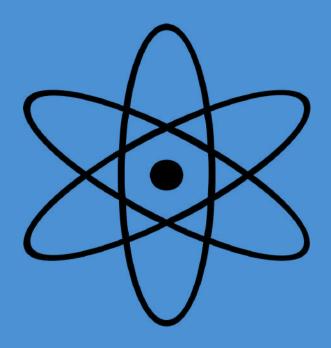
Computación cuántica

INFORME SITUACIÓN 2021





Plataforma Tecnológica Española de Tecnologías Disruptivas

Con financiación de:



INDICE

- Introducción
- Conceptos básicos
- Estado del arte de la computación cuántica
- Aplicaciones actuales y futuras
- Ecosistema
- Retos y oportunidades
- Casos de uso
- Apéndice
- Enlaces de interés

INTRODUCCIÓN

La computación cuántica representa un paradigma de computación distinto a la de computación clásica.

La unidad de información en computación cuántica es el qubit en lugar de bits y estos pueden tener varios estados: 0,1, superposición o valores intermedios.

La computación cuántica se basa en la **física cuántica** y la **mecánica** cuántica.

Lo cuántico viene de cuanto que es la mínima cantidad de cualquier entidad físicala física cuántica es la rama de la ciencia que estudia las características, comportamientos e interacciones de partículas a nivel atómico y subatómico.

La mecánica cuántica comenzó a desarrollarse a principios del siglo XX con científicos como **Max Planck**, **Albert Einstein** o **Niels Bohr**. En 1925, **Edwin Schrödinger** desarrolló su famosa ecuación de onda que describe la evolución temporal de una partícula cuántica.

La primera persona en proponer la idea de una **computadora cuántica** (una **máquina de Turing** que trabajase con las leyes de la mecánica cuántica) fue **Paul Benioff** en 1981. Más tarde **Richard Feynman**, entre 1981 y 1982 planteó que, una computadora cuántica que se basase en las leyes de la mecánica cuántica, podría hacer cálculos complejos de forma muy rápida.

Actualmente, la computación cuántica está en un estado de desarrollo muy incipiente, sin embargo, últimamente se están produciendo grandes avances en su desarrollo debido a que países como **China, Estados Unidos, Alemania, Rusia, India y la propia Unión Europea** están aumento su inversión en esta tecnología, ya que el liderazgo en la misma será estratégico, sobre todo en los próximos años.

Este informe pretende ser una foto del momento actual en el que se encuentra dicha tecnología en España y que sirva para poder comparar la situación en un futuro próximo.

CONCEPTOS BÁSICOS



Para entender el funcionamiento de la computación cuántica hay que tener en cuenta los siguientes conceptos:

- Estado cuántico
- Función de onda o vector de estado de un sistema de partículas
- Principio de incertidumbre de Heisenberg
- La ecuación de Schrödinger
- Superposición
- Entrelazamiento
- Decoherencia
- Algoritmo de Shor y Temple Cuántico
- Efecto túnel
- Puertas cuánticas
- Cristales de tiempo

Estado cuántico:

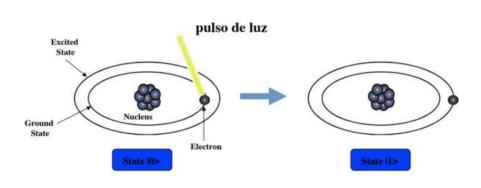
Es el estado físico que en un momento dado tiene un sistema físico en el marco de la mecánica cuántica. En la física clásica, teóricamente, al medir una magnitud física en un sistema varias veces, obtendríamos un mismo valor. Sin embargo en la física cuántica, en teoría, al medir una magnitud física podríamos obtener un valor diferente cada vez que se mide.

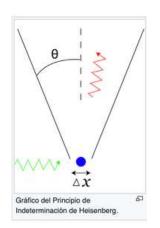
Principio de incentidumbre de Heisenberg

Afirma que no se puede determinar, en términos de la física cuántica, simultáneamente y con precisión arbitraria, ciertos pares de variables físicas, como son, la posición y el momento lineal de un objeto dado.

Función de onda:

Es una forma de representar el estado físico de un sistema de partículas.





Fuente: Wikipedia



Fuente: Wikipedia



El vicepresidente y CTO de Amazon, Werner Vogels, pronosticó en un artículo del MIT Technology Review del 1 de marzo de 2021 que la computación cuántica estaba comenzando a florecer.

Como explicábamos anteriormente, la principal diferencia entre un ordenador cuántico y uno clásico es su sistema de comunicación. Los ordenadores clásicos se comunican entre ellos a través de 'bits', el lenguaje binario que, por complejos cálculos matemáticos, convierte la información en 1 y 0.

En computación cuántica, los sistemas 'hablan' en 'qubits', que pueden ser 1 y 0 a la vez (por el mismo principio que rige al famoso gato Schrodinger, vivo y muerto al mismo tiempo), lo que multiplica exponencialmente el rendimiento de esta tecnología. Además, entre los qubits se produce un fenómeno, llamado entrelazamiento cuántico, por el que los qubits son capaces de 'comunicarse' entre sí a grandes distancias sin que exista ningún canal de transmisión, lo que amplía aún más sus posibilidades.

Sin embargo, aún no se ha avanzado lo suficiente en un hardware que pueda trabajar con un gran número de qubits (1000 ó 2000 qubits lógicos y 1 ó 2 millones de qubits físicos, según Sergio Boixo, jefe científico de teoría de la computación cuántica de Google) en grandes cálculos, ni en sistemas que permitan controlar muchos qubits y reducir sus errores, así como en los algoritmos que puedan ejecutarlos.

ESTADO DEL ARTE

En los últimos tres años hemos asistido a varios anuncios importantes en el desarrollo de esta tecnología entre los que destacan los siguientes:

Enero 2019:

IBM construye el primer ordenador cuántico para uso comercial: el IBM O System One, con un sistema de 20 qubits.

Agosto 2019:

Google anuncia que alcanza la supremacía cuántica, anuncio que no estuvo exento de <u>controversia</u>.

Septiembre 2019:

IBM anuncia que cuenta con un ordenador comercial de 53 qubits.

Junio 2020:

China anuncia la primera transmisión simultánea de un mensaje cifrado con tecnología cuántica que se ha enviado desde un satélite espacial hasta dos telescopios terrestres separados por 1.120 kilómetros, una distancia unas diez veces mayor a la lograda hasta ahora.

Finales 2020:

SpinQ Technology presenta el primer ordenador cuántico de sobremesa: SpinQ Gemini cuesta 50.000 dólares y anuncian un modelo portátil próximamente.



ESTADO DEL ARTE

Febrero 2021:

Jay Gambetta, vicepresidente de IBM Quantum anuncia que quieren alcanzar un tiempo de ejecución cien veces más rápido que todos los ordenadores cuánticos de IBM a lo largo de 2021.

Junio 2021:

El equipo dirigido por Hugues de Riedmatten, del ICFO, demuestra en un artículo publicado en la portada de la prestigiosa revista Nature el almacenamiento de dos fotones entrelazados en dos memorias cuánticas que estaban a 10 metros de distancia. El estudio supone una prueba de concepto clave, pues los investigadores han usado fotones con unas propiedades que permitirían enviar mensajes cuánticos usando la fibra óptica convencional que ya emplea internet. Además son los primeros en demostrar que su comunicación tiene hasta 60 modos diferentes de almacenar los fotones, un hito clave en el campo.

"Este trabajo es la demostración de un primer paso hacia un repetidor cuántico", explica Riedmatten. "Este es un paso muy importante hacia una primera red de comunicación cuántica terrestre", reconoce Juan José García-Ripoll, experto en comunicación cuántica del Consejo Superior de Investigaciones Científicas.

APLICACIONES ACTUALES Y FUTURAS

Principales áreas de la computación cuántica:

- Ciberseguridad y telecomunicaciones
- Sesórica
- Simulación
- Computación y algoritmos

Como hemos visto anteriormente, una de las principales aplicaciones hacia la que se están enfocando los últimos avances de la computación cuántica es hacia el desarrollo de redes de comunicación seguras, es decir, de un internet cuántico que complementará al actual.

Sin embargo, con las limitaciones actuales de la computación cuántica, las investigaciones se están centrando aprovechar las ventajas actuales de los ordenadores cuánticos, como son la gran capacidad de memoria para simular ecuaciones, como las de fluidos y ondas, distribución de probabilidad, soluciones a problemas de optimización, factorización de números o el bajo coste de generación de estados aleatorios con aplicación en el aprendizaje automático, análisis de riesgos o precios, etc. Asimismo, se el desarrollode algoritmos trabajando en está simulación cuántica que se inspiran en las capacidades de la computación cuántica pero se pueden ejecutar ordenadores clásicos.

Asimismo, empresas de nueva creación como <u>Quantum Mads</u>, <u>Multiverse Computing</u> o <u>Inspiration Q</u> están trabajando en intentar democratizar las ventajas de la computación cuántica desarrollando 'software' que pueda ser utilizado por cualquier empresa o institución y con aplicación en temas como la **optimización de carteras financieras**.



APLICACIONES ACTUALES Y FUTURAS

Sin embargo, las aplicaciones futuras de la computación cuántica pasan por los siguientes ámbitos, tal y como apunta Patricia Biosca en su <u>artículo del 6 de junio de 2021 en ABC</u>:

Inteligencia artificial

Uno de los requisitos de la inteligencia artificial es poder analizar grandes conjuntos de datos. En la actualidad se ha generado una ingente cantidad de información que muchas veces los equipos clásicos son incapaces de manejar. Los ordenadores cuánticos permitirían analizar y gestionar más datos en mucho menos tiempo.

Machine Learning

También, las computadoras cuánticas podrían potenciar el aprendizaje automático al permitir que los programas de inteligencia artificial busquen en estos mosntruosos conjuntos de datos elementos relacionados con la investigación médica, el comportamiento de los consumidores y los mercados financieros, y les den sentido. Incluso que encuentren una lógica que la mente humana no ha sido capaz de encontrar.

Simulaciones biomédicas

Actualmente, la creación de medicamentos implica años de experimentos de laboratorio durante las fases de descubrimiento, clínica y pre-clínica. Con la capacidad computacional exponencialmente mayor de la computación cuántica, los expertos creen que será posible simular con computadoras el efecto de diferentes compuestos químicos sobre organismos a nivel molecular. Esto permitiría diseñar nuevos medicamentos de manera mucho más rápida y barata.

APLICACIONES ACTUALES Y FUTURAS

Medicina 'a medida'

El campo de la óptica cuántica, que estudia cómo la materia y la radiación interactúan a nivel cuántico, tiene potencial para llegar a controlar moléculas individuales mediante la radiación que estas emiten y absorben, pudiendo alterarlas, modificarlas o incluso destruirlas. Se podría hacer lo mismo con las células cancerígenas y destruirlas sin perjudicar ninguna célula sana.

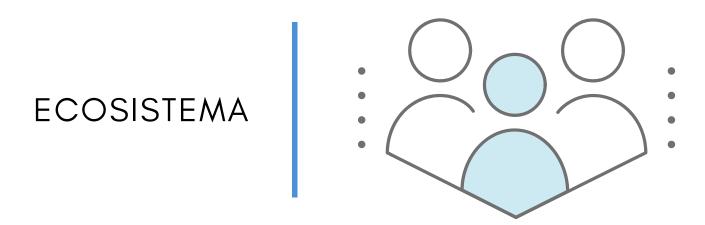
Industria Química

La industria química, por ejemplo, puede trabajar para identificar un nuevo catalizador para fertilizantes que ayude a reducir emisiones de efecto invernadero y mejorar la producción mundial de alimentos. Esto requiere de modelaje de interacciones moleculares muy complejas para las computadoras clásicas, pero perfectas para las cuánticas.

Nuevos materiales

Una aplicación potencial es el desarrollo de los materiales superconductores más eficientes, que permiten a su vez avanzar en el estudio de ordenadores más veloces y con mayor memoria, trenes de levitación magnética de alta velocidad y la posibilidad de generar energía eléctrica de manera más eficiente, por ejemplo.

Asimismo, podríamos añadir otros usos como por ejemplo la predicción de fenómenos atmosféricos, ciberseguridad o en el ámbito de la logística.



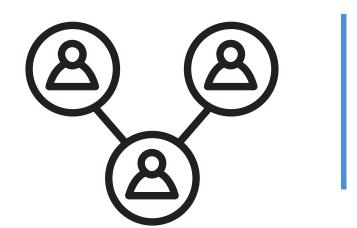
España cuenta con un ecosistema cada vez más importante en el ámbito de la computación cuántica.

España, a través de las <u>Agencia Estatal de Investigación</u> participa en la convocatoria de proyectos de investigación transnacionales sobre tecnologías cuánticas en el marco de la red europea de investigación ERANET <u>QuantERA</u>.

Barcelonaqbit es un think tank creado en el CERN/Ginebra en 2015 y con sede principal en Barcelona y cuyo principal foco está en evaluar el impacto social y económico de la información cuántica en especial, su go-to market y las oportunidades de negocio.

El Instituto de Física Fundamental perteneciente al Consejo Superior de Investigaciones Científicas (CSIC) cuenta con la **plataforma de tecnologías cuánticas** coordinada por el investigador **Juan José García Ripoll** y que agrupa a más de 40 grupos de investigación y una decena de centros del CSIC repartidos por toda España y trabajando en comunicación cuántica y muchos tipos de tecnologías así como investigando en redes de comunicación cuántica seguras y han creado con IBM una red de computación cuántica que está disponible a las empresas. Esta plataforma coordina el grupo de trabajo de computación cuántica de PTE Disruptive.

Pablo Hurtado dirige un grupo de investigación en la Universidad de Granada enfocado en la investigación de los cristales de tiempo que permitirán GPS más precisos, equipos de telecomunicaciones más avanzados o sistemas de criptografía más robustos, entre otras aplicaciones.



ECOSISTEMA

<u>Vicente Matin</u> coordina el Grupo de investigación en Información y Computación Cuántica (GIICC) de la Universidad Politécnica de Madrid

La Universidad del País Vasco cuenta con el **Qutis Center,** un equipo de investigación con gran influencia y relevancia en el campo de las tecnologías cuánticas.

Por su parte, la patronal de la industria digital **AMETIC**, además de contar con su propio grupo de trabajo en computación cuántica seguirá representando a España en el **Quantum Flagship**.

La Comisión Europea acaba de renovar el Consejo Asesor Estratégico para el principal grupo creado para impulsar la computación cuántica en la región, el Quantum Flagship. En representación de España han designado de nuevo a un miembro de AMETIC, **Carlos Kuchkovsky**, que colaborará en el desarrollo de regulaciones y estrategias para el desarrollo de esta tecnología.

Darío Gil es ingeniero eléctrico e Informático español y actual vicepresidente senior y director de IBM Research. Es uno de los propulsores del consorcio internacional del 2020, proyecto que surgió debido a la pandemia.

Ignacio Cirac es el director del Instituto Max Planck de Óptica cuántica.

ECOSISTEMA

<u>Sergio Boixo</u> es el jefe del comité de ciencia cuántica de Google.

The Institute of Photonic Science (ICFO) promovido por la UPC tiene como objetivo fundacional promover la ciencia y tecnología de la luz para crear una nueva comprensión de la realidad que aportara nuevas herramientas y soluciones que ayudasen a la industria y a la sociedad en general a abordar los principales retos de hoy en día.

Asimismo, además de las dos startups citadas anteriormente, en el <u>informe</u> realizado en 2019 por el <u>Grupo de trabajo de Información,</u> Computación y Ciberseguridad Cuánticas de AMETIC se incluye una relación de las startups, multinacionales españolas y multinacionales extranjeras con sede en España que trabajan en este ámbito, como por ejemplo: Entanglement Partners S.L., Metempsy, VLC Photonics, GMV, Telefónica, Accenture, IBM, etc...

El ecosistema está compuesto por más agentes y personas importantes, pero también queremos hacer un especial énfasis en el **talento femenino** en este ámbito, como por ejemplo, la física <u>Alba Cervera</u>, la doctora <u>Juani Bermejor Vega</u>, la investigadora científica <u>Ana Martín</u> o la física y doctora en Espintrónica y Nanofotónica, <u>Cristina Sanz</u>.



RETOS Y OPORTUNIDADES

Se espera que el valor de mercado de la computación cuántica se sitúe en torno a los **2.200 millones de dólares en 2026** según el informe de IQT Research: <u>Quantum</u> <u>Computing: A Seven-year Market Forecast</u>.

Según el profesor **Ahmed Banafa**, las principales dificultades que plantean los ordenadores cuánticos actualmente son las siguientes:

- Interferencia Durante la fase de cálculo de un cálculo cuántico, la más mínima perturbación en un sistema cuántico (por ejemplo, un fotón errante o una onda de radiación electromagnética) provoca el fallo del mismo, en un proceso que se conoce como decoherencia. Los ordenadores cuánticos deben estar totalmente aislados de toda interferencia externa durante la fase de cálculo.
- Corrección de errores Dada la naturaleza de la computación cuántica, la corrección de errores es de vital importancia, dado que un único error en un cálculo puede invalidar la totalidad de la computación.
- Observancia de salida Íntimamente relacionado con los dos anteriores, la captura de los resultados del cálculo cuántico también entraña un riesgo de corrupción de datos.

Además, podemos añadir, como apuntamos anteriormente la necesidad de trabajar y controlar grandes cantidades de qubits, preservar la información cuántica el tiempo suficiente para desarrollar cálculos y el desarrollo de algoritmos que ayuden a resolver más tipos de problemas a media de que dispongamos de hardware con mayor número de qubits.



RETOS Y OPORTUNIDADES

El desarrollo pleno de las ventajas de la computación cuántica tendrá un impacto en otras de las tecnologías disruptivas como son la **inteligencia artificial**, **blockchain o la ciberseguridad**.

En este sentido, la computación cuántica permite que los modelos de inteligencia artificial se puedan entrenar e implementar en tiempo real y que la criptograma actual quede obsoleta con la criptografía postcuántica.

Por tanto, el posicionamiento y la inversión en I+D en esta tecnología son estratégicos para situar a un país en el liderazgo tecnológico. En este sentido, Europa considera las tecnologías cuánticas como una prioridad y está dispuesta a competir con Estados Unidos y China.

El uso principal de las tecnologías cuánticas en Europa va de la mano de las comunicaciones. El principal objetivo de la Comunidad Europea en estos momentos es aplicar estas tecnologías en la creación de redes seguras. Estas redes deben permitir la interconexión entre los países europeos, pudiendo así tener tener redes más seguras frente a hackers. Estos proyectos son los mejores dotados de Europa en cuanto a financiación para investigación en la próxima década.

CASOS DE USO

A continuación os mostramos algunos de los ejemplos de casos de uso que DISRUPTIVE ha ido recopilando durante junio y julio de2021 y que puedes consultar con más detalle pinchando <u>aquí</u>



IMPLEMENTACIÓN SEGURA EN DISPOSITIVOS IOT - Fidesol

Actualmente los generadores cuánticos de números aleatorios (QRNG) son una de las tecnologías, también cuántica, más maduras. Contamos con trabajos fundamentales que demuestran su seguridad frente ataques de un adversario en escenarios denominados «independientes del dispositivo». Esto brinda una gran versatilidad en cuanto a la elección del dispositivo tecnológico que la implemente. Por otro lado, existen hoy aplicaciones concretas y comercializables de tales dispositivos QRNG. Dado que se ha logrado reducir suficientemente su tamaño y su consumo energético, pueden incorporarse dentro de dispositivos de la clase denominada loT, con el fin de dotar o reforzar su seguridad con criptografía liviana o basada en atributos.



Q-MADS, Q-CRYPTO y Q-ALLOCATE- Quantum Mads

Se trata de 3 soluciones que permite trabajar en los siguientes ámbitos: creación de serie sintéticas de datos, arbitraje en el mercado de las criptomonedas y optimización de carteras de inversiones.

SINGULARITY- Multiverse computing

Singularity permite entre otros usos los siguientes: Detección de la trayectoria óptima para la inversión/desinversión, formación de los operadores en las mejores trayectorias, optimización de la cartera, detección de tendencias/anomalías para la negociación, calificación del crédito (diferentes modelos) en los préstamos automatizados, etc.

APÉNDICE

En este apartado desarrollamos otros conceptos básicos que consideramos importantes para conocer mejor esta tecnología



Fuente: Wikipedia

Ecuación de Schrödinger:

Como podemos ver, la función de onda intenta dar solución al principio de incertidumbre de Heisenberg y a través de la ecuación de Schrödinger se intenta explicar la evolución temporal de la función de onda y, por tanto, del estado físico del sistema en el intervalo comprendido entre dos medidas. Pauli y Dirac completaron dicha ecuación introduciendo el efecto espín y los efectos relativistas.

Superposición

Es un principio fundamental de la mecánica cuántica que sostiene que un sistema físico tal como un electrón, existe en parte en todos sus teóricamente posibles estados (o la configuración de sus propiedades) de forma simultánea, pero, cuando se mide, da un resultado que corresponde a solo una de las posibles configuraciones.

Se trata de un efecto solo aplicable al mundo cuántico y subatómico y no al mundo macro, sin embargo, Schrödinger lo intentó describir mediante la **paradoja del gato.**

Entrelazamiento:

Al igual que la superposición, el entrelazamiento es un fenómeno cuántico, sin equivalente clásico, en el cual los estados cuánticos de dos o más objetos se deben describir mediante un estado único que involucra a todos los objetos del sistema, aun cuando los objetos estén separados espacialmente. Este fenómeno permite a los qubits comunicarse entre sí aunque existan grandes distancias entre ellos.

APÉNDICE



Visualización de la separación de del universo debido a dos estados mecánicos cuánticos superpuestos y entrelazados. Fuente: Wikipedia

Decoherencia:

Ocurre cuando un estado cuántico entrelazado da lugar a un estado físico clásico en el momento que al medirlo, colapsa la función de onda y da lugar a uno de los posibles estados.de un sistema físico.

Algortimo de Shor y Temple Cuántico

Ambos algoritmos son paradigmas de algoritmos en el ámbito cuántico. El primero de ellos permite encontrar factores de un número de manera eficiente y el segundo, es uno de los paradigmas del cómputo cuántico que más aplicaciones ha encontrado desde el plegado de proteínas, lógica matemática, visión por computadoras, entre otras

Efecto túnel:

Es un fenómeno cuántico por el que un electrón puede atravesar una barrera de potencial lo que estaría prohibido en física clásica ya que el electrón rebotaría como una pelota de frontón. Esto es posible debido al carácter ondulatorio del electrón.

Efecto túnel. Fuente: Wikipedia

Puertas cuánticas:

Es un circuito cuántico básico que opera sobre un pequeño número de qubits. Son para los ordenadores cuánticos lo que las puertas lógicas son para los ordenadores digitales.

Cristales de tiempo:

Es un cristal que puede ser capaz de cambiar su estructura con cierta periodicidad y recuperar su configuración inicial en intervalos regulares sin invertir energía. Para su creación son indispensables los ordenadores cuánticos y pueden ser utilizados para medir el tiempo y la distancia con una precisión extrema.

ENLACES DE INTERÉS

Aquí os remitimos a enlaces de noticias, webs, documentos normativos o informes de interés, así como a bibliografía sobre esta tecnología.

<u>Píldora formativa sobre computación cuántica de</u> APTEFORMA

La España cuántica: una aproximación empresarial

Computación cuántica ¿en qué se diferencia de la computación clásica?

<u>Introducción a la computación cuántica: Parte l</u>

Introducción a la computación cuántica: Parte II

<u>La superposición cuántica trasciende el mundo de las</u> <u>partículas elementales</u>

<u>La paradoja del gato de Schrödinger</u>

<u>Dos pasos más cerca de los ordenadores cuánticos del</u> <u>futuro</u>

Computación cuántica

¿Qué países invierten más en computación cuántica?

Repositorio de publicaciones científicas sobre computación cuántica

Ocho predicciones sobre el impacto de la tecnología en nuestra vida en 2021

<u>Un experimiento pone a prueba una interpretación de la mecánica cuántica</u>

Efecto túnel

<u>Cristales de tiempo</u>

Computación cuántica ¿qué hay detrás de la tecnología que esconde el gato de Schrödinger?

España adelanta a China en uno de los mayores problemas de computación cuántica

La computación cuántica como servicio se está generalizando

Quantum Computing Market is Expected to Reach \$2.2. Billion by 2026

Pompili, M. et al. "Realization Of A Multinode Quantum Network Of Remote Solid-State Qubits". Science, vol 372, no. 6539, 2021, pp. 259-264.

American Association For The Advancement Of Science (AAAS), doi:10.1126/science.abg1919.

Accessed 1 July 2021.https://science.sciencemag.org/content/372/6539/259

<u>Yin, Juan et al. "Satellite-Based Entanglement Distribution Over 1200 Kilometers". Science, vol 356, no. 6343, 2017, pp. 1140-1144. American Association For The Advancement Of Science (AAAS), doi:10.1126/science.aan3211. Accessed 1 July 2021.</u>

Lago-Rivera, Dario et al. "Telecom-Heralded Entanglement Between Multimode Solid-State Quantum Memories". Nature, vol 594, no. 7861, 2021, pp. 37-40. Springer Science And Business Media LLC, doi:10.1038/s41586-021-03481-8. Accessed 1 July 2021. https://www.nature.com/articles/s41586-021-03481-8

<u>Han-Sen Zhong, et al. "Quantum computational advantage using photons". Science. 2020.</u>

Ravitej Uppu et al. "Scalable integrated single-photon source". Science Advances. 2020.

15 tecnologías emergentes



Informe realizado por la <u>Asociación de Parques Científicos y</u> <u>Tecnológicos de España (APTE)</u>, entidad que gestiona la secretaría técnica de la <u>Plataforma Tecnológica Española de Tecnologías Disruptivas (DISRUPTIVE)</u> con la colaboración de su <u>grupo de trabajo de computación cuántica</u> durante los meses de julio y agosto de 2021





