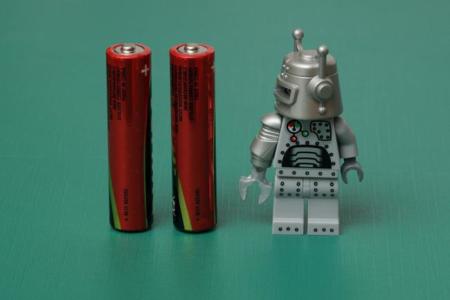
**LA COMPUTACIÓN CUÁNTICA EN LA PRÁCTICA: LOS RETOS A SUPERAR PARA CONVERTIR TEORÍA EN REALIDAD.**



**INTRODUCCIÓN**

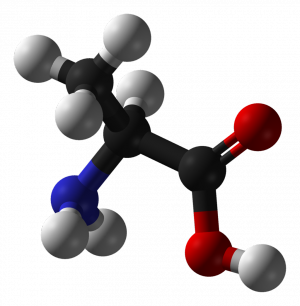
Hasta hoy se ha visto que la superposición de estados y entrelazamiento permite hacer varias operaciones al mismo tiempo sobre un *qubit.* Esto es lo que le ha dado a la computación cuántica ese potencial exponencial.

**¿QUÉ USAMOS PARA LOS QUBITS?**



En la computación tradicional, la electricidad es lo que representa los bits. Todavía no hay un equivalente definitivo para la computación cuántica.

Se ha hablado de los qubits que son objetos matemáticos que pueden estar en varios estados. Pero se debe escoger una partícula o elemento que represente este qubit en la práctica, como de la misma manera en la computación tradicional los bits son representados por un cable en el que pasa o no electricidad. Pero manipular estos efectos cuánticos no es fácil, como tampoco las mediciones de sus estados. De las posibilidades que se han ido explorado para implementar ordenadores cuánticos uno de los que tuvo mucho éxito es la **resonancia magnética nuclear (RMN).** Se dice que con un RMN se ejecutó el primer algoritmo cuántico de shor en el año 2001, que factorizaba números. La computación cuántica con RMN es basada en medir estados de *spin* de ciertos átomos en una molécula, esta técnica no sirve de mucho ya que el problema es que en las moléculas hay interferencias que van a modificar los qubits sin darse cuenta y las operaciones serian incorrectas, debido al ruido, que es un reto a superar por la comunicación cuántica. El ruido puede separar partículas en poco tiempo, y si sucede que el sistema está mal aislado como resultado no se tendría el qubit erróneo sin hasta cálculos que se tardarían más de un cierto tiempo y dejan de ser válidos.

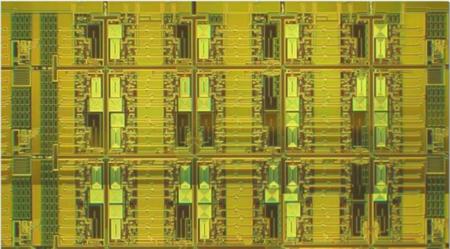


A la escala a la que se producen efectos cuánticos, el ruido es un problema serio y complicado de resolver.

## **D-Wave, Ordenadores con Circuitos Superconductores**

INTRODUCCIÓN.

D-Wave donde se dice que ha hecho más progresos en la representación de qubits con circuitos superconductores, donde según el tipo de circuito es la carga o direccion de los electrones que se mueven dentro de un bucle. Para que no haya perdidas el circuito se debe enfriar a un punto muy cercano a cero.



Un procesador de DWave, basado en circuitos superconductores.

Con toda esta tecnología D-Wave ha conseguido crear los primeros procesadores cuánticos comerciales, con aplicaciones prácticas (ejemplo, google). Se siguen buscando las posibilidades para obtener un ordenador cuántico de alcance universal y manejable.

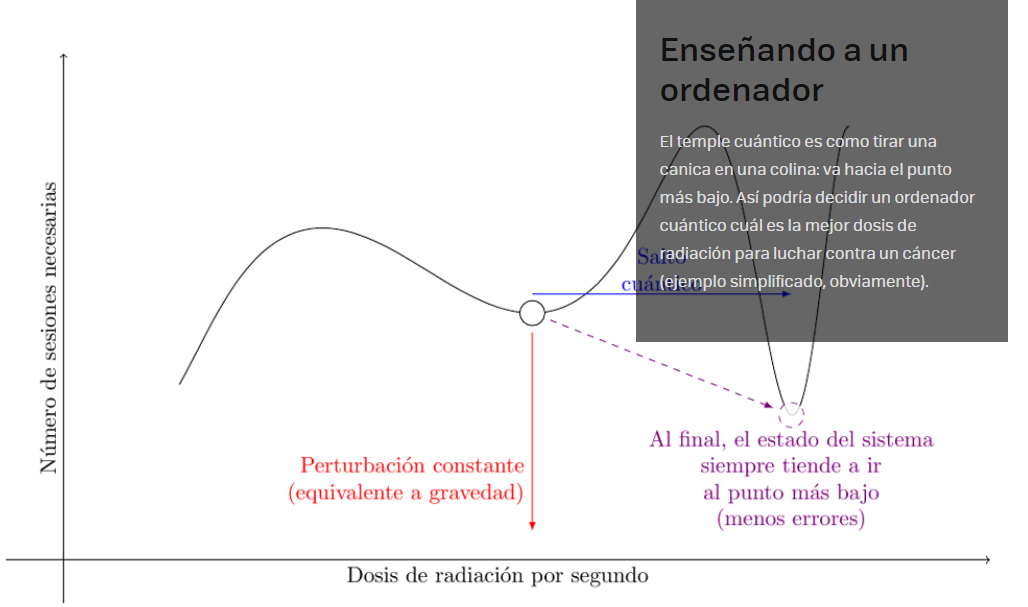
¿Seguro que eso es un ordenador cuántico?

No todos los ordenadores hechos con qubits sin cuánticos, ya que lo que la hacía especial es el entrelazamiento. Pues resulta que los que se hacía llamar ordenadores cuánticos no se han observado estos fenómenos con seguridad. Por ejemplo, el **D-Wave Two** no consiguió medir la mejora de velocidad que debería tener. Esto no descarta que no sea un ordenador cuántico. Para saber si las partículas están entrelazadas es difícil, mas sin en cambio el otro reto es la computación cuántica.

Y ahora que tengo un ordenador cuántico, ¿Qué hago?

Es verdad que no hay muchos algoritmos cuánticos que puedan explotar las posibilidades de un ordenador de este tipo. En este campo de inteligencia artificial la mayoría de esos sistemas avanzados capaces de reconocer caras y entender frases han sido creados aleatoriamente: Para esto se crea una función con ciertos parámetros que mide las veces que falla, modificando los parámetros y que el proceso se repita, hasta que este funciona.

Los ordenadores cuánticos pueden resolver fácilmente este tipo de problemas gracias a su algoritmo, que pone a los qubits con los parámetros iniciales de la función y esperar, aplicando modificaciones constantes y da como resultado los qubits con parámetros con una alta probabilidad y disminuyendo errores.



Una aplicación cuántica de ordenadores se basa en crear sistemas de aprendizaje automático rápido y preciso a los ordenadores tradicionales.

**¿Y para qué usamos el aprendizaje automático?**

Se usa en procesos en los que no se es capaz de recrear un ordenador, ejemplo, los sistemas de aprendizaje automático en los que se aplica la radioterapia, así poder escoger la adecuada para el paciente, para detectar imágenes o elaborar modelos estadísticos que predigan el alza de la bolsa. En general son procesos que uno no puede elaborar.



D-Wave Two, el segundo procesador cuántico comercial, está hecho para resolver problemas de optimización. Google y NASA tienen uno para investigar sus aplicaciones en inteligencia artificial.

La computación cuántica puede aplicarse en otros campos, como la seguridad, hay un algoritmo que dejaría del lado el RSA, este permitiría realizar factorización de números rápidamente y rompería la seguridad de internet. Para esto no se han creado ordenadores con esta capacidad.

¿Qué nos depara el futuro?



Aunque ya haya avances en los procesadores cuánticos, falta mucho por descubrir, ya que muchos ordenadores ni siquiera son cuánticos. Uno de los campos afectados por este avance es la criptografía, estos sistemas de clave pública son basados en problemas como factorización de enteros, problemas que un ordenador clásico tardaría años en resolver y los ordenadores cuánticos resolverían en menos tiempo rompiendo la seguridad de sistemas de internetcomo *HTTPS,* falta mucho por avanzar hasta que la computación cuántica logre tener un nivel de madurez.