POSITION PAPER

# ¿QUÉ ES LA **TECNOLOGÍA CUÁNTICA?**

OCTUBRE DE 2021

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

## ¿Qué es la tecnología cuántica?

Existen dos tipos de computación: la computación clásica y la computación cuántica. En el caso de la computación clásica, la información se envía en bits binarios, que representan un estado 0 (off) o 1 (on), mientras que en el caso de la computación cuántica, la información se envía en qubits, análogos a los bits binarios clásicos, pero que pueden estar en un estado 0, 1 o una combinación probabilística de ambos (p.e. 0 con un 20% y 1 con un 80% de probabilidad).

Una diferencia clave entre los bits clásicos y los qubits es que estos últimos incluyen dos bits de información con una codificación superdensa, mientras que el bit clásico sólo tiene un bit. Esta duplicación de la eficiencia por qubit junto con el concepto de entrelazamiento cuántico, permite incrementar de forma exponencial la capacidad de computación frente a la computación clásica gracias a la combinación de ambos fenómenos cuánticos. De esta forma, se puede aunar fuerzas y aumentar la codificación superdensa a un conjunto de qubits (en vez de que sea sólo uno).

Las principales tecnologías cuánticas incluyen los siguientes elementos:

- Sensores cuánticos. Son muy sensibles a variables físicas (gravedad, campo electromagnético), detectando cambios con muy alta precisión. Entre sus aplicaciones, se encuentran la metrología, el scanner o la navegación.
- Computación cuántica. Se basa en qubits con gran capacidad de procesamiento, que crece exponencialmente con el ´número de qubits entrelazados entre sí.
- Simulación cuántica. Permite simular sistemas complejos de forma natural, desde moléculas hasta galaxias.
- Comunicaciones cuánticas. Su principal ventaja es la seguridad frente a escuchas.

Este documento se va a centrar en la aplicación del concepto de computación cuántica a los entornos de Industria 4.0.

## Casos de uso en computación cuántica

En la actualidad, es limitado el número de aplicaciones de la computación cuántica en la Industria 4.0. Algunas empresas como Boeing están colaborando con Amazon Web Services utilizando su servicio de computación cuántica en la nube (Braket), para explorar la forma de desarrollar y validar algoritmos cuánticos en simulaciones para la búsqueda de nuevos materiales. Esta sección presenta diferentes casos de uso relacionados con tres categorías de aplicaciones: nuevos materiales y procesos de diseño, control y logística.

### Nuevos materiales y procesos de diseño

La computación cuántica permitirá comprender mejor los procesos físicos de la naturaleza que permitan la creación de nuevos materiales y nuevas formas más eficientes de diseño.

#### ❑ Ciencia de materiales

La simulación y predicción del comportamiento de sistemas complejos es crítica para el diseño de nuevos materiales, incluyendo los nuevos tipos de baterías o los medicamentos. McKinsey predice que la química cuántica será una de las primeras aplicaciones disruptivas de la computación cuántica. La modelización de polímeros, sólidos o moléculas de alta precisión sin

necesidad de sintetizar experimentalmente los materiales en el laboratorio permitirá identificar las estructuras moleculares eficientes que permitan cumplir una serie de propiedades.

Aunque los computadores actuales tienen limitaciones a la hora de modelizar moléculas de tamaño moderado con una precisión química total, la computación cuántica permitirá la modelización detallada de polímeros y moléculas muy sofisticados que beneficiará el desarrollo de nuevos materiales. Así, se podrán desarrollar materiales con ratios resistencia-peso más ventajosos, baterías con densidades de energía significativamente mayores, o procesos sintéticos y catalíticos más eficientes que ayuden en la generación de energía y la captura de $CO_2$.

Un ejemplo de aplicación similar a los procesos químicos es el diseño de medicamentos. La comercialización de un medicamento es un proceso complejo que puede llevar varios años y un coste medio de 2500 millones de euros. Por ello, la aplicación de computación cuántica puede ser de interés para las organizaciones farmacéuticas. Por ejemplo, la compañía Boehringer Ingelheim anunció recientemente su colaboración con Google Quantum AI para simular el comportamiento de la dinámica de las moléculas.

- Nuevos procesos de diseño

Actualmente, muchos productos se diseñan utilizando herramientas de simulación 3D y aplicando coeficientes de seguridad acumulativos, de modo que los productos finales están sobredimensionados tanto en material como en coste, lo que reduce su rentabilidad comercial. En el futuro, la computación cuántica permitirá simular las interacciones de los componentes dentro de los sistemas de forma más precisa, calculando las cargas, ruidos y vibraciones, lo que permitirá optimizar cada componente individual dentro del ecosistema global. De esta forma, se reducirá el impacto acumulativo de los coeficientes y se mejorará el coste sin poner en riesgo el funcionamiento del sistema.

Un ejemplo es el diseño de wingboxes de los aviones de Airbus, ya que las soluciones requieren la evaluación simultánea de diferentes factores para garantizar que se mantiene la integridad estructural. Por ello, los procesos actuales para abordar el problema son ineficientes y requieren recursos computacionales significativos con periodos largos de diseño. Este problema se ha acrecentado por la inclusión de modelos de diseño generativos muy intensivos en computación.

## Control

La computación cuántica permitirá encontrar nuevas correlaciones entre los datos, mejorar el reconocimiento de patrones y avanzar en la clasificación más allá de las opciones actuales de la computación clásica. La combinación entre la computación cuántica y Machine Learning (ML), así como su aplicación a la clasificación y segmentación tendrán un impacto en diferentes áreas como el incremento en los rendimientos de clasificación de clientes para una mejorar experiencia del usuario, así como la detección de imperfecciones en procesos y productos.

## Logística

Las cadenas logísticas están cambiando desde un modelo lineal con procesos discretos, secuenciales y basados en eventos hacia un modelo más responsivo basado en las demandas dinámicas del mercado en tiempo real. Adicionalmente, el despliegue de redes de sensores IoT está permitiendo el acceso a grandes volúmenes de datos. En este entorno, la computación cuántica podrá acelerar los procesos de toma de decisiones, optimizar la dinámica de los

procesos de producción y mejorar la gestión del riesgo para reducir los costes operativos y las pérdidas de ventas de productos discontinuos. La optimización de estas respuestas es clave para el desarrollo de toma de decisiones a tiempo real y poder crecer con los sistemas productivos actuales, que requieren mayor poder computacional.

- Optimización de procesos

Los algoritmos de optimización permiten identificar la mejor solución o proceso entre múltiples opciones viables. Estos problemas de optimización existen en todas las industrias y servicios, y algunos de estos problemas requieren demasiado tiempo para una resolución óptima con los recursos de computación tradicionales. Por ello, se espera que la computación cuántica tenga un gran impacto en industrias que se basen en la optimización para evaluar potenciales resultados, cada uno de los cuales incluye numerosas dependencias y limitaciones. Por ejemplo, la computación cuántica podrá abordar la optimización de rutas en tiempo real utilizando datos de los vehículos conectados, contenedores y paquetes, infraestructura viaria y ferroviaria, almacenes, puntos de venta o información meteorológica entre otros.

- Optimización de la cadena de valor

La computación cuántica ayudará a las empresas manufactureras a diseñar sus operaciones y procesos productivos gracias a la solución de sus problemas de optimización de la cadena de valor, como en la determinación de la disponibilidad y precios de las materias primas. Igualmente, se podrán construir cadenas logísticas más resilientes, ya que la computación cuántica permite una replanificación y relocalización de componentes en el caso de cierres inesperados, retrasos en los envíos o cancelaciones de pedidos.

- Optimización de rutas

Las variaciones del "Travelling Salesman problem" clásico que busca una de las mejores rutas para alcanzar diferentes destinos en el menor tiempo posible, supone la base de muchos retos de optimización. Con velocidades de computación 100 veces superiores a la computación tradicional, los ordenadores cuánticos son especialmente adecuados para optimizar estos procesos en un tiempo récord. Esto permitirá abordar la tendencia de personalización extrema de los bienes de consumo, que hace más compleja la gestión de pedidos. Por ejemplo, el año pasado Volkswagen en colaboración con D-Wave Systems puso en marcha un piloto para optimizar las rutas de los autobuses de Lisboa. Cada autobús recibió una ruta individual que se actualizaba en tiempo real sobre la base de las condiciones reales del tráfico.

## Casos de uso en comunicaciones cuánticas

### Internet cuántica

La aplicación más representativa y con mayor potencial de las comunicaciones cuánticas es la transformación de la red Internet actual en una Internet cuántica. Ahora bien, todavía es necesario un mayor desarrollo y madurez de tanto del software como hardware para completar la tecnología. El objetivo de la Internet cuántica es proporcionar una nueva tecnología de Internet que permita la comunicación cuántica entre dos puntos cualesquiera del mundo, que colaborará con la Internet clásica actual con toda probabilidad y conectará procesadores de información cuántica (nodos finales de la red) para conseguir capacidades difíciles o imposibles de conseguir con el tratamiento clásico de la información.

Aunque resulta difícil predecir los futuros casos de uso dada la novedad radical de esta tecnología, se están identificando algunas aplicaciones de interés que se presentan a continuación.

### ❑ Acceso remoto segura a computación cuántica en la nube

Un terminal cuántico simple con capacidad de preparar y medir qubits individuales puede utilizar la Internet cuántica para acceder a una computadora cuántica remota de forma que este computador no tenga ningún conocimiento sobre el procesamiento de información que ha realizado.

### ❑ Intercambios que requieren coordinación

Entre sus diferentes propiedades, el entrelazamiento cuántico proporciona una correlación y coordinación mucho mayor que la que se podría dar en el mundo clásico. Si se tienen dos qubits entrelazados en diferentes nodos de la red, cualquier medida que se haga en el qubit 1 afectará instantáneamente en el estado del qubit 2, habiendo transmisión de la información instantánea. Esta propiedad hace que el entrelazamiento sea muy adecuado para realizar tareas que requieren coordinación, como la sincronización de relojes o la ayuda a una pareja de jugadores on-line a coordinar sus acciones. Es la principal estrategia que se utiliza en comunicaciones cuánticas.

## Seguridad cuántica

La criptografía cuántica es una aplicación relacionada con el establecimiento de comunicaciones seguras y constituye en la actualidad, una de las tecnologías cuánticas más avanzadas con nuevos prototipos en desarrollo y equipos comerciales ya disponibles. Para ello, es importante la disponibilidad de equipos clave como la generación cuántica de números aleatorios (QRNG) y equipos para la distribución cuántica de claves (QKD).

### ❑ Generación cuántica de números aleatorios (QRNG)

Muchas aplicaciones de diferentes tipos utilizan números aleatorios, con ejemplos relacionados con la seguridad, la simulación numérica y la modelización de diferentes sistemas y procesos. Dado que las propiedades de la física cuántica proporcionan la única fuente verdaderamente aleatoria de la naturaleza, este tipo de soluciones es muy atractiva para la generación de flujo de bits aleatorios.

La QRNG es una de las tecnologías cuánticas más prácticas y con un desarrollo más avanzado actualmente. Incluso es probable que sea una de las primeras tecnologías cuánticas que sea explotada a gran escala. Ya existen dispositivos comercialmente disponibles, si bien limitados a una tasa de generación relativamente baja, de unos cuantos Mbps, y en desarrollo están nuevos esquemas de generación que han de permitir tasas del orden de Gbps. Por ello, se requiere aún desarrollo experimental y teórico para mejorar la eficiencia de la futura generación de dispositivos y explotar completamente todo su potencial. También se requiere establecer procesos adecuados de evaluación y certificación especialmente para su uso en sistemas criptográficos.

### ❑ Distribución cuántica de claves (QKD)

La QKD ofrece una forma probablemente segura de establecer un secreto compartido entre dos partes distantes, lo que se puede aplicar en varias aplicaciones criptográficas. En la actualidad,

ya existen dispositivos comerciales que permiten intercambiar claves de tipo QKD, y se han demostrado intercambios QKD tanto en segmentos de despliegue terrestre (fibra óptica) como en segmentos espaciales. Se están desarrollando nuevos dispositivos y protocolos que mejoren aspectos como la reducción del coste, la mejora de las prestaciones (la relación tasa de bits intercambiada/distancia), la integración con sistemas de comunicaciones actuales y el desarrollo de procesos de certificación.

Dado que existen aplicaciones en escenarios punto a punto, se deberá pasar de esquemas basados en nodos de confianza (trasmisión QKD "tramo a tramo" hasta el punto final) a esquemas basados en repetidores cuánticos. Para ello, serán necesarios nuevos dispositivos que permitan una comunicación cuántica extremo a extremo.

## Retos de la computación y comunicación cuántica

Aunque el potencial de esta tecnología es muy importante, todavía se está lejos de un uso generalizado. La computación cuántica presenta una serie de retos.

### Computación cuántica

- #### Pruebas de valor industriales

En la actualidad, no existen pruebas de valor para la aplicación de la computación cuántica en la industria dado el grado de desarrollo de la tecnología (hardware) para su escalado a nivel industrial. La falta de un método adecuado y coherente para calcular el impacto estimado en el negocio condiciona la falta de inversiones a largo plazo tanto por parte del dueño del caso de uso como de los colaboradores del ecosistema. Adicionalmente, la falta de un ecosistema y un mercado consolidado impide que los clientes pueden inferir el comportamiento previsto para las soluciones.

- #### Mejoras en el hardware y software

En la actualidad, los ordenadores cuánticos son análogos a los primeros ordenadores tradicionales, cuando hacía falta un hardware grande y complejo para cálculos básicos. Hay dos retos para la primera generación de ordenadores cuánticos: la reducción del ruido, lo que causa falta de coherencia en los sistemas cuánticos con la pérdida asociada de las propiedades cuánticas, y la mejora de la estabilidad de los qubits físicos, que realizan la corrección de los errores subyacentes para los qubits lógicos que realizan los cálculos cuánticos. En relación al software, el reto está en la creación de algoritmos cuánticos diferentes a los algoritmos tradicionales, lo que demanda nuevos profesionales.

### Comunicaciones cuánticas

Para conseguir una Internet cuántica, se requieren esfuerzos importantes para desarrollar y escalar las redes cuánticas de comunicaciones. Para ello, es necesario avanzar en física, ciencia de computadores e ingeniería. Se requiere diseñar y desarrollar de forma efectiva nuevos protocolos, nuevos desarrollos software y implementaciones hardware, a través de la experimentación física y de la ingeniería para su implementación.

Se espera que las primeras redes cuánticas multimodo aparezcan en los próximos años, aunque todavía hay incertidumbre sobre las componentes finales de la Internet cuántica. Para ello, será necesario avanzar en la mejora de las distancias a las que se pueden establecer transmisiones cuánticas fiables, la incorporación del entrelazado para desplegar esquemas que superen la

necesidad de tramos formados por nodos confiables, el desarrollo de los repetidores cuánticos basados en memorias cuánticas y la construcción de nodos finales, simples o computadores cuánticos completos, capaces de procesar la información a nivel cuántico.

## Situación en España

En mayo de 2019, se presentó el estudio "La España cuántica: Una aproximación empresarial" realizado dentro del grupo de Trabajo de Información, Computación y Ciberseguridad cuánticas de Ametic. En dicho estudio, se analizaba la situación del sector de las tecnologías cuánticas en España. Tal y como se menciona, el mercado de demanda es todavía muy incipiente y se centra en algunos pilotos sobre ciberseguridad cuántica realizados en el sector financiero.

En la actualidad, el sector financiero es el que más inversión está dedicando en el ecosistema nacional. Todos los bancos (BBVA, Santander, CaixaBank, Bankinter…) han establecido relaciones industriales con diferentes startups y empresas multinacionales para desarrollar pruebas de concepto que demuestren el uso de la computación cuántica en problemas intratables clásicamente. Aunque el mercado todavía está en auge debido a la madurez del hardware cuántico, cada vez se realizan más inversiones en tecnologías cuánticas debido a la necesidad de estar preparados para cuando llegue la madurez deseada del hardware cuántico.

Desde el mundo académico, existen grandes centros de investigación como el CSIC, la UPV o el ICFO que están participando en la iniciativa Quantum Flagship europeo tanto en la parte de comunicaciones como de computación cuánticas.