En sustitución de la ley de Moore, que predijo un crecimiento exponencial del número de transistores en un chip, se postula ahora para el caso de la computación cuántica la ley de Neven, todavía por demostrar a efectos prácticos, pero que predice un crecimiento doblemente exponencial del número de *qubits* en un chip cuántico. Este trabajo, se centrará en hacer algunas consideraciones sobre el estado del arte de la computación cuántica, los desafíos que es necesario afrontar, así como las principales contribuciones empresariales para el desarrollo de esta tecnología. Actualmente, el estado de esta tecnología es similar al de la computación clásica en los años 50 del siglo XX, sin embargo, la supremacía cuántica, esto es, el momento en que los computadores cuánticos superarán a los computadores clásicos, no se encuentra tan lejano. En el presente trabajo, se realizará una comparativa entre la computación clásica y la cuántica, algunas consideraciones sobre el estado del arte de la computación cuántica, así como los principales desafíos a los que se enfrenta esta nueva tecnología, para finalizar con las principales contribuciones de las empresas tecnológicas para su desarrollo.

COMPUTACIÓN CUÁNTICA: ESTADO DEL ARTE, DESAFÍOS Y CONTRIBUCIONES EMPRESARIALES

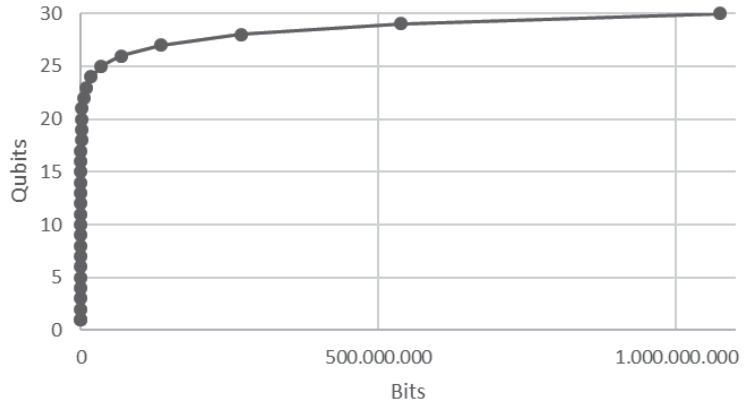
Así como la computación clásica o convencional, se encuentra basada en la teoría de la información y en la física clásica, la computación cuántica, se encuentra basada en la teoría de la información y en la física cuántica. Se realizará una comparativa entre el computador clásico cuyos componentes, circuitos, subsistemas y sistemas se encuentran basados en las leyes de la física clásica y el computador cuántico, cuyos componentes, circuitos, subsistemas y sistemas, se encuentran basados en las leyes de la física cuántica y se realizará también una comparativa entre la arquitectura de un computador clásico y un computador cuántico y de las diferencias que existen a nivel de componente, circuito, subsistema y sistema entre un computador clásico y un computador cuántico, para pasar después a describir las principales dificultades que hay que afrontar para construir un computador cuántico.

La figura 1 anterior pretende hacer visual la potencia de la computación cuántica, versus la computación clásica. En efecto, un computador cuántico de 30 *qubits*, es equivalente a un computador clásico de 2^{30} bits, es decir 1.073.741.824 bits. Ello quiere decir que 30 componentes cuánticos, implementados en forma de 30 *qubits* son equivalentes a 1.073.742.824 componentes clásicos o transistores. Recuérdese que un transistor en un instante dado, solo puede estar encendido o apagado, "*on*" u "*off*" y por lo tanto cada transistor solo puede implementar 1 bit en un instante dado. Con solo 30 *qubits*, se tienen implementados el equivalente a 2^{30} bits.

Se hará mención, a los principios que son más relevantes en la construcción de un computador cuántico por cuanto confieren mayor potencia de cálculo y prestaciones a los computadores cuánticos respecto a los computadores clásicos, y que hacen que la transición desde la computación clásica a la computación cuántica tenga sentido abordarse: la superposición y el entrelazamiento cuántico. También se tratará la decoherencia uno de los mayores problemas y dificultades de los computadores cuánticos. Se insistirá también en el principio más relevante para la construcción de una red de computadores cuánticos: el teletransporte cuántico.

Comenzando por la computación clásica, a nivel de componente, el componente más importante y que permitió el paso desde de los primeros computadores realizados mediante relés y posteriormente, mediante válvulas de vacío, computadores que ocupaban habitaciones enteras, es el transistor y más en concreto, en el computador clásico el componente por excelencia es el transistor CMOS de silicio a través del cual se implementa el bit clásico. Así, el transistor, en su funcionamiento como interruptor, es capaz de cortar o de dejar pasar la corriente y por tanto a través de transistores, es posible implementar la lógica clásica binaria del ámbito digital, el "1" y el "0", en definitiva, el bit o dígito binario, que, en un determinado instante de tiempo dado, puede encontrarse en estado "*on*" o en estado "*off*". A partir del transistor, y mediante otros componentes complementarios como diodos, resistencias, condensadores, inductancias, etc., se construyen los diferentes circuitos, implementados en forma de puertas lógicas, cuyo funcionamiento responde al Álgebra de Boole. Las puertas lógicas, las cuales operan con bits, esto es con "1s" y "0s", más relevantes son la

FIGURA 1
COMPUTACIÓN CLÁSICA VS COMPUTACIÓN CUÁNTICA



Fuente: elaboración propia.

puerta NOT la cual transforma un "1" en "0" y viceversa, la puerta AND, cuya salida es un "1", si y solo si todas sus entradas son "1" y la puerta OR, cuya salida es "1", si y solo si alguna de sus entradas es "1". Para realizar la operación de suma binaria, se necesita la puerta XOR (eXclusive OR) que implementa un semi-sumador y mediante la cual es posible construir un sumador completo. A partir de los diferentes circuitos, se construyen los diferentes subsistemas de un computador clásico que constituyen el sistema completo. En definitiva, los computadores clásicos realizan tareas mediante el uso de componentes que pueden encontrarse en dos estados, en uno u otro y que se denominan bits y que, alimentados como entradas de las puertas lógicas, se manipulan conforme a las reglas del Álgebra de Boole para producir una salida de bits que pueden medirse, p. ej., como voltaje o como corriente.

Pero las leyes de la física no son invariantes ante un cambio de escala y cuando se considera la escala nanométrica, en concreto por debajo de unos 100 nm, comienzan a ponerse de manifiesto las leyes de la física cuántica. Este hecho, hace posible considerar la viabilidad de construir un computador cuántico. En la conferencia sobre los computadores del futuro que Richard Feynman impartió en Japón en la Universidad de Gakushin (Tokio), el 9 de agosto de 1985, cuando todavía no se hablaba de computadores cuánticos, sino solo de los computadores del futuro, se indicó que las tres únicas limitaciones de estos computadores serían las siguientes:

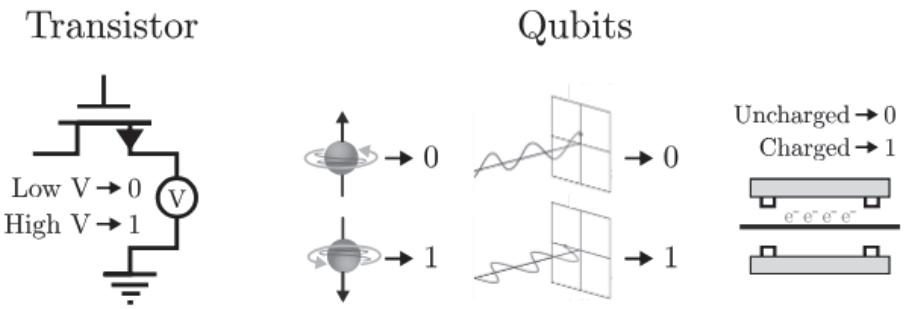
– Las limitaciones en tamaño al tamaño de los átomos.

– Los requisitos energéticos dependientes del tiempo, como los calculados por Bennet al estudiar la termodinámica de la computación. Las computadoras electrónicas degradan el trabajo en calor y la necesidad de eliminarlas establece un límite práctico para su desempeño. El estudio de la termodinámica de la computación, examinado en Bennett (1982), busca los límites en principio para la reducción de esta disipación. Dado que la disipación se reduce con el tamaño, las computadoras más eficientes termodinámicamente se buscan entre aquellas que usan moléculas individuales, cargas o dipolos magnéticos como dispositivos de almacenamiento de memoria.

– Una característica concerniente a la velocidad de la luz: no se puede enviar señales más rápidas que la velocidad de la luz.

Estas tres características que señala Feynman sobre los computadores del futuro se pueden utilizar y de hecho se han utilizado, para caracterizar las doce líneas disruptivas en *hardware*. En esta conferencia sobre los computadores del futuro, Feynman sugirió la posibilidad de almacenar 1 bit de información en un átomo y ello, al menos desde un punto de vista teórico es posible, aunque existen dificultades prácticas. El que 1 bit de información se pueda almacenar en un átomo, nos podría llevar a preguntarnos, si sería también posible almacenar un bit de información en un núcleo atómico. Un núcleo atómico es la parte central del átomo y se encuentra formado fundamentalmente por protones, partículas de carga positiva y por neutrones, partículas sin carga eléctrica o neutras. El tamaño del átomo medio es del orden de 10^{-10} m, o sea 0,1 nanómetros, aunque suele utilizarse como unidad el angstrom y así, el tamaño del átomo medio es de 1 angstrom. El tamaño del núcleo atómico es del orden de los 10^{-15} m, lo que es equivalente a 1 fermi y desde un punto de vista teórico, nada impediría tampoco que 1 bit de información pudiera ser almacenado en un núcleo atómico. Más problemático, sería considerar la posibilidad de almacenar 1 bit de información en un *quark*. Tanto los protones como los neutrones, se encuentran a su vez formados por partículas más elementales que se denominan *quarks*. En concreto, un protón se encuentra formado

FIGURA 2
COMPARACIÓN ENTRE BITS CLÁSICOS Y QUBITS, O BITS CUÁNTICOS



Fuente: www.brilliant.org

por 2 *quarks* de tipo u (*up*) y por un *quark* de tipo d (*down*). A su vez, un neutrón se encuentra formado por dos *quarks* de tipo d y por un *quark* tipo u. El radio del quark es menor que unos increíblemente pequeños 10^{-21} centímetros.

Ante la pregunta de si un bit de información pudiera ser almacenado en un *quark,* Feynman respondió que sí, pero que no se tenía control sobre los *quarks*, y que sería una forma de trabajar realmente impracticable, ya que habría tanta energía implicada en las interacciones entre *quarks* que sería muy peligroso manejarlos debido a la radioactividad y fenómenos semejantes. Podría pensarse ahora en la posibilidad de almacenar información en una partícula como el electrón, cuya dimensión es del orden de 10^{-20} m, de tal forma que el átomo medio, sería del orden de 10^{10} veces la dimensión del electrón y también, podría pensarse en utilizar fotones, es decir partículas de luz o cuantos de luz. Si se utilizasen fotones para almacenar información, se estaría hablando de la computación cuántica óptica.

Por tanto, la computación cuántica es diferente a la computación clásica y es que, desde un punto de vista teórico, en el caso de la computación cuántica podrían utilizarse átomos como componentes para implementar los "1s" y los "0s" cuánticos, incluso núcleos atómicos. Por lo que respecta a la teoría de la información, en el caso de la computación clásica, la unidad elemental de información es el bit, del inglés *binary digit*, que puede tomar dos valores: "1" o "0", es decir, "encendido" o "apagado", "nivel más alto de tensión" o "nivel más bajo de tensión", "paso de corriente" o "ausencia de paso de corriente".

Tal y como se representa en la figura anterior, por lo general, un bit se almacena en una computadora clásica utilizando un transistor que conduce una señal eléctrica, el estado 1 que representa "nivel alto de tensión", o no conduce, el estado 0 de "nivel de tensión bajo". Un *qubit* es similar, pero es un componente cuántico y no clásico: puede ser una partícula giratoria que puede apuntar hacia arriba o hacia abajo, un fotón que puede polarizarse vertical u horizontalmente, o un cable cuántico que está cargado ("encendido") o sin carga ("apagado"). Al igual que un bit clásico, las dos medidas posibles de un *qubit* tienen "1" o "0" asignado a un cierto giro, polarización o carga eléctrica. Con independencia del tipo de *qubit* ya sea un cable cuántico, un fotón o un átomo giratorio, se eligen los estados computacionales en función de las mediciones reproducibles que pueden hacerse, y se les da nombres especiales porque son estados cuánticos, no clásicos. Los dos estados medibles de un *qubit* se denominan $|0\rangle$ y $|1\rangle$. Hasta ahora, un *qubit* no es tan diferente de un bit clásico. Y, de hecho, un *qubit* puede hacer todo lo que hace un bit normal. En general, cualquier algoritmo que pueda ejecutarse con una computadora clásica también se puede llevar a cabo en una computadora cuántica construida a partir de *qubits*. Si bien el estado de un *qubit* aislado generalmente no cambiará, se puede cambiar un *qubit* de un $|0\rangle$ a un $|1\rangle$, a veces usando una descarga de electricidad, y otras usando un filtro o un destello de luz. Incluso se puede construir circuitos lógicos como sumadores a partir de muchos bits cuánticos que operan en *qubits* de entrada y crear salidas que pueden medirse. Pero la física cuántica, tiene una naturaleza probabilística. A veces, un estado puede estar en una combinación de dos estados, y nunca se puede estar seguro de lo que se medirá. Usando una descarga eléctrica diferente o incluso solo un filtro polarizador, es posible cambiar un *qubit* de un estado $|0\rangle$ a otro estado nuevo, un estado de superposición:

Un *qubit* es la implementación de un componente cuántico y, por lo tanto, se define por su función de onda:

$$|\psi\rangle = a \cdot |0\rangle + b \cdot |1\rangle$$

Los estados de superposición son una propiedad de la física cuántica que realmente distingue de lo que es capaz un *qubit* en comparación con un bit clásico. Un bit clásico solo puede existir en un estado "1" o "0", pero un *qubit* puede existir en cualquier combinación de los mismos, aunque solo se medirá en uno u otro:

$$|\psi\rangle = a \cdot |0\rangle + b \cdot |1\rangle$$

Los coeficientes a y b pueden ser cualquier número: no solo números enteros o números reales, sino incluso, cualquier número complejo. La magnitud relativa de estos dos coeficientes muestra cuánto se comporta este estado de superposición como $|0\rangle$ o como $|1\rangle$. Un *qubit* puede estar en todos los estados posibles, desde uno que tiene un 100% de posibilidades de ser medido $|0\rangle$ a uno que tiene un 100% de ser medido $|1\rangle$. Por ejemplo, se podría tener un *qubit* en el estado:

$$|\psi\rangle = 0{,}1 \cdot |0\rangle + 0{,}995 \cdot |1\rangle$$

La computación clásica se realiza cambiando los bits de "0" a "1" y viceversa con una serie de puertas y circuitos lógicos. La manipulación de *qubits* durante el cálculo utiliza puertas lógicas cuánticas que pueden modificar los coeficientes de una superposición, no solo cambiar el estado. Esto aumenta enormemente la densidad de información de un cálculo cuántico. Por esa razón pueden funcionar varios algoritmos cuánticos simultáneamente: cuando un *qubit* en superposición pasa a través de un circuito, el circuito opera en todos los estados simultáneamente, por lo que no requiere consultas separadas.

Se describen ahora los principios de física cuántica que confieren a la computación cuántica interesantes ventajas sobre la computación clásica, comenzando por la superposición. En el caso de la computación cuántica, la unidad más básica de información es ahora el *qubit* o *quantum bit*, con la gran diferencia con respecto al bit clásico, que el bit cuántico puede encontrarse en estado "1" o en estado "0" o bien en una superposición de ambos estados a la vez. Esto se debe a uno de los principales principios de la física cuántica que son aplicables a la computación cuántica. Se trata del principio de superposición. El principio de superposición es realmente importante puesto que si tres bits en computación clásica suponen 8 estados diferentes (2^3):

000,001,010,011,100,101,110,111

Esos 8 estados, se encuentran, debido a la superposición, en solo tres *qubits*, lo que nos da ya una primera idea de la potencia que puede tener la computación cuántica, mientras que para representar esos 8 estados simultáneamente se necesitarían 24 transistores. Si se añade un cuarto *qubit*, se tendrían 16 estados y con un quinto *qubit* 32 estados, de tal forma, que tanto los cálculos, como la información almacenada en un determinado instante de tiempo, crece de forma exponencial, en la forma 2^n, donde n es el número de *qubits*. Si se introduce un nuevo *qubit* en el chip se tendría: $2 \bullet 2^n = 2^{n+1}$, lo cual implica que un *qubit* adicional consigue duplicar el número de estados posibles, gracias a la superposición cuántica, y de esta forma, la computación cuántica, lo tendría muy fácil para asegurar el cumplimiento de la ley de Moore. Nótese que en computación clásica se tendría que doblar el número de transistores en el chip para doblar el número de estados posibles ("0" o "1") en un instante determinado de tiempo. Si se considerase p.ej., 50 bits en computación clásica se estaría hablando de 1.125.899.906.842.620 estados, o sea más de 1.125 billones de estados, que en computación cuántica se encuentran en tan solo 50 *qubits*. Esto significa, tal y como se ha mencionado al principio, que, para doblar el número de estados, no se necesita doblar el número de transistores para conseguir mejores prestaciones en el *hardware*, basta con implementar solamente un *qubit* adicional, asegurando con él la continuidad en el cumplimiento de la ley de Moore y por lo tanto el progreso en el *hardware*.

La superposición proviene de la dualidad onda-partícula de las partículas elementales de la física cuántica, tales como electrones, fotones, iones y átomos. Cada una es una función ondulatoria ψ de las probabilidades con respecto a su estado observable, como posición, espín, polarización para el caso de un fotón, o momento angular. Una partícula, o *qubit*, puede ocupar varios estados a la vez. Estos estados pueden "leerse" de forma muy parecida a la lectura de un bit de computación clásica como "0" o "1", pero un *qubit* tiene muchos más valores potenciales que corresponden a las probabilidades simultáneas de ser "0" o "1". Esa propiedad acelera exponencialmente el cálculo.

Una vez se dispone de la implementación de la unidad básica de información, es decir del bit o del *qubit*, es necesario construir a través de diversas puertas lógicas cuánticas, los circuitos cuánticos básicos que constituirán los computadores. En el caso de los computadores clásicos se trata de las clásicas puertas lógicas, OR, AND y NOT mediante las cuales se pueden construir los diferentes circuitos lógicos, con sus entradas y salidas, y cuya lógica responde al álgebra de Boole desarrollada en el siglo XIX. Esta electrónica lógica se implementa, por supuesto en sus correspondientes circuitos físicos, formados fundamentalmente por transistores. En el caso de la computación cuántica, se utilizarían fotones y puntos cuánticos si se considera la computación cuántica óptica. También es necesario mencionar, entre otras tecnologías que se describirán posteriormente, las trampas de iones y los superconductores.

Con respecto al entrelazamiento cuántico, está propiedad es la que permite que todos los *qubits* funcionen como un sistema. Así, en una computadora cuántica se usan estados entrelazados que implican muchos *qubits.* El entrelazamiento se produce cuando múltiples partículas sólo pueden ser descritas por un estado global, no individual. Esto es análogo a la lectura de un libro donde las páginas individuales no tienen sentido, pero donde la información surge una vez que se leen todas. Las computadoras normales luchan poderosamente para representar el entrelazamiento, lo que limita severamente su capacidad de simular sistemas cuánticos, como medicamentos farmacéuticos o materiales superconductores. Esta es una de las razones por las que se necesitan computadores cuánticos. (1)

Análogamente, en el caso de la computación cuántica, se contará con las correspondientes puertas lógicas cuánticas, entre otras, las puertas CNOT, Pauli, Hadamard, Toffoli o SWAP y es posible que se diseñen otras en el futuro. (2) Los *qubits* se entrelazan entre sí mediante estas puertas lógicas cuánticas que hacen que, p.ej., el espín de un *qubit* se entrelace con el de otro, de forma que los detalles vengan establecidos por el programa que esté ejecutando la máquina. El proceso continúa, pero el programa está diseñado con esmero para que, al terminar, los *qubits* vuelvan a estar desentrelazados, es decir recuperen estados simples, como arriba o abajo ("0" o "1"). El estado final de todo el conjunto arroja el resultado de la computación, que se puede leer realizando mediciones sobre los *qubits*. De momento, no está claro cómo interpretar mejor la ventaja computacional que ofrece el entrelazamiento. Una propiedad es que como cualquier *qubit* puede aportar a la vez un "0" y un "1" a cualquier estado dado, cada vez que se introduce un nuevo *qubit* en la computadora, se genera una cantidad verdaderamente descomunal de contribuciones (p.ej., 2^{100} = 1267 mil cuatrillones para tan solo 100 *qubits*). En ciertos aspectos, la computadora cuántica funciona como una cantidad inmensa de computadoras clásicas que calculan todas a la vez. Sin embargo, esta imagen no capta todo lo que está pasando, porque cada parte suelta de cualquier cálculo cuántico de ese tipo no puede ser completamente independiente, y además hay que volver a unirlas, o sea, hacer que interfieran entre sí, antes de obtener un resultado significativo. (3)

A partir de aquí, es posible construir subsistemas y sistemas, ya sean clásicos o cuánticos, pero para ello y en el caso de la computación cuántica, será también necesario el desarrollo de nuevos algoritmos cuánticos, es decir *el software*. El computador cuántico, no podrá, en principio, operar en condiciones ambientales, de ahí que el modelo que se plantee para su utilización, sea el modelo SaaS (*Software as a Service*).

Uno de los conceptos que es más importante señalar es que si las operaciones que se implementan con las puertas lógicas clásicas y los bits responden al Álgebra de Boole, las puertas lógicas cuánticas y los *qubits* responden al álgebra matricial. No es objeto de este trabajo introducir cálculos matemáticos matriciales, aunque sean sencillos, sino únicamente comprender lo que hacen las puertas lógicas cuánticas con los *qubits* de una forma análoga a lo que hacen las puertas lógicas clásicas con los bits.

Considerando ahora las puertas de un *qubit* y recordando que en lugar de bits tenemos que volver a usar *qubits*, que son una mezcla de "1" y "0": un qubit era a·|0> + b·|1>, lo que quiere decir que hay una probabilidad $|a|^2$ (es decir, el cuadrado del módulo de a) de que valga 0, y una probabilidad $|b|^2$ (es decir, el cuadrado del módulo de b) de que valga 1.

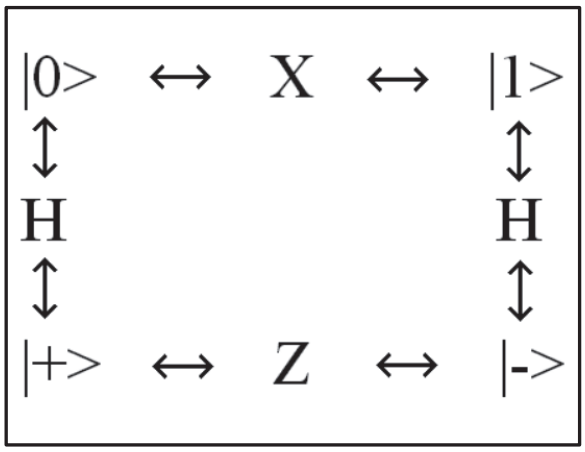
La puerta I (identidad) deja en la salida lo mismo que en la entrada: si entra el *qubit* a ·|0> + b ·|1>, se obtiene en la salida el *qubit* a·|0> + b·|1>, es decir, el mismo, sin cambiarlo. Esta puerta es la equivalente a la puerta SI en computación clásica, y es incluso menos útil que allí. Solamente se usa para hacer demostraciones matemáticas.

La puerta X (*bit flip*) es la equivalente a la puerta NO. Si el *qubit* de entrada es |0>, el de salida es |1>, y viceversa. Si el *qubit* que entra es el *qubit* general a·|0> + b·|1>, el de salida será a·|1> + b·|0>, o escrito de la forma más usual, b·|0> + a·|1>. El nombre alternativo de esta puerta, *bit flip*, se debe a que "cambia" (*flip*) los bits, es decir, donde había un 0 pone un 1 y donde había un 1 pone un 0, exactamente como hacía la puerta NO en computación clásica. La puerta intercambia las probabilidades de tener un 1 y de tener un 0; si al principio teníamos un 90% de probabilidades de tener un 0, y un 10% de tener un 1, ahora tendremos un 90% de probabilidades de tener un 1 y un 10% de probabilidades de tener un 0.

La puerta Z (*phase flip*) Si el *qubit* que entra es un |0> no hace nada, pero si el que entra es un |1> le cambia el signo, y en la salida tenemos un -|1>. En general, si entra un *qubit* a·|0> +b· |1>, sale un *qubit* a·|0> - b|1>. Esta puerta no tiene un equivalente clásico. De hecho, lo más parecido a un equivalente clásico sería la puerta SI, igual que la identidad. El nombre en inglés de esta puerta, *phase flip*, se debe a que cambia la "fase" (para los físicos: la fase relativa de cada estado; para los no físicos: el signo) del *qubit*. Esta puerta no cambia las probabilidades de que al medir el *qubit* hallemos un 0 o un 1: el valor a lo deja sin cambiar, por lo que la probabilidad de medir un 0 sigue siendo la misma $|a|^2$; el valor b lo cambia por su opuesto… pero el cuadrado de su módulo sigue siendo el mismo, por lo que la probabilidad sigue siendo $|b|^2$. Es como si no cambiara nada, parece inútil la puerta, entonces… pero es que la fase (el signo) se puede utilizar en los cálculos.

La puerta H (puerta de Hadamard) convierte el *qubit* |0> en el *qubit* |+> (que es solamente una forma fácil de llamar al *qubit* 1/√2 ·|0> +1/√2 ·|1>) y el *qubit* |1> en el qubit |-> (que igual que el |+> es una forma fácil de llamar a otro *qubit*, en este caso el 1/√2 ·|0> -1/√2 ·|1>, es decir, igual que el |+> pero con el signo cambiado). Esta puerta es muy importante, ya que tiene muchísimas aplicaciones en muchos circuitos; casi no hay ningún algoritmo cuántico que no la use. La transformación del *qubit* general es complicada a primera vista, pero no es más que combinar lo anterior: el *qubit* a·|0> + b·|1> se convierte en (a+b)/√2 ·|0> +(a-b)/√2 ·|1>, pero lo bueno es que este *qubit* escrito usando |+> y |-> se vuelve mucho más simple: a·|+> +b·|->, como se podía esperar de la definición del principio.

FIGURA 3
LA CASI MÁGICA RELACIÓN ENTRE X, Z Y H



Fuente:https://eltamiz.com/elcedazo/2014/04/05/computacion-cuantica-iii-las-puertas-logicas-de-un-qubit/

Estas son las puertas más importantes de un *qubit*, y además las que sólo necesitan números reales para definirse. Hay una relación muy bonita además entre las puertas X, Z y H y los *qubits* |0>, |1>, |+> y |->: (4)

Una puerta X convierte un *qubit* |0> en un *qubit* |1> y viceversa, mientras que la H convierte el |0> en |+> y el |1> en |->. Pero si se piensa un poco en cómo funcionan las puertas Z y H se verá que Z convierte |+> en |-> (y viceversa), y que H funciona también en sentido inverso, convirtiendo |+> en |0> y |-> en |1>. Esto es importante a la hora de diseñar algoritmos.

Hay otras puertas de un *qubit*, pero son mucho menos utilizadas y, además, en general necesitan números complejos Principalmente son cuatro; se usan en algunos algoritmos:

– La puerta Y. Ésta ni tiene nombre propio siquiera, pero complementa a las puertas I, X y Z. Si a la entrada se pone el *qubit* a·|0> + b·|1>, a la salida se obtiene b|0>-a|1>, por lo que funciona como una combinación de las puertas X y Z.

– La puerta S (*phase gate*, no confundir con *phase flip*). Cambia a·|0> + b·|1> por a·|0> + a·|0> + b i |1>. Si se aplica dos veces seguidas la puerta S se obtiene una puerta Z, como se puede comprobar fácilmente.

– La puerta T (puerta $\pi/8$, "pi octavos"). Cambia a·|0> + b·|1> por a·|0> + b·$\frac{1+i}{\sqrt{2}}$·|1>. Si se aplica dos veces se obtiene una puerta S.

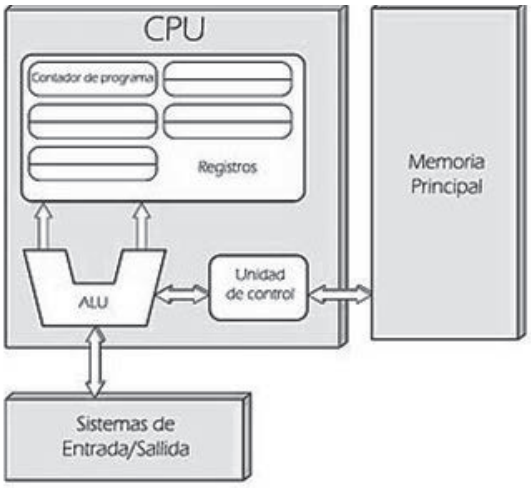
– La puerta R (*phase shift*, no confundir con *phase flip* ni *phase gate*) – Cambia a·|0> + b·|1> por a·|0> +b·$\frac{\cos\theta+\sin\theta}{\sqrt{2}}$·|1>, donde θ es un ángulo cualquiera que se le da externamente. Puede simular tanto la puerta Z, como la S, como la T y es muy importante en la llamada Transformada de Fourier Cuántica (QFT, por sus siglas en inglés).

La puerta general, escrita normalmente como U, no es ninguna puerta en particular, es solamente una notación para llamar a cualquier puerta de un *qubit*, sea de las que se han visto o no. Resulta útil en algunos circuitos en los que hay una parte que no se especifica, porque según el uso que se le dé será de una manera o de otra; en esos casos se utiliza esta puerta. Y hasta aquí las puertas lógicas de un *qubit*. Resumiendo, las puertas siempre tienen que tener el mismo número de entradas que de salidas, y con el funcionamiento de la relación entre X, Z y H y |0>, |1>, |+> y |->, se tiene ya todo lo que se necesita para continuar.

Tal y como se ha descrito, las puertas lógicas clásicas se implementan con elementos no lineales como los transistores. En el caso cuántico, las puertas lógicas deben representarse mediante operadores unitarios U que se consiguen en la práctica con interacciones reversibles entre los elementos cuánticos. En el caso cuántico no sólo se actúa sobre dos posibles estados del bit, sino sobre los infinitos estados del *qubit* que se derivan de las diferentes probabilidades de los estados $|0\rangle$ y $|1\rangle$ que derivan de su función de onda. Existen 4 puertas unarias, de las cuales sólo dos son reversibles, la identidad y la puerta NOT.

Todas las puertas lógicas clásicas son susceptibles de ser implementadas también cuánticamente. La extensión de las puertas lógicas a la teoría cuántica se debe a David Deutsch (1985). Otra puerta cuántica relevante es la de Hadamard, en honor al matemático francés Jacques Hadamard. Esta puerta mezcla los estados equiprobablemente, poniéndolos como suma y diferencia. Las puertas de múltiples *qubits*, las más sencillas de las cuales son las puertas binarias, aunque su implementación en el laboratorio es extremadamente difícil, pues hay que poner en interacción controlada dos *qubits* espacialmente separados. Cirac y Zoller lo hicieron con iones fríos en una trampa lineal. De las puertas binarias se puede destacar la puerta NOT-controlado, CNOT, en don-

FIGURA 4
ARQUITECTURA DE VON NEUMANN



Fuente: Wikipedia

de se distingue el primer *qubit* como de control y el segundo como blanco. Si el primer *qubit* es 0 el segundo se deja intacto, y si es 1, se cambia. La puerta CNOT se puede implementar con una molécula de cloroformo $CHCl_3$. Su estado corresponde a los estados de espín de los núcleos de carbono e hidrógeno, que invierten su sentido mediante pulsos de ondas de radio. Siempre es posible asegurarse que el núcleo de hidrógeno invierte su espín sólo cuando el espín del núcleo de carbono apunta hacia arriba (el núcleo de carbono sería el control y el de hidrógeno la puerta XOR). Nótese que la puerta XOR clásica sería irreversible (no invertible), dado que su tabla de verdad no nos permite, conociendo el resultado, deducir los estados iniciales. Se produce pérdida de información. En cambio, como puerta cuántica unitaria siempre será invertible. La puerta CNOT es de gran importancia, ya que cualquier puerta de múltiples *qubits* puede ser construida mediante la puerta CNOT y puertas cuánticas monarias.

En los años 80 Tommaso Toffoli y Edward Fredkin vieron que hacía falta un mínimo de tres *qubits* para cualquier computación clásica. La extensión a tres *qubits* de la puerta CNOT es la llamada puerta de Toffoli o CCNOT. En este caso hay dos bits de control que sólo actúan si están a 1. Esta puerta se suele usar para simular puertas clásicas irreversibles y demostrar que cualquier computador cuántico puede hacer lo mismo que uno clásico. Entre su singularidad está el que en sus tripas está una de las puertas clásicas más importantes, la puerta NAND (NOT AND). Otra puerta interesante es la que intercambia los estados de dos *qubits*, en el caso binario es la puerta intercambiadora o SWAP y en el ternario se denomina intercambiador controlado o puerta de Fredkin (5).

En cuanto a las arquitecturas, la arquitectura de un computador clásico, es la arquitectura de Von Neumann. De esta forma, un computador clásico, tal y como puede verse en la figura siguiente, se encuentra formado por una CPU o unidad central de proceso, compuesta a su vez por una unidad aritmético-lógica (ALU) y por la unidad de control. Además, hay que tener en cuenta la memoria principal, así como los sistemas de entrada/salida o input/output.

A pesar de todas las diferencias que existen entre la física clásica y la física cuántica, parece ser que las conclusiones con respecto a la computación cuántica son que vuelve a validarse la arquitectura de Von Neumann que había sido utilizada en la computación clásica. Además de la arquitectura de Von Neumann, en computación clásica una de las técnicas que ha venido siendo utilizada para aumentar la velocidad de proceso es la computación paralela y de esta forma, la gran cantidad de operaciones que requeriría la solución de un problema real, p.ej., mediante la aplicación del método de elementos finitos, con cientos o miles de nodos y de ecuaciones, haría en muchas ocasiones necesaria la implantación del programa sobre arquitecturas paralelo. La ganancia de velocidad que se obtendría ejecutando el programa sobre una arquitectura paralelo viene dada por la ley de Amdahl:

$$S_p = \frac{1}{\left(R + \frac{(1-R)}{N}\right)}$$

Donde S_p es la ganancia de velocidad, R es la fracción del código del programa que no puede ser ejecutada en paralelo y N es el número de procesadores en paralelo utilizados. Es fácil ver a partir de la ecuación anterior que sí $R = 0$, esto es, que si todo el código puede ejecutarse en paralelo, la máxima ganancia de velocidad que podría obtenerse coincidiría con el número de procesadores que se han implementado en paralelo, esto es:

$$S_p = N$$

Pero gracias a la superposición y al entrelazamiento cuántico, la computación cuántica promete un procesamiento paralelo instantáneo por medio del cual será posible resolver problemas hasta ahora lejos del alcance del ser humano (6), pudiéndose realizar 2^n cálculos al mismo tiempo, lo último en procesamiento paralelo. Ciertos problemas que una supercomputadora convencional tardaría años en resolver, podrían descifrarse en una fracción de segundo. (7) Para que esto sea realidad, además del avance teórico de los algoritmos y del conocimiento de las propiedades cuánticas, se necesita un material que haga las funciones del silicio en la computación clásica, es decir, pueda generar y procesar los unos y los ceros propios de la computación.

Desde un punto de vista teórico se ha mencionado a los átomos, y a los núcleos atómicos, incluso a los electrones y a los fotones, como posibles componentes cuánticos. Sin embargo, actualmente y desde un punto de vista práctico, para la construcción de computadores cuánticos, parece que la cita original de Feynman del año 1959: "*There is plenty of room at the bottom*" y que hace referencia, en última instancia, a que no existe nada en las leyes de la física que impida manejar los objetos átomo a átomo, debería ser modificada. Nuevas observaciones conducen actualmente a una modificación de aquella cita por esta otra: "*There is plenty of room in the middle*" y hace referencia a la viabilidad actual de construir computadores cuánticos a partir de componentes de tamaños algo mayores a los de los átomos, entre los 5 y los 50 nanómetros. Es lo que se denomina la computación cuántica topológica ya que es necesaria la estabilidad de los *qubits* y para ello, es necesario implementarlos actualmente en objetos cuánticos más grandes que los átomos, que los núcleos atómicos, que los fotones y que los electrones. Según Chad Orzel, el objeto más grande que se ha comprobado que sigue mostrando propiedades cuánticas ascendería a un millón de electrones. Por lo tanto, se está hablando de dimensiones del orden de $10^{6} \cdot 10^{-20} = 10^{-14}$ m. Según Bruce Rosenblum y Fred Kuttner, la teoría cuántica no impone límites. El tamaño de los objetos susceptibles de evidenciar efectos cuánticos, parece restringido sólo por la tecnología y el presupuesto. (8)

En efecto, muchos de los problemas de los computadores cuánticos, están relacionados con el hecho de que hay que manipular átomos individuales, que son muy susceptibles a las perturbaciones del medioambiente y, por lo tanto, una posible solución es utilizar objetos un poco mayores. Actualmente, se estaría hablando e incluso utilizando, en algunos casos, para la construcción de los computadores cuánticos, de las trampas de iones y de los bucles superconductores basados en la unión de Josephson. Otras opciones como el grafeno, los nanotubos de carbono, los puntos cuánticos, etc. se encuentran también dentro de los posibles componentes cuánticos.

EL ESTADO DEL ARTE Y PRINCIPALES DESAFÍOS PARA EL DESARROLLO DE LA COMPUTACIÓN CUÁNTICA

A pesar del gran esfuerzo y avance que se está realizando en computación cuántica, podría afirmarse que su estado de desarrollo sería similar al estado de desarrollo de la computación clásica en los años 50, cuando ésta se encontraba basada en los típicos armarios cuyo componente fundamental eran las válvulas de vacío, con necesidades especiales de refrigeración, al igual que sucede hoy en día con los computadores cuánticos y con fallos que se producían por su calentamiento excesivo y por los típicos bugs, aunque no se refieren en este caso a los errores de programación en el caso de desarrollo de software, sino a que literalmente un insecto podía interferir en el funcionamiento de un relé. En efecto, aunque la computación cuántica se encuentra todavía muy lejos de sustituir a la computación clásica, de hecho, lo más probable es que ambas coexistirán durante mucho tiempo, no es menos cierto que ya existen computadores cuánticos comerciales. La industria tecnológica está muy lejos de la democratización de la tecnología de computación cuántica. Lian Jye Su, analista principal de inteligencia artificial y aprendizaje automático de ABI Research, opina que "la computación cuántica definitivamente no está ni remotamente cerca de la etapa de implementación comercial a gran escala". (9)

D-Wave Systems, una empresa canadiense ha instalado más de 50 millones de dólares en sistemas cuánticos en las instalaciones de sus clientes. El sistema D-Wave 2000Q está disponible para su venta o arrendamiento como un sistema independiente, o a través de su nube cuántica. También prestan servicios de aprendizaje automático, servicios de desarrollo de aplicaciones y fabricación personalizada de circuitos superconductores y han desarrollado ya docenas de prototipos de aplicaciones y herramientas de software, muchas de las cuales han sido publicadas y presentadas en conferencias y foros de usuarios. La computación cuántica no revolucionará a corto plazo la informática en los hogares ni en las oficinas, pero podría catalizar avances científicos que influirían enormemente en el desarrollo tecnológico. La razón de que actualmente la computación cuántica se encuentre limitada al entorno profesional en centros de cálculo, es que lo más parecido que existe actualmente a un computador cuántico es una nevera gigante cuyo interior está a temperaturas bajas. Parece previsible que el modelo de negocio de la computación cuántica se oriente, al menos inicialmente, más hacia un modelo de software como servicio (SaaS), que hacia un modelo de negocio basado en la venta de *hardware* (10), sobre todo en lo referente a la electrónica de consumo. En el ámbito de la electrónica profesional es probable que como sucede con los clientes de D-wave Systems se comercialicen sistemas basados en computación cuántica.

Un computador cuántico es una máquina que, a diferencia de uno convencional, basa su funcionamiento en fenómenos cuánticos. Se trata de fenómenos naturales que no pueden ser explicados por la física convencional; su explicación requiere de una teoría alternativa, la física cuántica, capaz de explicar satisfactoriamente lo que ocurre en la estructura básica de la materia, es decir en los átomos. Pese a lo que pudiera parecer, estos fenómenos se manifiestan en nuestra vida diaria. Gracias a ellos, podemos explicar, por ejemplo, por qué un objeto es sólido, las propiedades físicas de los materiales o los colores. Mientras que un computador clásico representa los datos como secuencias de unos y ceros, es decir bits, los ordenadores cuánticos como ya se ha mencionado, lo hacen con *qubits*. La posibilidad de construir un computador cuántico se remonta a 1982, a partir de las investigaciones del célebre físico Richard Feynman, el primer científico en concebir esta clase de computadores. En la actualidad su diseño está todavía en sus primeros pasos. Hasta la fecha se han realizado algunos experimentos con unos pocos *qubits*. También se han diseñado simuladores que emulan esta clase de computadores con otros convencionales, pero para que uno convencional pueda ejecutar un algoritmo cuántico, necesita una gran memoria y una gran capacidad de cálculo, además de otras prestaciones de *hardware*.

En el año 2011 la empresa canadiense D-Wave Systems anunció la venta del primer computador cuántico comercial, bautizado como D-Wave One. Según la empresa su ordenador disponía de un microprocesador de 128 *qubits*. Ese mismo año un equipo de investigadores de Estados Unidos, China y Japón anunció que esta clase de computadores pueden construirse según el modelo clásico de arquitectura de Von Neumann. En 2012, la empresa IBM anunció que también había realizado avances significativos hacia la construcción de una máquina de estas características. Más de medio siglo después, se repite aparentemente el mismo escenario que tuviera lugar tiempo atrás con ENIAC, Colossus y los otros ordenadores. Sin embargo, esto no es del todo así, ya que la construcción de un computador cuántico es un proyecto con tantas dificultades que en esta ocasión investigadores de distintos países han aunado esfuerzos, formando equipos multinacionales y dejando así atrás, como antaño, la competencia entre países. Entre sus aplicaciones, además de la criptografía, se espera que puedan realizarse experimentos de simulación con gran realismo, por ejemplo, las interacciones de los medicamentos en el cuerpo humano, la realización de cálculos en áreas como la física, la química o la astronomía, o su aplicación a problemas matemáticos de cierta envergadura, como es la factorización de grandes números.

Aunque por ahora sea una mera curiosidad, también hay varias versiones cuánticas del Juego de la Vida de Conway. Más aún, en la actualidad han sido propuestos varios modelos de redes neuronales artificiales, cuyas neuronas están simuladas con puertas cuánticas, lo que abre la puerta a futuras investigaciones de lo que podría denominarse como inteligencia artificial cuántica. Otra de las aplicaciones es la obtención de números aleatorios que sean verdaderamente aleatorios, como si tales números hubieran sido obtenidos con un bombo de lotería. De hecho, ya es posible obtener números aleatorios a partir de fenómenos cuánticos a través de Internet (11).

El potencial de la computación cuántica es innegable, pero su despliegue también se puede ver frenado por ciertos obstáculos. Los expertos de Microsoft apuntan que uno de los mayores desafíos para construir una computadora cuántica son las exigencias que plantea el entorno de los *qubits*. "Un sistema cuántico sólo puede permanecer en un estado cuántico cuando no está siendo perturbado, por lo que las computadoras cuánticas están diseñadas para entornos increíblemente fríos y únicos. Es por eso que se están enfocando en *qubits* topológicos, ya que creen que son más capaces de soportar desafíos como el calor o el ruido eléctrico, lo que les permite permanecer en un estado cuántico por más tiempo. Eso, a su vez, los hace mucho más prácticos y efectivos", explican. En este sentido, incidir en que la computación requiere una temperatura de enfriamiento "menor que la que existe en el espacio exterior", además de exigir mucho espacio para su correcto funcionamiento. Por este motivo, no vale con desarrollar procesadores de muchos *qubits* para conseguir el éxito. De hecho, cuantos más *qubits*, mayor es la probabilidad de error. Además de crear un entorno óptimo para evitar la incidencia de las condiciones ambientales, es fundamental desarrollar sistemas capaces de autochequearse y corregir los posibles errores, permitiendo la fiabilidad y estabilidad de los resultados. De este modo, la responsable de Altim considera que "será difícil que en el corto plazo se aplique como la computación normal", ya que "es difícil que tenga la movilidad o que sea accesible a todos en su versión *'on premise'*".

El principal desafío que existe para la construcción de un computador cuántico es la decoherencia. La decoherencia se refiere a la pérdida de las propiedades cuánticas de los computadores cuánticos. Como se ha mencionado, los *qubits* deben encontrarse entrelazados entre sí y tener propiedades como la superposición y la decoherencia provoca que pierdan estas propiedades. Además, un computador cuántico exitoso tiene que reunir una serie de características que lo equiparen con una máquina clásica. El físico teórico David P. DiVincenzo publicó en el año 2000 una lista de criterios que un computador cuántico tiene que cumplir para ser de utilidad. Consta de siete puntos, de los cuales los cinco primeros se refieren a la computación en sí, mientras que los dos últimos

son necesarios para la comunicación entre dos máquinas distintas. Son los siguientes:

1. El sistema tiene que ser escalable, con *qubits* bien caracterizados: si no lo es, cualquier diseño tendrá que ser repensado desde cero en cuanto se requiera un computador cuántico con más *qubits*. Esto contrasta con el caso de un computador clásico, que permite crear un computador más potente simplemente añadiendo transistores: no hace falta idear un diseño radicalmente distinto cada vez que se quiera aumentar su capacidad de proceso.

2. Tiene que ser posible preparar un estado inicial genérico, como el |00000…>. Si no, será imposible introducir datos con el computador y esto será completamente inútil.

3. Los tiempos de decoherencia deben ser mínimamente largos para poder realizar un número suficiente de operaciones aprovechando el entrelazamiento cuántico.

4. Se necesita un conjunto universal de puertas cuánticas, es decir, se tiene que poder fabricar una variedad suficiente de puertas cuánticas para permitir cualquier operación lógica. Normalmente basta con dos: la puerta de Hadamard, que equivale a una rotación del estado cuántico, y el no controlado que invierte uno de los *qubits* basándose en el estado del otro.

5. Se requiere una forma de medir los *qubits*, sin la que sería posible extraer la información procesada por el computador.

6. Tiene que haber un sistema para convertir *qubits* almacenados en *qubits* mensajeros, es decir, tiene que existir un mecanismo para transmitir información. Esto es crítico, si se quiere realizar computación distribuida o sencillamente enviar datos a otro lugar.

7. Es necesario que los *qubits* transmitidos lo hagan de forma fidedigna, por la misma razón que en el punto anterior.

Un computador cuántico con aplicaciones prácticas tiene que cumplir todos los requisitos de DiVicenzo o, de lo contrario, habrá fallos fundamentales en su construcción que impedirán su uso. A pesar de que todas las condiciones son perfectamente razonables, dar con un diseño que las cumpla todas es una tarea difícil (12). La capacidad de un computador cuántico aumentará exponencialmente a medida que crezca el número de *qubits* que integre, si bien, a mayor número de *qubits*, mayores dificultades habrá para mantener la coherencia cuántica. Es necesario señalar también con respecto a la computación cuántica, que se ha estimado que una computadora cuántica de 150 o 300 *qubits* tendría la misma capacidad de cálculo que todas las computadoras del mundo juntas. (13)

CONTRIBUCIÓN DE LAS EMPRESAS TECNOLÓGICAS A LA COMPUTACIÓN CUÁNTICA

Se describen a continuación los principales desarrollos acometidos por las empresas que más están contribuyendo al desarrollo de la computación cuántica, principalmente las grandes empresas tecnológicas con independencia de que la computación cuántica pueda ser un terreno importante para la colaboración con pequeñas empresas y con *start-ups* de base tecnológica.

IBM

IBM creó Quantum Experience –o Q Experience- en 2016 (14). Se trata de una plataforma accesible a todo el mundo desde la nube que permite a los usuarios hacer experimentos para probar sus teorías, aprovechando el potencial de un procesador cuántico de cinco *qubits*. Un año después, puso a disposición de los usuarios un procesador de 20 *qubits*, a la par que anunciaba la nueva generación de ordenadores cuánticos IBM Q, con la construcción del primer prototipo de procesador de 50 *qubits*. Además, la compañía ofrece QISkit, un kit de desarrollo de software de código abierto para programar y ejecutar ordenadores cuánticos. IBM consideraba que se puede duplicar el número de *qubits* cada 8 meses, como recogía Nextbigfuture.com. Siguiendo esta proyección, se hubiera llegado a 400 *qubits* a finales de 2019.

Microsoft

Microsoft señala que "ha estado trabajando constantemente para crear una máquina cuántica de propósito general escalable durante más de una década, adoptando una estrategia distinta dentro de la industria: la búsqueda de una tecnología escalable y tolerante a fallos, conocida como informática cuántica topológica". La empresa apuesta por un desarrollo "integral". "Desde *hardware* hasta sistemas de control y herramientas de desarrollo y programación, están adoptando un enfoque *full stack*, con el objetivo de hacer que el poder de la computación cuántica sea accesible para el conjunto más amplio de usuarios y clientes. Su programa depende de tres pilares clave: construir una computadora cuántica usando un enfoque topológico revolucionario, aprovechando los *qubits* topológicos confiables, escalables y tolerantes a fallos, que permiten cálculos cuánticos más largos y potentes; diseñar un nivel de control criogénico único, con una extremadamente baja disipación de potencia y calor para controlar de manera eficiente un sistema cuántico a gran escala; y el desarrollo de una completa compilación de *software* para permitir la programación de la computadora cuántica y el control del sistema a escala", desgranan los expertos de Microsoft.

Intel

Por su parte, Intel firmó en 2015 un acuerdo de colaboración con QuTech, el instituto de investigación cuántica de la Delft University of Technology (Holanda). Esta alianza abarca todo el sistema cuántico, desde procesadores *qubit* hasta la arquitectura de *hardware* y *software* precisa para controlar dichos dispositivos. Fruto de la misma, primero presentó un chip de 17 *qubits*. Y después logró desarrollar un procesador de 49 *qubits*. Además, está comenzando a probar el chip más pequeño para la computación cuántica. Se trata de '*spin qubit*', con *qubits* de alrededor de 50 nanómetros de diámetro y un tamaño más pequeño que la goma de borrar de un lápiz.

Google

Google también ha presentado Bristlecone. Se trata de un procesador cuántico de 72 *qubits*. Además, la compañía trabaja codo con codo con la NASA en el desarrollo del ordenador cuántico D-Wave. La actual versión de esta computadora cuántica, el D-Wave 2000Q, cuenta con 2048 *qubits*. Recientemente afirmó haber conseguido la supremacía cuántica publicando un artículo que posteriormente fue retirado, mientras que IBM negó que se hubiera llegado a conseguir.

Efectivamente son fundamentalmente las grandes empresas tecnológicas las que se encuentran involucradas en el desarrollo de la computación cuántica y además se encuentran con grandes dificultades para encontrar PYMES proveedoras de componentes cuánticos, al tratarse de una tecnología muy complicada. En efecto, no se trata de un terreno sencillo para las PYMES ni para las *start-ups*, entre las cuales se podría mencionar a Rigetti Computing con sede en Berkeley, California, de circuitos cuánticos integrados utilizados para computadoras cuánticas. La compañía también desarrolla una plataforma en la nube llamada Forest que permite a los programadores escribir algoritmos cuánticos (15) e IonQ, una compañía de *hardware* y *software* de computación cuántica con sede en College Park, Maryland, cuyos computadores cuánticos se basan en trampas de iones. Están desarrollando una computadora y *software* de iones cuánticos atrapados de uso general para generar, optimizar y ejecutar circuitos cuánticos. (16)

CONCLUSIONES

Entre las principales aplicaciones de los computadores cuánticos, se encontrarán la simulación de sistemas complejos, sistemas que actualmente y debido a la gran cantidad de variables y de datos involucrados, no pueden ser simulados mediante computadores clásicos en tiempos razonables, ni con resultados suficientemente fiables. Por ello, los computadores cuánticos, serán la tecnología que acuda al rescate, aportando mejoras drásticas a la capacidad de proceso de los computadores clásicos. Además, no es solo que los computadores cuánticos sean mucho más rápidos que los computadores clásicos en cuanto a velocidad de proceso, es que serán capaces de realizar tareas que son imposibles, incluso en un principio, para los computadores clásicos. Sin embargo, la computación clásica no es probable que desaparezca, al menos, en el corto plazo. Además, en un principio, el computador cuántico no podrá operar en condiciones ambientales, por lo que el verdadero salto no se producirá hasta que esta nueva tecnología se vuelva, al igual que la computación clásica, ubicua, con independencia de que la computación cuántica pueda usarse a través de la nube en la modalidad SaaS (*Software as a Service*).

"Es un mercado potencial de más de 50.000 millones de euros", asegura Paul Bunyk, uno de los líderes de D-Wave, la primera compañía en vender ordenadores cuánticos en el planeta. Portada de Time, cada una de sus máquinas cuesta 15 millones de euros. Llevan 30 años en este negocio, la otra vía frente a los computadores clásicos. Anuncian una nueva generación de sus aparatos, el salto definitivo, esperan. Estas máquinas cuánticas funcionan de otro modo. No usan los bits tradicionales basados en el lenguaje binario de unos y ceros, sino que como se ha explicado, utilizan cúbits o *qubits* que funcionan de modo tan distinto que se puede decir que actúan en un estado de superposición subatómico. Lo que, simplificando mucho, significa que pueden ser ceros y unos al mismo tiempo. Es la clave para dominar la tecnología del futuro. Por ello, Europa va a invertir 1.000 millones en su programa para desarrollar la tecnología cuántica. China, entre 10.000 y 50.000 millones. Rusia no se quiere quedar atrás y se estima que dará a sus científicos entre 500 y 2.500 millones en los próximos años. ¿Es posible la derrota del computador clásico tan pronto? Muchos discrepan. Alexei Fedorov, uno de los prodigios rusos, cree que lo anunciado por Neven es sencillamente alentador. "Pero nadie puede aún garantizar nada. Eso sí, la supremacía cuántica está muy cerca. Sin duda". (17)

■ **Juan Miguel Ibáñez de Aldecoa Quintana**

NOTAS

(1) https://scientificclan.com/la-investigacion-cuantica-basica-transformara-la-ciencia-y-la-industria/
(2) https://www.xataka.com/investigacion/que-estado-actual-se-encuentra-computacion-cuantica-que-podemos-espera
(3) Cuántica. Jim Al-Khalili. Alianza Editorial.
(4) https://eltamiz.com/elcedazo/2014/04/05/computacion-cuantica-iii-las-puertas-logicas-de-un-qubit/
(5) http://www.fisicafundamental.net/misterios/computacion.html
(6) https://cuonda.com/universo-paralelo/242-los-materiales-topologicos-y-la-computacion-cuantica-universo-paralelo-18072018
(7) Cuántica. Jim Al-Khalili. Alianza Editorial.
(8) El enigma cuántico. Bruce Rosenblum y Fred Kuttner.
(9) IT Reseller nº 53 Febrero de 2020.
(10) https://lapastillaroja.net/2016/09/computacion-cuantica/
(11) www.randomnumbers.info
(12) Las tecnologías cuánticas. La física que revolucionará las máquinas. Eduardo Arroyo.
(13) https://www.esquire.com/es/tecnologia/a28317511/fisica-cuantica-para-entenderla-por-fin/
(14) https://quantum-computing.ibm.com/
(15) https://en.wikipedia.org/wiki/Rigetti_Computing
(16) https://en.wikipedia.org/wiki/IonQ
(17) https://www.neotrading.es/el-sorpasso-cuantico-ya-esta-aqui

REFERENCIAS

NEREID. NanoElectronics Roadmap for Europe. From Nanodevices and Innovative Materials to System Integration. https://www.nereid-h2020.eu/roadmap

Turing. La computación. Pensando en máquinas que piensan. RBA

Las tecnologías cuánticas. La física que revolucionará las máquinas. Eduardo Arroyo

Simulando la física con los computadores. Richard P. Feynman

Cuántica. Jim Al-Khalili. Alianza Editorial