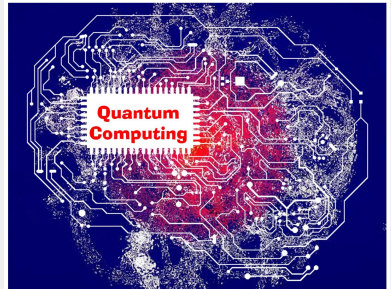


COMPUTACIÓN CUÁNTICA

JOSE LUIS IZQUIERDO MAÑAS
ELVIRA CASTILLO FERNÁNDEZ

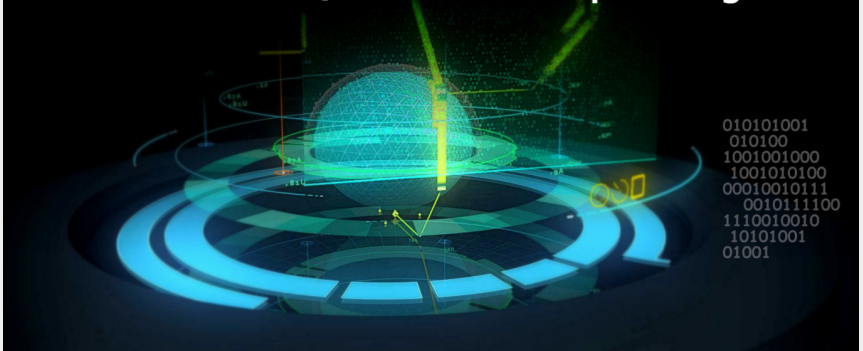
9 DE DICIEMBRE DE 2018



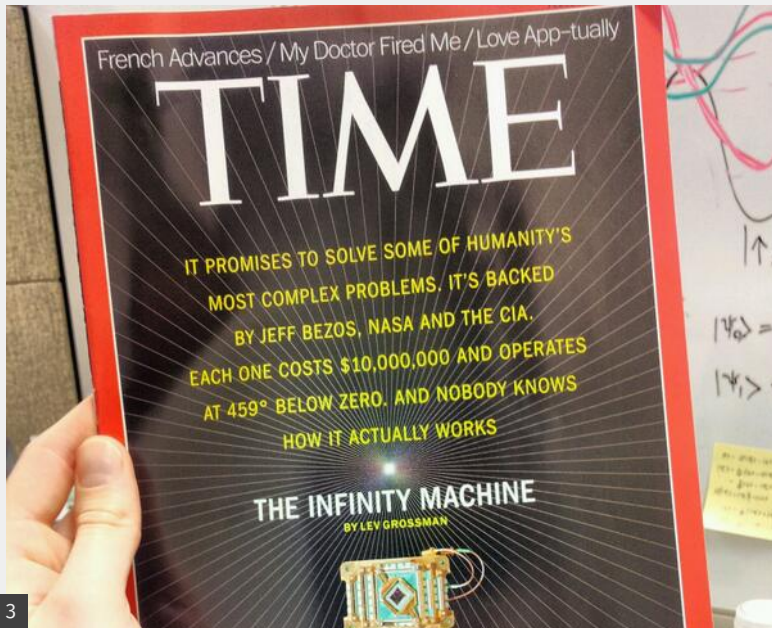
- 1 ¿Qué es la computación Cuántica?
 - Mitos
 - Computadores cuánticos VS Super Computadores
- 2 Principios de la física cuántica
- 3 ¿Como funciona un computador cuántico?
- 4 Deficiencias
- 5 Campos de Aplicación
 - Historia
 - Usos en el futuro
 - Usos en la actualidad
- 6 Posicionamiento en la curva de Gartner
- 7 Conclusiones
- 8 Dónde ampliar más información
- 9 Bibliografía

¿QUÉ ES LA COMPUTACIÓN CUÁNTICA?

What is Quantum Computing?



Aprovechar y explotar las sorprendentes leyes de la mecánica cuántica para **procesar información**



Intelligent Machines

Google's Quantum Dream Machine

Physicist John Martinis could deliver one of the holy grails of computing to Google—a machine that dramatically speeds up today's applications and makes new ones possible.

by Tom Simonite December 18, 2015

TECHNOLOGY



Newsroom

Top News Sections

News By Category

All News

Search

News Release

September 3, 2015

Share this Article

Q Search

INTEL INVESTS US\$50 MILLION TO ADVANCE QUANTUM COMPUTING

Bloomberg Opinion

Sign In

Editorial Board

Quantum Computers Are Coming. The World Might Not Be Ready.

They could do wonders for medicine, chemistry, banking and information-gathering. There's just one problem.

By Editorial Board

6 de septiembre de 2016 8:00 CEST

TECH & SCIENCE

EUROPE'S BILLION EURO BET ON QUANTUM COMPUTING

BY ANTHONY CUTHBERTSON ON 4/26/16 AT 9:09 AM

TECH • QUANTUM COMPUTING

Alibaba's cloud unit teams with Chinese researchers on quantum computing

The New York Times

Microsoft Makes Bet Quantum Computing Is Next Breakthrough

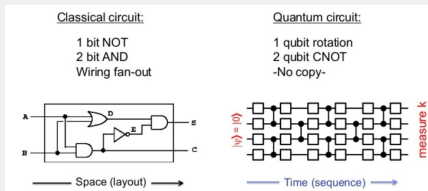
Interview
McKinsey Global
Institute
February 2016

The growing potential of quantum computing

COMPUTADORES CUÁNTICOS VS SUPER COMPUTADORES

Un ordenador cuántico hace lo mismo que uno usual, pero de forma distinta.

- ➡ Bits cuánticos. **Qubits.**
- ➡ Procesamiento: puertas lógicas cuánticas.
- ➡ Superposición de estados.
- ➡ Entrelazamiento.
- ➡ Más rápido.
- ➡ Más eficiente.



Estados de un Qubit

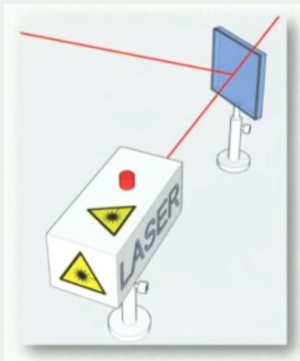
- Puede valer 0
- Puede valer 1
- Puede valer 0 y 1 a la vez.

PRINCIPIOS DE LA FÍSICA CUÁNTICA

PRINCIPIO DE SUPERPOSICIÓN

Experimento:

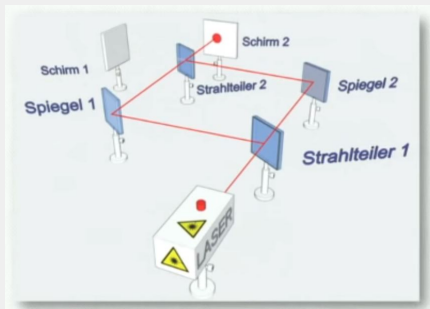
- Láser
- Espejos
- Receptores de fotones



PRINCIPIO DE SUPERPOSICIÓN

Experimento:

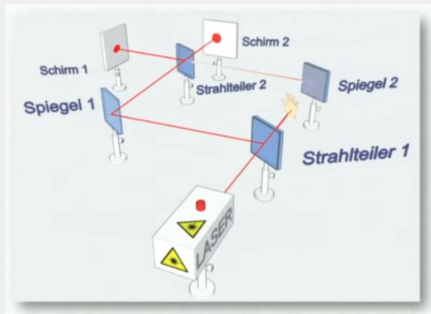
- Láser
- Espejos
- Receptores de fotones



PRINCIPIO DE SUPERPOSICIÓN

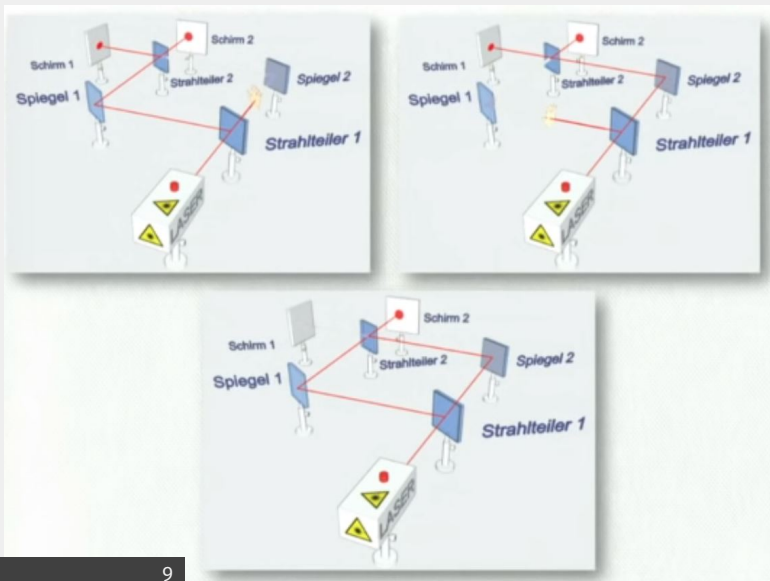
Experimento:

- Láser
- Espejos
- Receptores de fotones

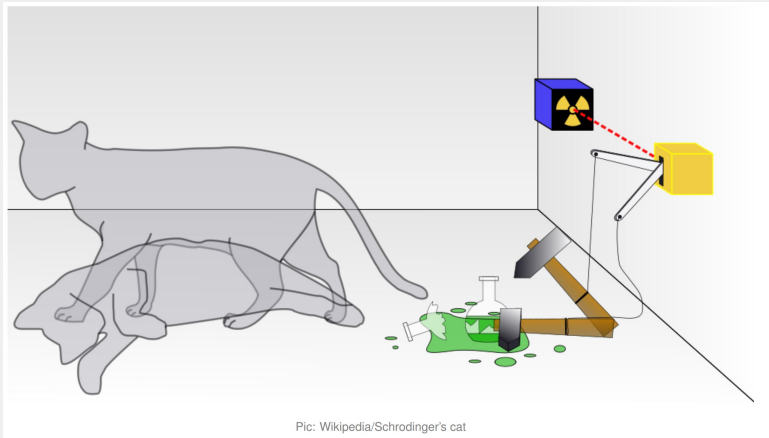


PRINCIPIO DE SUPERPOSICIÓN

Experimento:

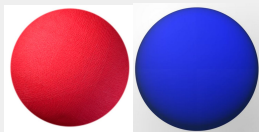


PRINCIPIO DE SUPERPOSICIÓN



PRINCIPIO DE ENTRELAZAMIENTO

El entrelazamiento cuántico permite que una partícula influya el estado de otra instantáneamente, aunque estén a años luz de distancia.



Permite desarrollar dos algoritmos muy relevantes:

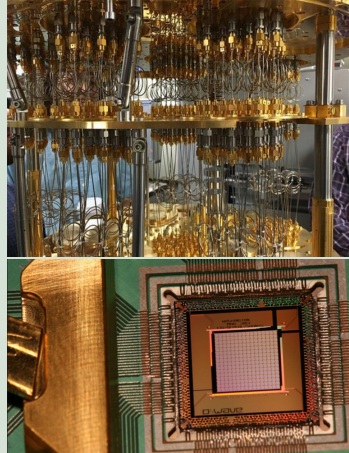
- El temple cuántico (1989)
- El algoritmo de Shor (1994)

¿COMO FUNCIONA UN COMPUTADOR CUÁNTICO?

¿COMO FUNCIONA UN COMPUTADOR CUÁNTICO?

Ejemplos

- ➡ Funcionamiento
- ➡ Computador Cuántico IBM
- ➡ Vista 360º



DEFICIENCIAS

¿PODEMOS REALMENTE CONSTRUIR UNO?



¿PODEMOS REALMENTE CONSTRUIR UNO?



iiiSÍ!!! con una gran cantidad de "*peros*"...

¿PODEMOS REALMENTE CONSTRUIR UNO?

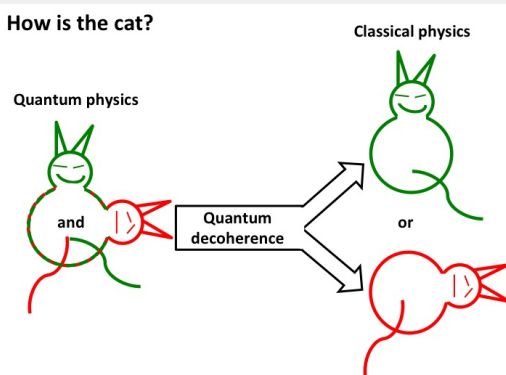
El gran problema

Construir un **computador cuántico** es súper complejo y costoso por culpa de la "***decoherencia***".

¿PODEMOS REALMENTE CONSTRUIR UNO?

El gran problema

Construir un **computador cuántico** es súper complejo y costoso por culpa de la "**decoherencia**".



¿PODEMOS REALMENTE CONSTRUIR UNO?

Se produce cuando...

los componentes tienen contacto con el mundo exterior.

¿PODEMOS REALMENTE CONSTRUIR UNO?

Se produce cuando...

los componentes tienen contacto con el mundo exterior.

Se necesitan unas condiciones muy particulares para su correcto funcionamiento:

- ⇒ Vacío
- ⇒ Temperaturas de -273°C
- ⇒ Materiales especiales muy costosos

¿PODEMOS REALMENTE CONSTRUIR UNO?

Se produce cuando...

los componentes tienen contacto con el mundo exterior.

Se necesitan unas condiciones muy particulares para su correcto funcionamiento:

- ⇒ Vacío
- ⇒ Temperaturas de -273°C
- ⇒ Materiales especiales muy costosos

La simple acción de

un único **fotón** que sea capaz de colarse en el computador, manda todo a la "porra"

¿PODEMOS REALMENTE CONSTRUIR UNO?

De hecho actualmente no se puede mantener este estado de **coherencia** necesario para que los computadores cuánticos funcionen por mas de **200ms...**

Se usan técnicas de redundancia

para paliar con la **decoherencia**

Estas técnicas

complican el hardware y el número de qubits de forma **exponencial**

¿PODEMOS REALMENTE CONSTRUIR UNO?

Noticia publicada en **Enero** del año **2018**: Intel's 49-Qubit Chip Shoots for Quantum Supremacy

Parece que Google

ha sacado un computador cuántico con suficientes qubits como para comenzar a exceder los límites prácticos de los computadores clásicos modernos.

CAMPOS DE APLICACIÓN

En **Wikipedia** hay una lista muy exhaustiva de la evolución de la computación cuántica **desde los años 60** hasta nuestros días. En **Youtube** podemos encontrar una pequeña charla contada por un ingeniero de **IBM**.

NECESIDAD DE LOS ORDENADORES CUÁNTICOS

Podemos pensar

Si queremos más capacidad de cómputo basta con hacer un **Súper computador** más grande o **mejorar** la tecnología subyacente.



NECESIDAD DE LOS ORDENADORES CUÁNTICOS

Podemos pensar

Si queremos más capacidad de cómputo basta con hacer un **Súper computador** más grande o **mejorar** la tecnología subyacente.



La realidad es **muy distinta**:

- ➡ Ni el computador más potente puede resolver todos los problemas.
- ➡ Si se siguen **miniaturizando** los materiales de un **chip** empezarán a aparecer **efectos cuánticos**.



En el año **1981** se produce la primera conferencia sobre física de la computación.



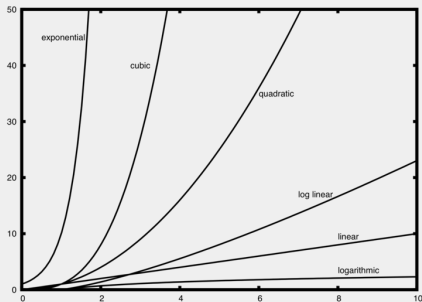
En el año **1981** se produce la primera conferencia sobre física de la computación.

El físico **Richard Feynman**

propone el desafío de desarrollar un computador basado en conceptos cuánticos.

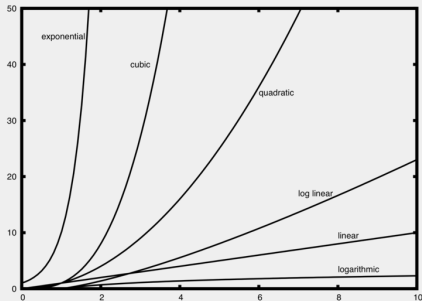
La computación cuántica

por su naturaleza podría resolver problemas de **complejidad exponencial** transformándolos en problemas de **complejidad polinómica**.



La computación cuántica

por su naturaleza podría resolver problemas de **complejidad exponencial** transformándolos en problemas de **complejidad polinómica**.



Debido al corto funcionamiento

de los computadores cuánticos a corto plazo se cree que serán **coprocesadores** que ayuden a supercomputadores.

Se usa para

búsquedas en **bases de datos** no indexadas.

USOS EN EL FUTURO - ALGORITMO DE GROVER

Se usa para

búsquedas en **bases de datos** no indexadas.



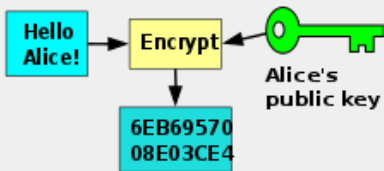
✎ **Actualmente** estas búsquedas nos cuentan **$O(n)$**

✎ Este algoritmo tiene una eficiencia **$O(\sqrt{n})$**

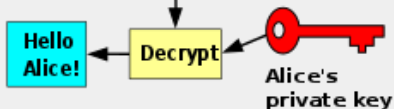
Si tuviéramos que realizar **veinte millones** de búsquedas realizaríamos en el peor de los casos **4472** búsquedas.

USOS EN EL FUTURO - CRIPTOGRAFÍA

Bob



Alice



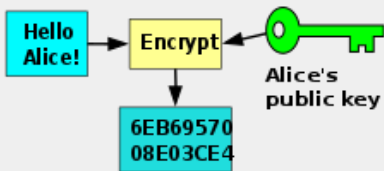
La mayoría de algoritmos que utilizamos a día de hoy para cifrar nuestra información, emplean la siguiente fórmula:

$$p * q = C_{publica}$$

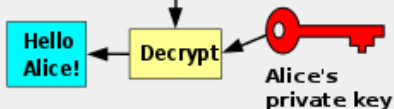
Siendo p y q números primos que conforman una **clave privada**.

USOS EN EL FUTURO - CRIPTOGRAFÍA

Bob



Alice



La mayoría de algoritmos que utilizamos a día de hoy para cifrar nuestra información, emplean la siguiente fórmula:

$$p * q = C_{publica}$$

Siendo p y q números primos que conforman una **clave privada**.

Su seguridad se fundamenta en

que obtener los números p y q que producen la **clave pública** es un problema con tanta complejidad en tiempo (**NP-Completo**) que es imposible obtener dichos valores en una vida.

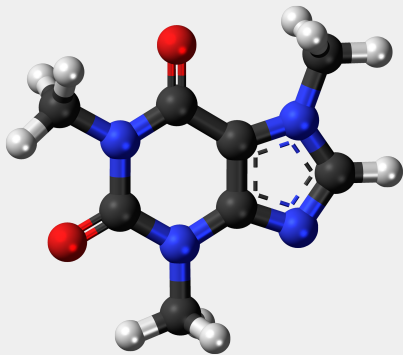


Peter shor propuso un algoritmo **cuántico** capaz de encontrar los factores de un número en un tiempo **polinómico**.



IBM demostró

en el año 2001 que el algoritmo de shor funcionaba utilizando para ello un procesador cuántico de 7 qubits.

USOS EN EL FUTURO - QUÍMICA, MATERIALES



Los **supercomputadores actuales** se usan para

-  Síntesis **ADN** o **Moléculas**.
-  Simulación de partículas.

Los ordenadores cuánticos

podrían revolucionar estos campos.

Es una tecnología que se encuentra en la niñez:

Es una tecnología que se encuentra en la niñez:

- ⇒ Estamos en una etapa similar a la que se vivió antes de la invención del **transistor**, cuando los computadores empleaban **las válvulas termoiónicas**.
- ⇒ Su programación se hace "*a pelo*".
- ⇒ sólo son capaces de resolver problemas de "*juguete*".
- ⇒ aun así se comercializan.

Es una tecnología que se encuentra en la niñez:

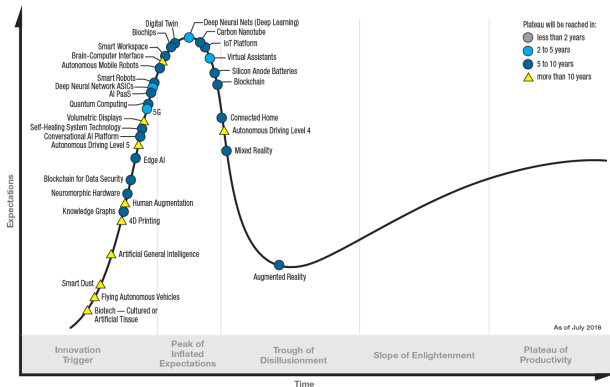
- ⇒ Estamos en una etapa similar a la que se vivió antes de la invención del **transistor**, cuando los computadores empleaban **las válvulas termoiónicas**.
- ⇒ Su programación se hace "*a pelo*".
- ⇒ sólo son capaces de resolver problemas de "*juguete*".
- ⇒ aun así se comercializan.

Ya existen empresas que aplican fenómenos cuánticos para resolver problemas de criptografía.

POSICIONAMIENTO EN LA CURVA DE GARTNER

POSICIONAMIENTO EN LA CURVA DE GARTNER

Hype Cycle for Emerging Technologies, 2018

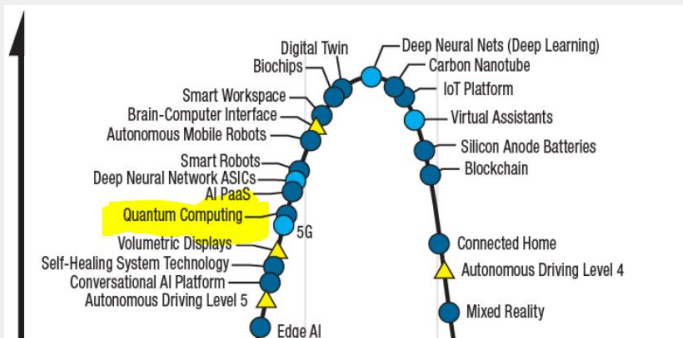


gartner.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner.

HYPE CYCLE FOR EMERGING TECHNOLOGIES 2018



Está a medias entre el final de la primera fase de lanzamiento de la nueva tecnología y el principio del pico de expectativas sobredimensionadas.

Video resumen

Microsoft Quantum

CONCLUSIONES

DÓNDE AMPLIAR MÁS INFORMACIÓN

DÓNDE AMPLIAR MÁS INFORMACIÓN

- MIT,

Página oficial: <https://quantumcurriculum.mit.edu/>

- IBM

Página oficial: <https://www.research.ibm.com/ibm-q/>

- GOOGLE

Página oficial: <https://ai.google/research/teams/applied-science/quantum-ai/>

BIBLIOGRAFÍA

- Gartner, <https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/>
- Así cambiará el mundo sobre computación cuántica: Ignacio Cirac <https://www.youtube.com/watch?v=WJ3r6btgzBM>
- Artículos inicios computación cuántica
 - ▶ <https://www.mckinsey.com/industries/high-tech/our-insights/the-growing-potential-of-quantum-computing>
 - ▶ <https://www.technologyreview.com/s/544421/googles-quantum-dream-machine/>
 - ▶ <https://www.efefuturo.com/ciencia/cirac-ordenadores-cuanticos/>
- MIT <https://www.technologyreview.com/s/610250/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/>

- MIT <https://www.technologyreview.com/s/612509/quantum-computers-encryption-threat/>
- Ordenador cuántico Intel <https://www.xataka.com/ordenadores/asi-ordenador-cuántico-49-qubits-intel-dentro>
- University of Waterloo <https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101#Quantum-effects-matter>

- Wikipedia decoherencia Cuántica
https://es.wikipedia.org/wiki/Decoherencia_c%C3%A1ntica
- El Confidencial Ya puedes utilizar un ordenador cuántico desde casa
https://www.elconfidencial.com/tecnologia/2016-05-04/ibm-computacion-cuantica-informatica_194604/
- nobbot Así funciona un ordenador cuántico
<https://www.nobbot.com/futuro/funciona-ordenador-cuantico-aplicaciones/>
- Wikipedia Timeline of quantum computing
https://en.wikipedia.org/wiki/Timeline_of_quantum_computing#cite_note-manin1980vychislmo-3
- IEEE SPECTRUM Intel's 49-Qubit Chip Shoots for Quantum Supremacy <https://spectrum.ieee.org/tech-talk/computing/hardware/intels-49qubit-chip-aims-for-quantum-supremacy>

- IAS What Can We Do with a Quantum Computer?
<https://www.ias.edu/ideas/2014/ambainis-quantum-computing>
- Youtube 14:24 Quantum Computing: The Past, Present and Future. <https://www.youtube.com/watch?v=XwUEtUgQJHc>
- Youtube 1:15:19 Así cambiará el mundo, sobre computación cuántica: Ignacio Cirac
<https://www.youtube.com/watch?v=WJ3r6btgzBM>
- Youtube 51:34 Programando Ordenadores Cuánticos - Francisco Galvez | T3chFest 2018
<https://www.youtube.com/watch?v=qCrVHKDroRg>

¡ MUCHAS GRACIAS !