Universidad Autónoma de Madrid

excelencia UAM CSIC

Escuela Politécnica Superior

Computación Cuántica

Procesamiento de Datos a Gran Escala

Máster en Ciencia de Datos

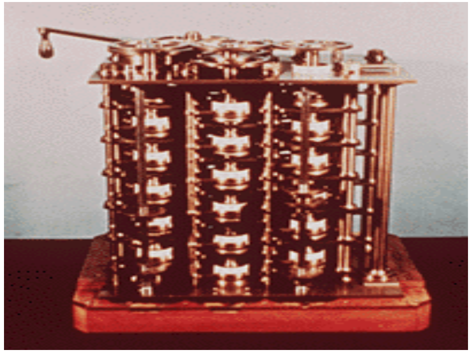
Francisco J. Gómez Arribas

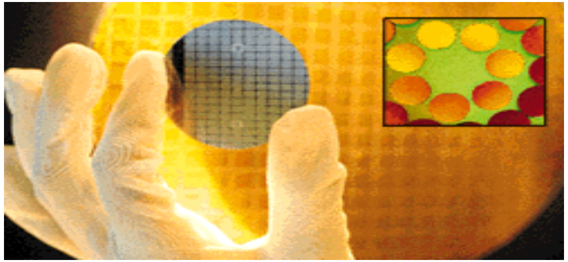
Contenidos

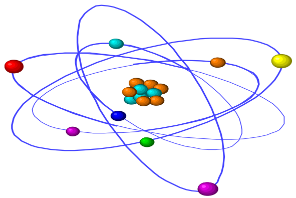
- Evolución de la tecnología: supremacía cuántica
- Bases de Mecánica Cuántica
  - Principio de Superposición.
  - Entrelazamiento, Interferencia y medida.
- Bases de la computación cuántica
  - Qubit y puertas cuánticas
  - Sistemas de n qubits : producto tensorial
  - Circuitos cuánticos: QisKit
  - Ordenador cuántico
- Algoritmos cuánticos
  - Deutschs_Jozsa
  - Bernstein-Vazirani
  - Groover
  - Shor (QFT)

Evolución Tecnológica

La tecnología está haciendo los componentes de los computadores cada vez más pequeños…

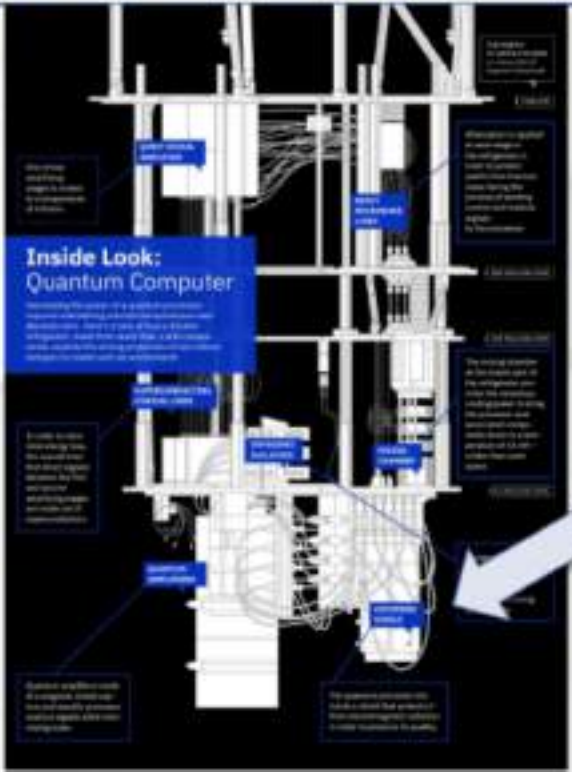






…estamos alcanzando el punto donde la física clásica deja de ser válida => ha llegado el momento de la física cuántica

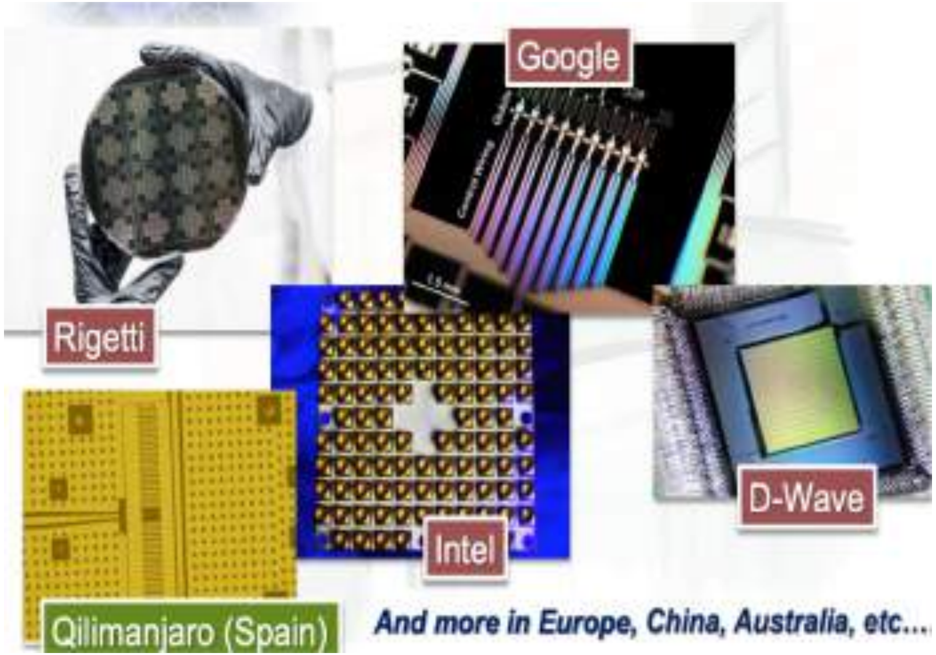
Yuri Manin (1980) and Richard Feynman (1981) proposed independently the concept of Quantum Computer



I'm here very "hot"!!
-273ºC

Source: IBM

Supremacía cuántica



Google asegura haber logrado que un computador cuántico realice en segundos una tarea que a un ordenador clásico le llevaría miles de años

* **ejecutar en 200 segundos** una operación para calcular números aleatorios que al superordenador más potente del mundo le hubiera llevado al menos 10.000 años.

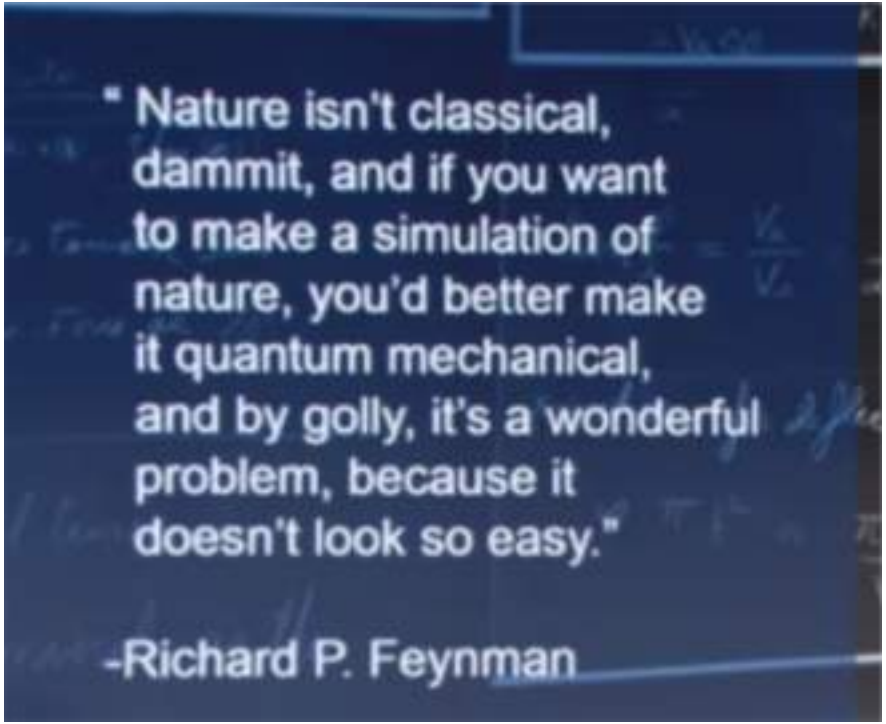
Poco después del anuncio, IBM lo ha puesto en duda, ya que considera que un superordenador basado en computación clásica (SUMMIT) podría ejecutar el mismo experimento que propone Google en dos días y medio.

Nadie entiende la mecánica cuántica

"No, you' re not going to be able to understand it. . . . You see, my physics students don' t understand it either. That is because I don' t understand it. Nobody does. ... The theory of quantum electrodynamics describes Nature as absurd from the point of view of common sense. And it agrees fully with an experiment. So I hope that you can accept Nature as She is -- absurd.

Richard Feynman

Mejor hacer un ordenador cuántico



Computación Cuántica: Qubit

Quantum bit

- Un sistema físico, con dos estados distinguibles, le denominamos **quantum bit (or qubit).**
- Denominamos a los dos estados distinguibles con |0> y |1>
- A diferencia de un bit clásico, un qubit puede estar en cualquier combinación lineal de estos estados:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$

Donde α y β son números complejos.

- Si se realiza una medida el qubit, se encontrará en uno de los dos estados |0> o |1> con probabilidades $|\alpha|^2$ o $|\beta|^2$, y el sistema se quedará en el estado |0> o |1>. Al medir se colapsa la función de onda a uno de lo estados observables.

Computación Cuántica: Principios

Principio de superposición:

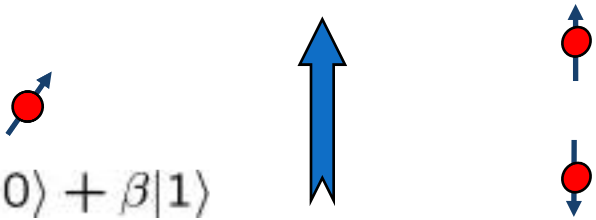
- La mecánica cuántica describe la información que tenemos de un sistema
  - La función de onda ψ describe la información del sistema (no describe la realidad)
- Si dos historias son diferentes pero compatibles, se suman
  - $\Psi = \psi_0 + \psi_1$

Evolución

- La mecánica cuántica dicta que la evolución del estado (n qubits $\longrightarrow$ 2^n estados) es determinista.
- Los qubits se procesan en paralelo intrínsecamente. ¡Todo es en paralelo!

Medidas

- La medida de observables sobre este estado son probabilísticas.
- Es imposible conocer de forma exacta el estado de un sistema

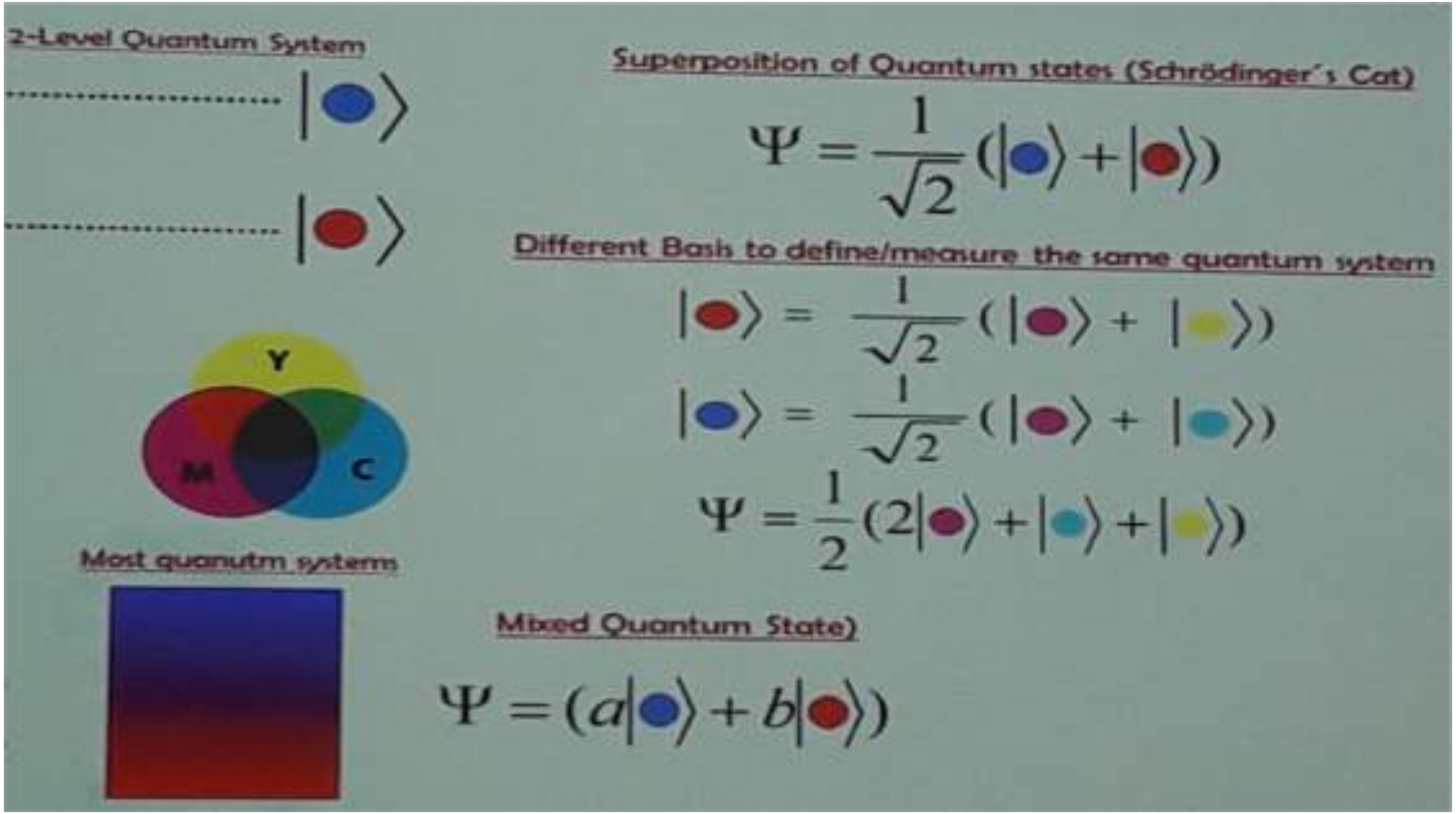


$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$P_{S_z,|\psi\rangle}(0) = |\alpha|^2$$

$$P_{S_z,|\psi\rangle}(1) = |\beta|^2$$

Computación Cuántica: Sistema de 2 estados

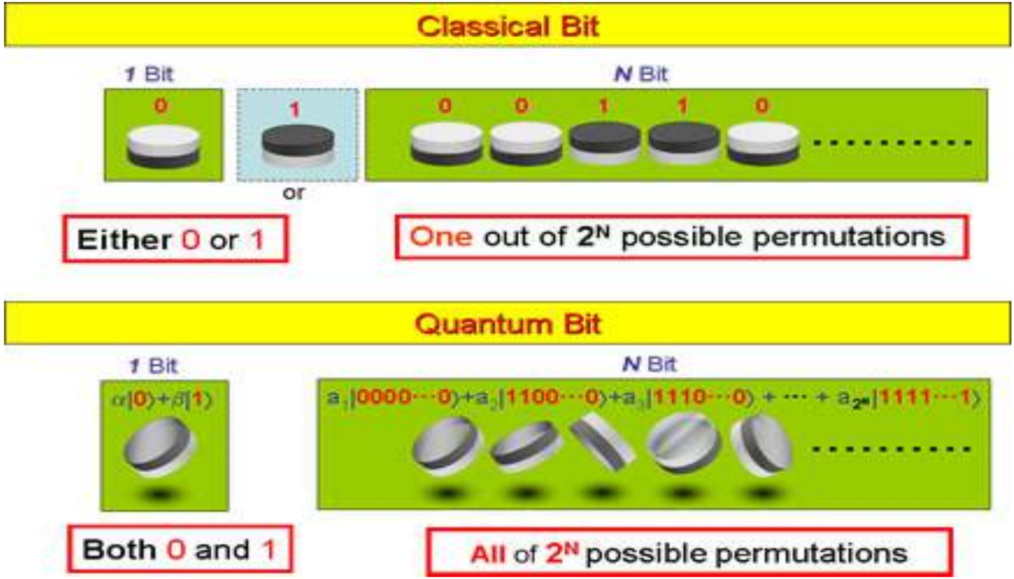


Computación Cuántica: Registro de mútiples Qubit

- In general, an n qubit register can represent the numbers 0 through 2^n-1 simultaneously.

Sound too good to be true?…It is!

- If we attempt to retrieve the values represented within a superposition, the **superposition randomly collapses** to represent just one of the original values.

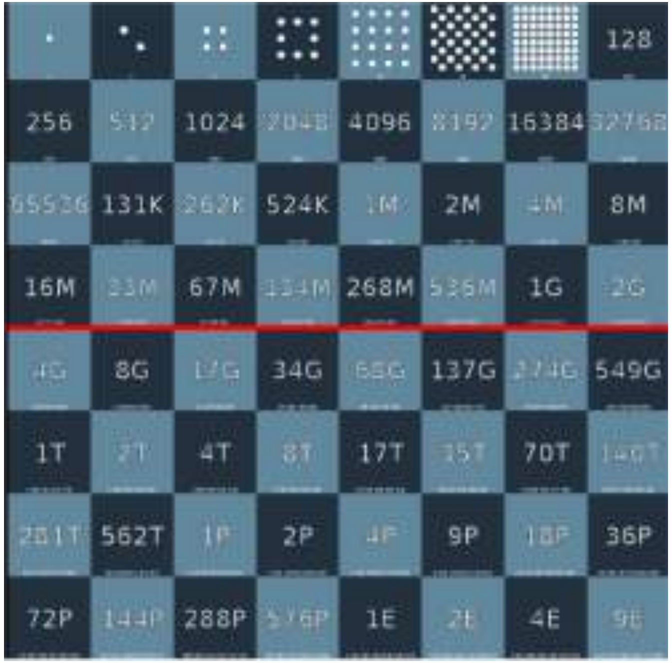


- Measurement Example:

  $0.316|00\rangle + 0.447|01\rangle + 0.548|10\rangle + 0.632|11\rangle$

  The probability to read the rightmost bit as 0 is $|0.316|^2 + |0.548|^2 = 0.4$

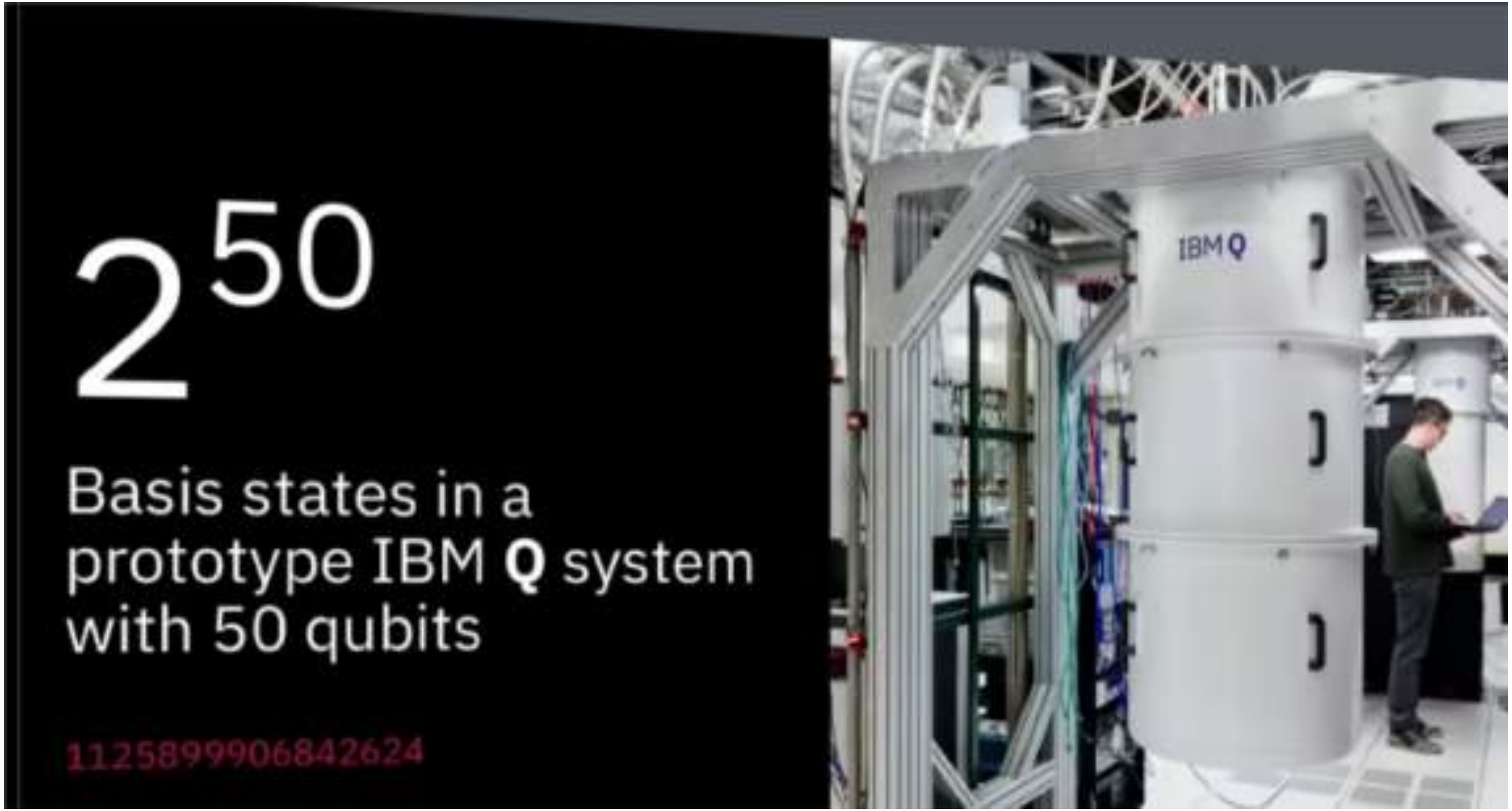
Computación Cuántica: Número de estados (Escala exponencial)



$$T_{64} = 2^0 + 2^1 + 2^2 + \cdots + 2^{63}$$

$$s = 2^{64} - 1 \quad = \quad 18\,446\,744\,073\,709\,551\,615$$

Computación Cuántica: Escala exponencial



Computación Cuántica: Escala exponencial

Computación Cuántica: Podemos computar pero no ver el resultado

But, there is a big catch! We can manipulate information in a very high dimensional space but we cannot read those coefficients directly. When all operations are completed, the only way to "read" the qubits is to measure it which returns one of the states only (not the coefficient).

no direct access

$$|\psi_2\rangle = a_0\,|000\rangle + a_1\,|001\rangle + a_2\,|010\rangle + a_3\,|011\rangle + a_4\,|100\rangle + a_5\,|101\rangle + a_6\,|110\rangle + a_7\,|111\rangle$$

Get one of the states when measured

Relaciones entre datos: Entrelazamiento de estados (**Entanglement**)

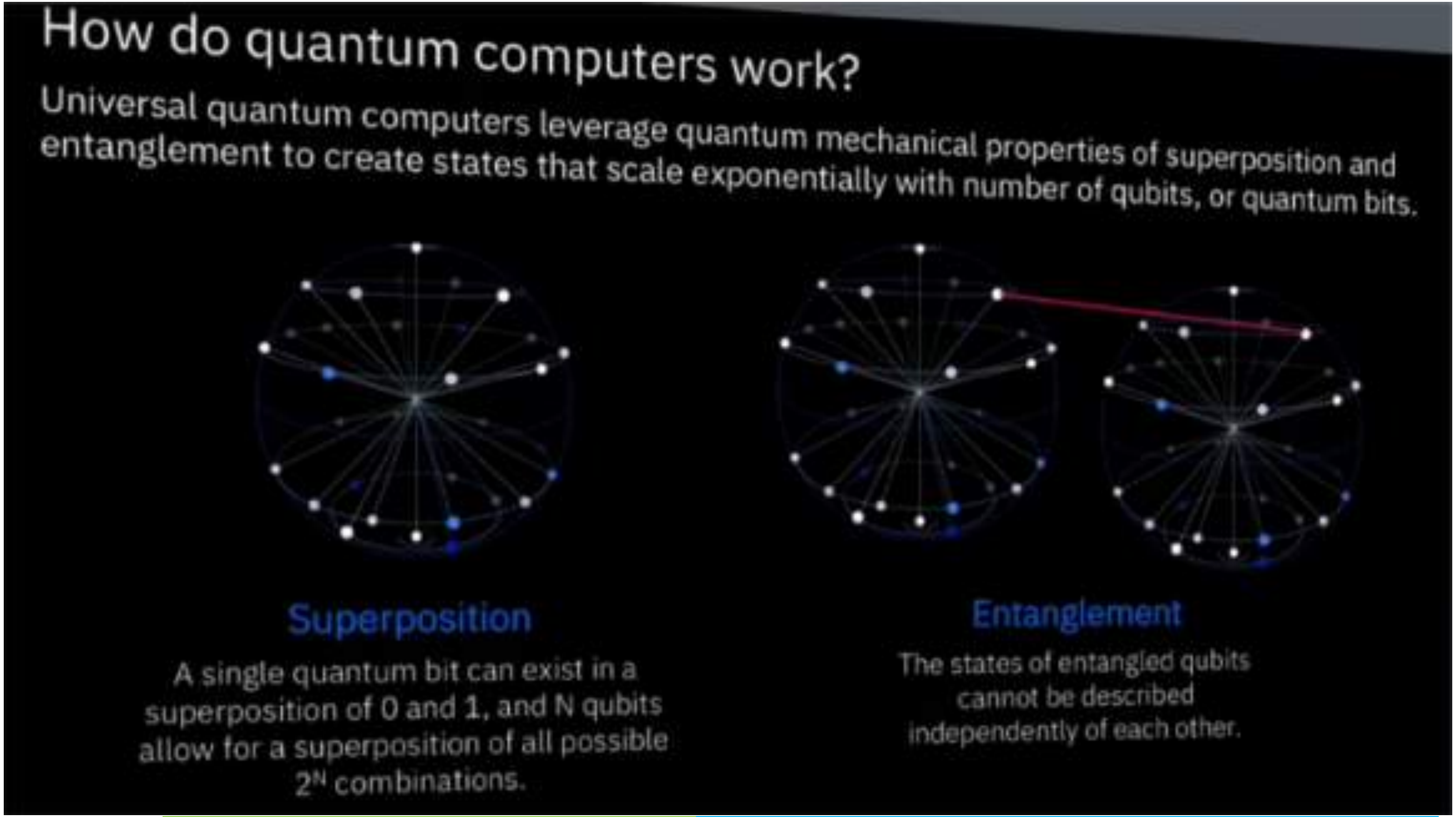
- ***Entrelazamiento*** es la capacidad de un sistema cuántico de exhibir correlaciones dentro de una superposición.
  - El entrelazamiento es un fenómeno cuántico, sin equivalente clásico, en el cual los estados cuánticos de dos o más objetos se deben describir mediante un estado único que involucra a todos los objetos del sistema, aún cuando los objetos estén separados espacialmente.
  - El estado de un qubit depende del estado de otro qubit.
  - Observando el estado de un qubit puedo conocer el estado del otro al que está entrelazado sin necesidad de medir el segundo.

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Principio de Interferencia

- ***Interferencia*** entre funciones de onda que modifica, aumentando o disminuyendo las amplitudes, incluso las puede llegar a anular.
- Es la base de los algoritmos cuánticos. QAE (Quantum Amplitud Estimation)

Bases del funcionamiento del computador cuántico



Representación de un Qubit

- Qubit - |1>, |0> o superposición de ambos
- |x> Registro en el computador cuántico

  - Superposición de estados: $$\sum_{i=0}^{2^N-1} a_i |s_i\rangle \quad \text{con:} \quad \sum_{i=0}^{2^N-1} |a_i|^2 = 1$$

Sistema de 1Qubit $$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Sistema de 2Qubits $$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

Sistema de nQubits $$\alpha_0 \cdot |\psi_0\rangle + \alpha_1 \cdot |\psi_1\rangle + \cdots + \alpha_{2^n} \cdot |\psi_{2^n}\rangle \qquad \sum_{i=0}^{2^n-1} |\alpha_i| = 1$$

Representación de un Qubit

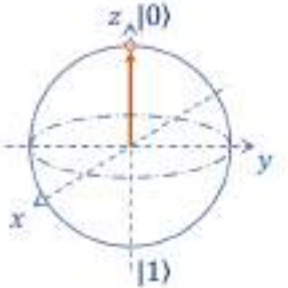
n qubits: 2^n**x**1 matrix represents the state

1 qubit:

- |0> would be represented by $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$

- |1> would be represented by $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$

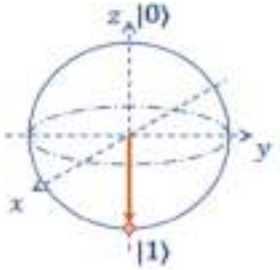
- Equal superposition would be $\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$



$$1 \cdot |0\rangle + 0 \cdot |1\rangle = \binom{1}{0}$$

$$P(0) = 1^2 = 1 = 100\%$$

$$P(1) = 0^2 = 0 = 0\%$$



$$0 \cdot |0\rangle + 1 \cdot |1\rangle = \binom{0}{1}$$

$$P(0) = 0^2 = 0 = 0\%$$

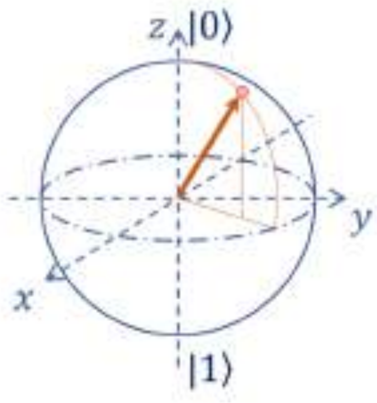
$$P(1) = 1^2 = 1 = 100\%$$

$$\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

$$P(0) = \left(1/\sqrt{2}\right)^2 = 1/2 = 50\%$$

$$P(1) = \left(1/\sqrt{2}\right)^2 = 1/2 = 50\%$$

Representación de un Qubit



1 Qubit (n=1)

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}; \quad |\alpha|^2 + |\beta|^2 = 1 \Rightarrow \begin{array}{l} P(0) = |\alpha|^2 \\ P(1) = |\beta|^2 \end{array}$$

2 Qubits (n=2)

$$\alpha \cdot |00\rangle + \beta \cdot |01\rangle + \gamma \cdot |01\rangle + \delta \cdot |01\rangle = \begin{pmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{pmatrix}$$

$$P(00) = |\alpha|^2$$
$$P(01) = |\beta|^2$$
$$P(10) = |\gamma|^2$$
$$P(11) = |\delta|^2$$

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

Qubit

Representación Matemática: Vector complejo expresado en una base de un espacio de Hilbert

Un qubit es un vector de la forma $\binom{\alpha}{\beta}$ donde $\alpha, \beta \in \mathbb{C}$ y $|\alpha|^2 + |\beta|^2 = 1.$

Se considera una base del espacio de qubits, por ejemplo:

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

entonces un qubit tendrá la forma

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Llamaremos $|0\rangle$ al vector $\binom{1}{0}$ y $|1\rangle$ al vector $\binom{0}{1}$, así, a cualquier qubit $|\psi\rangle$ lo escribiremos como

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

Puertas Cuánticas (1qubit)

¡Deben ser reversibles!

Una Compuerta Cuántica para 1 qubit será una matriz U tal que

$$UU^\dagger = U^\dagger U = I$$

donde $U^\dagger = (U^*)^T$
Por ejemplo:

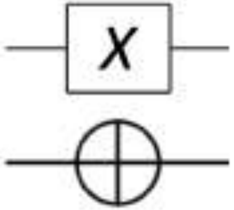
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Veamos cómo actúa esta compuerta sobre un qubit $|\psi\rangle$ cualquiera:

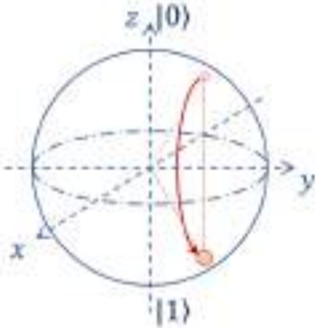
$$X|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$= \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Puertas Cuánticas: NOT cuántica



Y	NOT(Y)
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\|\psi\rangle$	$X(\|\psi\rangle)$



$$Pauli - X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

En los qubits de la base canónica vemos que

$$X|0\rangle = |1\rangle, \qquad X|1\rangle = |0\rangle$$

Por lo cual, la compuerta X es comunmente llamada *compuerta NOT*.

En general, la aplicación de una compuerta cuántica a un qubit se puede ver de la siguiente manera:

$$U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$$

Por lo cual, con sólo describir de qué manera actúa en una base, ya habremos descripto la compuerta completamente.

Puertas Cuánticas: Hadamard

- Simplest gate involving one qubit

and is called a ***Hadamard Gate***

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

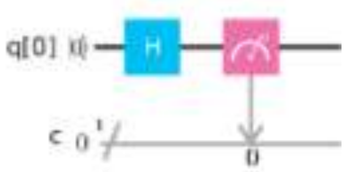
- Used to put qubits into superposition.

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |+\rangle$$

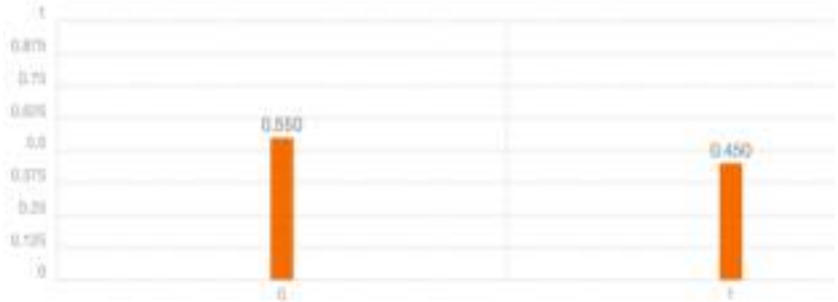
$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |-\rangle$$

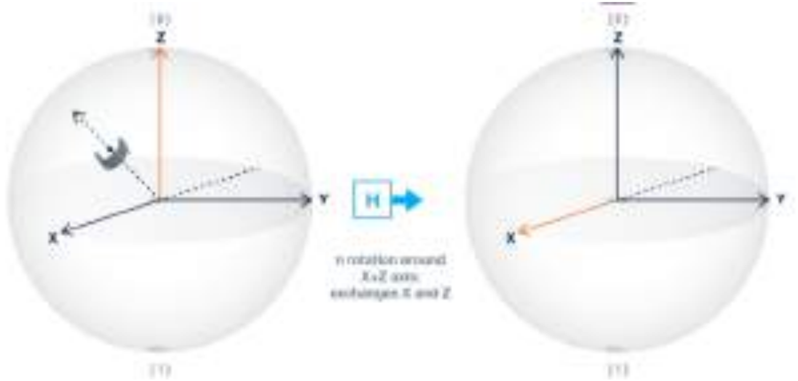
Interpretación con la Esfera de Bloch

$$H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

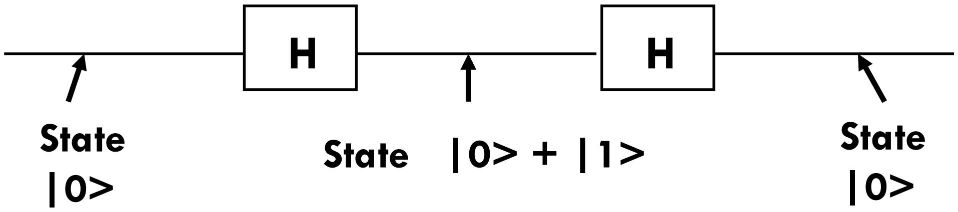


$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

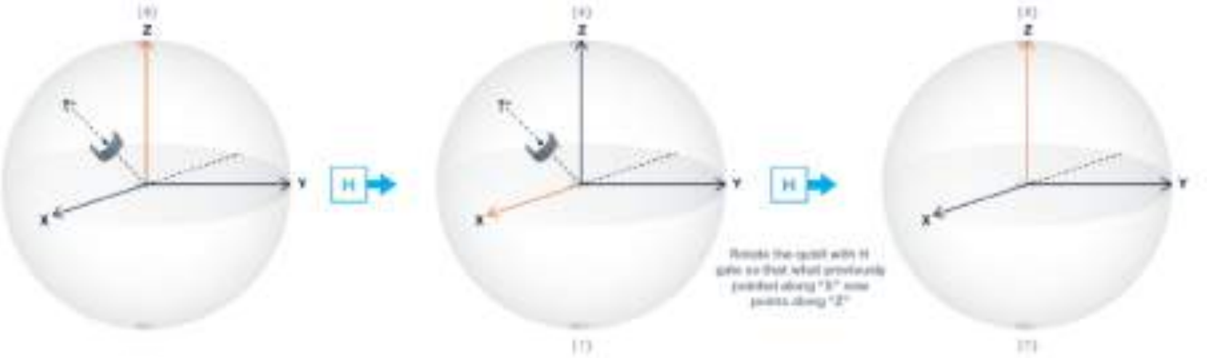


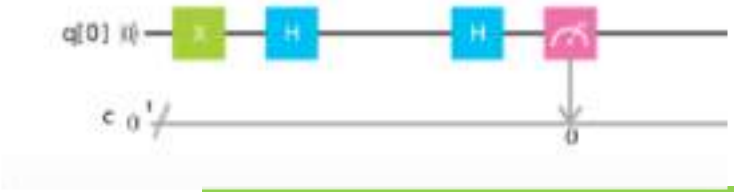


Interpretación puerta Hadamard con la Esfera de Bloch



$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$





https://qiskit.org/textbook/ch-states/single-qubit-gates.html https://qiskit.org/textbook/ch-states/single-qubit-gates.html

https://docirs.cl/math_computacion_cuantica.asp

Puertas Cuánticas de 1 Qubit

Hadamard	H	Inicial	$\lvert 0\rangle$	$\lvert 1\rangle$	$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$
		Final	$\frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$	$\frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle)$	
Puerta X	X	Inicial	$\lvert 0\rangle$	$\lvert 1\rangle$	$X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
		Final	$\lvert 1\rangle$	$\lvert 0\rangle$	
Puerta Y	Y	Inicial	$\lvert 0\rangle$	$\lvert 1\rangle$	$Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$
		Final	$i\lvert 1\rangle$	$-i\lvert 0\rangle$	
Puerta Z	Z	Inicial	$\lvert 0\rangle$	$\lvert 1\rangle$	$Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$
		Final	$\lvert 0\rangle$	$-\lvert 1\rangle$	
Puerta S	S	Inicial	$\lvert 0\rangle$	$\lvert 1\rangle$	$S = \begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}$
		Final	$\lvert 0\rangle$	$i\lvert 0\rangle$	
Puerta T	T	Inicial	$\lvert 0\rangle$	$\lvert 1\rangle$	$T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$
		Final	$\lvert 0\rangle$	$e^{i\pi/4}\lvert 1\rangle$	

Puertas Cuánticas: Otras bases son posibles

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

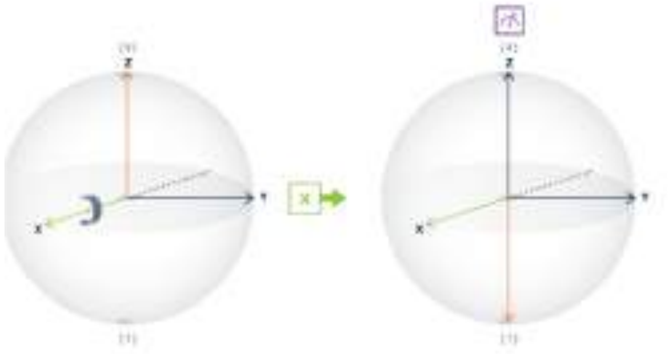
son ortogonales, por lo tanto forman base:

$$B = \{|+\rangle, |-\rangle\}$$

Ejercicio: demostrar la ortogonalidad de |+> y |->

Puertas cuánticas: Not vs CNot Gate

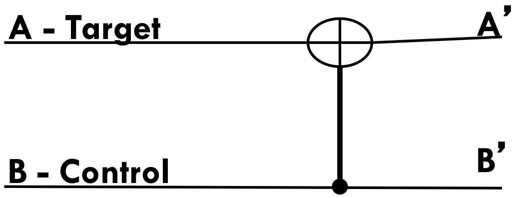
Not or X Gate: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$



Controled Not Gate (Cnot):

A gate which operates on two qubits is called a ***Controlled-NOT (CN) Gate.***
If the bit on the control line is 1, invert the bit on the target line.

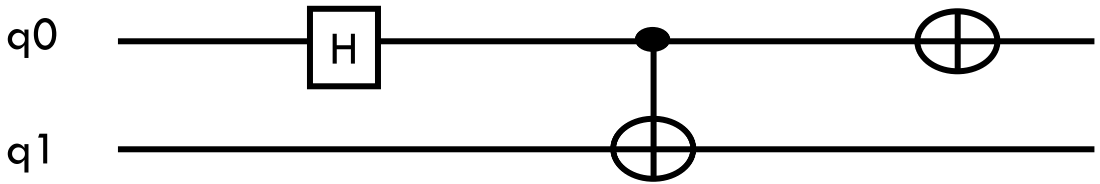
A	B	A'	B'
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} a \\ b \\ d \\ c \end{bmatrix}$$

Visualización de un Circuito Cuántico

Quantum circuits are a way of representing unitary transformations as a composition of simple unitaries acting on one or two q-bits at a time.



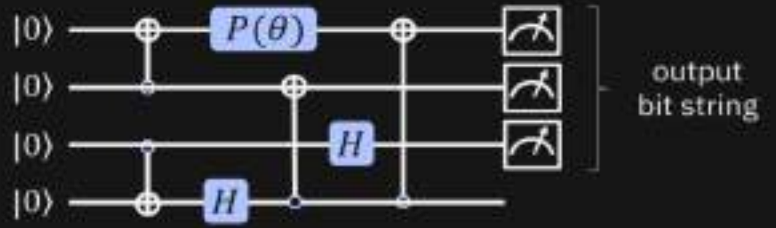
$$|00\rangle \longrightarrow \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle \longrightarrow$$

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \longrightarrow \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

Circuito cuántico

(Static) quantum circuits

IBM Quantum



Time flows from left to right.

Each line is a qubit, *width* refers to the number of qubits.

Depth is the minimum number of steps required to execute the circuit.

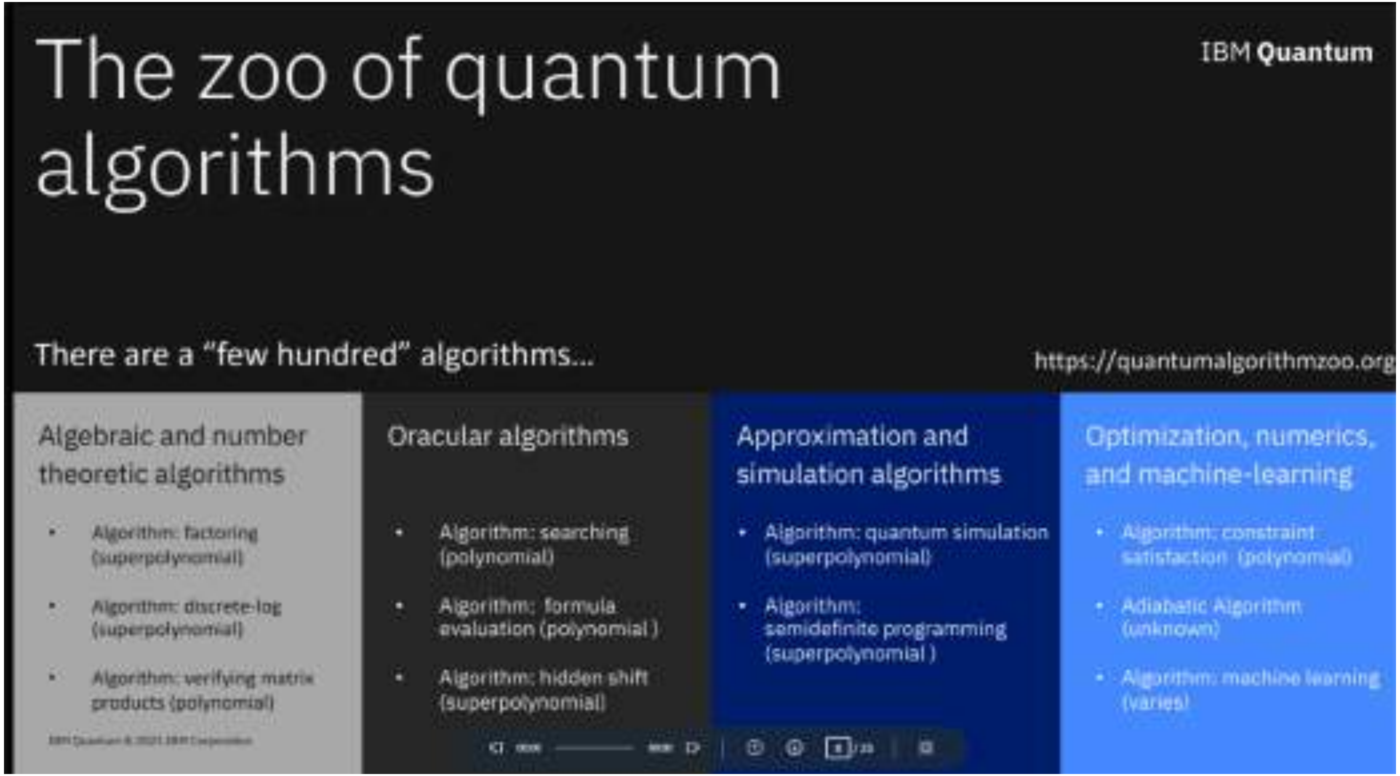
All interesting quantum circuits can be built from a universal set of gates.

Quantum circuit

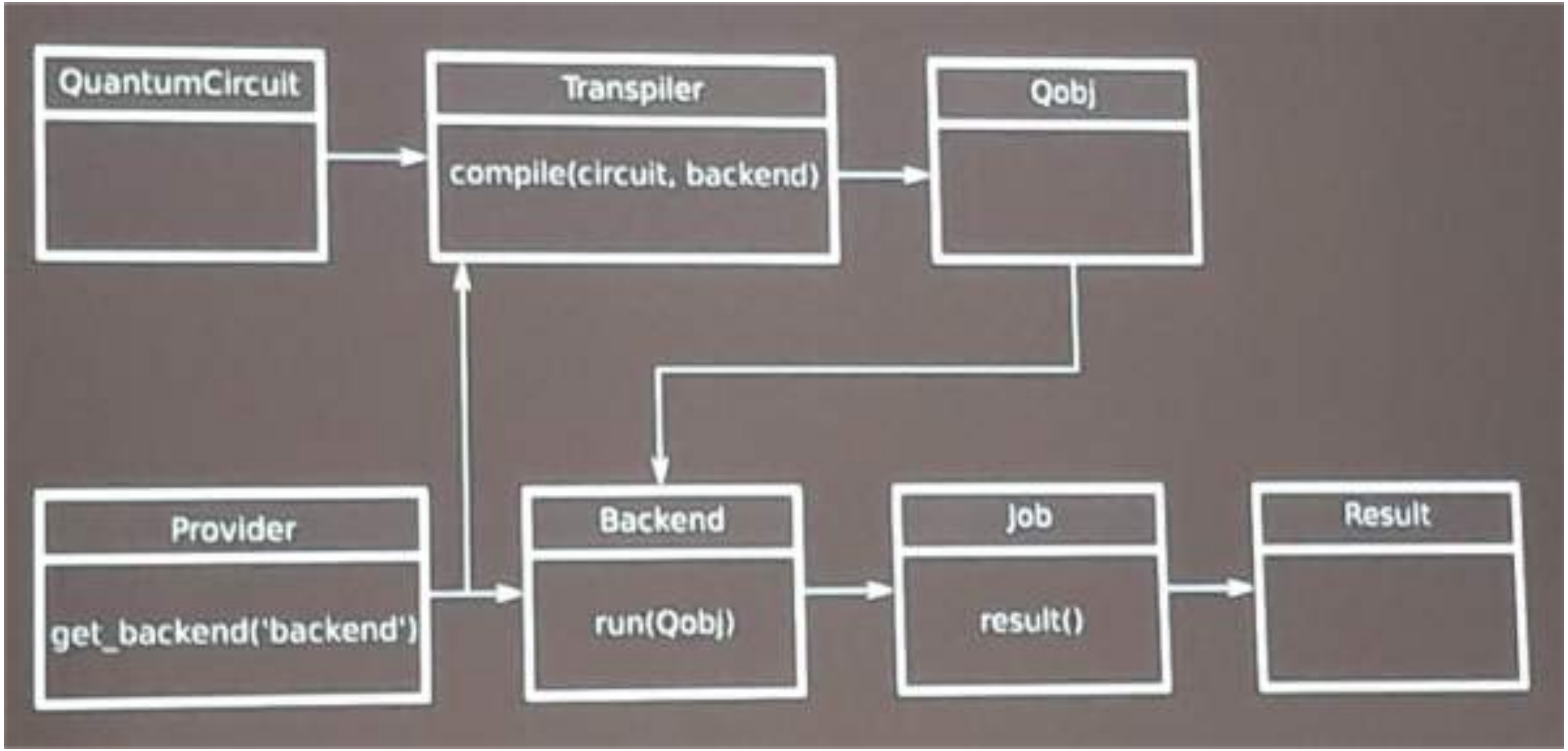
A quantum circuit is a computational routine consisting of coherent quantum operations on quantum data, such as qubits, and concurrent real-time classical computation. **It is an ordered sequence of quantum gates, measurements and resets, which may be conditioned on and use data from real-time classical computations.** A set of quantum gates is said to be universal if any unitary transformation of the quantum data can be efficiently approximated arbitrarily well as as sequence of gates in the set. Any quantum program can be represented by a sequence of quantum circuits and non-concurrent classical computation.

http://qiskit.org/textbook/ch-circuits/defining-circuits.html

Algoritmo cuántico



Circuito cuántico en un ordenador



Puertas lógicas cúanticas universales

- Conjunto universal de puertas:
  {CNOT, Hadamard, fase relativa}

Arbitrary relative phase

$$
\begin{aligned}
U_\phi|0\rangle &= |0\rangle \\
U_\phi|1\rangle &= e^{i\phi}|1\rangle
\end{aligned}
$$

Hadamard

$$
\begin{aligned}
U_H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
U_H|1\rangle &= \frac{1}{\sqrt{2}}(|1\rangle - |1\rangle)
\end{aligned}
$$

CNOT (XOR)

$$
\begin{aligned}
U_{CNOT}|0\rangle|0\rangle &= |0\rangle|0\rangle \\
U_{CNOT}|0\rangle|1\rangle &= |0\rangle|1\rangle \\
U_{CNOT}|1\rangle|0\rangle &= |1\rangle|1\rangle \\
U_{CNOT}|1\rangle|1\rangle &= |1\rangle|0\rangle
\end{aligned}
$$

Sistema de 2 Qubits

Para extender este sistema a 2 qubits haremos un “producto tensorial” entre las bases de cada sistema de 1 qubit.

$$|a\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}, \quad |b\rangle = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

$$|ba\rangle = |b\rangle \otimes |a\rangle = \begin{bmatrix} b_0 \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \\ b_1 \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} b_0 a_0 \\ b_0 a_1 \\ b_1 a_0 \\ b_1 a_1 \end{bmatrix}$$

Producto tensorial entre matrices

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix}$$

Producto tensorial entre vectores: ídem matrices

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \otimes w = \begin{pmatrix} v_1.w \\ v_2.w \\ \vdots \\ v_n.w \end{pmatrix}$$

Sistema de 2 Qubits

Para extender este sistema a 2 qubits haremos un "producto tensorial" entre las bases de cada sistema de 1 qubit.

$$|0\rangle \otimes |0\rangle \equiv |00\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|1\rangle \otimes |0\rangle \equiv |10\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$|0\rangle \otimes |1\rangle \equiv |01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|1\rangle \otimes |1\rangle \equiv |11\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Sistema de 3 Qubits

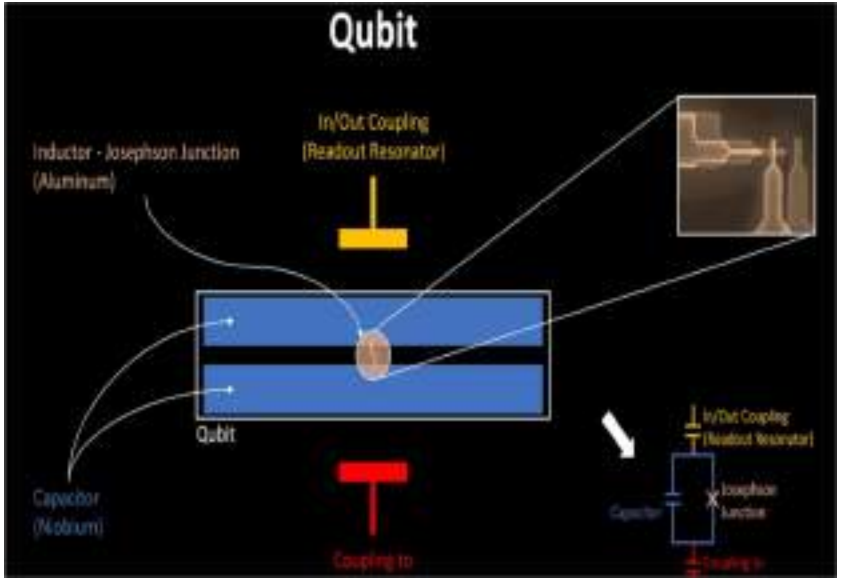
Para extender este sistema a 3 qubits haremos un "producto tensorial" entre las bases de cada sistema de 1 qubit.

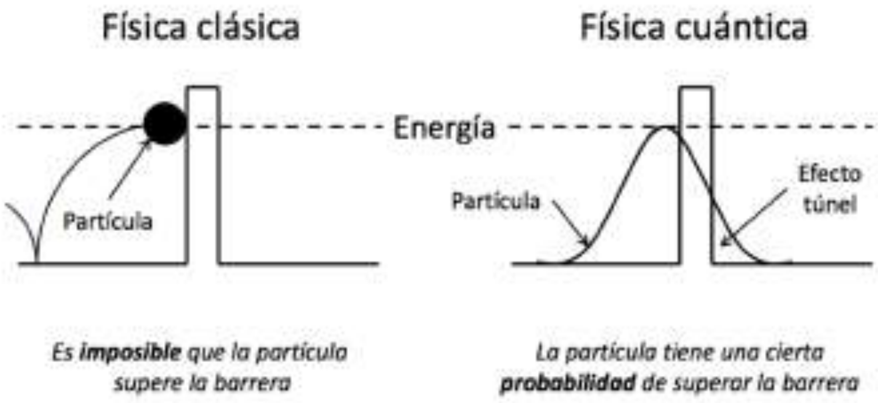
$$|1\rangle \otimes |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

https://qiskit.org/textbook/ch-gates/multiple-qubits-entangled-states.html

Como hacer un Qubit: Solid-state device

- Circuito superconductor basado en una unión de Josephson que crea un enlace débil entre dos superconductores.

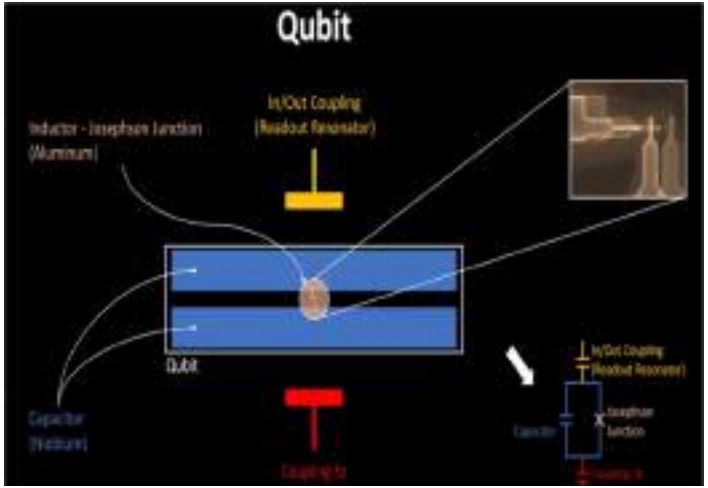


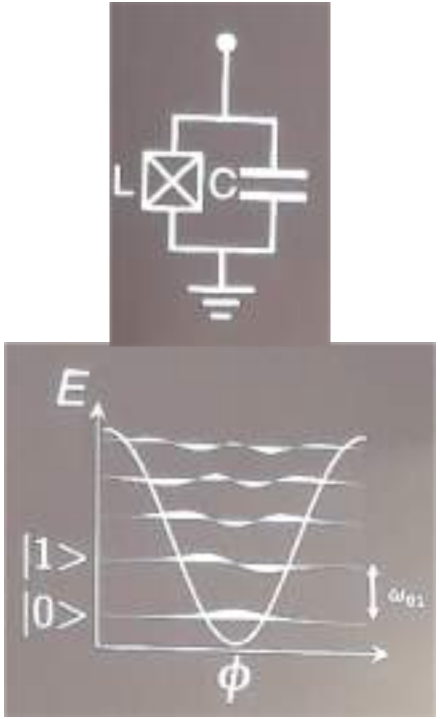


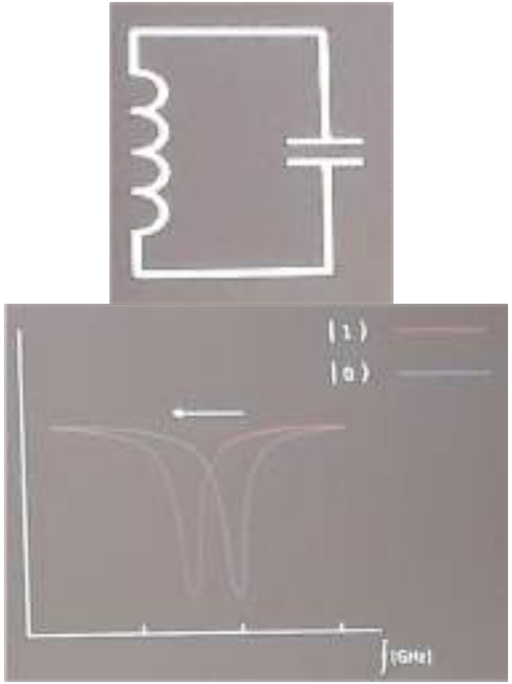
Efecto tunel

Como hacer un Qubit: Solid-state device

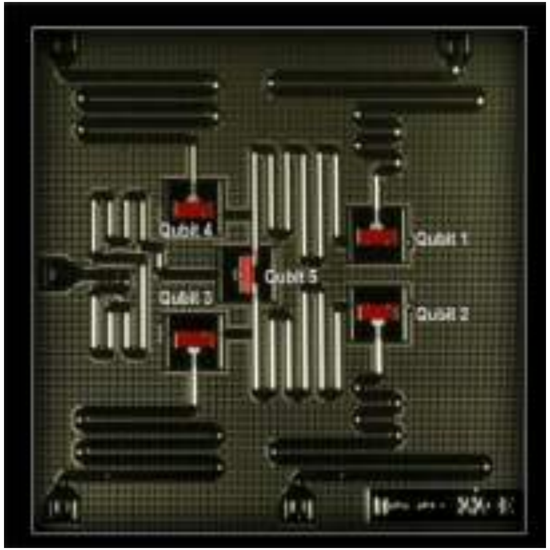
- Estados |0> y |1> con diferente energía

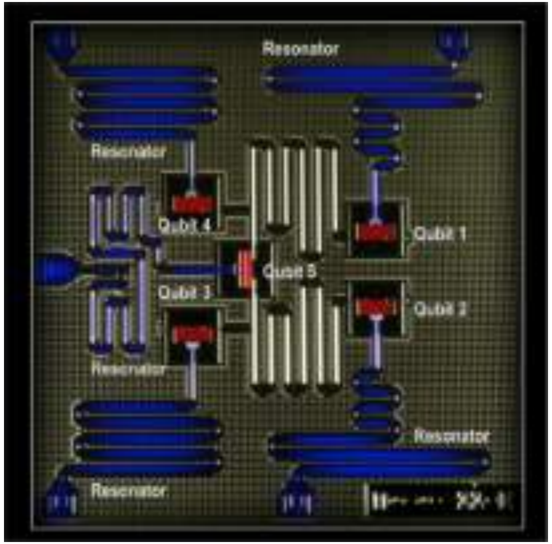


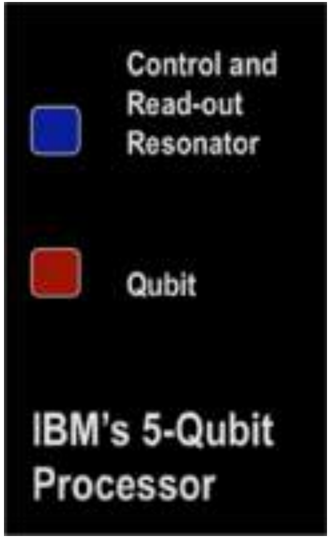




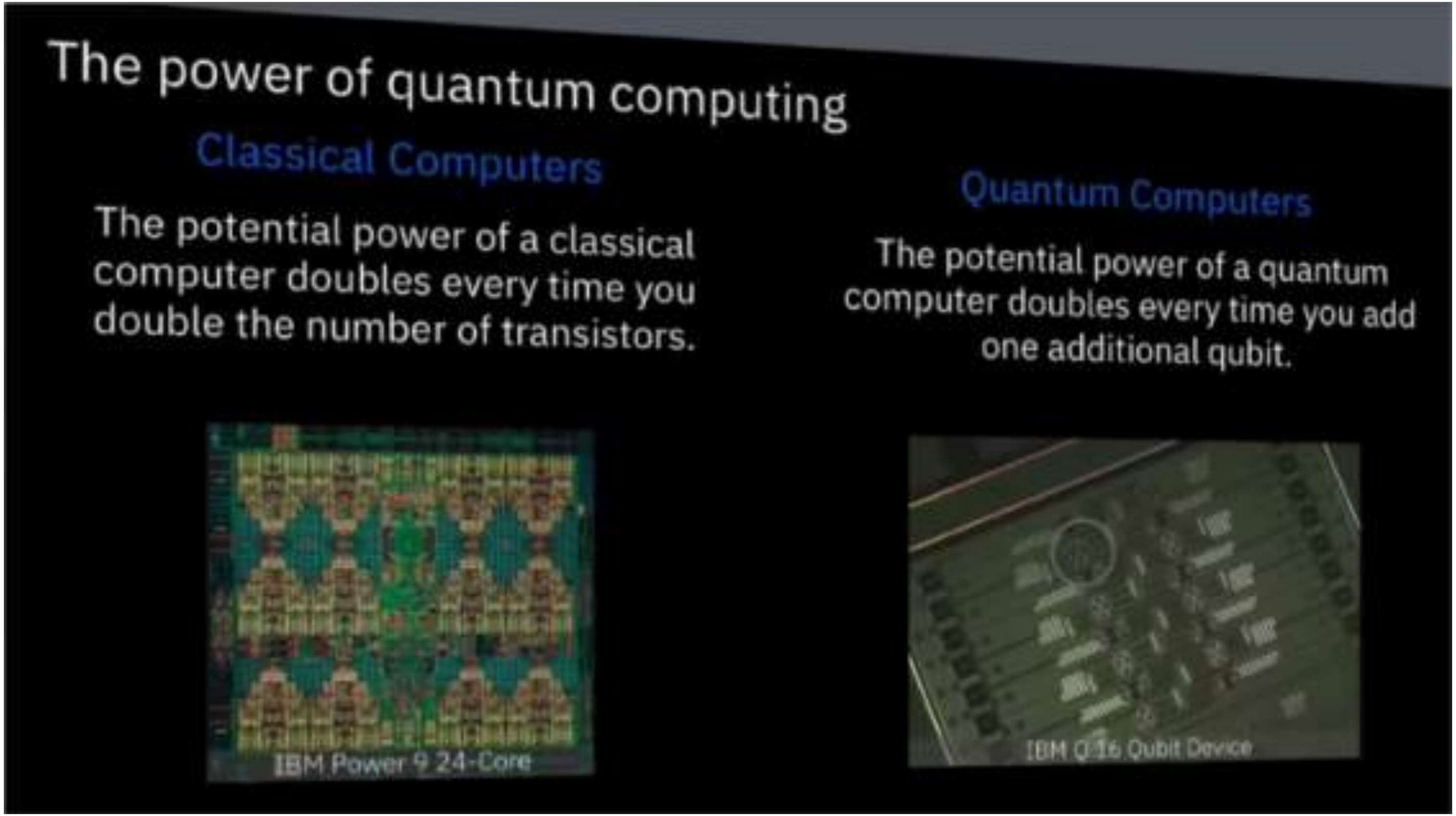
Conectando y controlando los Qubit







Escalado de potencia en un computador cuántico



Escalado de potencia en un computador cuántico

- Quantum computers, would be based on the strange principles of quantum mechanics, in which the smallest particles of light and matter can be in different places at the same time.
- In a quantum computer, one "qubit" - quantum bit - could be both 0 and 1 at the same time. So with three qubits of data, a quantum computer could store all eight combinations of 0 and 1 simultaneously. That means a three-qubit quantum computer could calculate eight times faster than a three-bit digital computer.
- Typical personal computers today calculate 64 bits of data at a time. A quantum computer with 64 qubits would be 2 to the 64th power faster, or about 18 billion billion times faster. (Note: billion billion is correct.)

Computador clásico

Registros de bits + Puertas Lógicas y Memoria = Computador Clásico

0

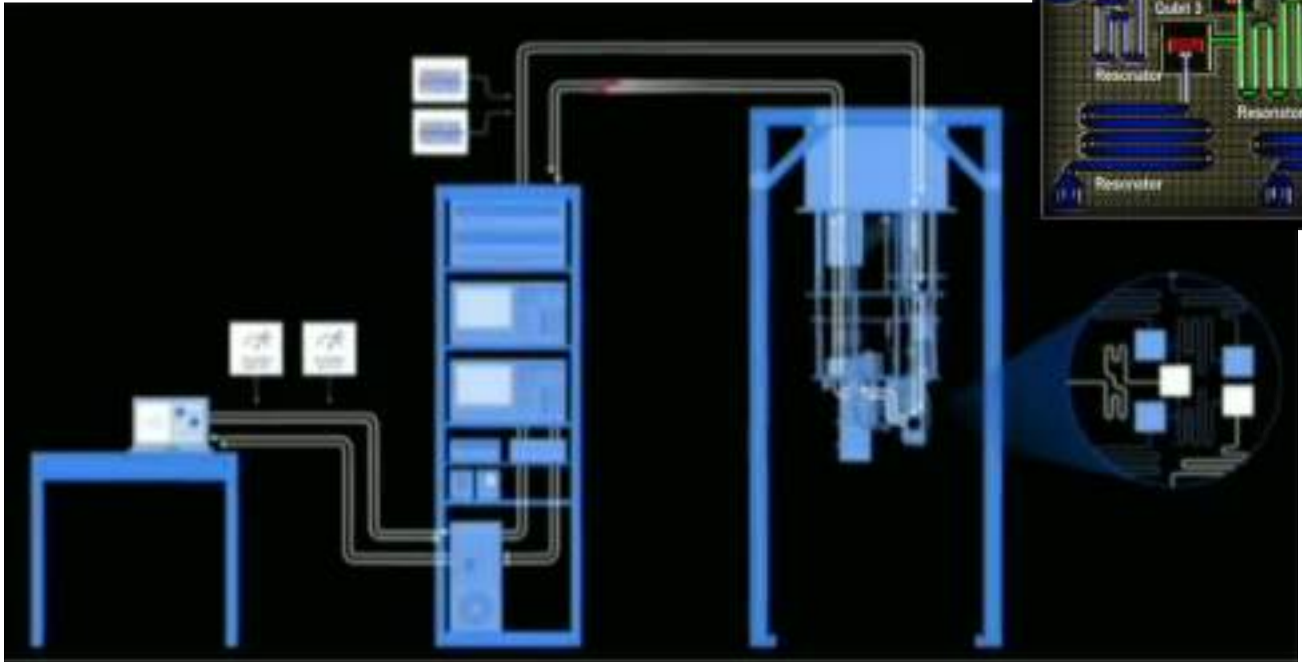
1

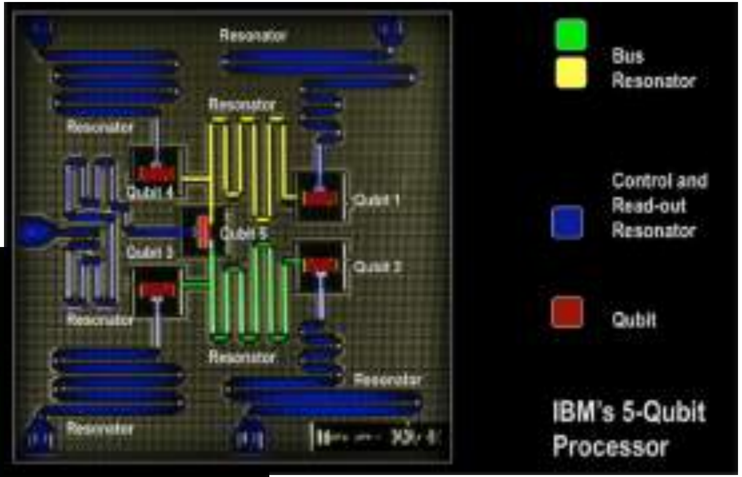
+

=

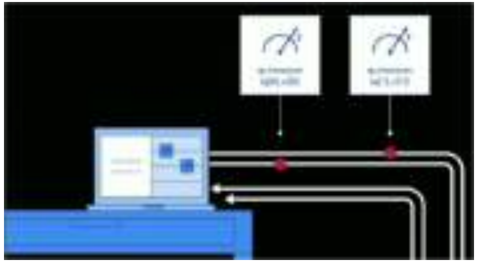
Computador cuántico de IBM

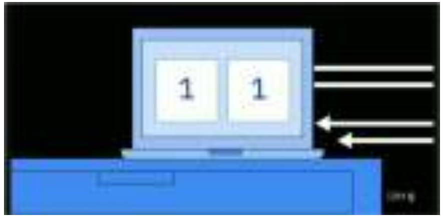
Join the IBM Q Experience Community
https://quantumexperience.ng.bluemix.net

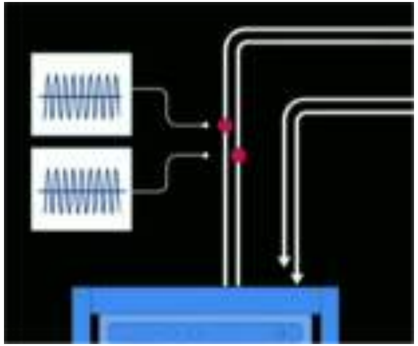


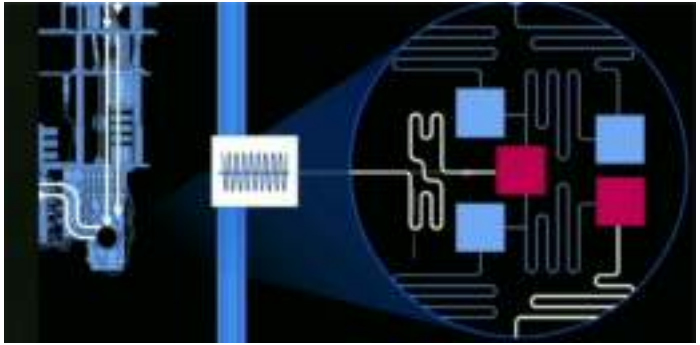


Cómo funcionan los Qbit

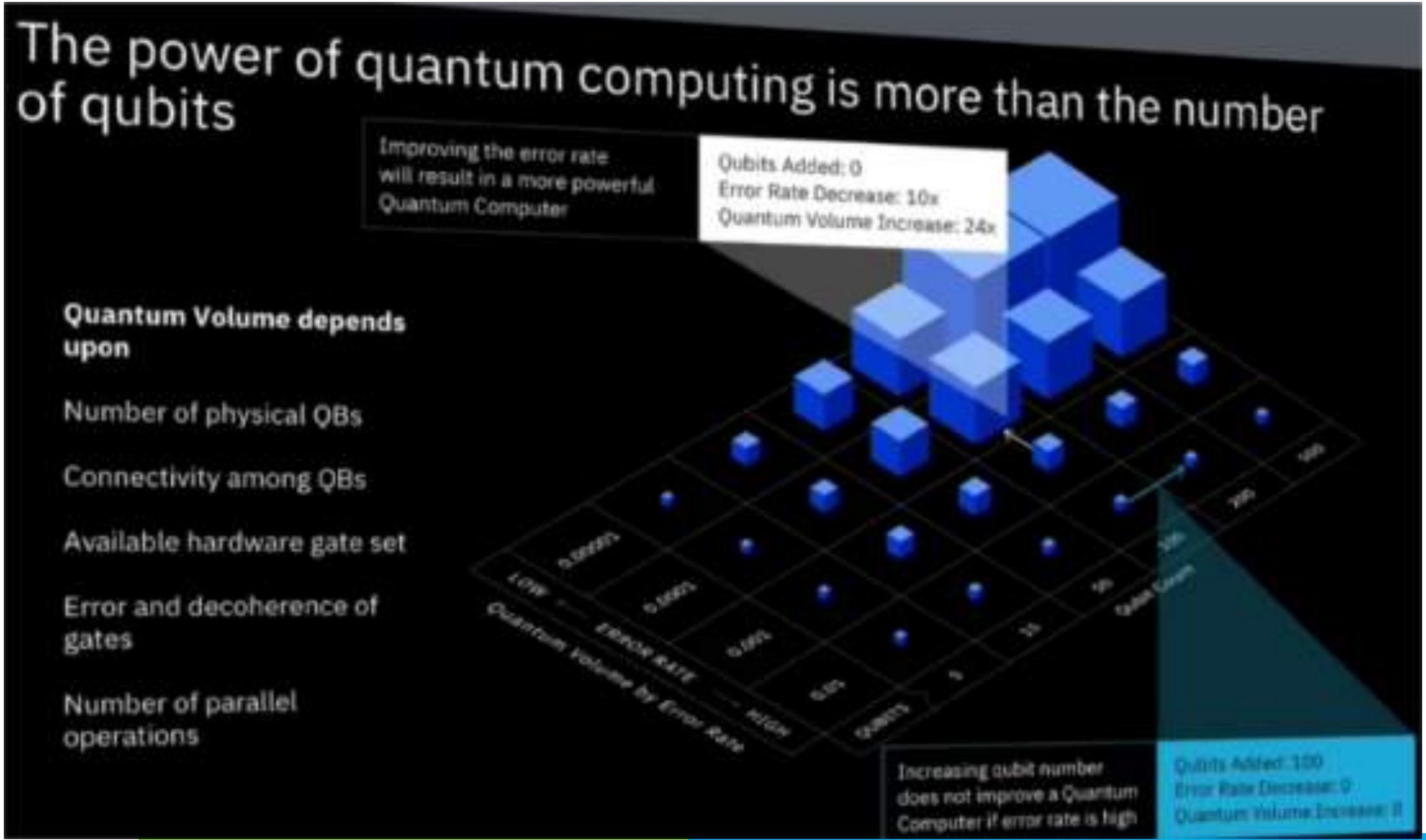




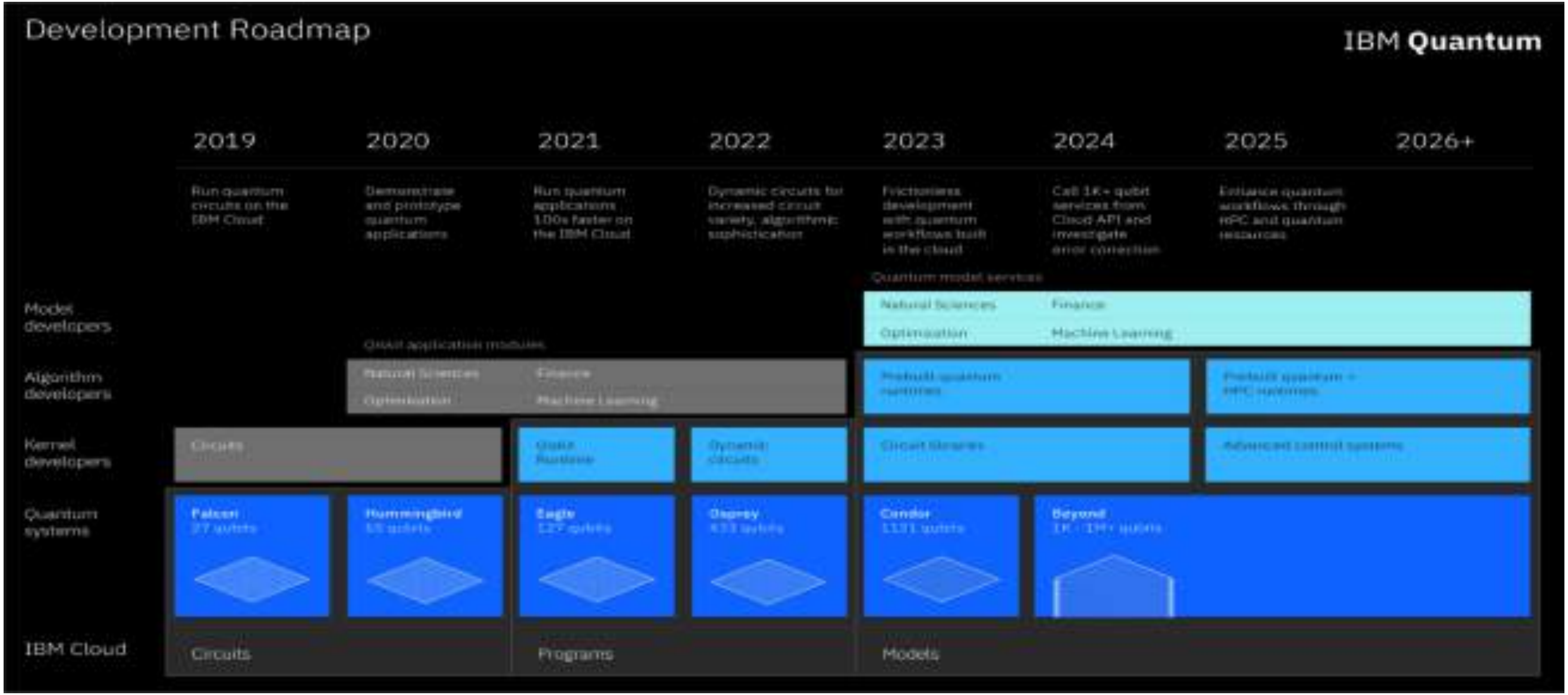




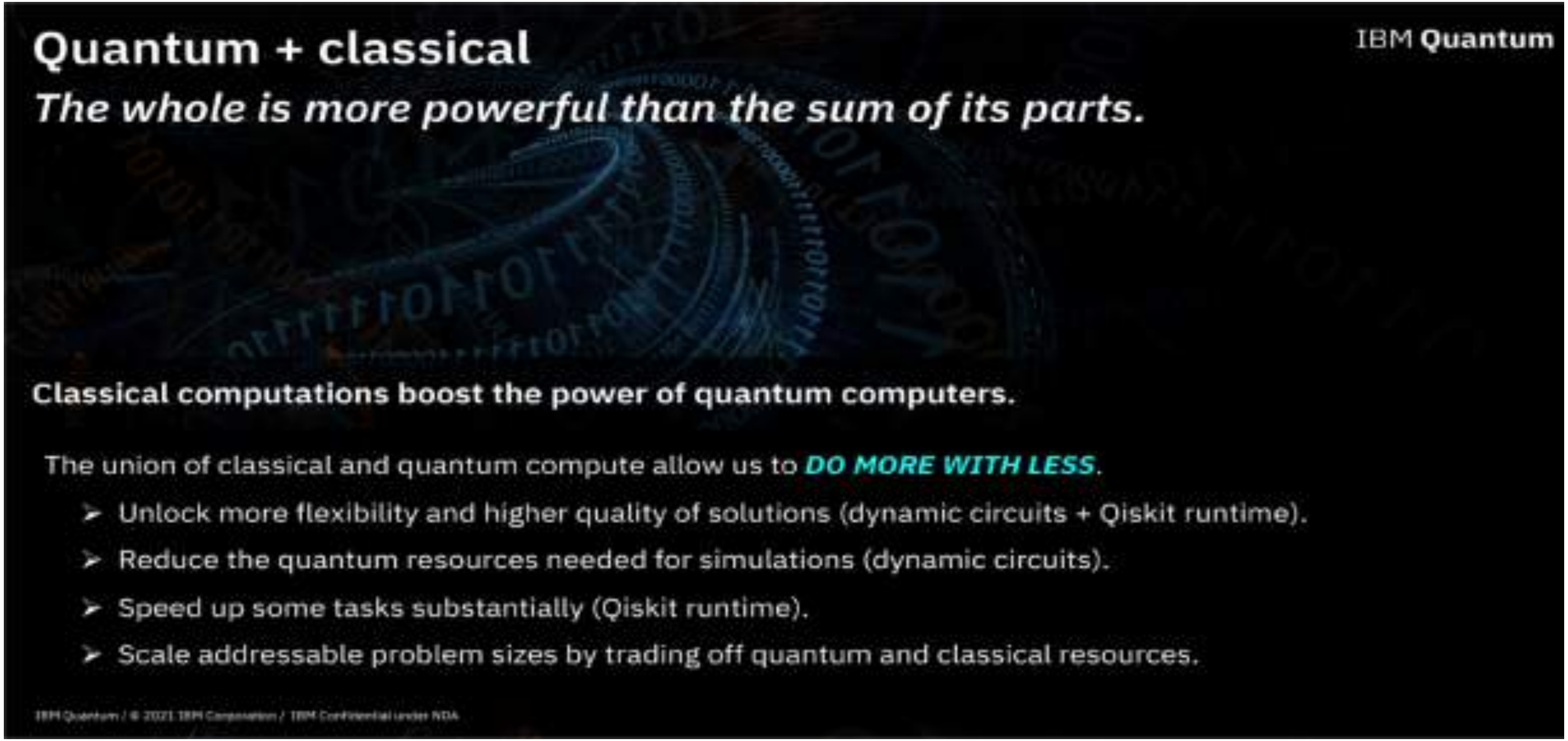
Volumen Cuántico



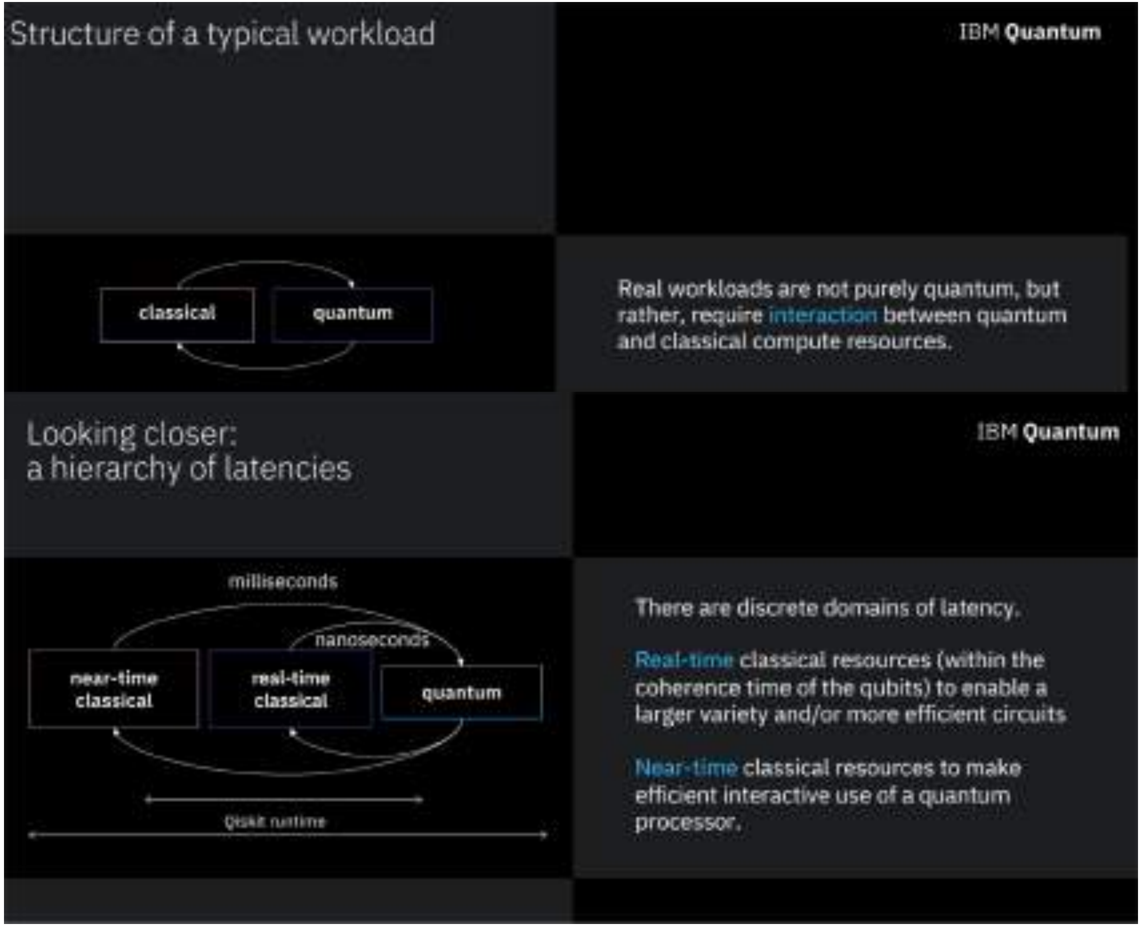
Roadmap Cuántico



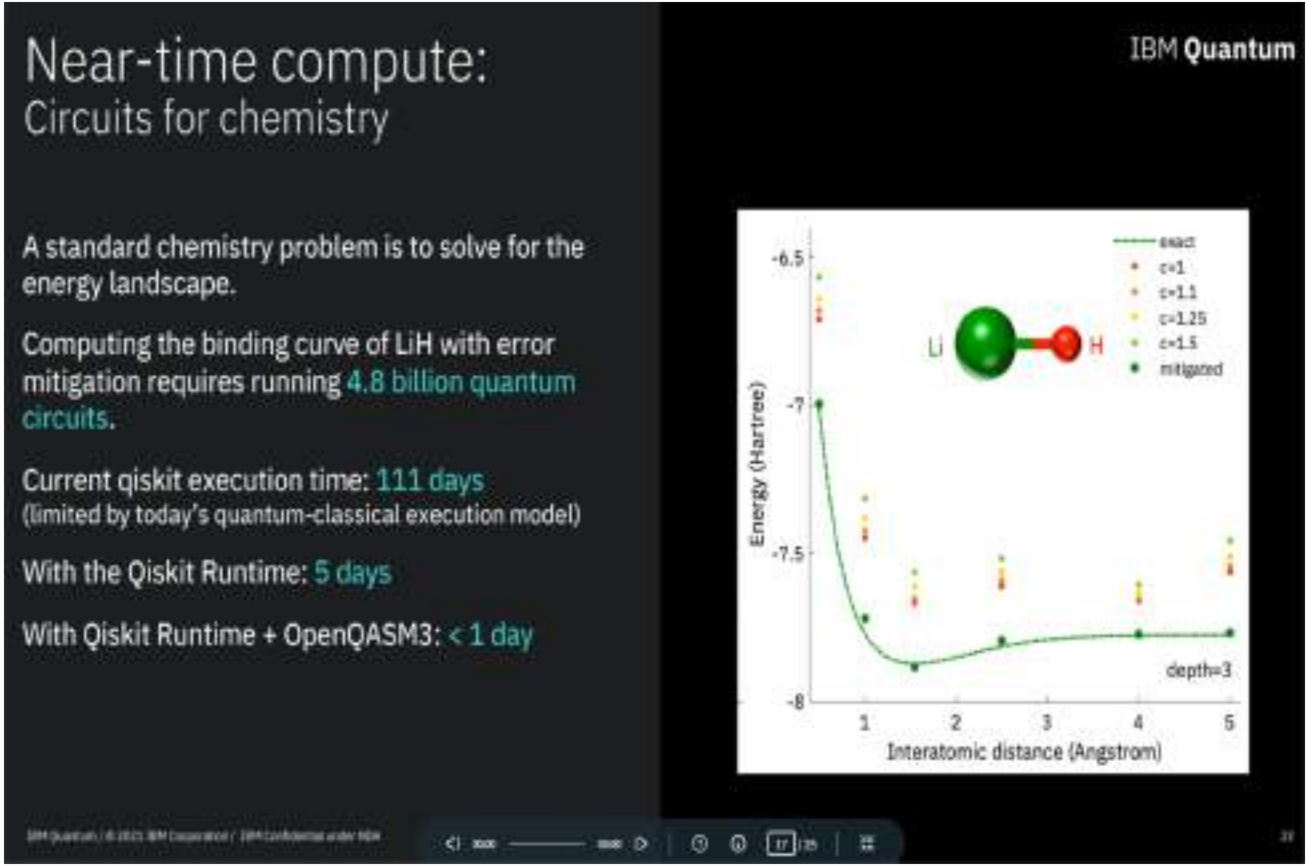
Quantum + Classical



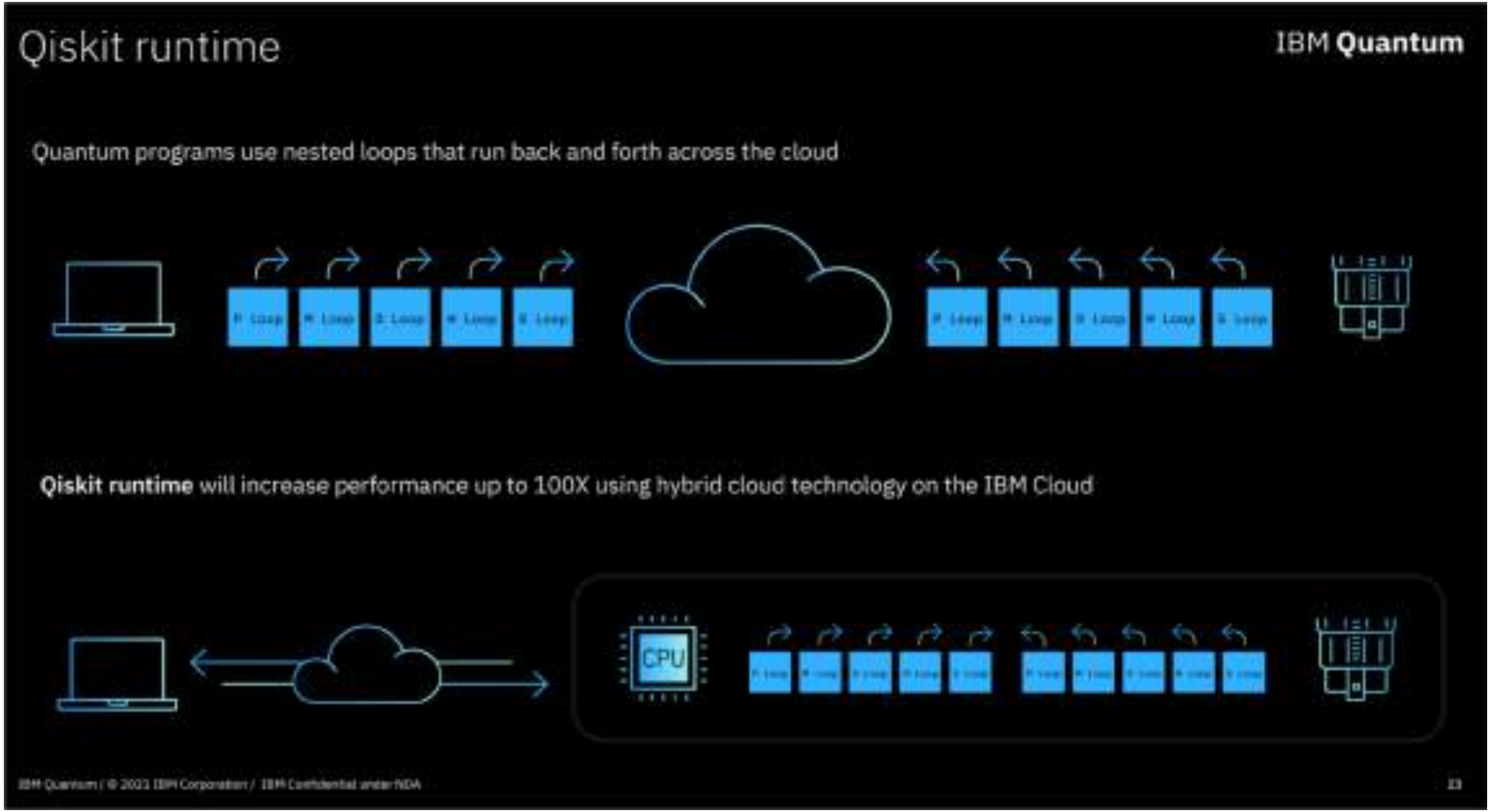
Real-time and near-time



Real-time and near-time

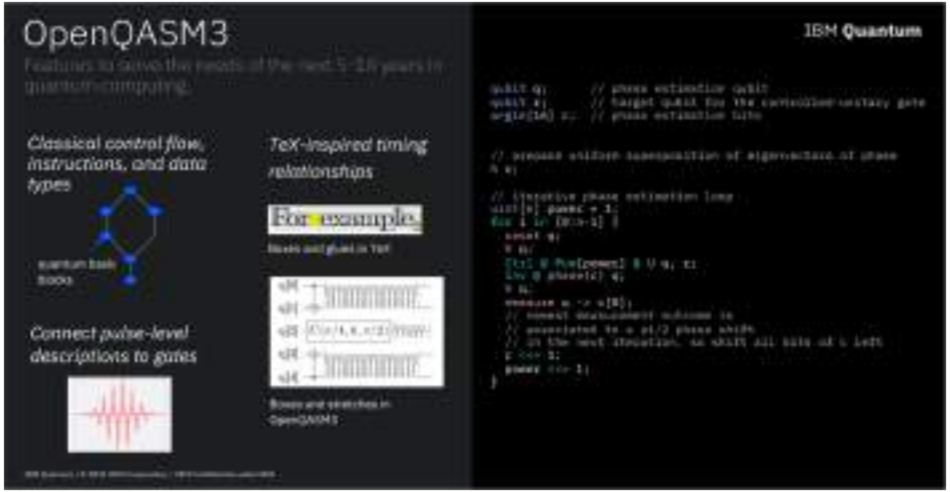


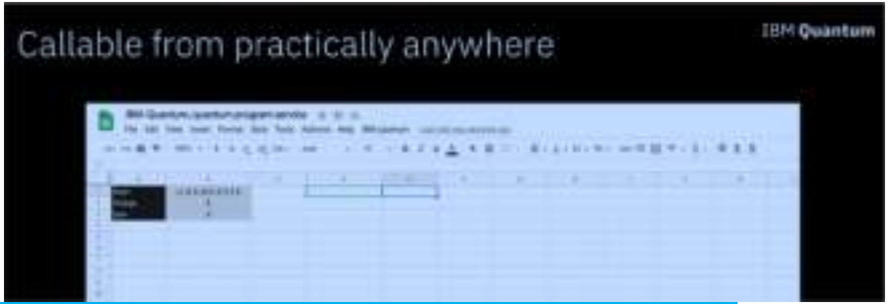
Quantum + Classical



Quantum + Classical

Quantum + Classical

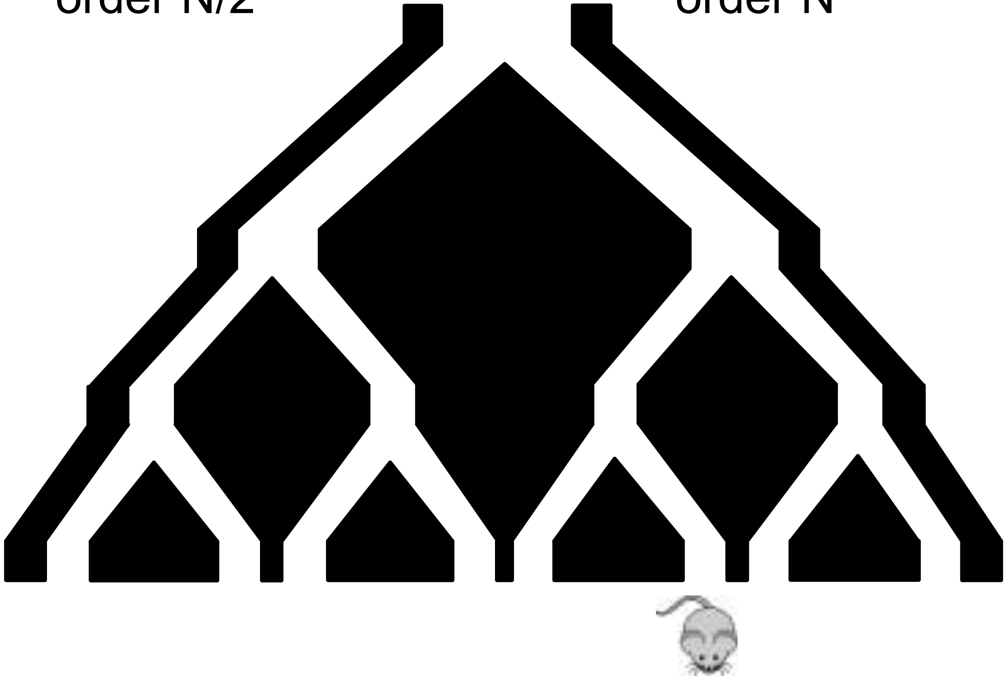


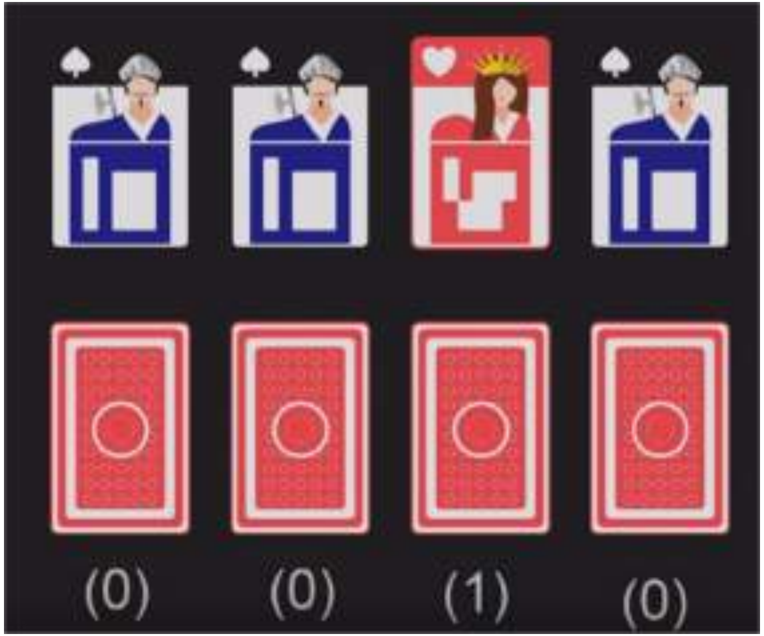


Algoritmos para computadores cuánticos: Grover

Clasical search:
order N/2

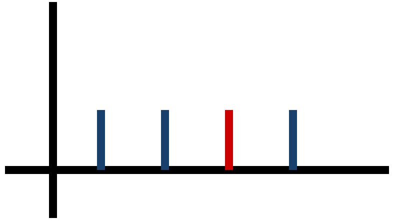
Quantum search:
order $N^{1/2}$



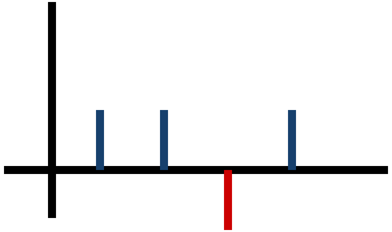


Algoritmo de Grover

$$G = (2|\psi\rangle\langle\psi| - I)O$$



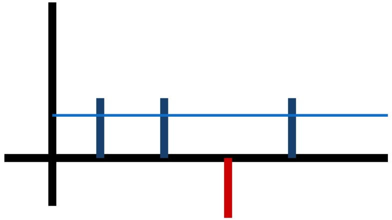
Amplitudes Originales



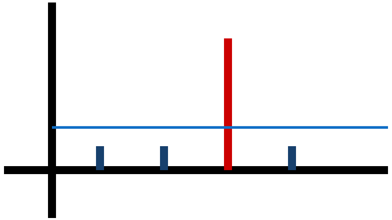
Invertir la amplitud que indica el "oraculo"

oracle function

$$|\mathbf{x}\rangle|q\rangle \xrightarrow{O} |\mathbf{x}\rangle|f(\mathbf{x})\oplus q\rangle$$



Amplitude media



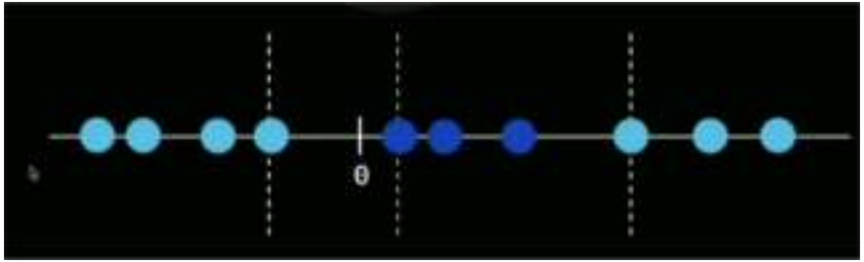
Cambiar (Flip) Amplitudes respecto a la media

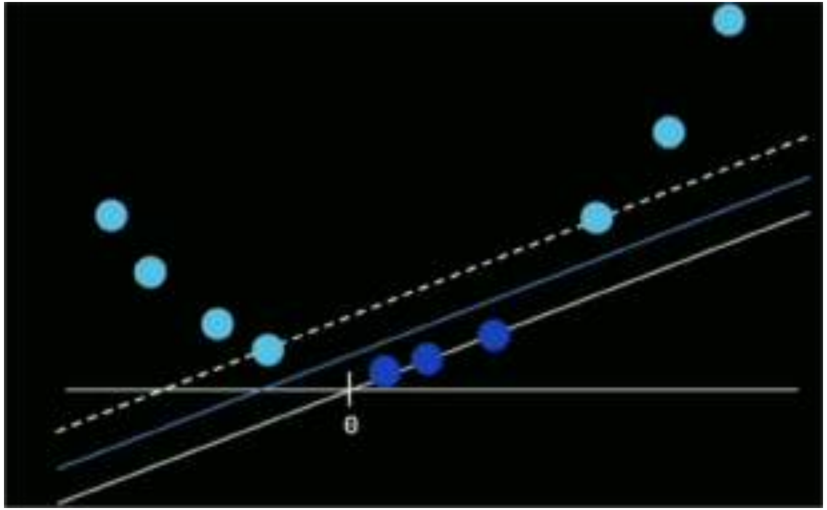
$$(2|\psi\rangle\langle\psi| - I)\sum_i a_i|i\rangle = \sum_i \underbrace{(2\langle a\rangle - a_i)}_{\text{flip around the average}}|i\rangle$$

where $\langle a\rangle = \frac{\sum_i a_i}{\sum_i 1}$

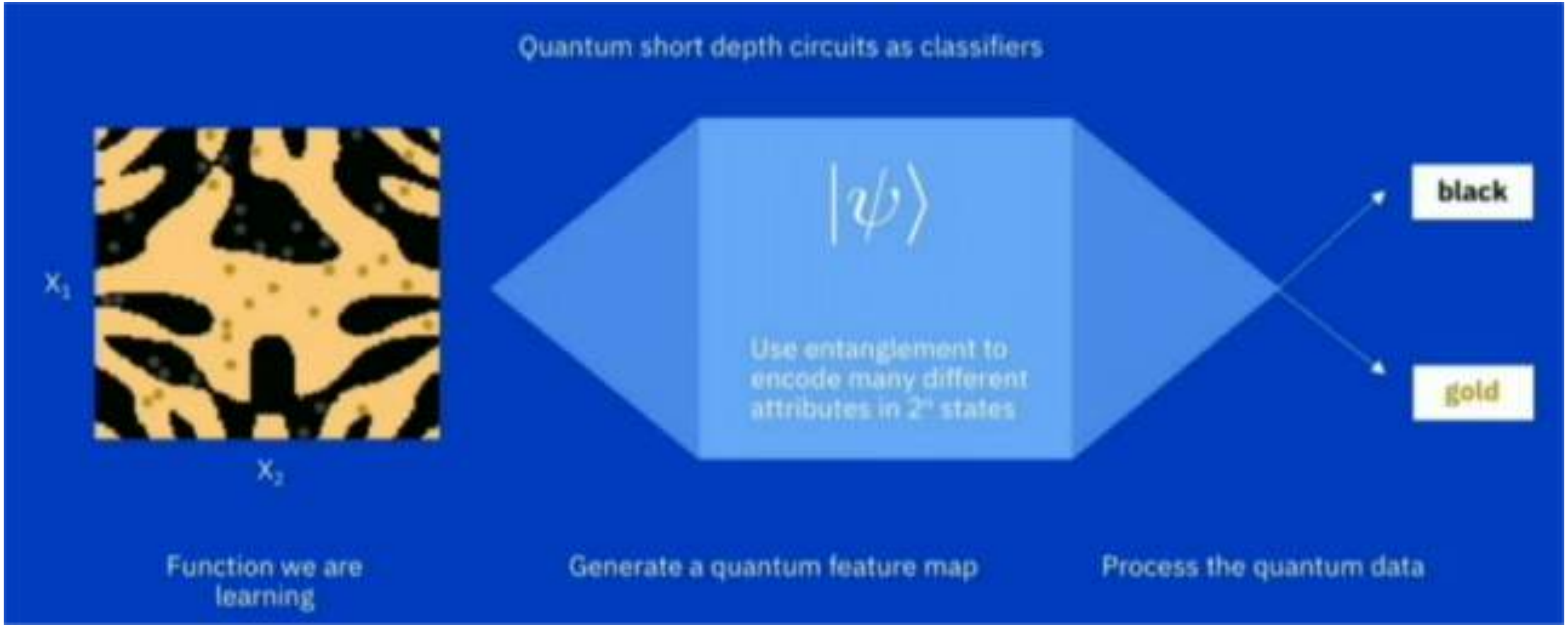
Machine Learning: Algoritmos de Clasificación

Idea de base: Incremento de la dimensión del espacio de busqueda para facilitar la separación de las clases





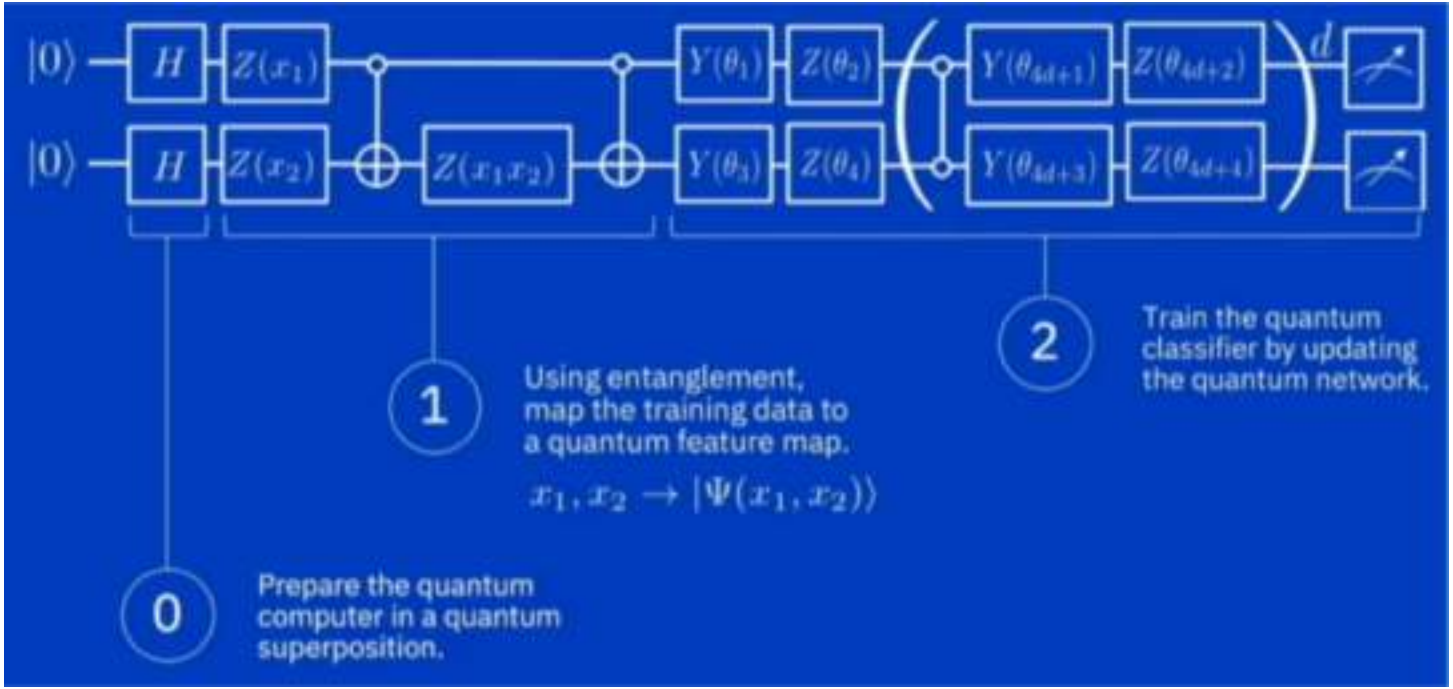
QC-ML: Algoritmos de Clasificación con entrelazamiento



Supervised learning with quantum-enhanced feature spaces

Vojtěch Havlíček, Antonio D. Córcoles, Kristan Temme, Aram W. Harrow, Abhinav Kandala, Jerry M. Chow & Jay M. Gambetta Nature volume 567, pages 209–212 (2019) https://www.nature.com/articles/s41586-019-0980-2

QC-ML: Clasificador cuántico



Ejemplo de Algoritmo Cuántico: Deutsch

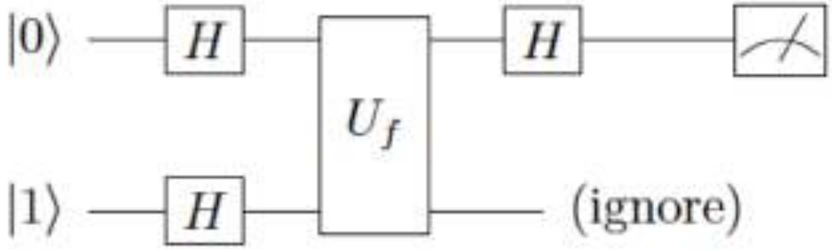
x	1
0	0
1	1

x	$\neg$
0	1
1	0

x	$[0]$
0	0
1	0

x	$[1]$
0	1
1	1

So exactly two of our unary ops are *constant* and the other two are *balanced* = *one-to-one* = *not constant*.



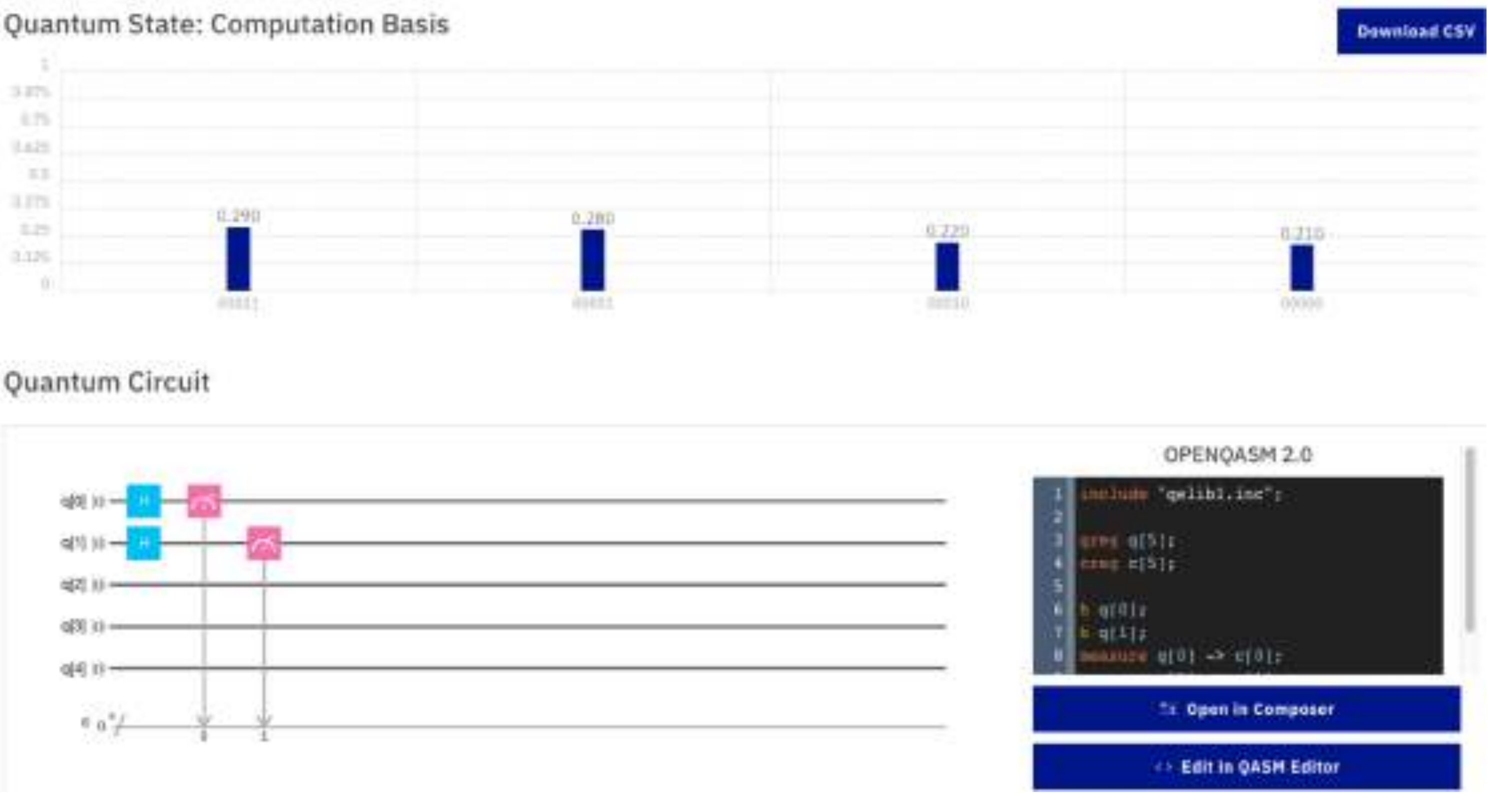
$$U_f\left(|x\rangle\,|-\rangle\right) \;=\; (-1)^{f(x)}\,|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \;=\; \left((-1)^{f(x)}\,|x\rangle\right)|-\rangle\,,$$

Referencias

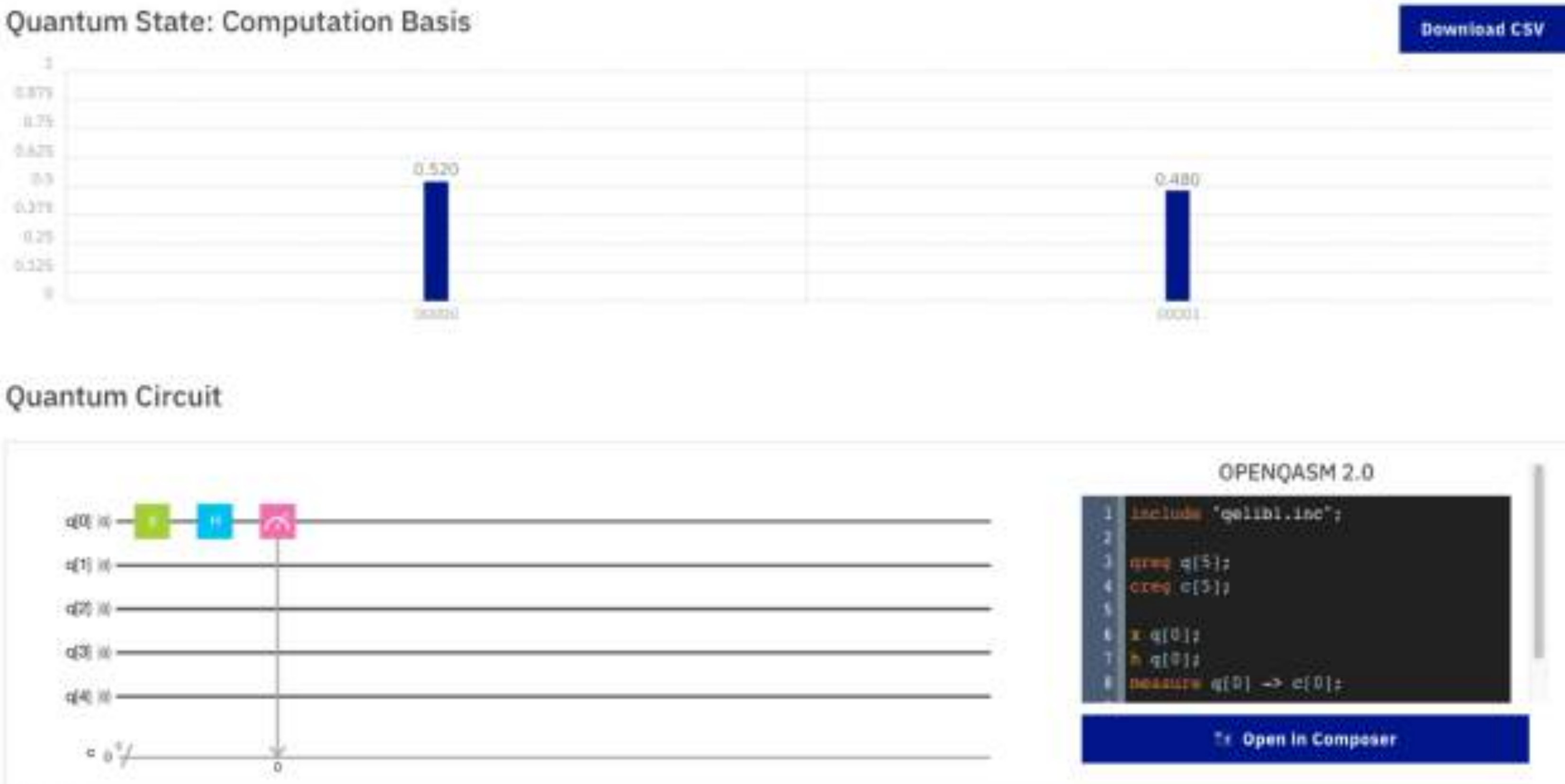
- https://qiskit.org/textbook/preface.html

- Quantum Computation and Quantum Information by Michael A. Nielsen & Isaac L. Chuang

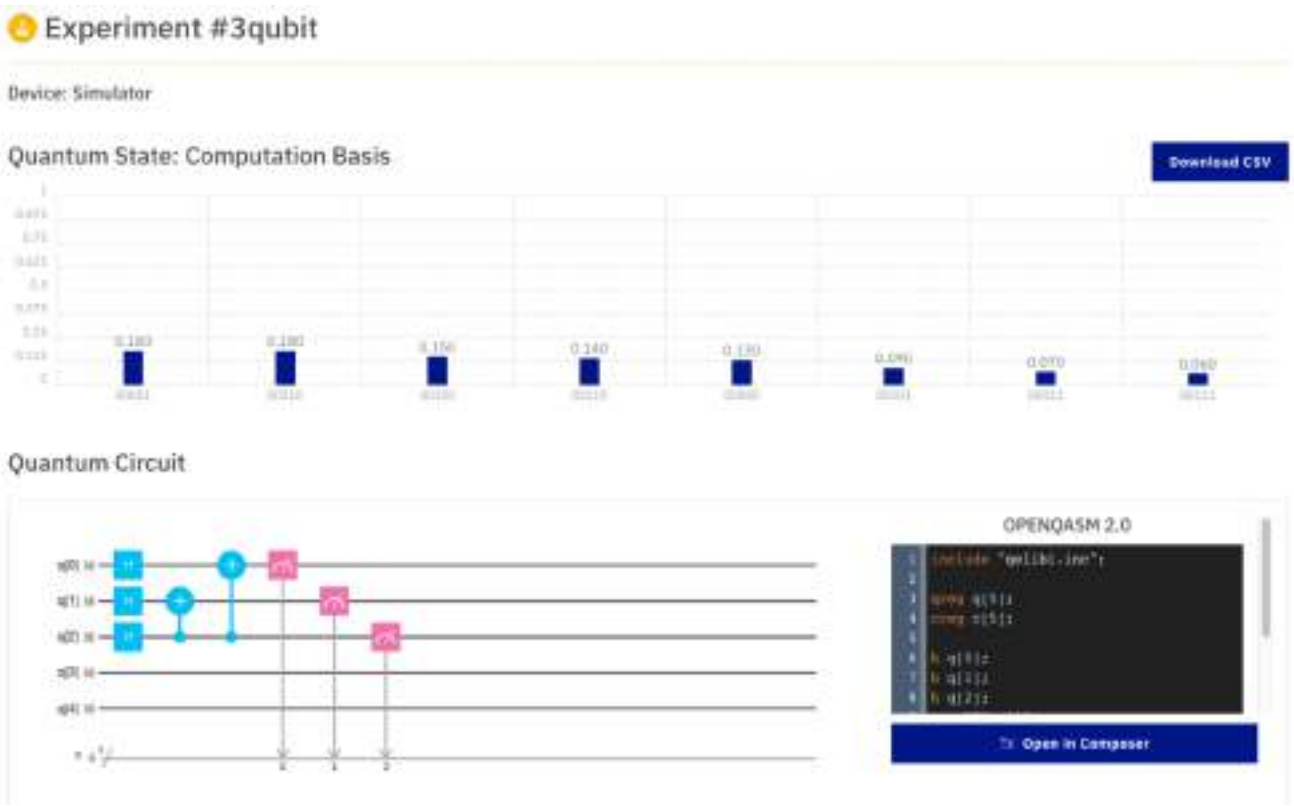
Apéndice : Ejemplos de circuitos cuánticos para IBMQ



Apéndice : Ejemplos de circuitos cuánticos para IBMQ



Apéndice : Ejemplos de circuitos cuánticos para IBMQ



Apéndice : Ejemplos de circuitos cuánticos para IBMQ

Apéndice : Bernstein-Vazirani Algorithm

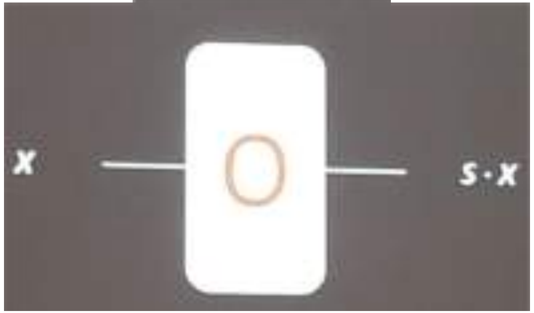
$$f: \{0,1\}^n \rightarrow \{0,1\}$$

$$f(x) = s \cdot x = \sum_{i=1}^{n} s_i \cdot x_i$$

s: contraseña secreta

$$s = 101$$

$$f(x) = s \cdot x$$



$$f(000) = 1 \cdot 0 + 0 \cdot 0 + 1 \cdot 0 = 0$$

¿?

$f(001) = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 1 = 1$!! $s = ??1$

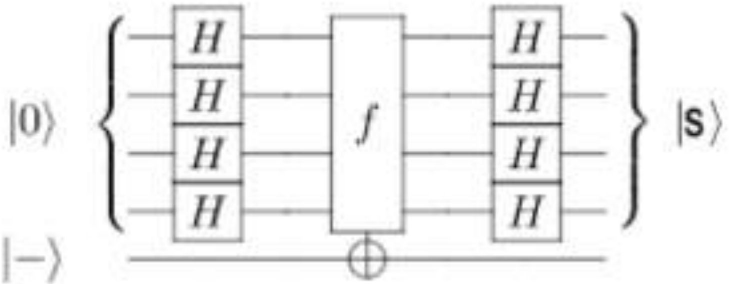
$f(010) = 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 0 = 0$!! $s = ?01$

$f(100) = 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 0 = 1$!! $s = 101$!!

https://www.youtube.com/watch?v=sqJIpHYl7oo

https://qiskit.org/textbook/ch-algorithms/bernstein-vazirani.html

Apéndice : Bernstein-Vazirani Algorithm



$$|a\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x}|x\rangle.$$

$$H|a\rangle = \sum_{x\in\{0,1\}} (-1)^{a\cdot x}|x\rangle.$$

$$H^{\otimes 2}|00\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle$$

$$H^{\otimes 2}|01\rangle = |00\rangle - |01\rangle + |10\rangle - |11\rangle$$

$$H^{\otimes 2}|10\rangle = |00\rangle + |01\rangle - |10\rangle - |11\rangle$$

$$H^{\otimes 2}|11\rangle = |00\rangle - |01\rangle - |10\rangle + |11\rangle$$

$$|00\dots 0\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \xrightarrow{f_a} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x}|x\rangle$$

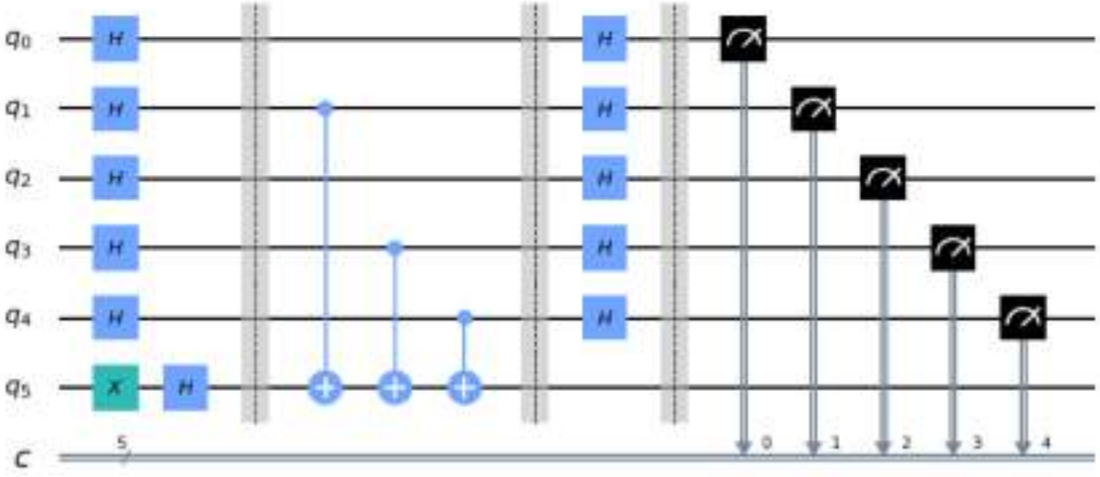
$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x}|x\rangle \xrightarrow{H^{\otimes n}} |a\rangle$$

https://qiskit.org/textbook/ch-algorithms/bernstein-vazirani.html

Apéndice : Bernstein-Vazirani Algorithm

S = 11010

Bernstein-Vazirani Oraculo




```
simulator = Aer.get_backend('qasm_simulator')
resultado= execute(circuito,backend = simulator, shots = 1).result()
counts = resultado.get_counts()
print(counts)
```

```
{'11010': 1}
```

https://www.youtube.com/watch?v=sqJIpHYl7oo

https://qiskit.org/textbook/ch-algorithms/bernstein-vazirani.html