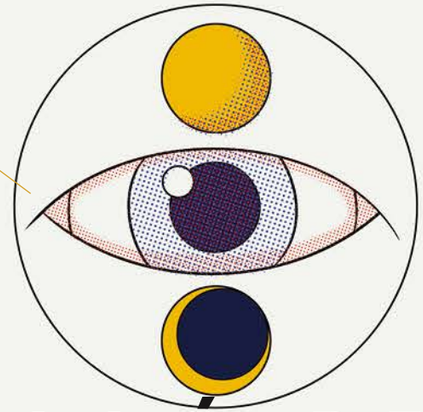
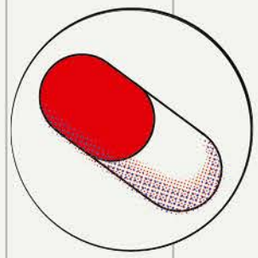
Palabras clave: computación cuántica, revolución industrial, qubits, ciberseguridad, soberanía nacional





Cerebros, soberanía nacional e Isaac Asimov

MÁS ALLÁ DE LOS QUBITS

La computación cuántica está en casi todos los medios hoy en día. Todos hablan de qué es un *qubit* y por qué trabajamos en esta revolución. ¿Qué implicaciones tiene? ¿Por qué los principales países y empresas están invirtiendo grandes cantidades de dinero en hacer realidad esta tecnología? ¿Qué problemas va a resolver? Y, sobre todo, ¿qué nuevos problemas va a crear?

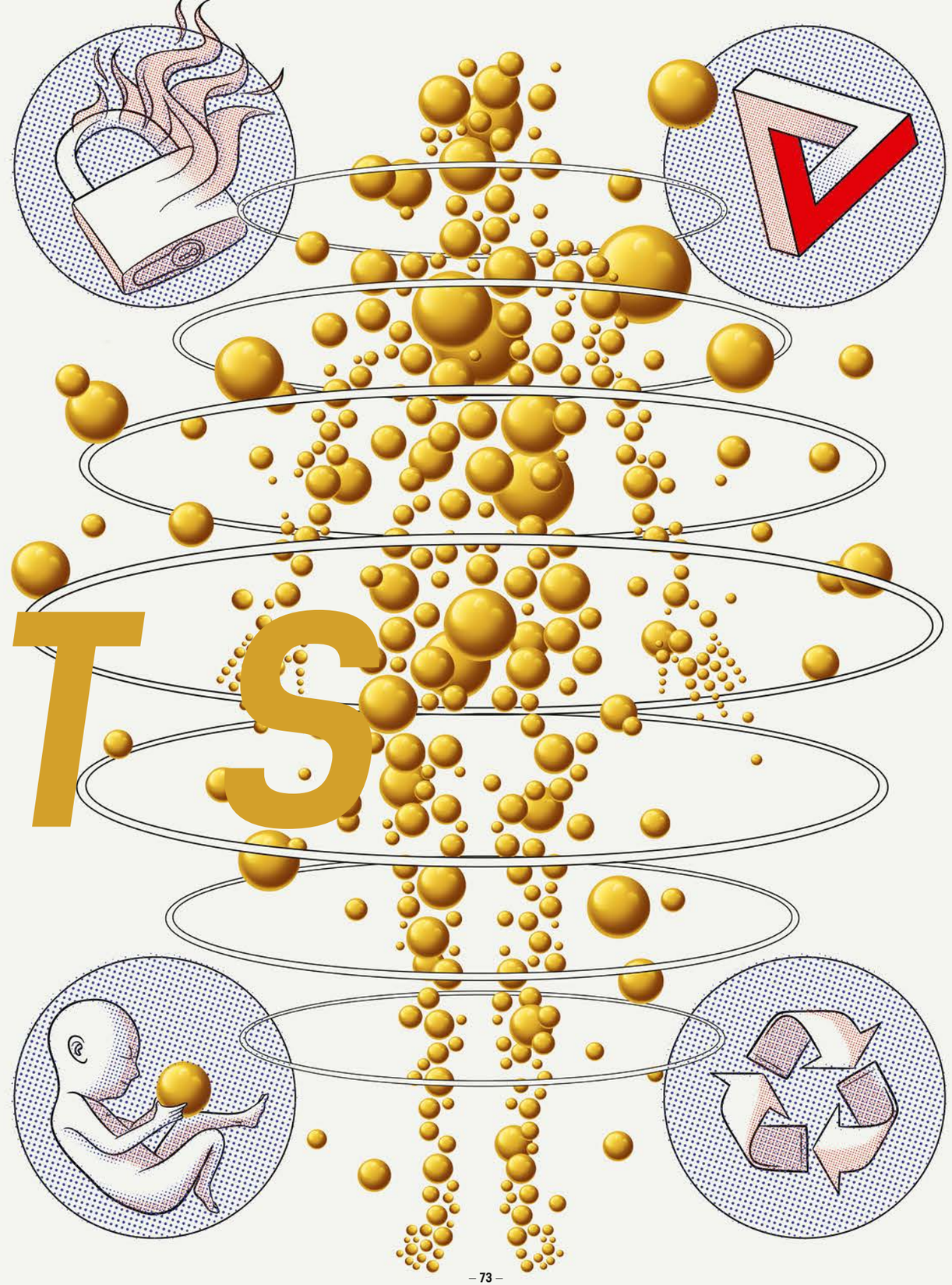
SERGIO GAGO

Brains, national sovereignty and Isaac Asimov

BEYOND QUBITS

Quantum computing is in almost every media today. Everyone is talking about what a qubit is and why we are working on this revolution. What are its implications? Why are major countries and companies investing huge amounts of money in making this technology a reality? What problems will it solve? And, above all, what new problems will it create?

Keywords: *quantum computing, industrial revolution, qubits, cyber security, national sovereignty.*



En las novelas de la Fundación de Isaac Asimov, el matemático Hari Seldon desarrollaba una ciencia llamada psicohistoria con la cual podía predecir el futuro de grandes masas de población. En función de unos parámetros, hechos y evoluciones, Hari podía establecer la probabilidad de que un futuro determinado ocurriera o no. Y de esta manera inicia su trilogía: con la predicción del derrumbe del imperio galáctico.

Claramente Hari Seldon debía tener acceso a una capacidad computacional increíble. La cantidad de datos necesaria para hacer dichas inferencias (y la matemática para hacerlo relevante) tendría que ser tan grande que ningún ordenador con el que soñamos hoy podría ni siquiera rascar la superficie del problema.

Y de hecho no tenemos que ir demasiado lejos. Cualquier banco de nuestro barrio que nos vende hipotecas o nos da préstamos tiene un problema similar de predicción del futuro (aunque mucho más pequeño). Las entidades de crédito necesitan tener un control muy exhaustivo de cuánto dinero prestan y asumir que habrá un porcentaje de personas que no será capaz de pagar sus plazos. No es de extrañar, entonces, que los bancos se esfuercen por calcular —aunque sea aproximadamente— cuántas personas dejarán de poder pagar la hipoteca, cualquiera que sea la razón por la que esto ocurra.

Esto es por lo que dicen que nunca te darán un préstamo hipotecario por más del 80 % del valor de tasación, o que exigen tus nóminas y contrato fijo u otro tipo de avales. La estadística dice que un contrato fijo tiene menos posibilidades de perder pagos y, por tanto, el banco ganará pingües beneficios con ese producto hipotecario sin casi riesgo.

Al igual que ocurría con el *overbooking* en los aviones, que consideraba que siempre habría un pasajero perdiendo el avión, y por tanto se podían vender más billetes que asientos, este cálculo es peligroso debido a que se basa en la probabilidad. El banco tiene que asumir un riesgo y unas probabilidades de perder dinero, y de guardar una cierta cantidad en reserva para no entrar en quiebra (os podéis imaginar lo que pasaría si nadie pagara sus préstamos durante un mes). El cálculo no debería ser difícil. Si sabemos que una familia de cada 100 deja de pagar su hipoteca, es tan fácil como guardarnos ese dinero en la caja de caudales y listo, ¿no?

Imagina ahora que el banco tiene que hacer el cálculo con 10.000 hipotecas firmadas durante una semana. ¿Cómo podemos calcular cuántas familias, de media, dejarán de pagar su préstamo para poder contar con ese problema? (*spoiler*: en 2008 lo calculamos MUY MAL. Hoy, quizá un poquito mejor). Y es que el problema de calcular estas probabilidades es terriblemente complicado. Tan complicado que solo podemos estimarlo burdamente a base de tirar los dados muchas, muchísimas veces (lo que llamamos análisis de Montecarlo) y que consiste en preguntarnos millones de veces: ¿Y si esta familia quiebra, o si esta otra lo hace? ¿Y si hay una crisis financiera, o bien si la empresa que emplea a 20.000 personas en esta ciudad cierra?

Estos procesos son muy largos y costosos, pueden durar días, y los bancos, *hedge funds*, aseguradoras y otros agentes en el entorno financiero los usan continuamente. De hecho, hay un trabajo específico que se dedica a esto: analista cuantitativo. Uno de los puestos más demandados y mejor pagados de Wall Street.

La razón por la que estos problemas son tan difíciles de resolver es porque su complejidad aumenta con su tamaño. Cuantas más hipotecas vende el banco, más difícil es su simulación. Un sudoku de 10x10 es fácil de resolver para cualquier ordenador — o para un humano a mano—, pero la dificultad de 15x15, o 20x20 no es lineal, sino exponencial. Es decir, el tiempo necesario para que un ordenador resuelva el problema aumenta más rápido que el propio tamaño del problema en sí mismo. Por tanto, nos encontramos con un techo invisible que incluso con nuestra ley de Moore a punto de caducar —donde podíamos meter el doble de transistores cada dos años en el mismo chip—, hace imposible calcular este tipo de problemas.

Calcular hipotecas o seguros, o resolver sudokus está muy bien, pero no son problemas tan generales como para poner el mundo patas arriba. Por suerte o por desgracia este tipo de problemas —que para los entendidos, llamaremos Clase NP— están en todas partes, en cualquier industria, en nuestro día a día. ¿Necesitas crear una vacuna para un nuevo virus? Ahí tienes problemas NP. ¿Estás buscando optimizar la eficiencia de un nuevo combustible? Problemas NP. ¿Quieres optimizar la captación de las células de los paneles solares? Problemas NP. ¿Quieres saber la ruta óptima para entregar paquetes lo más rápido posible en un barrio? Lo has adivinado, problema NP.

Pero esto no acaba aquí, y se puede poner un poco más tétrico ¿Quieres romper la encriptación de Internet y descifrar cualquier transacción bancaria o mensaje? ¿Quieres desarrollar un nuevo gas nervioso? ¿Te interesa aumentar la potencia de un explosivo? ¿Quizá desarrollar sistemas de escucha y contraespionajes inquebrantables? Todos estos son (o contienen) también problemas que actualmente los ordenadores no pueden atacar fácilmente, pero los *qubits*[1] sí podrán. Por tanto, la computación cuántica no es únicamente relevante para que las empresas puedan conseguir o mantener ventaja competitiva en sus mercados, sino para que las grandes potencias puedan mantener o incrementar su soberanía nacional, información y capacidad de negociación.

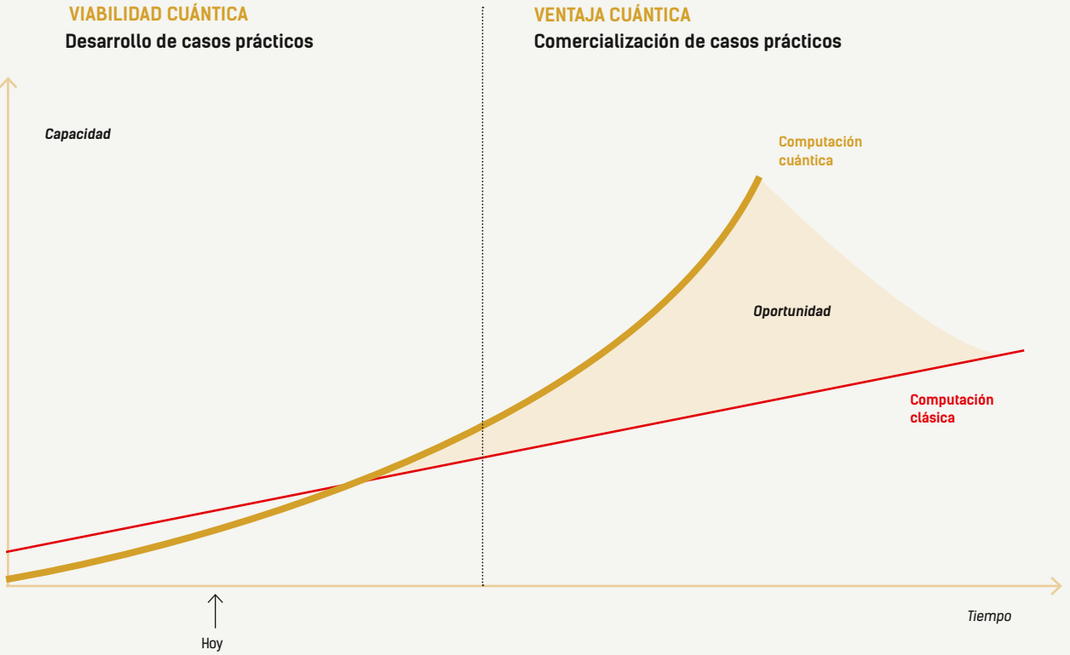
La computación cuántica es relevante para que grandes potencias puedan mantener o incrementar su soberanía nacional

No en vano, son algunos los que opinan que si algún país hubiera encontrado ya la ventaja cuántica como para desencriptar Internet (que necesita del orden de varios millones de *qubits*,

1 Fundeu recomienda el uso de cúbit en vez del inglés *qubit*. No obstante, al estar extendido el uso de *qubit*, hemos preferido mantener el criterio de cada autor/a.

¿ENTONCES CUÁL ES LA VENTAJA CUÁNTICA?

Fuente: IBM



y llevamos solo 127 en el momento de escribir esto), realmente los ciudadanos de a pie no lo sabríamos. Hay precedentes: Alan Turing descifró desde Bletchley Park la máquina de encriptación *Enigma* de los alemanes durante la Segunda Guerra Mundial, pero el mundo no lo supo hasta varios años después.

La comunidad científica considera esta opción (incluso China, con su hegemonía y billones invertidos en el sector) poco plausible. El desarrollo científico en estas áreas está más compartido de lo que pensamos y China ha publicado muchos de sus descubrimientos e hitos (Pan Jianwei y su equipo en la Universidad de Ciencia y Tecnología de China ya demostraron ventaja cuántica en un problema muy concreto que, si bien no tiene utilidad práctica, demuestra que vamos por el buen camino).

Si esto no es suficiente problema, la tendencia actual consiste en "Hack now, decrypt later", es decir: consigamos los datos encriptados hoy, que sabemos que mañana los podremos leer con los ordenadores cuánticos. Seguro que hay secretos de Estado o comunicaciones que aún serán relevantes en diez o quince años.

Realmente es un concepto difuso, pero viene a señalar el punto de inflexión en el futuro en el que un ordenador cuántico resolverá un problema real (aplicable) mejor que cualquier ordenador (o superordenador) clásico. Esto es una auténtica carrera de fondo.

En el momento que un algoritmo cuántico promete mejores velocidades (mejoras exponenciales en su cálculo), rápidamente los desarrolladores de algoritmos clásicos se ponen las pilas para demostrar que ellos siguen siendo primeros con pura ingenuidad humana, y así nos vamos presionando los unos a los otros.

Sin embargo, esta es la definición puramente científica, el "exponencial *speedup*", pero no tiene que ser la única. Los ordenadores cuánticos nos traen otro tipo de ventajas a nivel de eficiencia o sostenibilidad. Algunos cálculos requieren una huella de carbono mucho menor procesados en *qubit*s que en cientos de operaciones en supercomputadoras normalmente operadas con minicentrales eléctricas para darles soporte. Otros cálculos pueden preferir resultados en tiempo real en lugar de tardar días a cambio de una pequeña pérdida en precisión. Estas dimensiones, puramente empresariales, son también muy relevantes a la hora de plantear potenciales ventajas cuánticas.

Es cierto que a día de hoy ejecutar algoritmos en alguno de los más de 50 ordenadores cuánticos y simuladores disponibles en el mundo es caro. Requiere personas preparadas que sepan utilizar y adaptar los problemas (no muy distintos de las supercomputadoras). Pero las economías de escala y la facilidad de resolver problemas harán que este tipo de ejecuciones sean más sostenibles y baratas en el futuro.

En este sentido, la computación cuántica puede servir para que la humanidad dé un salto de gigante en su evolución, pero también para generar más desigualdad. Muchos desarrollos tecnológicos del pasado no hicieron más que aumentar la brecha entre países en desarrollo y las grandes potencias, o entre grandes fortunas y el resto del mundo. Tenemos que ser muy cuidadosos para aprender de nuestros errores y no repetir la historia. No solo a nivel empresarial, sino también geopolítico. No en vano son ya muchas las voces que hablan de trabajar la ética para la computación cuántica desde ya, antes de que la tecnología sea de uso general y no encontrarnos los problemas que tenemos hoy con la inteligencia artificial.

¿Nos encontramos al borde de una transformación tecnológica sin precedentes? Sin ninguna duda. La computación cuántica representa un avance como fue la arquitectura de Von Neumann a los ordenadores "clásicos" que usamos hoy. Cuando Bank of America presentó su primer ordenador en 1955 para procesamiento, las grandes mentes pensaban que habría sitio para unas pocas computadoras en el mundo, pero las empresas vieron que habría un antes y un después (y poco se imaginaban que hoy tendríamos computadoras ultrapotentes en nuestros bolsillos en forma de *smartphones*).

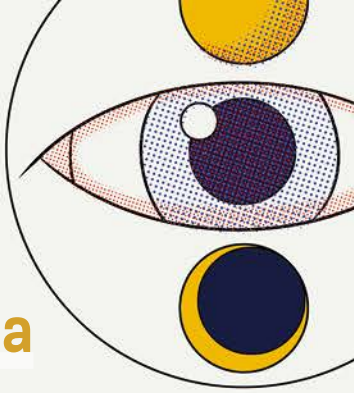
Ley de Moore

En la actualidad, hasta los enchufes obedecen a la ley de Moore y tienen circuitos integrados inteligentes dentro. De la misma manera que los ordenadores tardaron varias décadas en imponerse y transformar nuestra sociedad, la cuántica requerirá de varias décadas para encontrar su sitio correcto en el mundo y transformar la realidad tal y como la conocemos.

De la misma manera que nos ocurrió con las computadoras, los problemas ya estaban ahí. En los años 20, una computadora era una persona que se dedicaba a hacer aritmética manualmente y, por tanto, escalar para realizar millones de cálculos al día no era viable. Los problemas que resuelven los ordenadores cuánticos están ahí. Simplemente hasta ahora no teníamos la capacidad de atacarlos en condiciones. ¿Dónde nos encontramos? Más o menos una década después del ENIAC. Si alguien recuerda los Amstrad o los Spectrum que funcionaban con cintas de casete… bueno, todavía ni siquiera estamos ahí. Esto significa que en el sector hay más *hype* que realidad, que aunque necesitamos avanzar rápido, muy rápido, todavía falta mucho desarrollo. Que no os vendan la moto.

¿Qué necesitamos para avanzar? Pues exactamente lo mismo que la

En cuántica, nos encontramos más o menos una década después del ENIAC, el primer ordenador del mercado



La computación cuántica puede servir para que la humanidad dé un salto de gigante en su evolución, pero también para generar más desigualdad

computación tradicional en los años 60 (y es que la historia se repite). Y curiosamente lo mismo en la inteligencia artificial en los 90: *hardware* y cerebros.

Por un lado, necesitamos un "volumen cuántico" mayor. Esto es, no solo más *qubits* donde codificar nuestros problemas, sino *qubits* de calidad. Digamos que los que tenemos hoy son bastante ruidosos y generan excesivos errores. Y como tenemos pocos *qubits,* tampoco podemos hacer códigos de corrección de errores como los que usamos en el mundo clásico (para los entendidos, los códigos Hamming son prácticamente imposibles por el mero hecho de que observar un estado cuántico destruye el estado en sí mismo lo cual afecta, entre otras cosas, a la dificultad para tener una memoria RAM en el sistema). Pero no sufran, decenas de empresas, grandes y pequeñas, así como países (incluida la humilde aportación por parte de España) están trabajando duramente en ello. Mientras tanto, tenemos que crear un *stack* completo de abajo arriba. Desde el control de los *qubits*, lenguajes de programación, algoritmos y aplicaciones. Y para esto hacen falta cerebros.

De la misma manera que nos faltaban "informáticos" en los 70 y 80 (y hoy en día), nos faltan "informáticos cuánticos" que entiendan de dominio, de mecánica cuántica y, sobre todo, de desarrollo y despliegue de soluciones. La forma de pensar en algoritmos cuánticos es muy distinta a cómo pensamos en algoritmos clásicos. Es otro paradigma. Sin embargo, esto no implica que podamos dejar el pasado de lado. Nuestra revolución será híbrida o no lo será y es que ya no empezamos de cero: ya tenemos la computación en la nube, todas las plataformas y *frameworks* de *Machine Learning*, materiales, herramientas y *datasets* que hemos desarrollado hasta ahora. La investigación converge y es más accesible que nunca. Un estudiante de instituto puede convertirse en experto en cuántica únicamente con una buena conexión a Internet. No es de extrañar que accedamos a casi todos los ordenadores cuánticos en el mercado a través de la nube usando las mismas herramientas que los científicos de datos usan cada día en su trabajo.

Vaya, que tenemos entre manos una auténtica revolución tecnológica comparable a la bombilla y la vela. Nos faltan manos y *qubits* pero sabemos que llegarán tarde o temprano, y tanto empresas como gobiernos están dando pasos de gigante para poder estar ahí. No se trata únicamente de "optimizar problemas" sino de encontrar soluciones a grandes problemas de la humanidad. Tanto en economía, sostenibilidad, medicina y comunicaciones. Es el momento de empezar a pensar en cuántica. No en "bras" y "kets", operadores y observables, hamiltonianos y fotones, sino en las distintas capas que tenemos que crear. Programadores, matemáticos, físicos, empresarios, todos trabajando en conjunto para hacer realidad este sueño que nos hará avanzar como especie.

No sé si desarrollaremos una psicohistoria como Hari Seldon, o si los *qubits* nos servirán para simular la naturaleza como decía Richard Feynman. Lo que sí tengo claro es que desarrollaremos vacunas mucho más rápido, analizaremos mejor los riesgos, nos comunicaremos de forma más segura y, ¿por qué no?, resolveremos sudokus gigantes en milisegundos.

Bibliografía

Aaronson, S. (2013): *Quantum Computing since Democritus*. Cambridge, Cambridge University Press.

Coecke, B. y **Kissinger, A.** (2017): *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge, Cambridge University Press.

Gimeno-Segovia, M., Harrigan, N. y **Johnston, E.** (2019): *Programming Quantum Computers: Essential Algorithms and Code Samples*. Sebastopol (California), O'Reilly Media.

Nielsen, M. A. y **Chuang, I. L.** (2000): *Quantum Computation and Quantum Information*. Cambridge, Cambridge University Press.

Wittek, P. (2014): *Quantum Machine Learning What Quantum Computing Means to Data Mining*. Cambridge, Academic Press.