántica. Las apuestas parecen ser demasiado altas como para ignorar esta tecnología todavía naciente.

QUÉ TAN DIFERENTES SON LOS COMPUTADORES CUÁNTICOS

Los computadores cuánticos funcionan a partir de principios muy diferentes a los de los computadores clásicos, electrónicos. Explotan el comportamiento de las partículas sub-atómicas tal y como son descritas por la mecánica cuántica, un sub-campo de la física que explica el comportamiento complejo y extraño de las partículas – esto es, objetos más pequeños que los átomos. Por ejemplo, los electrones pueden existir al mismo tiempo en múltiples estados distintos, un fenómeno conocido como superposición. Y es imposible saber con seguridad en cualquier instante en cualquier estado un electrón pueda estar, porque el mismo acto de observar el estado lo cambia. Además, las partículas sub-atómicas pueden estar "enredadas," de manera que un cambio en una influye en otra, incluso si las dos partículas están físicamente distantes unas de otras. Para capturar esas complejidades, la mecánica cuántica describe de manera probabilística el estado de las partículas sub-atómicas usando "números complejos."[10]

Hace cerca de 30 años, el legendario físico Richard Feynman reflexionó señalando que ningún computador era suficientemente poderoso para realizar los cálculos que se necesitan para simular el comportamiento complejo de las partículas sub-atómicas. Sin embargo, esas partículas se comportan de maneras predecibles. Su comportamiento predecible podría ser visto como un tipo de cálculo, uno que fue realizado por las partículas mismas. ¿Podríamos aprovechar esas partículas, se preguntó, para realizar cálculos que vayan más allá del alcance de los computadores más rápidos conocidos?[11] (Vea el recuadro "Mucho más rápido – en teoría" para un breve relato de cómo ello ocurrió.)

Típicamente, la computación se ha acelerado cuando los ingenieros han desarrollado hardware más poderoso. Pero los algoritmos cuánticos superan a sus contrapartes clásicas no porque operen en hardware más rápido – sino a causa de las matemáticas de la mecánica cuántica que requieren menos pasos. (Vea el recuadro "Construyendo un computador cuántico.")



MUCHO MÁS RÁPIDO – EN TEORÍA

La idea del computador cuántico fue una curiosidad durante años. Luego vino la prueba teórica de que la computación basada en la mecánica cuántica podría ser más eficiente que la computación clásica. En el año 1994, un investigador de AT&T's Bell Labs que se llama Peter Shor mostró que un computador cuántico podría en teoría resolver un cierto tipo de problema – encontrar los factores primos de un entero – mucho más rápido que los métodos de la computación clásica.[12] Esto llevó a ser un resultado de enorme importancia, dado que los sistemas de encriptado usados en todo el mundo confían en el hecho de que los computadores clásicos no pueden factorizar números grandes en una cantidad práctica de tiempo. Un computador cuántico puede algún día hacer que esos sistemas de encriptado sean obsoletos.

Dos años después, otro investigador en Bell Labs, Lov Grover, probó que un computador cuántico también podría sobresalir en resolver otros tipos de problemas. El *phonebook problema* [problema del directorio telefónico] es el nombre para la tarea de encontrar algo en una lista sin clasificar – al igual que buscar alguien en el directorio telefónico por su número de teléfono más que por su nombre. En computación clásica, el algoritmo estándar es inspeccionar cada entrada hasta que se encuentre el número de teléfono correspondiente, requiriendo muchos pasos de inspección como haya entradas en el directorio telefónico. Grover demostró que un computador cuántico podría resolver este problema en mucho menos pasos – de manera específica, el número de pasos igual a la raíz cuadrada del número de entradas en el directorio telefónico. Encontrar el número telefónico buscado en una lista de un billón de entradas requeriría solo 31,623 operaciones – la raíz cuadrada de un billón – y, obviamente, una pequeña fracción de tiempo.[13]

Es cierto, probablemente no existen algoritmos cuánticos superiores para cada clase de problema computacional. De hecho, los investigadores todavía no conocen todos los tipos de problemas en los cuales la computación cuántica podría sobresalir. Pero las aplicaciones son amplias. Incluyen problemas de optimización – encontrar la mejor solución para un problema cuando numerosas soluciones sean factibles – lo cual tiene aplicaciones en muchos campos; factorización, con aplicaciones inmediatas en criptografía; simulación física; teoría del número; y topología.[14]

Los desafíos de ingeniería involucrados en la construcción de un computador cuántico son formidables. El dispositivo creado por D-Wave Systems, por ejemplo, tiene que operar en un recinto cuidadosamente aislado del ambiente exterior a una temperatura mucho más fría que el espacio interestelar.[15] Un bit cuántico típico, o qubit, es perecedero: mantiene su estado por quizás 50 microsegundos antes que surjan errores en él.[16] La diferencia en energía entre un cero y un uno es de 10^{-24} joules[17] - una de diez-trillones de veces más que un fotón de rayos X.[18]

CONSTRUYENDO UN COMPUTADOR CUÁNTICO

La prueba de la superioridad teórica de los métodos de la computación cuántica ha estimulado la investigación sobre cómo los ingenieros pueden construir un computador cuántico que funciones. Quizás sin sorpresa, es un desafío.

Tal y como nosotros sabemos, la unidad fundamental de información en un computador clásico es el bit, la forma corta para el dígito binario. El bloque de construcción análogo de un computador cuántico, que encarna las propiedades misteriosas y poderosas de las partículas sub-atómicas, es conocido como bit cuántico, o qubit. Los computadores clásicos usan carga la eléctrica para representar los bits. Y realizan los cálculos usando circuitos que implementan el álgebra Booleana (la lógica de *verdadero/falto, y/o*). Los computadores cuánticos, en contraste, toman ventaja de la mecánica cuántica más que de la conductividad eléctrica. Y para manipular esas propiedades, usan el álgebra lineal para manipular matrices de números complejos más que el álgebra Booleana para manipular bits.

Si bien la fabricación de semiconductores capaces de almacenar y manipular bits está bien establecida, elaborar qubits y puertas cuánticas es mucho un trabajo en progreso, si bien firmas tales como IBM, Google, y Microsoft están explorando[19] una variedad de métodos, incluyendo el uso de lazos de super-conducción, inones atrapados, qubits topológicos, y diamantes microscópicos.[20]

Investigadores en todo el mundo de manera regular anuncian progreso en la lucha de los desafíos de ingeniería de la computación cuántica.[21] Pero la producción masiva de la computación cuántica de manera amplia se considera está a años por delante.[22]

Las empresas están buscando aplicaciones

A pesar del estado naciente de la computación cuántica, docenas de organizaciones de los sectores público y privado ya están investigando aplicaciones de enorme valor. Las empresas de servicios financieros son especialmente activas. Por ejemplo, Barclays,[23] Goldman Sachs,[24] y otras instituciones financieras están investigando el uso potencial de la computación cuántica en áreas tales como optimización de portafolio, fijación del precio del activo, presupuestación de proyectos de capital, y seguridad de datos. En la industria aeroespacial, Airbus está explorando aplicaciones en comunicaciones y criptografía,[25] mientras que Lockheed Martin está investigando aplicaciones en verificación y validación de sistemas complejos y está acelerando el desarrollo de algoritmos de aprendizaje de máquina.[26] La US Navy está pagando por entrenamiento en computación cuántica y planea desarrollar algoritmos para problemas de optimización tales como almacenamiento de datos y recuperación de datos eficiente en términos de energía con robots sub-acuáticos autónomos,[27] y la NASA está explorando aplicaciones en comunicaciones, navegación distribuida, y diagnóstico del sistema.[28] Jugadores de la tecnología de la información tales como Alibaba,[29] Google,[30] e IBM[31] están trabajando en aplicaciones tales como criptografía resistente al hackeo, depuración de software, y aprendizaje de máquina. Las empresas de ciencias de la vida están buscando aplicaciones de computación cuántica en medicina personalizada y descubrimiento de drogas.[32]

Otras organizaciones están mirando aplicaciones en logística, química industrial, y energía, las cuales podrían ser extremadamente valiosas. Por ejemplo, los procesos estándar para fabricar fertilizantes usan entre un 2 a 5 por ciento de la producción global de gas natural cada año; la simulación cuántica podría llevar al descubrimiento de un proceso más eficiente que podría ahorrar anualmente billones de dólares y trillones de pies cúbicos de gas natural. Otra aplicación intrigante es usar computación cuántica para descubrir nuevos diseños de alta densidad que de manera dramática podrían ampliar la capacidad de las baterías usadas en todo desde electrónica portátil hasta vehículos eléctricos. Los mejoramientos en la densidad de la batería han estado operando en apenas el 5 a 8 por ciento anualmente – dolorosamente lento comparado con el ritmo exponencial de la familiar Ley de Moore.[33]

CUANDO LOS DATOS Y LAS TRANSACCIONES YA NO ESTÁN SEGUROS

Un área en la cual la computación cuántica ya está teniendo un impacto es el encriptado. Las técnicas más ampliamente usadas para encriptar y proteger transacciones dependen de la imposibilidad de encontrar rápidamente los factores primos de números grandes. Por ejemplo, a un computador clásico le llevaría 10.70 quintillones de años romper el estándar de encriptado AES de 128 bits, mientras que a un computador cuántico posiblemente rompería este tipo de encriptado en aproximadamente seis meses.[34] Esto ha llevado a la búsqueda de métodos de encriptado que serían resistentes a ataques provenientes de computadores cuánticos – hacer que los sistemas de información sean "resistentes a lo cuántico."

En el año 2015, el Information Assurance Directorate de la National Security Agency anunció que comenzaría a guiar a las agencias y a los contratistas privados que les atienden en la transición hacia algoritmos resistentes a lo cuántico. Entidades de los sectores público y privado han comenzado a hacer planes para realizar la transición hacia sistemas de encriptado – la así denominada criptografía pos-cuántica – que podría resistir a ataques de un futuro sistema de computación cuántica.[35] Las empresas ya están pensando en los riesgos para sus datos encriptados incluso antes que los ataques del encriptado cuántico se vuelvan una realidad. Están restringiendo el acceso a o eliminando por completo datos sensibles, incluso en formatos encriptados, para prevenir hostilidades provenientes de capturar esos datos codificados con la esperanza de en el futuro des-encriptarlos con computadores cuánticos.

No se trata solo del hardware

Cumplir el potencial de la computación cuántica depende más que solo de construir nuevo hardware. El nuevo software también será crucial: dado que la computación cuántica toma un enfoque completamente diferente para solucionar el problema, algoritmos completamente nuevos que tomen ventaja de este enfoque se necesitarán para logar una aceleración cuántica en el desempeño. También se requerirán nuevas herramientas de desarrollo de software. Ahora está surgiendo un ecosistema de tecnología de computación cuántica – compuesto por compañías de *startup*, firmas de tecnología establecidas, e instituciones de investigación – que tenga la intención de proveer el software que se necesita.

CRECIENTE INVERSIÓN ESTÁ RESPALDANDO UN ECOSISTEMA NACIENTE DE TECNOLOGÍA

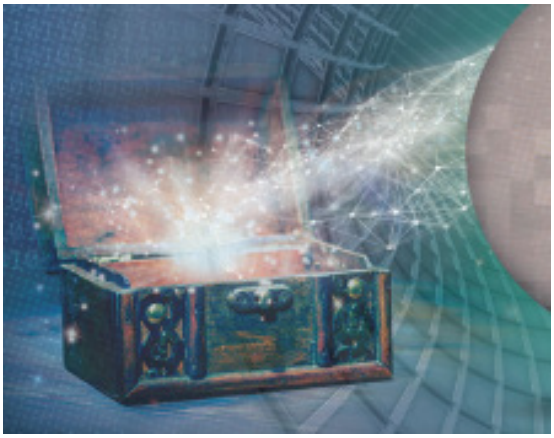
Algunos proveedores de TI establecidos tienen programas activos de investigación en computación cuántica que eventualmente lleven a productos comerciales. Ellos incluyen Google,[36] IBM,[37] Intel,[38] Hewlett Packard Enterprise,[39] Microsoft,[40] Nokia Bell Labs,[41] y Raytheon.[42] Están explorando diversas áreas, incluyendo elaboración de componentes tales como qubits y puertas cuánticas (circuitos básicos) y explorando algoritmos cuánticos, software y herramientas, y técnicas de encriptado.

Una serie de *startups*, algunas respaldadas por capital de riesgo, también han ingresado en el mercado. Además de D-Wave Systems, que está desarrollando computadores cuánticos, casi una docena de compañías está desarrollando componentes de computación cuántica o algoritmos de computación cuántica, herramientas de software, o aplicaciones.[43]

QUÉ VER

Los descubrimientos en computación cuántica están llegando rápidamente, con algunos investigadores diciendo que los desafíos han progresado desde la ciencia básica hacia la ingeniería.[44] Aun así, nadie sabe cuándo los computadores cuánticos pueden volverse ampliamente disponibles comercialmente. Para mantenerse al tanto de la computación cuántica, hay unas pocas áreas específicas que valen la pena seguir:

Ingeniería fundamental de hardware. Hay una cantidad de progreso todavía por realizar en la creación de los bloques de construcción básicos de los computadores cuánticos tales como qubits y puertas cuánticos. Un ejemplo reciente de progreso: investigadores de la University of New South Wales en Australia recientemente crearon un qubit que permanece estable 10 veces más que la tecnología previa. En asociación con el gobierno de Australia, los investigadores están trabajando para desarrollar un prototipo de chip de silicón cuántico que podría llevar a la creación de un computador cuántico práctico.[45]



Algoritmos y software cuántico. El diseño de algoritmos cuánticos requiere capacidades especializadas. Y los diseños son específicos para el tipo de computador cuántico usado. En el sistema de D-Wave, por ejemplo, las tareas computacionales tienen que ser expresadas como problemas de optimización. En la medida en que el hardware cuántico evolucione, el software escrito para computadores cuánticos también tendrá que evolucionar.[46] El nivel de actividad e innovación en herramientas de software cuántico, sistemas de operación, y algoritmos – así como también en ingeniería fundacional – ayudará a señalar el progreso hacia la computación cuántica práctica.

Supremacía de lo cuántico. Un hito simbólico a ver es el logro de la "supremacía de lo cuántico" – la creación de un computador cuántico de propósito general que puede realizar una tarea que un computador clásico no pueda hacer. Google, que ya anunció un computador cuántico de 9-quibit, ha publicado un documento que sugiere que sus investigadores consideran que un computador planeado de 50-quibit podría lograr esa meta en los próximos dos años.[47]

Implicaciones para las empresas

Si bien la corriente principal de las aplicaciones comerciales de la computación cuántica es probable estén a unos años de distancia, los ejecutivos pueden hacer una serie de cosas para preparar a sus empresas para el área de la computación cuántica.

Re-imagine las cargas de trabajo de las analíticas. Muchas compañías de manera regular operan cálculos de escala grande para administración del riesgo, pronosticación, planeación y optimización. La computación cuántica podría hacer más que acelerar esos cálculos – podría permitir que las organizaciones vuelvan a pensar cómo operan, y hacerle frente a nuevos desafíos. Los ejecutivos deben preguntarse a sí mismos, "¿Qué ocurriría si pudiéramos hacer esos cálculos un millón de veces más rápido? La respuesta podría llevar a nuevos conocimientos acerca de las operaciones y la estrategia.

Las compañías pueden ser capaces de cosechar algunos beneficios de la computación cuántica aún antes que las máquinas mismas estén comercialmente disponibles. Los investigadores de la computación cuántica han descubierto maneras mejoradas para resolver problemas usando computadores convencionales, por ejemplo. Algunos investigadores están tratando de llevar el "pensamiento cuántico" a los problemas clásicos.[48] Kyndu, una *startup* que ofrece tecnología de computación inspirada-en-lo-cuántico para inteligencia de máquina, afirma estar viendo incrementos en la velocidad computacional usando este enfoque.[49]

Actualice las arquitecturas de computación de desempeño-alto. Empresas en industrias tales como aeroespacial y defensa, petróleo y gas, ciencias de la vida, fabricación, y servicios financieros que ya han invertido en computación de desempeño alto [high-performance computing (HPC)] deben familiarizarse con

el impacto que la computación cuántica pueda tener en la arquitectura de los sistemas de HPC. Las arquitecturas híbridas que vinculen sistemas convencionales de HPC con computadores cuánticos pueden volverse comunes. D-Wabe ha descrito un híbrido HPC-cuántico para la simulación y el diseño de un sistema de distribución de agua, por ejemplo; usa computación cuántica para reducir el conjunto de opciones de diseño que necesiten ser simuladas en el sistema convencional, con el potencial para reducir de manera importante el total del tiempo computacional.[50]

Explore asociaciones académicas de I&D. Puede valer la pena considerar asignar dólares de I&D a colaboraciones con una institución académica de investigación que trabaje en esta área, tal y como lo está haciendo el Commonwealth Bank of Australia.[51] Una asociación académica de investigación podría ser una manera efectiva de lograr un inicio temprano en la construcción del conocimiento y en la exploración de las aplicaciones de la computación cuántica para su organización. Las instituciones de investigación actualmente activas en computación cuántica incluyen University of SouthernCalifornia, Delft University of Technology, University of Waterloo, University of New South Wales, University of Maryland, y Yale Quantum Institute.

Cree un plan de largo plazo de seguridad cibernética posterior a lo cuántico. No es demasiado temprano para comenzar a planear para fortificar las defensas cibernéticas contra un futuro cuántico. Un cuerpo emisor de estándares, respaldado por el gobierno de Estados Unidos, recientemente valoró la amenaza de los computadores cuánticos y aconsejó a las organizaciones desarrollar "agilidad críptica" – esto es, la capacidad para cambiar rápidamente los algoritmos por unos más nuevos, más seguros, cuando sean lanzados.[52] Las empresas necesitan prestar atención a esos desarrollos y tener en funcionamiento hojas de ruta para hacerle seguimiento a esas recomendaciones. Un riesgo es que los adversarios podrían capturar y almacenar datos hoy encriptados para su des-encriptado en el futuro, cuando los computadores cuánticos estén disponibles.[53]

EL FUTURO DE LO CUÁNTICO

En los próximos dos años la mayoría de CIOS no estarán presentando presupuestos con elementos de línea para la computación cuántica. Pero eso no significa que los líderes deban ignorar este campo. Dado que está avanzando rápidamente, y dado que su impacto es probable que sea grande, los estrategas de negocios y tecnología deben tener ahora un ojo puesto en lo cuántico. Por algún tiempo para la mayoría de las compañías no tendrán sentido inversiones de gran escala. Pero las inversiones en entrenamiento interno, asociaciones de I&D, y planeación estratégica para un mundo cuántico pueden pagar dividendos.

AUTORES

David Schatsky es director administrativo en Deloitte LLP. Le hace seguimiento y analiza las tendencias emergentes en tecnología y negocios, incluyendo el impacto creciente de las tecnologías cognitivas, para los líderes de la firma y sus clientes.

Ramya Kunnath Puliyakodil es una analista en Deloitte Services India Pvt. Ltd., siguiendo y analizando las tendencias emergentes en tecnología y negocios para líderes y clientes de Deloitte. Antes de unirse a Deloitte, trabajó para la oficina de estrategia de una firma de *Fortune* 500, manejando proyectos relacionados con el mercado de tecnologías financieras.

AGRADECIMIENTOS

Los autores desean agradecer a **Ragu Gurumurthy** y **Craig Muraskin** de Deloitte LLP y a **Yang Chu de** Deloitte Advisory LLP.

NOTAS FINALES

1 Análisis de Deloitte, basado en datos de CB Insights y boletines de prensa.

2 D-Wave Systems Inc., "D-Wave announces D-Wave 2000Q quantum computer and first system order," January 24, 2017, www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order.

3 Frank Chen, "Quantum computing: A primer," Andreessen Horowitz, June 26, 2016, http://a16z.com/2016/06/26/quantum-computing-explained/.

4 Brian Robinson, "NIST looks for defense against code-cracking quantum machines," GCN, December 22, 2016, https://gcn.com/articles/2016/12/22/nist-quantum-encryption.aspx; *In Compliance News*, "ETSI launches Quantum Safe Cryptography specification group," April 24, 2015, http://incompliancemag.com/etsi-launches-quantum-safe-cryptography-specification-group/.

5 Davide Castelvecchi, "Quantum computers ready to leap out of the lab in 2017," *Nature*, January 3, 2017, www.nature.com/news/quantum-computers-ready-to-leap-out-of-the-lab-in-2017-1.21239.

6 Nicole Kobie, "The quantum clock is ticking on encryption—and your data is under threat," *Wired*, October 4, 2016, www.wired.co.uk/article/quantum-computers-quantum-security-encryption.

7 Jack Clark and Saijel Kishan, "Quantum computers entice Wall Street vowing higher returns," *Bloomberg Technology*, December 9, 2015, www.bloomberg.com/news/articles/2015-12-09/quantum-supercomputers-entice-wall-street-vowing-higher-returns.

8 Mary-Ann Russon, "Google boasts quantum computing breakthrough with first display of real-world use," *International Business Times*, July 22, 2016, www.ibtimes.co.uk/google-boasts-quantum-computing-breakthrough-first-display-real-world-use-1571823.

9 Análisis de Deloitte a boletines de prensa, anuncios gubernamentales de financiación, y CB Insights.

10 Ben Deen, "On the road to a quantum computer," *Yale Scientific*, February 26, 2009, www.yalescientific.org/2009/02/on-the-road-to-a-quantum-computer/.

11 Andris Ambainis, "What can we do with a quantum computer?", Institute for Advanced Study, 2014, www.ias.edu/ideas/2014/ambainis-quantum-computing.

12 Jennifer Chu, "The beginning of the end for encryption schemes?", *MIT News*, March 3, 2016, http://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303.

13 Chen, "Quantum computing: A primer."

[14] National Institute of Standards and Technology, "Quantum algorithm zoo," http://math.nist.gov/quantum/zoo/, accessed April 6, 2017.

[15] D-Wave Systems Inc., "The D-Wave 2000Q™ system," www.dwavesys.com/d-wave-two-system, accessed April 6, 2017.

[16] Chris Lee, "How IBM's new five-qubit universal quantum computer works," *Ars Technica*, May 4, 2016, https://arstechnica.com/science/2016/05/how-ibms-new-five-qubit-universal-quantum-computer-works/.

[17] Ibid.

[18] Chen, "Quantum computing: A primer"; NASA, "Regions of the electromagnetic spectrum," https://imagine.gsfc.nasa.gov/science/toolbox/spectrum_chart.html, accessed April 6, 2017.

[19] Gabriel Popki, "Scientists are close to building a quantum computer that can beat a conventional one," *Science*, December 1, 2016, www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one.

[20] Benjamin Skuse, "The trouble with quantum computing," *Engineering & Technology*, November 8, 2016, https://eandt.theiet.org/content/articles/2016/11/the-trouble-with-quantum-computing/; Jacob Aron, "Quantum computing race heats up as trapped ions rival microchips," *New Scientist*, August 3, 2016, www.newscientist.com/article/2099886-quantum-computing-race-heats-up-as-trapped-ions-rival-microchips/; Popki, "Scientists are close to building a quantum computer that can beat a conventional one"; Agam Shah, "Diamonds could be building blocks for quantum computers," *PC World*, November 7, 2016, www.pcworld.com/article/3139445/hardware/diamonds-could-be-building-blocks-for-quantum-computers.html.

[21] R. Colin Johnson, "Quantum computing on cusp," *EE Times*, January 7, 2017, www.eetimes.com/document.asp?doc_id=1330680.

[22] Edwin Cartlidge, "Quantum computing: How close are we?", *Optics & Photonics News*, October 2016, www.osa-opn.org/home/articles/volume_27/october_2016/features/quantum_computing_how_close_are_we/; Timothy Prickett Morgan, "Is quantum computing set for an investment boom?", *Next Platform*, September 3, 2015, www.nextplatform.com/2015/09/03/is-quantum-computing-set-for-an-investment-boom/.

[23] Natasha Lomas, "Post-quantum encryption no longer a laughing matter," *TechCrunch*, June 22, 2015, https://techcrunch.com/2015/06/22/pq-solutions/.

[24] Zoe Thomas, "Quantum computing: Game changer or security threat?", *BBC*, April 5, 2016, www.bbc.com/news/business-35886456; Clark and Kishan, "Quantum computers entice Wall Street vowing higher returns."

[25] Airbus, "Quantum computing using the power of atoms," www.airbusgroup.com/int/en/news-media/corporate-magazine/Forum-87/quantum-computing.html, accessed April 6, 2017.

[26] Lockheed Martin, "Quantum," www.lockheedmartin.co.in/us/what-we-do/emerging/quantum.html, accessed April 6, 2017; D-Wave Systems Inc., "Customers," www.dwavesys.com/our-company/customers, accessed April 6, 2017; George Leopold, "Quantum computing center upgrades to focus on AI," *Defense Systems*, August 12, 2016, https://defensesystems.com/articles/2016/08/12/quantum-center-upgrade-lockheed-usc.aspx.

[27] Chris Jennewein, "SPAWAR testing military applications of quantum computing," *Times of San Diego*, April 25, 2016, http://timesofsandiego.com/tech/2016/04/25/spawar-testing-military-applications-of-quantum-computing/.

[28] NASA, "Quantum computing," www.nas.nasa.gov/projects/quantum.html, accessed April 6, 2017.

[29] Jack Clark, "Alibaba secures data centers with quantum research lab," *Bloomberg Technology*, July 30, 2015, www.bloomberg.com/news/articles/2015-07-30/alibaba-secures-data-centers-with-quantum-research-lab.

[30] Nick Statt, "Google is working to safeguard Chrome from quantum computers," *Verge*, July 7, 2016, www.theverge.com/2016/7/7/12120280/google-chrome-canary-quantum-computing-encryption-new-hope; Tom Simonite, "Google's quantum dream machine," *MIT Technology Review*, December 18, 2015, www.technologyreview.com/s/544421/googles-quantum-dream-machine/.

[31] Cliff Saran, "IBM develops quantum as a service," *ComputerWeekly*, May 4, 2016, www.computerweekly.com/news/450295510/IBM-develops-quantum-as-a-service.

[32] DNA SEQ alliance, "About us," www.dna-seqalliance.com/about-us, accessed April 6, 2017.

[33] Fred Lambert, "Musk: Tesla Gigafactory will produce cells with 'moderate' battery technology improvement over current products," *Electrek*, December 15, 2015, https://electrek.co/2015/12/15/musk-tesla-gigafactory-will-produce-cells-with-moderate-battery-technology-improvement-over-current-products/.

[34] Lamont Wood, "The clock is ticking for encryption," *ComputerWorld*, March 21, 2011, www.computerworld.com/article/2550008/security0/the-clock-is-ticking-for-encryption.html.

[35] Dan Goodin, "NSA preps quantum-resistant algorithms to head off crypto-apocalypse," *Ars Technica*, August 21, 2015, http://arstechnica.com/security/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/; Bruce Schneier, "NSA plans for a post-quantum world," Schneier on Security, August 21, 2015, www.schneier.com/blog/archives/2015/08/nsa_plans_for_a.html.

[36] Simonite, "Google's quantum dream machine."

[37] *Economist*, "Quantum computing," May 5, 2016, www.economist.com/news/science-and-technology/21698234-ibm-making-quantum-computer-available-anyone-play-now-try.

[38] Intel, "Intel invests US$50 million to advance quantum computing," September 3, 2015, https://newsroom.intel.com/news-releases/intel-invests-us50-million-to-advance-quantum-computing/.

[39] HP, "Areas of interest," www.hpl.hp.com/research/qip/areas.html, accessed April 6, 2017.

[40] Microsoft, "Quantum Architectures and Computation Group (QuArC)," www.microsoft.com/en-us/research/group/quantum-architectures-and-computation-group-quarc/, accessed April 6, 2017.

[41] Nokia Bell Labs, "Overcoming the physical and computational limits of conventional computing," www.bell-labs.com/our-research/disciplines/quantum-computingcommunications/, accessed April 6, 2017.

[42] Raytheon, "Quantum information," www.raytheon.com/capabilities/products/quantum/, accessed April 6, 2017.

[43] Los ejemplos incluyen Rigetti Computing, Sparrow Quantum, IonQ, Quantum Circuits Inc., Cambridge Quantum Computing, QxBranch, QC Ware, y 1Qbit.

[44] Castelvecchi, "Quantum computers ready to leap out of the lab in 2017."

[45] Michael Cruickshank, "Australian scientists make quantum computing breakthrough," *Manufacturer*, November 7, 2016, www.themanufacturer.com/articles/australian-scientists-make-quantum-computing-breakthrough/.

[46] Nicole Hemsoth, "So, you want to program quantum computers . . .," *Next Platform*, September 14, 2016, www.nextplatform.com/2016/09/14/want-program-quantum-computers/.

[47] Jacob Aron, "Revealed: Google's plan for quantum computer supremacy," *New Scientist*, August 31, 2016, www.newscientist.com/article/mg23130894-000-revealed-googles-plan-for-quantum-computer-supremacy/.

[48] Natalie Wolchover, "Classical computing embraces quantum ideas," *Quanta Magazine*, December 18, 2012, www.quantamagazine.org/20121218-classical-computing-embraces-quantum-ideas/.

[49] Arun Majumdar, "Quantum inspired computing: QuIC," LinkedIn Pulse, April 29, 2015, www.linkedin.com/pulse/quantum-inspired-computing-quic-arun-majumdar.

[50] D-Wave Systems Inc., "Applications," www.dwavesys.com/quantum-computing/applications, accessed April 6, 2017.

[51] Rohan Pearce, "Behind the Commonwealth Bank's investment in quantum computing," *ComputerWorld*, June 2, 2016, www.computerworld.com.au/article/600879/behind-commonwealth-bank-investment-quantum-computing/.

[52] Lily Chen et al., *Report on post-quantum cryptography*, National Institute of Standards and Technology, April 2016, http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf, p. 7.

[53] Tina Amirtha, "Everyday quantum computing is years off—so why are some firms already doing quantum encryption?", ZDNet, June 2, 2016, www.zdnet.com/article/everyday-quantum-computing-is-years-off-so-why-are-some-firms-already-doing-quantum-encryption/.

Deloitte. University Press

Siga @DU_Press

Inscríbase en DUPress.com para las actualizaciones de Deloitte University Press.

Acerca de Deloitte University Press
Deloitte University Press publica artículos originales, reportes y publicaciones periódicas que proporcionan conocimientos para los negocios, el sector público y ONG. Nuestra meta es aprovechar la investigación y la experiencia de nuestra organización de servicios profesionales, y la de co-autores en la academia y negocios, para avanzar la conversación sobre el espectro amplio de temas de interés para ejecutivos y líderes del gobierno.

Deloitte University Press es una huella de Deloitte Development LLC.