

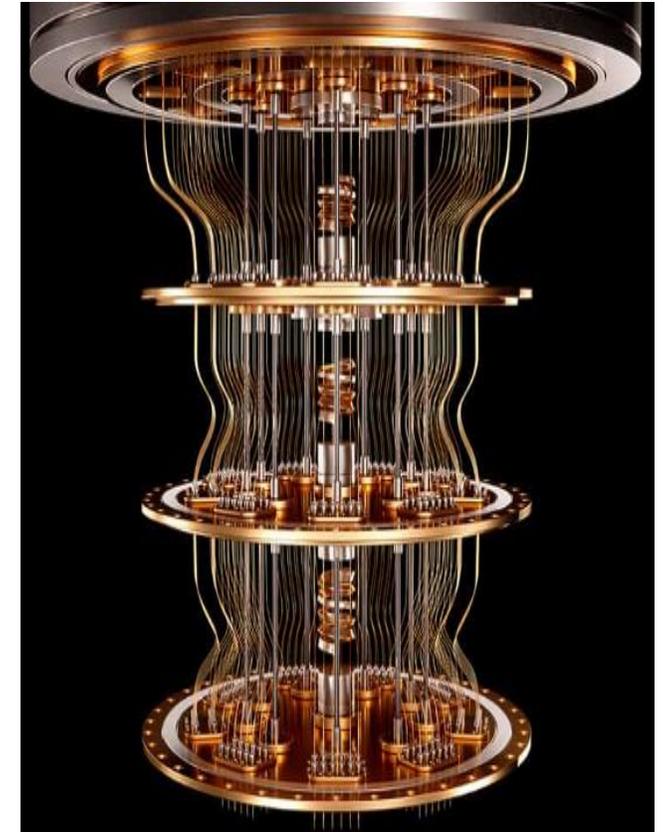
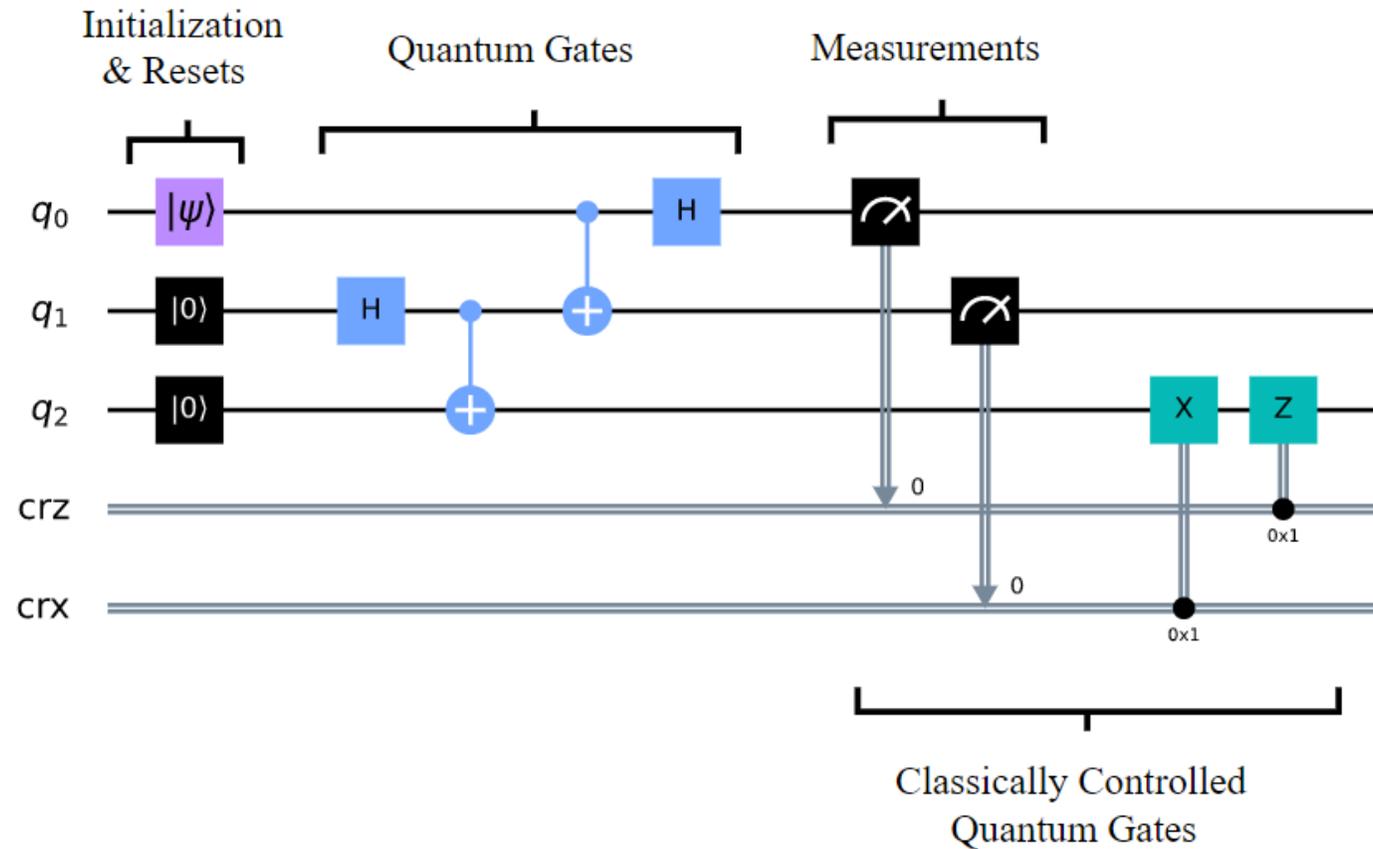


CESGA
GALICIA SUPERCOMPUTING CENTER

An introduction to Quantum Algorithms

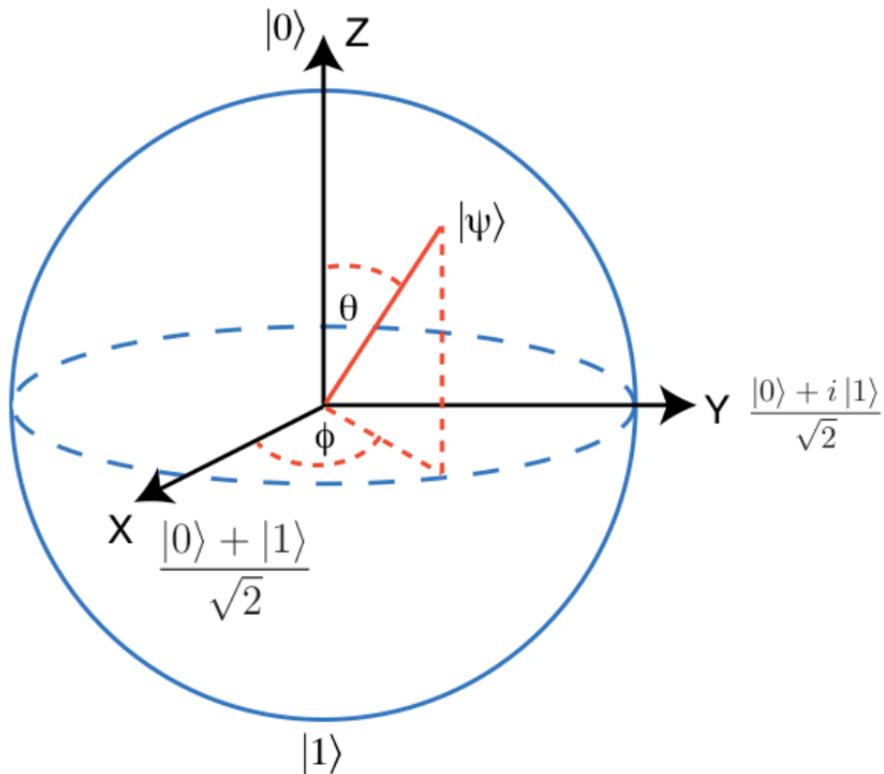
Daniel Faílde Balea
dfailde@cesga.es

¿Qué es un Algoritmo Cuántico?



Principios básicos (I): Superposición

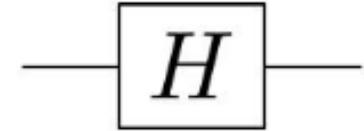
$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$



* Qiskit: An Open-source Framework for Quantum Computing

Ejemplo

Hadamard gate



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

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Principios básicos (II): Entrelazamiento

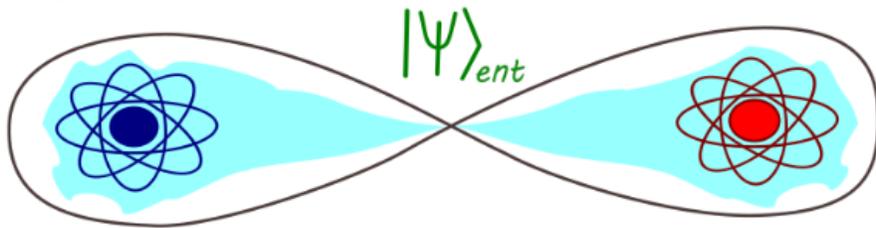
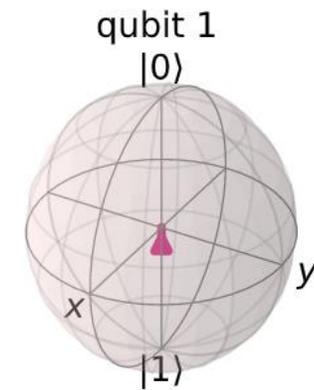
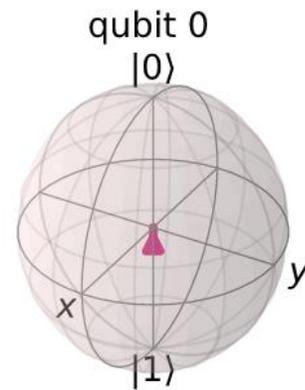
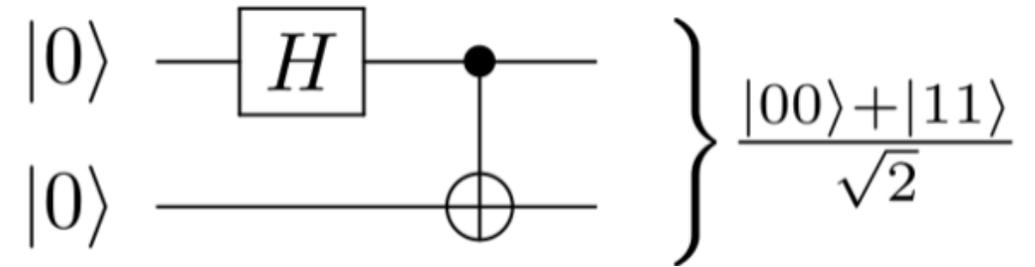
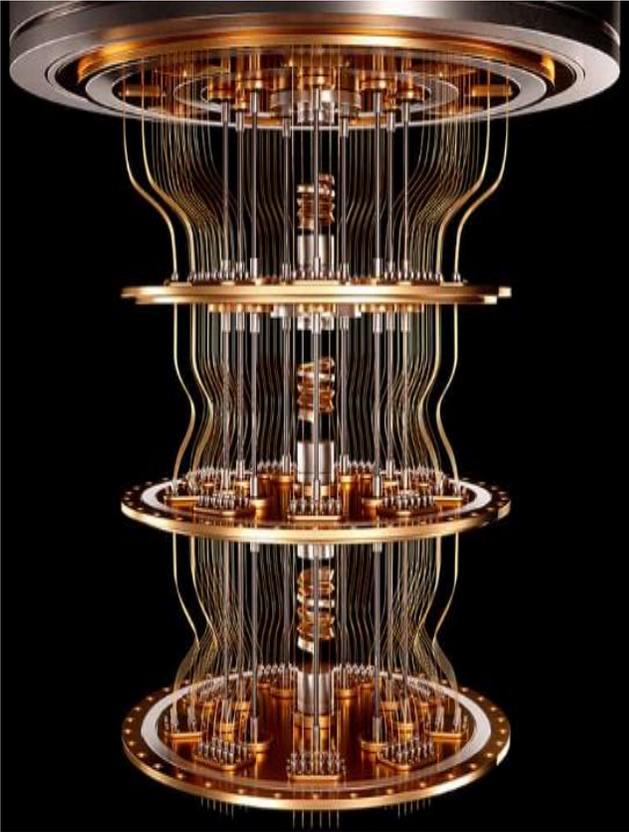


Image credits: Quantum 3, 185 (2019)



Ventaja cuántica

Capacidad de los sistemas cuánticos para resolver ciertos problemas de manera más eficiente que los sistemas clásicos.



Tipos de ventaja cuántica

- Velocidad
- Capacidad
- Seguridad
- Consumo energético
- Precisión



- Bernstein-Vazirani (1992)
- Deutsch-Jozsa (1992)
- Shor (1994)
- Grover (1996)
- ...

Primeros algoritmos cuánticos con ventaja cuántica teórica

Quantum Fourier Transform

Transformada de Fourier cuántica

Equivalente cuántico a la transformada de Fourier discreta.

Clásica

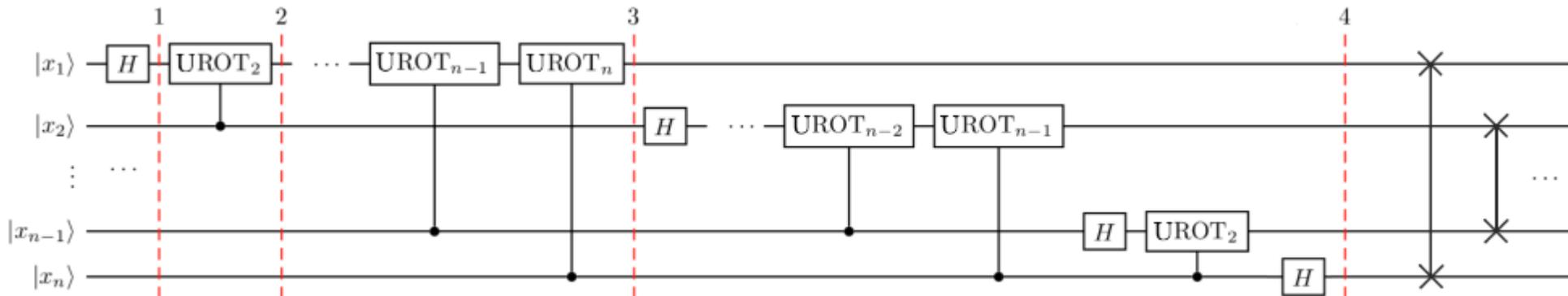
$$\mathcal{O}(n2^n)$$

Cuántica

$$\mathcal{O}(n^2)$$

Clásica: $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk}$ donde $\omega_N^{jk} = e^{i 2\pi \frac{jk}{N}}$

Cuántica: $|X\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \rightarrow |Y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$ a través de un operador $U_{QFT} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle \langle j|$



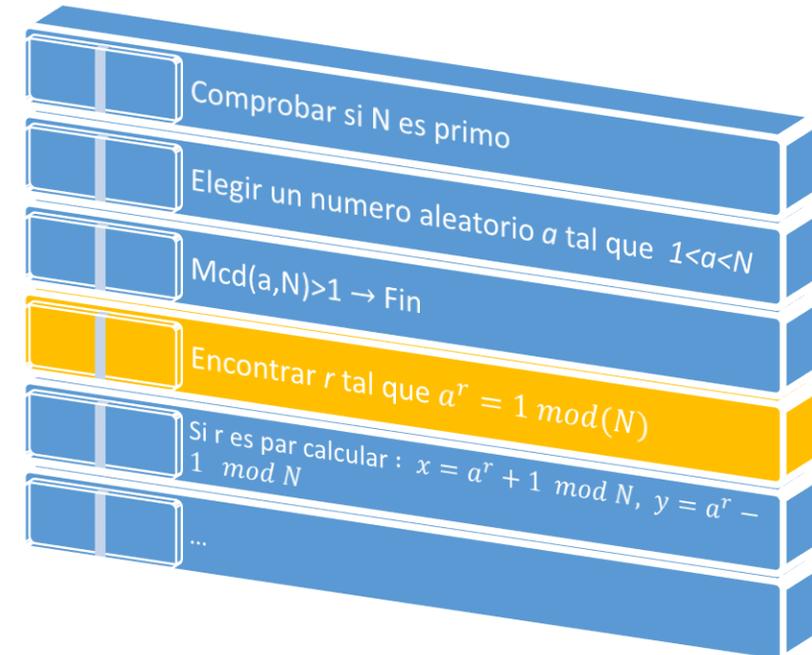
- 1) Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.
- 2) <https://indico.cern.ch/event/970903/> Elias Fernandez-Combarro Alvarez
- 3) Qiskit: An Open-source Framework for Quantum Computing

Algoritmo de Shor

Algoritmo de Shor

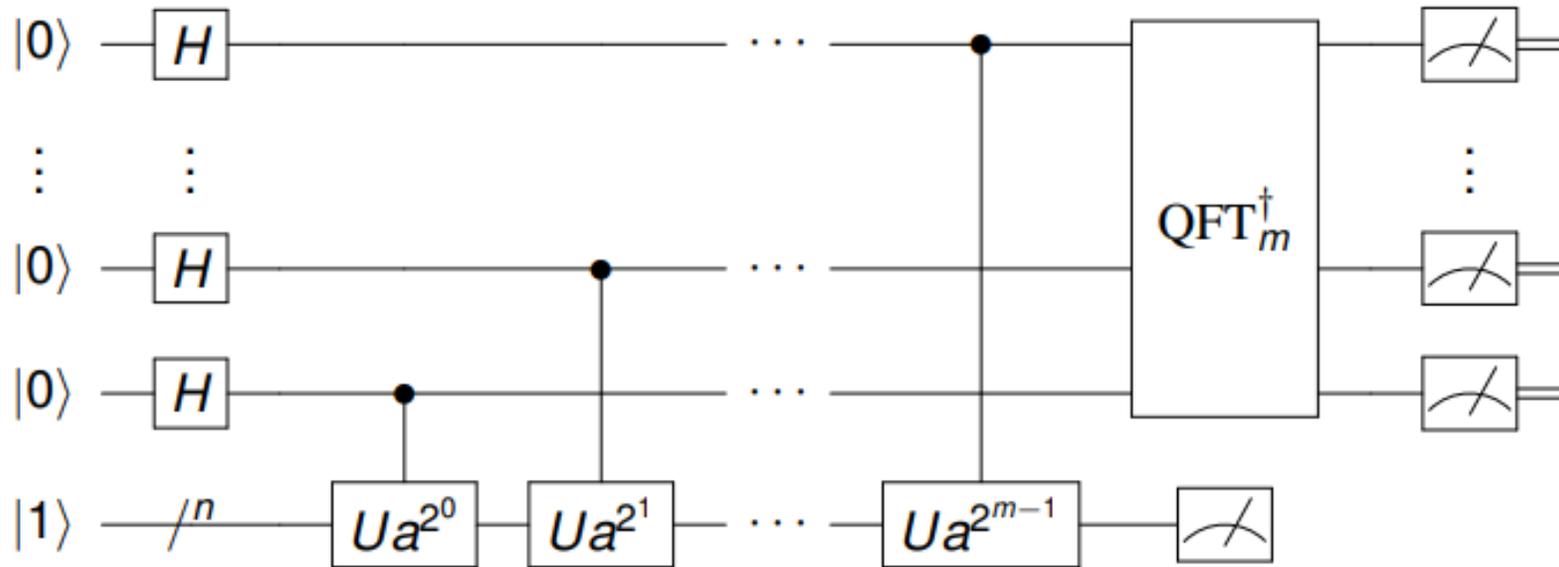
Objetivo: Encontrar los números enteros p, q que factorizan un entero dado $N = p \cdot q$

	Tiempo para factorizar un entero de n-bits
Algoritmo clásico	$O(e^{cn^{\frac{1}{3}}(\log n)^{\frac{2}{3}}})$
Algoritmo cuántico de Shor	$O(n^2(\log n)(\log \log n))$



- 1) Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.
- 2) <https://indico.cern.ch/event/970903/> Elias Fernandez-Combarro Alvarez
- 3) Qiskit: An Open-source Framework for Quantum Computing

Encontrar el periodo r

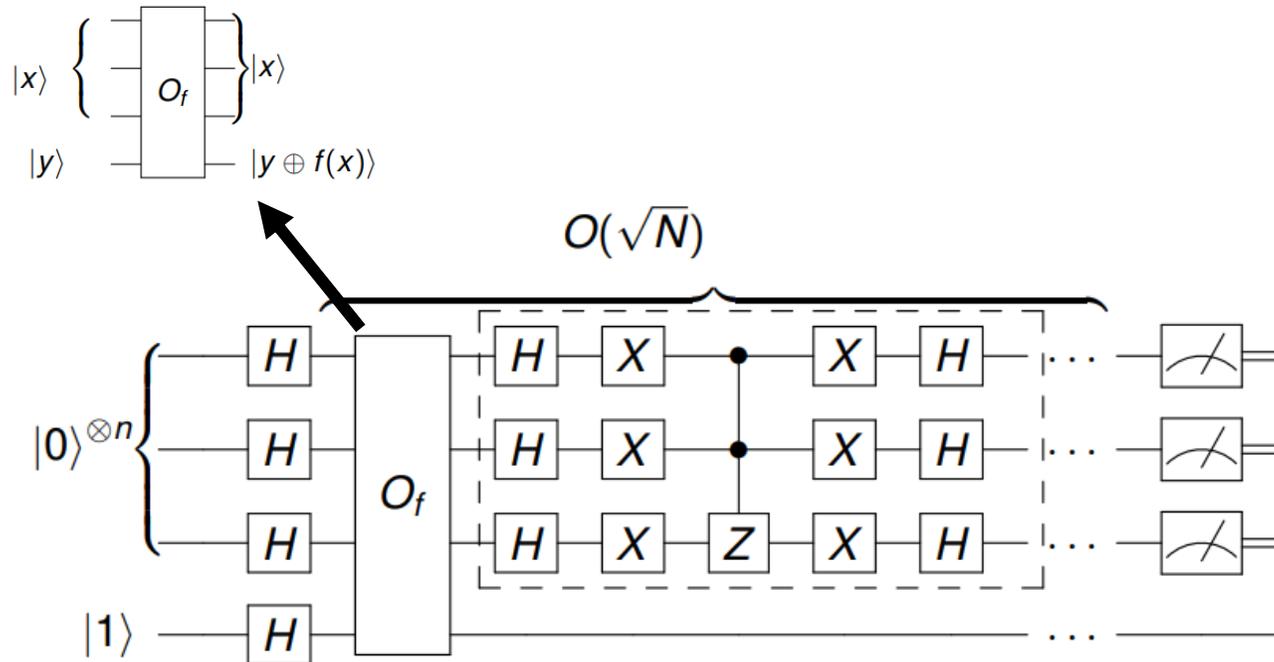


- 1) Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.
- 2) <https://indico.cern.ch/event/970903/> Elias Fernandez-Combarro Alvarez
- 3) Qiskit: An Open-source Framework for Quantum Computing

Algoritmo de Grover

Algoritmo de Grover

Objetivo: Encontrar el (los) elemento(s) en una lista que satisfacen una determinada condición



Clásica

$$O(N)$$

Cuántica

$$O(\sqrt{N})$$

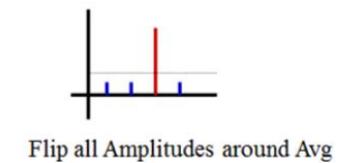
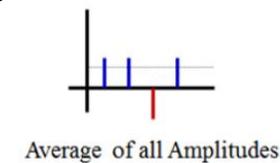
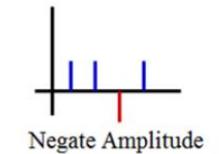
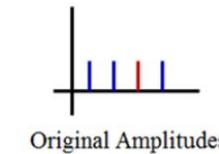


Image credits: quantumcomputing.stackexchange.com

Image credits: <https://indico.cern.ch/event/970903/>

- 1) Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.
- 2) <https://indico.cern.ch/event/970903/> Elias Fernandez-Combarro Alvarez
- 3) Qiskit: An Open-source Framework for Quantum Computing

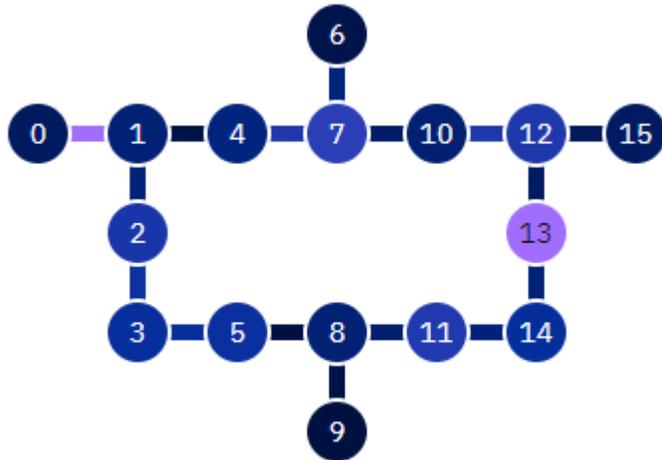
¿Otros procesos con ventaja cuántica?

NUMBER THEORETIC APPROXIMATION	ORACLE
Exponential speed-up <ul style="list-style-type: none">FactoringDiscrete logPell's equationPrincipal idealUnit groupClass groupGauss sumsQuantum simulationKnot invariantsThree-manifold invariantsPartition functionsApproximate optimizationZeta functionsWeight enumeratorsString rewritingMatrix powersSome differential equationsLattice vectors	Exponential speed-up <ul style="list-style-type: none">Abelian hidden subgroupNon-abelian hidden subgroupHidden shiftPattern matchingLinear systemsWelded treeHidden non-linear structuresGroup membershipGraph isomorphism
Polynomial speed-up <ul style="list-style-type: none">Exponential congruencesMatrix elements of group representationsVerifying matrix productsSubset-sumDecodingConstraint satisfactionSimulated annealingSemidefinite programming	Polynomial speed-up <ul style="list-style-type: none">SearchingFormula evaluationGradientsGraph propertiesCollision findingElement distinctnessGraph collisionMatrix commutativityCenter radial functionStatistical differenceCounterfeit coinsMatrix rankMatrix multiplication over semiringsSubset findingSearch with wildcardsNetwork flowsMachine learning

Image credits: Ignacio Cirac at ICM
(<https://www.youtube.com/watch?v=UP0wkDV19SE>)

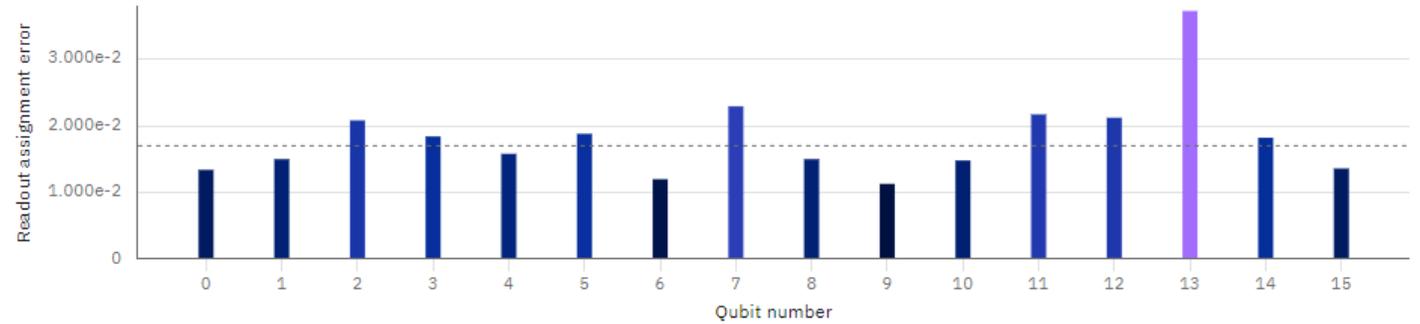
Problemas

NISQ era

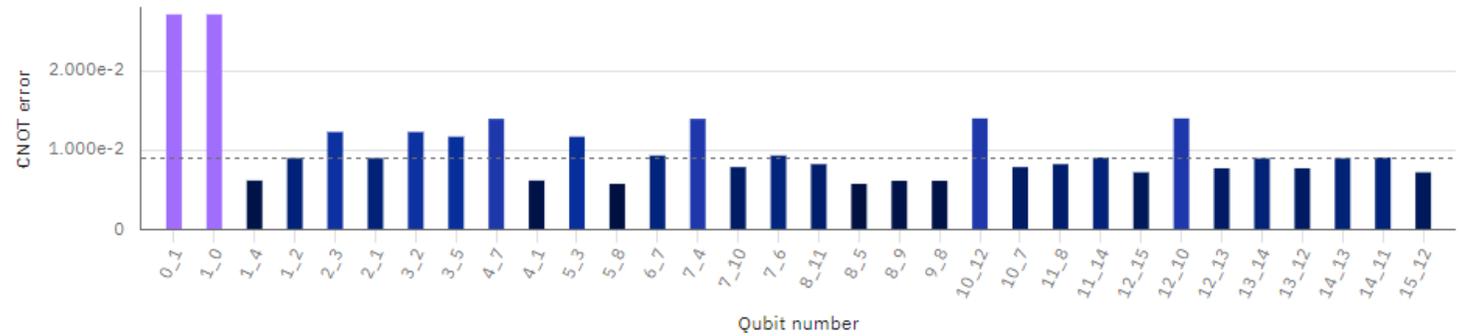


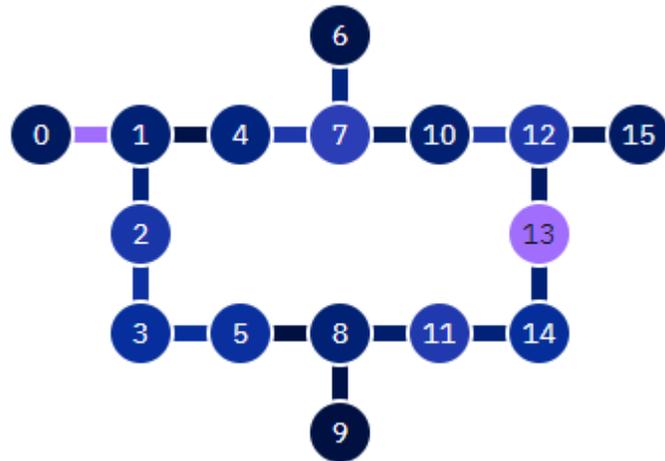
Esquema QPU IBM Guadalupe

Esquema error de medida



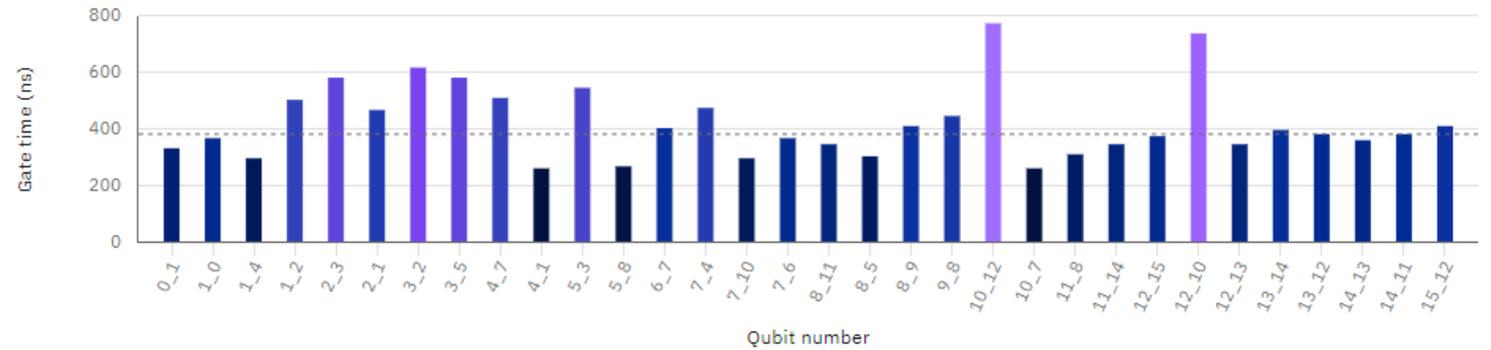
Error puerta CNOT



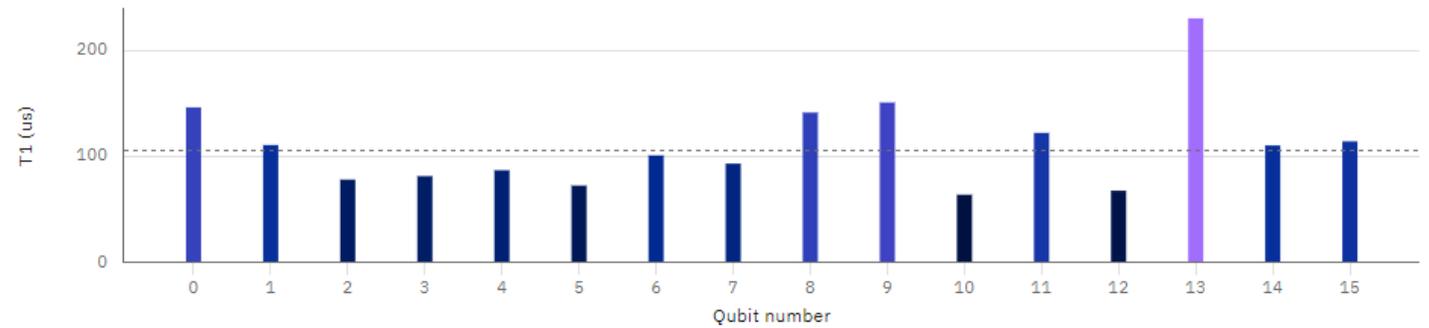


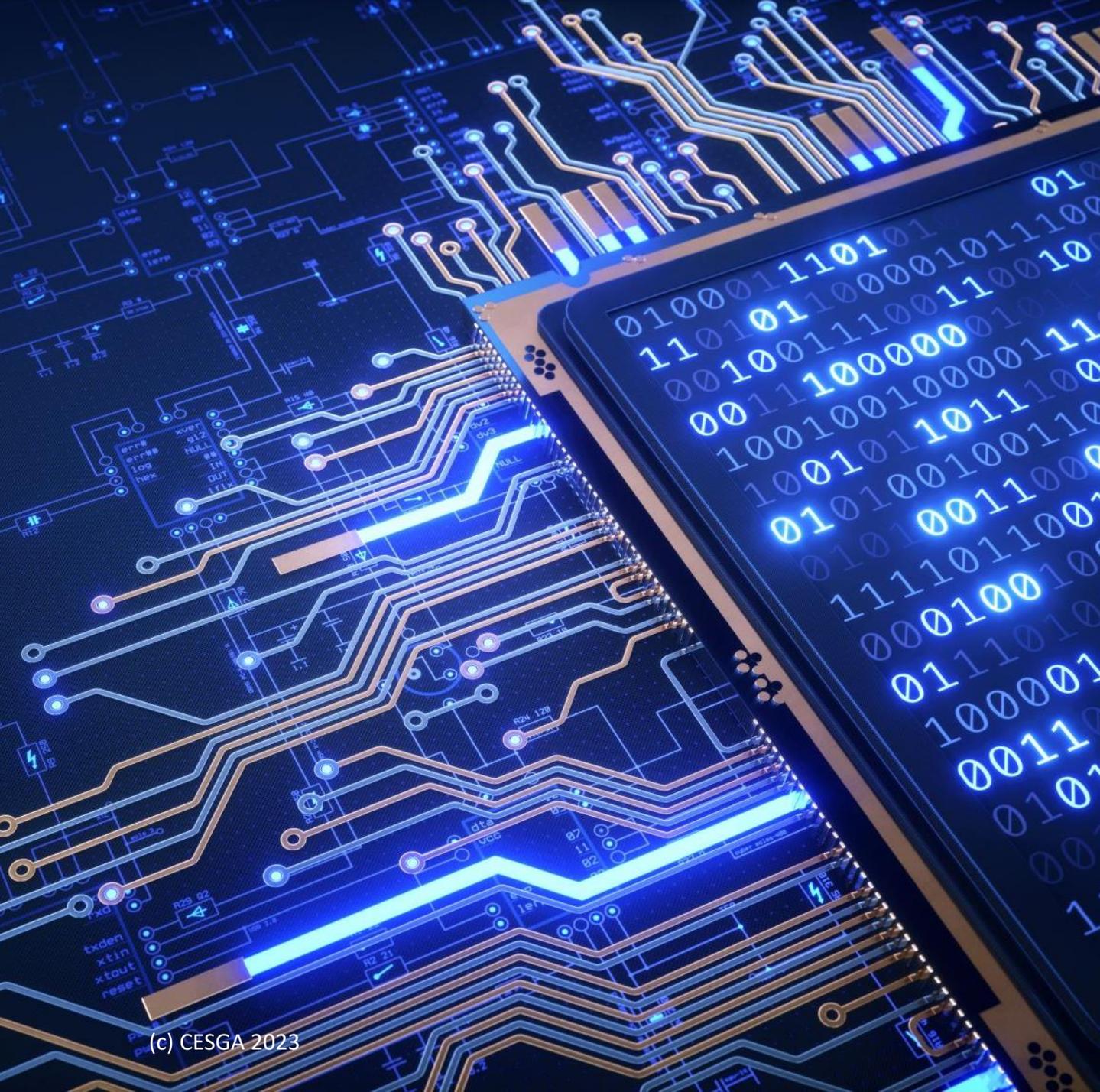
Esquema QPU IBM Guadalupe

Tiempo promedio ejecución puertas de 2 qubits



Tiempos de coherencia T_1





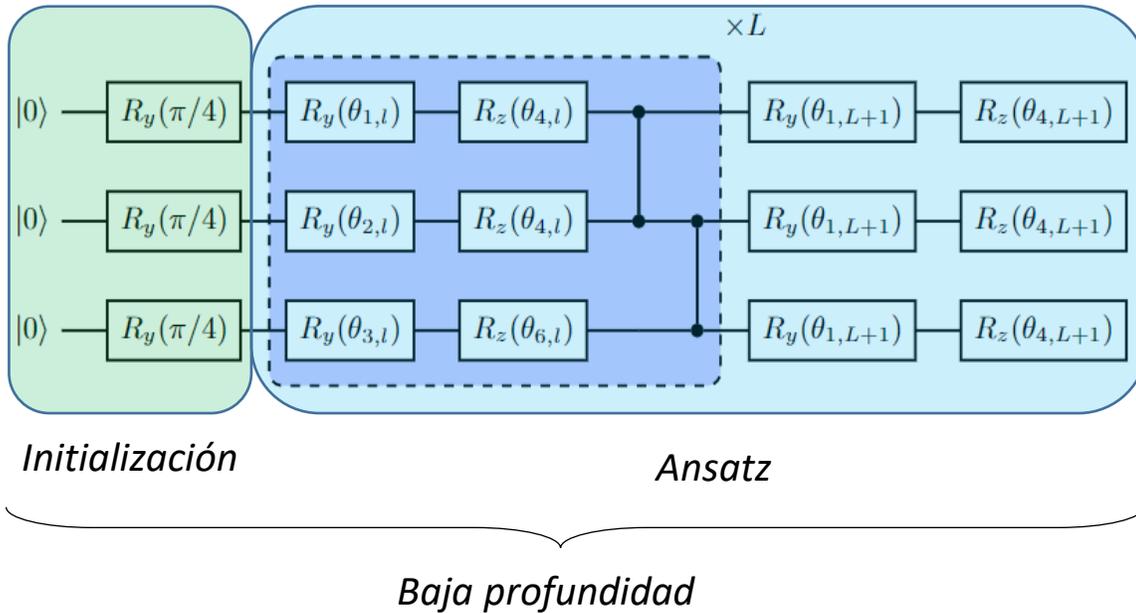
Shor, Grover, etc. no son viables en los ordenadores cuánticos actuales. Emplean circuitos demasiado largos a medida que crecemos el número de qubits.

- Modificaciones de los algoritmos que permitan reducir la profundidad de los circuitos y el número de puertas y acercas al hardware cuántico actual.
- Otras algoritmos (**Variational Quantum Algorithms**).
- Implementación de técnicas de corrección de errores.

Algoritmos Cuánticos Variacionales

Variational Quantum Algorithms (VQAs)

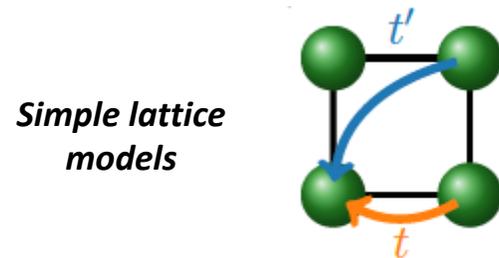
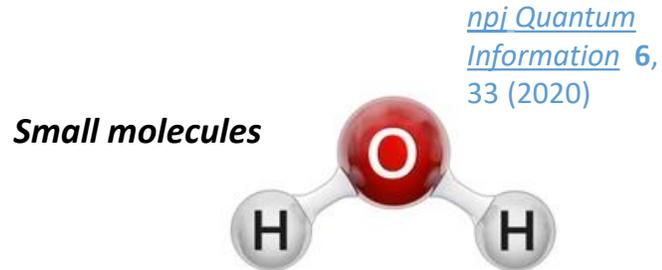
Circuito Variacional Cuántico



VQAs
Aplicaciones

- Combinatorial Optimization
- Ground State calculation (VQE)
- Quantum Machine Learning
- Dynamical Simulations
- Factoring
- Systems of equations
- Error correction
- ...

VQE: current and future applications



Phys. Rev. Research **4**, 013165 (2022)

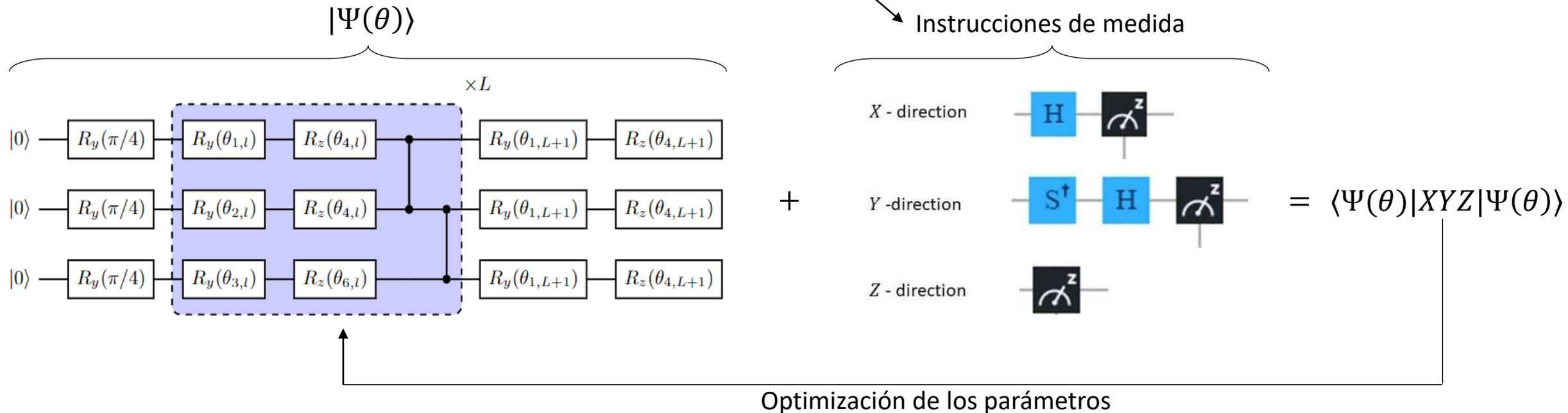
Large scale applications in chemistry/solids

- Exact calculations on highly correlated systems
- Molecular/electron dynamics
- Uncover exotic states of matter
- New bateries
- ...

VQE resumido

Paso 1. Traducir nuestro sistema (Hamiltoniano) del cual queremos obtener su configuración de mínima energía en instrucciones de qubits (matrices de Pauli).

Por ejemplo $Sistema = XYZ$.



Conclusiones

- Los ordenadores cuánticos actuales tienen limitaciones. Muchos algoritmos cuánticos que presentan una ventaja cuántica significativa no son escalables en los dispositivos actuales.
- Los circuitos variacionales son circuitos cuánticos cortos y escalables en el hardware actual. Sin embargo tampoco están exentos de dificultades ya que sufren de problemas en el espacio de optimización.
- No existe una única manera de resolver un problema en computación cuántica. El desarrollo de algoritmos cuánticos más eficientes es una línea de investigación muy activa actualmente.
- Actualmente algunos dispositivos cuánticos existentes son suficientemente grandes en número de qubits para proporcionar una ventaja cuántica. Sin embargo como usar eficientemente los qubits y mitigar los errores inherentes a la tecnología actual son ingredientes fundamentales.

¡Gracias!

dfailde@cesga.es



AXENCIA
GALEGA DE
INNOVACIÓN



UNIÓN EUROPEA



Xacobeo 21-22



CESGA

Centro de Supercomputación de Galicia