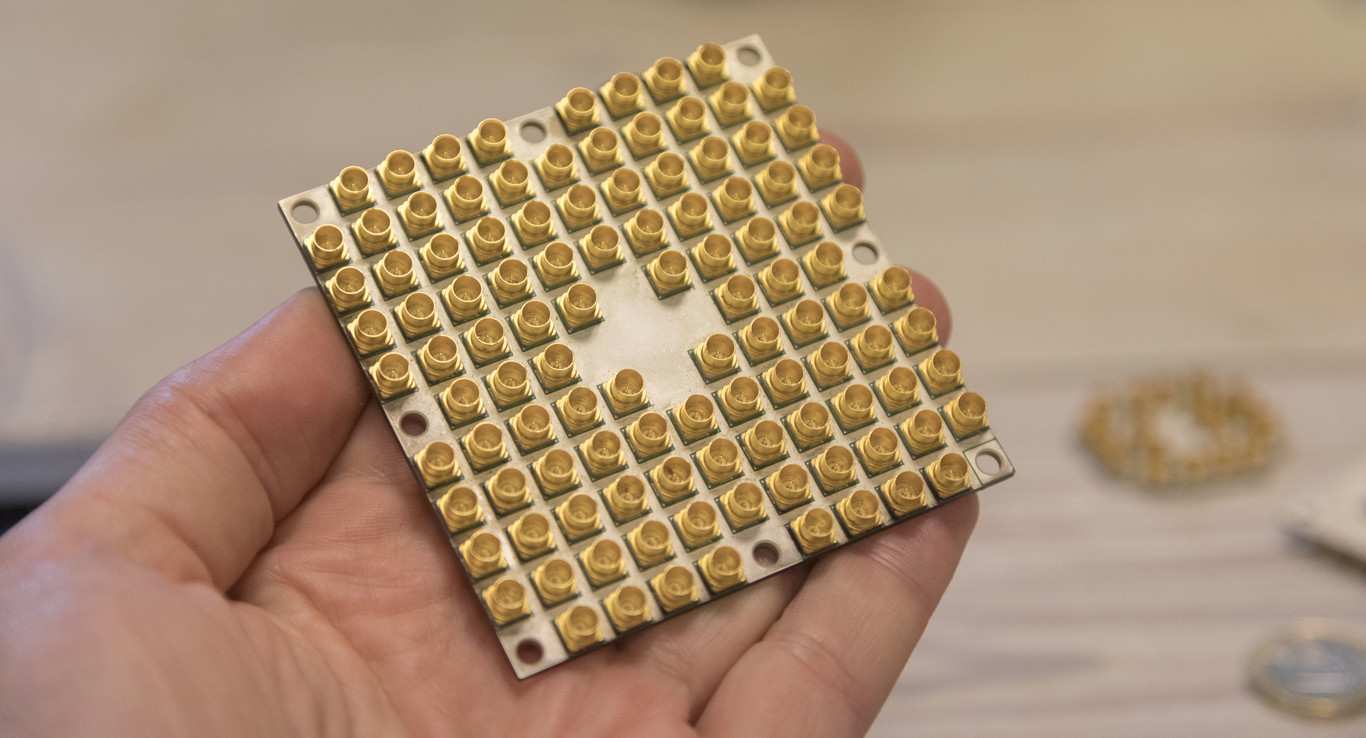
***COMPUTACIÓN CUÁNTICA***



PROYECTO FINAL DE ARQUITECTURA DE COMPUTADORES REALIZADO POR: JOSE LUIS PEDRAZA ROMÁN

***CONTENTS:***

1. *Introduction*
2. *What is Quantum Computing?*
3. *What is Qbit?*
4. *Diferecias con la computación tradicional*
5. *Problemas de la computación cuaántica*
6. *Introduction*

*-En las ultimas 5 decadas, los procesadores se han vuelto cada vez mas rapidos y pequeños, pero los limites de la tecnología se acercan a su margen. Si la industria quiere seguir construyendo computadoras todavía más potentes, algo tiene que cambiar.*

*Es todo cuestión de fascinantes promesas tecnológicas. Chips compuestos de luz, computadoras que funcionan a -260 grados, algoritmos que resuelven problemas 3600 veces mas rápido que los de las maquinas tradicionales, inteligencias artificiales que aprenden a la velocidad de un dios. Todo eso será, o sería, asunto para la computación cuántica, que se desarrolla lentamente hace tres décadas.*

-No es sencillo ubicar con precisión en el tiempo el momento exacto en el que la computación cuántica comenzó a hacer ruido más allá de los ámbitos académico y de investigación. Quizá lo más razonable es aceptar que esta disciplina empezó a ser conocida por el gran público **hace aproximadamente dos décadas**, un período durante el que los ordenadores clásicos han experimentado un desarrollo muy notable.

Aunque hay científicos que defienden con cierta vehemencia que la computación cuántica a la que aspiramos es imposible, como Gil Kalai, un matemático israelí que da clase en la Universidad de Yale, lo cierto es que ha avanzado mucho durante los últimos años. Desde fuera puede parecer que es una «eterna promesa» más, pero los avances de los que estamos siendo testigos, como la construcción del primer prototipo funcional de 50 qubits en el que está trabajando IBM, **nos invitan a ser razonablemente optimistas**. Sí, los retos que tienen por delante matemáticos, físicos e ingenieros son casi titánicos, pero esto hace si cabe más apasionante esta disciplina. Comencemos nuestro viaje.

1. *What is Quantum Computer?*

-En los últimos años, algunas grandes empresas de tecnología [como IBM](https://www.xataka.com/investigacion/la-computacion-cuantica-tiene-un-nuevo-lider-ibm-y-su-ordenador-cuantico-de-50-qubits), [Microsoft](https://www.xataka.com/investigacion/microsoft-refuerza-su-apuesta-en-busca-del-premio-gordo-de-la-computacion-cuantica), [Intel](https://www.xataka.com/ordenadores/asi-ordenador-cuantico-49-qubits-intel-dentro) o [Google](https://www.xataka.com/investigacion/google-dice-que-su-ordenador-cuantico-es-100-millones-de-veces-mas-rapido-que-uno-convencional) están trabajando en relativo silencio sobre algo que suena muy bien: la **computación cuántica**. El principal problema de esto, al menos para nosotros, es que es complicado saber qué es exactamente y para qué puede ser útil.

Hay algunas preguntas que se pueden resolver fácilmente. Por ejemplo, la computación cuántica no va a servir de momento para que tengas más FPS en tu tarjeta gráfica. Tampoco será todo tan fácil como cambiar la CPU de tu ordenador por una cuántica para que se vuelva hiperrápido. La computación cuántica es **fundamentalmente distinta** a la computación a la que estamos acostumbrados.

-Para diferentes científicos la computación cuántica será el futuro de las computadoras, aunque actualmente solo grandes empresas como Google y la NASA han podido adquirir una.

Hace unos años supimos que Google y NASA adquirieron una computadora cuántica en su búsqueda por alcanzar la mayor velocidad de resolución de problemas y analizar datos de una forma más precisa.

Diferentes científicos describen a la computación cuántica como un bebé en pañales que será el futuro de las computadoras, aunque actualmente solo las grandes empresas ya mencionadas, Google y NASA, tienen acceso a ellas.

Primero, definamos qué es una computadora u ordenador cuántico. Teóricamente se trata de una computadora que utiliza los qubits para realizar las operaciones en vez de los tradicionales bits de las computadoras clásicas, lo cual le permite resolver problemas mucho más rápido, lo que a una computadora ordinaria le tomaría demasiado tiempo o hasta, incluso, podría ser incapaz de resolver.

El ordenador cuántico con el que cuentan Google y NASA es el famoso D-WAVE 2. Lo adquirieron en el 2013 y ambas entidades han colaborado en su desarrollo. Este ordenador les permite realizar trabajos de investigación y desarrollo de manera mucho más rápida, especialmente en los trabajos de inteligencia artificial que vienen desarrollando, sobre todo Google.

1. *What is Qbit?*

-A principios del siglo XX, Planck y Einstein proponen que la luz no es una onda continua (como las ondas de un estanque) sino que está dividida en pequeños paquetes o **cuantos**. Esta idea, en apariencia simple, servía para resolver un problema llamado la "catástrofe ultravioleta". Pero a lo largo de los años otros físicos fueron desarrollándola y llegando a conclusiones sorprendentes sobre la materia, de las cuales a nosotros nos interesarán dos: **la superposición de estados y el entrelazamiento**.

Pues bien, la superposición y el entrelazamiento nos permiten reducir esas limitaciones: con la superposición podemos a**lmacenar muchos más que sólo 2^n estados** con n bits cuánticos (qubits), y el entrelazamiento mantiene fijas ciertas relaciones entre qubits de tal forma que **las operaciones en un qubit afectan forzostamente al resto**.

*-*comparemos y recordemos que la computación actual trabaja en bits. Tu ordenador sólo sabe “leer” la información en dos estados: cero o uno (encendido o apagado). Para los bits tenemos normalmente solo voltajes: aplicamos 3V en un alambre = 1; aplicamos 0.5V en el mismo alambre = 0. Y todo lo que se hace en un ordenador es transcrito a este sistema por transistores, una suerte de pequeñas cajitas que pueden almacenar energía y liberarla cuando sea necesario.

Entender a los transistores es importante para la comparación: cuando una cajita tiene electricidad almacenada interpretamos un 1, y cuando no, un 0. Se utilizan unos 6 transistores por bit y, además, hay unos circuitos llamados puertas lógicas, que miden el estado de las cajitas y guardan energía en nuevas cajitas en función de los estados que midan. Por ejemplo, la puerta OR mide si hay electricidad en dos cajitas, y únicamente si hay electricidad en alguna de ellas guarda electricidad en otra cajita.

Simplificándolo mucho para el caso que nos ocupa, estos son los elementos físicos que llevan a cabo los cálculos que nosotros mandamos hacer a través de programas y apps. Como puedes imaginar, este sistema tan “mecánico” hace que la velocidad a la que un ordenador puede procesar la información sea lineal a la cantidad de bits que posea, dependa del hardware y por defecto tenga un límite técnico.

El límite técnico podría parecer una exageración, hacer ordenadores más grandes y ya está, pero no es así. El límite se torna evidente cuando pensamos que ni todos los ordenadores clásicos del mundo son lo suficientemente inteligentes para resolver problemas de optimización cuando la cantidad de datos es demasiado grande. Y en este momento de la historia, como civilización, generamos inmensas cantidades de datos: climáticos, poblacionales, geonómicos, patrones de comportamiento... No podemos crear versiones útiles o patrones de ellos por la imposibilidad de que un ordenador clásico los asimile todos.

La diferencia que hace especial a la tecnología cuántica, y por lo que tiene un potencial tan inmensamente grande, es que sus bits trabajan también con la superposición de ambos estados: encendido y apagado. Esto pasa porque el proceso no ocurre mecánicamente, sino gracias a las normas de la física cuántica. Al aplicar la ‘lógica’ cuántica al mundo de la informática, se consiguen resolver problemas a toda velocidad, paralelamente y con multitud de resultados para cada variable.

Los bits de la computación cuántica se llaman qubits. Igual que un bit, un qubit representa una unidad básica de información, pero una unidad de información cuántica, que se rige por las normas de la física cuántica y por ello el qubit puede ser 0 o 1, o algo entre estos. De hecho, puede ser 1 y 0, paralelamente.

Por su parte, el efecto “contenedor” de los transistores y puertas lógicas se sustituyen por otros procesos más complicados, y hay varios, pero la idea es la misma: “aislar” al qubit como ocurre dentro del transistor.

*4* ***-DIFERENCIA CON LA COMPUTACIÓN TRADICIONAL***

En el mundo cuantico (fenomenos fisicos a escalas microscopicas) una particula puede poseer dos o mas valores de una cantidad observable, por ejemplo: veamos a esta particula como si fuera una manzana. Esta manzana puede estar en 2 o mas lugares al mismo tiempo, puede tener ninguna, 2 o mas mordidas al mismo tiempo, puede ser verde, azul, roja, amarilla o negra al mismo tiempo etc. A este fenomeno se le llama Superposicion Cuantica.

Los acontecimientos en un ambiente macroscopico no parecen exhibir este tipo de propiedades de la fisica cuantica, he ahi la disonancia entre la fisica cuantica y la fisica newtoniana, he ahi la diferencia entre la computacion cuantica y la computacion clasica.

1-    En la computación digital, un bit sólo puede tomar dos valores: 0 ó 1. En cambio, en la computación cuántica, intervienen las leyes de la mecánica cuántica, y la partícula puede estar en superposición coherente: puede ser 0, 1 y puede ser 0 y 1 a la vez (dos estados ortogonales de una partícula subatómica). Eso permite que se puedan realizar varias operaciones a la vez, según el número de qubits.

2-    Con los bits convencionales, si teníamos un registro de tres bits, había ocho valores posibles y el registro sólo podía tomar uno de esos valores. En cambio, si tenemos un vector de tres qubits, la partícula puede tomar ocho valores distintos a la vez gracias a la superposición cuántica.

3-    Un computador cuántico de 30 qubits equivaldría a un procesador convencional de 10 teraflops (millones de millones de operaciones en coma flotante por segundo), cuando actualmente las computadoras trabajan en el orden de gigaflops (miles de millones de operaciones).

4-    En la computación clásica se utiliza el sistema binario y en la computación cuántica se utiliza el sistema unario.

*5* ***-PROBLEMAS DE LA COMPUTACION CUANTICA***

Uno de los obstáculos principales para la computación cuántica es el problema de la [decoherencia cuántica](http://es.wikipedia.org/wiki/Decoherencia_cu%C3%A1ntica), que causa la pérdida del carácter unitario (y, más específicamente, la reversibilidad) de los pasos del algoritmo cuántico.

Los tiempos de decoherencia para los sistemas candidatos, en particular el tiempo de relajación transversal (en la terminología usada en la tecnología de resonancia magnética nuclear e imaginería por resonancia magnética) está típicamente entre nanosegundos y segundos, a temperaturas bajas. Las tasas de error son típicamente proporcionales a la razón entre tiempo de operación frente a tiempo de decoherencia, de forma que cualquier operación debe ser completada en un tiempo mucho más corto que el tiempo de decoherencia.

Si la tasa de error es lo bastante baja, es posible usar eficazmente la corrección de errores cuánticos, con lo cual sí serían posibles tiempos de cálculo más largos que el tiempo de decoherencia y, en principio, arbitrariamente largos.

Se cita con frecuencia una tasa de error límite de 10-4, por debajo de la cual se supone que sería posible la aplicación eficaz de la corrección de errores cuánticos.

Otro de los problemas principales es la escalabilidad, especialmente teniendo en cuenta el considerable incremento en qubits necesarios para cualquier cálculo que implica la corrección de errores. Para ninguno de los sistemas actualmente propuestos es trivial un diseño capaz de manejar un número lo bastante alto de qubits para resolver problemas computacionalmente interesantes hoy en día.

*6 – Posibilidad de investigación*

Con usos potenciales en los sectores de la salud y las finanzas, esta revolución promete abrir una nueva era tecnológica.

Como ávido aficionado del juego de mesa Go, Mark Griswold quedó cautivado por la partida que se celebró en 2016 entre el mejor jugador del mundo y un ordenador, un hito en la historia de la inteligencia artificial. Aún recuerda el movimiento 102 de la primera partida con asombro.

El ordenador, desarrollado por la filial de **Alphabet DeepMind**, colocó una ficha blanca en una posición que sorprendió incluso a los expertos. Resultó un golpe de ingenio que los jugadores humanos habrían tenido problemas para planificar, y un momento clave en una contienda que terminó con la victoria de la máquina sobre el hombre.

Esta tecnología promete incrementos exponenciales de la capacidad de procesamiento

La gente está limitada por las posibilidades que pueden percibir y analizar, obligándoles a pensar de forma tradicional, señala ahora Griswold. "Los humanos somos innovadores, pensamos de forma creativa. Pero no podemos hacerlo al mismo ritmo que un ordenador".

Profesor de radiología en Cleveland (Ohio), Griswold acaba de tener su propio encuentro con un ordenador que piensa de forma creativa. La máquina en cuestión está programada para simular el comportamiento de un ordenador cuántico, una tecnología que podría revolucionar la informática.

Los humanos utilizan una mezcla de experiencia e intuición a la hora de abordar un problema cuyo análisis completo resulta demasiado complejo, señala. En su caso, eso implica ajustar la configuración de una máquina de resonancias magnéticas para obtener el mejor análisis posible en una situación concreta, algo que compara con extraer el mejor sonido a un instrumento de música.

Sin embargo, tras sólo unas semanas de experimentar con la tecnología cuántica, Griswold explica que el ordenador ya ha conseguido resultados que superan los de su propia experiencia.

Es, afirma, el **inicio de una nueva era, en la que los ordenadores cuánticos desafiarán gran parte de lo que pensamos saber sobre el mundo**: "Vamos a ver constantemente cosas que desafían nuestra intuición. Es tan apabullante que no podemos entenderlo, no sabemos cuánto potencial existe", explica Griswold.

La computación cuántica podría incluso ayudar a diseñar nuevos materiales

Los **ordenadores cuánticos**, que acceden a la mecánica cuántica, una rama de la física que trata el comportamiento de partículas subatómicas, son un viejo sueño del mundo de la tecnología. Al aprovechar propiedades que van más allá de los límites de la física clásica de Isaac Newton, prometen incrementos exponenciales de la capacidad de procesamiento.

Tras décadas en los laboratorios, la tecnología está empezando a hacer la transición desde los experimentos científicos a prototipos rudimentarios que afectan a campos tan diversos como la química y la banca, y que dan pie a que ya se estén realizando estudios en compañías que van desde **Samsung** a **Daimler-Benz** y **JPMorgan Chase**.

1. **Plazos**

"Tienen que pasar 30 años para que este estudio básico sea viable -en el caso de la informática cuántica, ese tiempo ya ha pasado-", afirma **Mladen Vouk, profesor de Ciencias Informáticas en la Universidad Estatal de Carolina del Norte**. El resultado es que investigadores como los de esta universidad tienen la primera oportunidad de probar la tecnología.

Según tecnológicas como **IBM y Microsoft**, así como *start up* especializadas como Rigetti Computing, los primeros beneficios reales de la computación cuántica podrían verse en un plazo de cinco a diez años, un espacio de tiempo que plantea posibilidades tentadoras para las compañías que esperan ser las primeras en emplear la tecnología.

Los ordenadores cuánticos desafiarán gran parte de lo que creemos saber sobre el mundo

JPMorgan Chase empezó a destinar parte de su presupuesto de investigación a la computación cuántica hace dos años. A la pregunta desi ser uno de los primeros aportaría ventajas claras sobre los rivales, Bob Stolte, director gerente en el banco corporativo y de inversión de la entidad, comenta: "Pienso que podría haberlas, potencialmente". Pero advierte: "Es demasiado pronto para afirmarlo".

Los **resultados podrían superar incluso a los sistemas de inteligencia artificial más potentes actuales**. Refiriéndose a los chips especializados, o unidades de procesamiento gráfico (GPU), utilizados en la mayoría de los sistemas de aprendizaje automático más avanzados que existen en la actualidad, Stolte explica: "Si no se estuviese limitado al número de GPU que se pueden conseguir en un centro de datos, ¿qué problemas se podrían solucionar, y qué productos se podrían ofrecer a los clientes?" Los investigadores que intentan aprovechar el nuevo hardware se centran en tres tipos principales de problemas para cuyo tratamiento se espera que las máquinas cuánticas estén especialmente bien preparadas.

El primero implica analizar el mundo natural, utilizando ordenadores para modelar el comportamiento de moléculas con una precisión que nunca podrían igualar los ordenadores actuales. "La naturaleza es mecánica cuántica así que, si se tuviese un ordenador que funcionase con principios cuánticos, todo sería mucho más directo", señala Bob Sutor, un investigador de IBM.

En comparación con los ordenadores actuales, que tienen que hacer aproximaciones para elaborar un modelo del comportamiento de las partículas subatómicas, los ordenadores cuánticos podrían hacerlo con precisión.

1. **Aplicaciones**

Ilyas Khan, el consejero delegado de **Cambridge Quantum Computing**, una *start up* que diseña aplicaciones para la tecnología, sugiere que uno de los primeros sectores en beneficiarse será la industria química. El enorme incremento de la capacidad de procesamiento permitirá descubrir nuevos materiales,augura.

Los **ordenadores tradicionales nunca podrían procesar una tarea de esta envergadura**. En el ámbito cuántico, esto de pronto se vuelve posible. Esto podría facilitar el diseño de nuevos materiales, o hallar mejores formas de gestionar los procesos existentes. Microsoft, por ejemplo, prevé que podría llevar a una forma más eficiente de capturar nitrógeno de la atmósfera para emplearlo en fertilizantes, un proceso conocido como fijación de nitrógeno, que en la actualidad consume enormes cantidades de energía.

A primer vista, podría parecer que la tecnología avanza rápidamente hacia estos niveles. Tras elaborar los primeros sistemas básicos a partir de un pequeño número de bits cuánticos (qubits) hace dos años, compañías como **IBM, Rigetti y Google** avanzan deprisa hacia ordenadores que comprenden docenas de qubits.

Los números, no obstante, no explican toda la realidad. Los qubits actuales son inestables, sólo mantienen su estatus cuántico durante una diminuta fracción de segundo, y, a medida que se juntan crecientes números, las impredecibles interacciones entre ellos llevan a que se produzcan altas tasas de error. Aprender a extraer resultados de estos "ruidosos" sistemas supone ya un inmenso reto, y extenderlo a ordenadores de 100 qubits está más allá de las capacidades actuales.

1. **Aplicaciones en el mundo real**

Las **empresas químicas** han sido unas de las primeras en empezar a experimentar con la tecnología. Una de ellas es **JSR Corporation**, la multinacional de materiales japonesa que ha adquirido una participación del 5,5% en Cambridge Quantum Computing, y que también es una de las primeras firmas que colabora con IBM. Las **farmacéuticas**, que podrían obtener beneficios similares de la tecnología cuántica a largo plazo, siguen manteniéndose al margen. "Tratan de dilucidar cuándo habrá suficientes qubits para gestionar las moléculas con las que trabajan", explica Bob Sutor, investigador de IBM, ya que son mucho más grandes y complejas. También se espera que la informática cuántica aporte beneficios al **aprendizaje automático**. En lugar de limitarse a añadir más capacidad de procesamiento para acelerar la programación de los sistemas de aprendizaje automático actuales, la tecnología está preparada para abordar problemas concretos que suponen un reto para los ordenadores tradicionales. Otra área de trabajo es la optimización de complejos problemas que presentan demasiadas variables para los ordenadores actuales. Los nuevos sistemas deberían abordar cualquier problema matemático difícil que tenga la posibilidad de traducirse en un formato que puedan manejar los algoritmos cuánticos especializados, señala Sutor.

1. *Conclusion*

Los ordenadores cuánticos se basan en el uso de los qubits (bits cuánticos) en lugar de bits, y da lugar a nuevas puertas lógicas que hacen posibles nuevos algoritmos.

Poseen una capacidad de cálculo muy superior a los computadores actuales gracias al paralelismo masivo (exponencial) debido a la superposición de estados en los qubit.

En el campo de la criptografía proponen un nuevo enfoque: control absoluto de seguridad a nivel de comunicación y su capacidad para realizar operaciones de factorización (descomposición en números primos), que representa una amenaza para las comunicaciones encriptadas que emplean muchas [instituciones](https://www.monografias.com/trabajos13/trainsti/trainsti.shtml) en sus sistemas de seguridad, y que se basan a su vez en la dificultad de hacer códigos. Finalmente decir que la computación cuántica es un campo en el que aún queda mucho por descubrir.

1. *Ultimos avances y noticias 2019 (MICROSOFT QUANTUM NETWORK)*

La **computación cuántica** es uno de los ingredientes del futuro de la informática, por lo que varios grandes de la tecnología tienen su avance como uno de sus objetivos a medio y largo plazo. Por ejemplo, **Microsoft**, que de cara a dar impulso a esta tecnología, [ha puesto en marcha](https://cloudblogs.microsoft.com/quantum/2019/02/28/announcing-the-microsoft-quantum-network/) una red denominada **Microsoft Quantum Network**.

Esta red es una coalición de socios que comparten la misma visión y objetivo: “compartir el conocimiento y colaborar con los mayores innovadores en cuántica” de cara a ayudar al progreso de la computación cuántica. Su objetivo final es **ayudar al desarrollo del primer ordenador cuántico y escalable**, así como al de aplicaciones cuánticas.

En palabras de la compañía, es una “comunidad global de individuos y organizaciones que trabaja con Microsoft para aprender, investigar y lanzar hardware y aplicaciones de computación cuántica con acceso al Kit de Desarrollo Cuántico, a investigación relevante y a expertos“. Los miembros de la red también contarán con **acceso exclusivo a servicios de Azure**, así como con **talleres sobre programación cuántica y desarrollo de algoritmos**.

Para dar el pistoletazo de salida a esta red, Microsoft ha celebrado la cumbre **Startup Summit**, en la que ha quedado formalizada la coalición. Durante esta cumbre, los de Redmond han anunciado dos **nuevas incorporaciones a su red de colaboradores en computación cuántica**, de la que ya forman parte entidades y empresas como 1QBit, Borh Technology, Cambridge Quantum Computing, Entropica Labs, GTN, OTI Lumionics, ProteinQure, QC Ware, Qulab, QxBranch, Riverlane Research, Solid State AI, Strangeworks y Zapata Computing. Se trata de **HQS Quantum Simulations** y **Rahko**.

La primera de ellas se encarga de desarrollar algoritmos cuánticos para la predicción de propiedades moleculares para las industrias química y farmacéutica. Mientras tanto, la segunda empresa de machine learning cuántico que desarrolla soluciones químicas cuánticas y escalables para, entre otros fines, ordenadores cuánticos.

En esta cumbre, el**Vicepresidente del Grupo de sistemas hardware de Azure**, **Todd Holmdahl**, ha destacado que “la Red Microsoft Quantum muestra nuestro compromiso para establecer los acuerdos necesarios para desarrollar la fuerza de trabajo y la economía cuánticas. Creemos que ambas son vitales para la resolución de algunos de los problemas más complicados del mundo“.

### Nuevo hito en computación cuántica de IBM: doble rendimiento cuántico

Mientras Microsoft sigue adelante con su red, **IBM** también sigue cosechando avances en computación cuántica. La compañía ha presentado hace unas semanas [su primera computadora cuántica comercial](https://www.muycomputerpro.com/2019/01/08/q-system-one-computadora-cuantica), y ha confirmado que **ha conseguido el mejor rendimiento logrado hasta la fecha con un ordenador cuántico**. Además, según [Computer Business Review](https://www.cbronline.com/news/ibm-quantum-computing" \t "_blank), este hito viene acompañado de l**as menores tasas de error que se han medido hasta ahora** en el mundo de la computación cuántica.

El rendimiento logrado, que se ha doblado cada año desde 2017, **se ha medido con el índice Quantum Volume**, un sistema métrico que recoge los qubits que tiene un ordenador cuántico, así como los errores de medida y umbral. También la comunicación entre dispositivos y la conectividad, así como la eficacia del compilador del software de circuitos.

Así lo ha confirmado el **equipo de investigación Q de IBM**, que ha detallado que ya **se ha logrado un volumen cuántico de 16**. Hasta ahora, el máximo que el equipo de investigación encargado de trabajar en el avance de la computación cuántica en IBM era de 8. Eso sí, a pesar de los avances registrados, los ordenadores cuánticos siguen produciendo demasiado “ruido” como para conseguir cálculos con cierta importancia y peso. Los resultados se van a presentar en el **Encuentro de la Sociedad americana de física (APS)**, que comienza hoy.