La carrera hacia un futuro cuántico

La computación cuántica abre el camino a la posibilidad de ejecutar cálculos masivos y en paralelo con una potencia a la que la computación clásica nunca llegaría, especialmente valiosa para problemas de optimización y simulación, íntimamente ligados al ámbito de las finanzas cuantitativas.

Borja Foncillas @borja_foncillas | *Consejero delegado de Afi y socio director del área de Soluciones Digitales*
María del Mar Ruiz | *Consultora del área de Soluciones Digitales de Afi*

Siendo realistas, explicar la base de la computación cuántica en un artículo de esta extensión está más allá de las capacidades de los autores del artículo. Baste indicar que un cúbit (qubit en inglés), es la unidad mínima de información sobre la que trabaja un computador cuántico, y que las propiedades de superposición y entrelazamiento permiten que, dada una cantidad n de cubits, se puedan evaluar de forma simultánea 2^n «posibilidades». Puesto en números, de forma ilustrativa y grosera, una computadora cuántica de 53 cubits (como la empleada por Google en su artículo publicado en Nature el pasado mes de octubre) sería «equivalente» a una computadora clásica empleando 2^{53} bits (9.007.199.254.740.990 bits).

Sea como fuere, y matices y detalles cuánticos aparte, la **computación cuántica abre el camino a la posibilidad de ejecutar cálculos masivos y en paralelo con una potencia a la que la computación clásica** y la ley de Moore nunca llegarían. La capacidad de evaluar simultáneamente todas las posibles combinaciones de los cubits de la computadora es especialmente valiosa para problemas de optimización y simulación, problemas íntimamente ligados al ámbito de las finanzas cuantitativas.

Hasta el momento, todo intento de desarrollar computadores cuánticos se ha movido en el plano de lo experimental, siendo su exponente más destacado el ejercicio realizado por Google, comentado anteriormente, en el que se consiguió crear una red de 53 cubits entrelazados en una red bidimensional, contenida en procesador cuántico al que llamaron «Sycamore». La novedad en este caso es el hecho de que, por primera vez, un equipo de investigadores afirma que ha puesto en la práctica una demostración de la conocida como «supremacía cuántica», en la que un ordenador cuántico es capaz de resolver un problema irresoluble con computación clásica. Según Google los 200 segundos de procesamiento que fueron necesarios para resolver el problema, habrían requerido 10.000 años en el mejor superordenador clásico existente en la actualidad. Sin embargo, su principal competidor, IBM, publicó de forma casi consecutiva un artículo explicando que el *benchmark* utilizado por Google para realizar la comparativa entre su procesador y uno clásico es muy ineficiente, y redujeron la expectativa de 10.000 años a 2,5 días «con mucha mayor fidelidad [que la lograda por Google]». En todo caso, parece que ambos competidores están de acuerdo en tres puntos importantes: 1) que el avance tecnológico publicado por Google «es impresionante», 2) que la expectativa de crecimiento exponencial de la capacidad de cómputo de esta tecnología es realista y 3) que el campo de la computación cuántica se encuentra en un momento de continuo empuje hacia adelante.

La **construcción real de un ordenador cuántico presenta notables dificultades por la naturaleza de los cubits, que son hipersensibles a cualquier tipo de interferencia**. Para garantizar esta independencia de interferencias, se está tratando de blindarlos electromagnéticamente y mantenerlos en temperaturas de casi cero absoluto. Actualmente son pocos los que han conseguido construir computadores cuánticos en entornos de laboratorio. Además de los anteriormente mencionados, Alibaba y Microsoft declaran haber construido ordenadores de laboratorio, aunque siempre de capacidad reducida (un máximo de 72 cubits). La incapacidad de construir ordenadores reales de mayor tamaño queda determinada por limitaciones físicas: al aumentar el número de cubits es más fácil que el exterior interfiera en su estado y no se pueda alcanzar el estado de superposición. Para paliar estos problemas se están tratando de utilizar algoritmos de corrección de errores que subsanen estos efectos. Sin embargo, la aplicación de estos métodos supone un tiempo adicional de cómputo, que minimiza notablemente las ventajas del uso de estos métodos frente a la computación tradicional.

De forma añadida a las dificultades técnicas, la creación de algoritmos cuánticos difiere mucho de la creación de algoritmos tradicionales. Por hacer un símil simplificado, un algoritmo cuántico ha de prepararse para evaluar de forma simultánea una cantidad ingente de posibilidades, mientras que los algoritmos clásicos se basan en la ejecución ordenada (y repetida de un conjunto de instrucciones). Las puertas lógicas empleadas en computación cuántica son muy diferentes de las puertas lógicas clásicas y el nivel de capacitación (y de inteligencia) requerido para trabajar en este ámbito es claramente superior. **Muy pocos programadores clásicos serían capaces hoy de trabajar en programación cuántica**. Para paliar esta carencia, grandes jugadores, como Microsoft, ya han puesto a disposición de posibles creadores de software versiones simuladas de ordenadores cuánticos, sobre las que probar nuevos modelos y algoritmos de programación.

Es muy difícil predecir cuándo dispondremos de los primeros ordenadores cuánticos reales (aún hay parte de la comunidad científica que duda de que en algún momento se alcance la anteriormente descrita «supremacía cuántica»). En todo caso, llegado ese momento, y disponiendo de algoritmia cuántica equivalente a la actual, el escenario financiero cambiaría radicalmente. Disponer de esta tecnología por parte de una parte minoritaria de la industria, les daría una ventaja descomunal con respecto al resto de la industria: sería como si hoy en día unos pocos jugadores pudieran simular y valorar empleando ordenadores, mientras el resto de jugadores estuvieran haciendo cálculos con el ábaco. Este problema, en todo caso, sería menor, porque la ventaja se produciría en todos los órdenes, incluyendo los de seguridad y criptografía. Por eso, en la computación cuántica no sólo está en juego la mejora de la capacidad de cómputo, sino un profundo desequilibrio de las fuerzas y poderes actualmente existentes ::