Este artículo es parte del libro
"El poder de las conexiones. Una historia de innovación".
Todos los derechos reservados.
Telefónica Innovación Digital

Comunicación cuántica y las redes del futuro

Juan Ignacio Cirac
Director del Instituto Max-Planck de Óptica Cuántica (Alemania), vicepresidente del Consejo Asesor de Telefónica Tech y antiguo vocal del Consejo de Administración de Telefónica.

"Las superposiciones cuánticas y el teletransporte nos abren un mundo de posibilidades en comunicación"

«¿Dónde está la Luna cuando no la miramos?» Esta famosa frase de Albert Einstein expresa su desconcierto causado por las extrañas predicciones de la física cuántica, una teoría que estaban desarrollando él y otros físicos a principios del siglo pasado. Esa teoría nos dice que, al menos en el mundo microscópico, las propiedades físicas se difuminan y solo quedan definidas cuando observamos. Esto ocurre con propiedades como la velocidad, la posición o la energía, y así es imposible saber dónde está y cómo se mueve un átomo o un electrón cuando no lo miramos. Desde su descubrimiento, las leyes de la física cuántica han dado lugar a un mar de paradojas y situaciones que desafían nuestra intuición y que perviven hoy en día. Pues bien, con toda seguridad, Einstein se quedaría todavía más sorprendido si, como esperamos, el funcionamiento de las telecomunicaciones del futuro se base en los

fenómenos más exóticos de esa teoría, constituyendo lo que hoy denominamos «comunicaciones cuánticas». Desde hace años, Telefónica lidera la investigación y desarrollo de redes de comunicación cuántica y se prepara para ponerlas al servicio de sus clientes en cuanto sean demandadas.

Comparada con las telecomunicaciones actuales, la cuántica ofrece más seguridad y eficiencia, así como nuevos usos de las redes. En efecto, los fenómenos extraordinarios que aparecen en el mundo microscópico permiten operar las redes de una manera muy distinta a cómo se hace hoy en día. Para comprender esto, revisemos primero la forma en la que, tradicionalmente, hemos enviado información por nuestras redes.

Lo primero, traducimos los mensajes a lenguaje binario; esto es, transformamos las palabras, los números o cualquier símbolo, a un conjunto de ceros y unos, que llamamos bits. Esos bits son los que se transmiten por las redes y, una vez en su destino, se vuelven a traducir al mensaje original. Para mejorar la eficiencia de nuestras redes, podemos utilizar nuevas formas de enviar los bits. Por ejemplo, hace tiempo se enviaban a través de señales eléctricas, algo que es relativamente lento y costoso. El advenimiento de la fibra óptica y de redes inalámbricas nos permite aumentar la velocidad, la capacidad de las redes, así como disminuir el gasto energético al sustituir las señales eléctricas por ópticas. Eso se debe a que la luz viaja más rápido que la electricidad, puede acomodar más bits, y tiene muy pocas pérdidas. También podemos mejorar las comunicaciones haciendo una traducción más eficiente de la información a bits, codificando mejor las señales ópticas, o utilizando el progreso vertiginoso de las tecnologías láser, de los emisores y receptores de radiofrecuencias y de las fibras ópticas. Además, para proteger la información, podemos encriptarla, de tal forma que cualquiera que la intercepte, no pueda leerla. Todos estos avances, con Telefónica a la cabeza, han revolucionado la forma en la que nos comunicamos y están dando lugar a la era digital, lo que supone una de las mayores transformaciones que ha vivido la humanidad.

Los avances tecnológicos nos permiten mejorar la eficiencia y las prestaciones de nuestras redes continuamente. La tecnología inalámbrica 5G ya está implantada, aumentando la velocidad en la transmisión de datos, y en unos años será sustituida por la 6G, que abrirá nuevas prestaciones. Las fibras pueden acomodar cada vez más datos, mejoramos la latencia a través del *edge computing* (computación periférica), y las redes están pasando a ser

Espacio del Technology & Automation Lab, el laboratorio donde Telefónica investiga el potencial de las comunicaciones cuánticas.

Este artículo es parte del libro
"El poder de las conexiones. Una historia de innovación".
Todos los derechos reservados.
Telefónica Innovación Digital

inteligentes, explotando la inteligencia artificial. Existe, sin embargo, otra forma completamente distinta de mejorar algunos aspectos de nuestras redes que no se basa ni en optimizar la forma en la que traducimos la información a bits, ni las señales que transmitimos por las redes. Es un cambio mucho más dramático, ya que implica el uso de otras leyes de la naturaleza: las de la física cuántica. Los mensajes y la información ya no se traducen a bits, sino a bits cuánticos, normalmente llamados cúbits (*qubits*). Estos no solo pueden tomar los valores 0 y 1, sino que explotan el llamado principio de superposición cuántica. De acuerdo con ese principio, una propiedad de un objeto microscópico puede tomar, simultáneamente, dos o más valores, siempre y cuando esté adecuadamente aislado. Por ejemplo, la luz está formada por fotones, que poseen una propiedad llamada polarización, que puede tomar el valor 0 (vertical), 1 (horizontal), pero también puede tomar los dos valores a la vez, en cuyo caso decimos que está en un estado de superposición cuántica. Mientras esté aislado y no lo observemos, el fotón no tiene definida esa propiedad y solo cuando medimos la polarización, esta queda definida como 0 o 1. El resultado es completamente aleatorio y, por tanto, antes de medir no tenemos ninguna certeza de cuál será el resultado. Esta es la incertidumbre a la que se refería Heisenberg en sus investigaciones pioneras del siglo pasado, la misma que causaba malestar a Einstein cuando hablaba de la posición de la Luna, y también la que le llevó a afirmar que no creía que la naturaleza fuera así, ya que «Dios no juega a los dados».

Las superposiciones pueden también dar lugar a la teletransportación cuántica. Este fenómeno está conectado con la existencia de unas superposiciones muy especiales que ocurren cuando tenemos dos o más objetos microscópicos. Si tenemos dos fotones, es posible tener sus polarizaciones verticales (00), horizontales (11) y una vertical y otra horizontal (01 o 10). De acuerdo con el principio de superposición, es posible tener, por ejemplo 00 y 11 a la vez, en cuyo caso decimos que tenemos un estado entrelazado de los fotones. Lo curioso en este caso es que, si medimos la polarización del primer fotón, no solo su polarización quedará automáticamente definida, sino también la del segundo, a pesar de que no lo hayamos observado. Esto es, si la del primero

Desde hace tiempo Telefónica aprovecha su extenso despliegue de fibra óptica y su liderazgo en I+D+i para probar y mejorar distintos protocolos de distribución de claves cuánticas y, a la vez, desarrolla la tecnología necesaria para transformar sus redes de fibra óptica en redes de comunicación cuántica.

queda definida en 0, la del segundo también quedará en 0 (y si queda en 1, la del segundo también quedara en 1), pues en la superposición solo están contempladas estas posibilidades. En resumidas cuentas, midiendo un fotón, afectamos el estado del segundo y esto ocurre independientemente de dónde se encuentre. Uno podría estar en Barcelona y el otro en Madrid, y esto seguiría ocurriendo. A Einstein esto también le parecía muy extraño y lo acuñó como *spooky action at a distance* (acción misteriosa a distancia). Los estados entrelazados nos permiten también hacer que una superposición desaparezca de un objeto y aparezca en otro, lo que se conoce como teletransportación cuántica.

Las superposiciones cuánticas y el teletransporte nos abren un mundo de posibilidades en comunicación. En primer lugar, podemos utilizarlas para asegurar las comunicaciones secretas; en efecto, existen protocolos llamados de distribución de claves cuánticas que utilizan el envío de fotones en estados de superposición para establecer una comunicación segura. Si alguien intenta interceptar la comunicación al observar la polarización de los fotones, obtendrá un resultado aleatorio, destruirá la superposición y, con ello, irremediablemente, será detectado por el emisor y el receptor. La teletransportación también nos permite realizar comunicaciones seguras ya que podemos teletransportar la información (en forma de superposición) de tal forma que desaparezca de un lugar y aparezca en otro sin que pase por ningún sitio, con lo que no puede ser interceptada. Por otro lado, existen una gran variedad de protocolos cuánticos para realizar tareas de manera segura, como votaciones telemáticas, firmas digitales, transacciones financieras, o compartición de secretos colectivos. Además, algunas tareas pueden ser realizadas de manera más rápida y eficiente. Por ejemplo, el proceso necesario para concertar una cita a distancia puede realizarse más eficientemente a través de la comunicación cuántica. En efecto, existe un protocolo para encontrar una fecha en la que dos personas tengan su agenda libre intercambiando unos pocos cúbits, muchos menos que los bits necesarios para encontrar la fecha utilizando la comunicación tradicional.

Más allá de la comunicación, la física cuántica permite procesar la información de una manera muy especial explotando las superposiciones y el entrelazamiento. Así funcionan los ordenadores cuánticos, que prometen realizar algunas operaciones en mucho menos tiempo que los más potentes superordenadores que existen actualmente. Y estos ordenadores pueden también tener un impacto extraordinario en las telecomunicaciones y hacer que las redes cuánticas no sean algo deseable sino, más bien, necesario. En efecto, una de las potenciales aplicaciones de los ordenadores cuánticos se enmarca en el campo de la criptografía: un ordenador cuántico sería capaz de desarmar los sistemas actuales de encriptación de mensajes. En consecuencia, si fuéramos capaces de construir alguno lo suficientemente potente, los sistemas de comunicación que utilizamos cotidianamente dejarían de ser seguros. Esto crearía un gran problema social ya que, en la actualidad, todos utilizamos esos métodos (por ejemplo, cuando hacemos compras por Internet, o cuando retiramos dinero en un cajero automático). Además, sin comunicaciones seguras, los bancos, las empresas, e incluso los Gobiernos, dejarían de operar. Una solución a este problema nos la proporcionan las comunicaciones cuánticas, ya que la distribución cuántica de claves o el teletransporte son seguros, incluso si el atacante posee un ordenador cuántico. Esto enfatiza la necesidad de desarrollar y desplegar las redes cuánticas, ya que, probablemente, los ordenadores cuánticos estén disponibles en un futuro no muy lejano. También esperamos que, para cuando estén desarrollados, podamos conectarlos a través de redes cuánticas y crear una Internet cuántica, que dé lugar a nuevas posibilidades. En definitiva, existen ya muchas razones para desarrollar este tipo de redes y estar preparados para la era de la información cuántica.

A través de su modelo de innovación abierta, Telefónica lleva más de diez años trabajando en el área de las comunicaciones cuánticas y lidera, en colaboración con otras empresas y centros de investigación tanto españoles como de otros países europeos, la investigación y el desarrollo en este campo. Desde hace tiempo aprovecha su extenso despliegue de fibra óptica y su liderazgo en I+D+i para probar y mejorar distintos protocolos de distribución de claves cuánticas y, a la vez, desarrolla la tecnología necesaria para transformar sus redes de fibra óptica en redes de comunicación cuántica. También participa en distintos proyectos y foros internacionales para definir e implementar la hoja de ruta de las comunicaciones cuánticas. De hecho, hoy en día ya es posible la distribución de claves cuánticas entre algunas de sus centrales, separadas por varias decenas de kilómetros, estableciendo récords en la velocidad de transmisiones. A su vez, el desarrollo de otros componentes, como los repetidores cuánticos, permitirán en el futuro extender el ámbito de las comunicaciones cuánticas. Y, con el advenimiento de los ordenadores cuánticos, se podrá construir una Internet cuántica que, con toda seguridad, nos traerá nuevas aplicaciones y casos de uso que, hoy en día, no podemos ni imaginar. ●

Cables. Fibra óptica.