

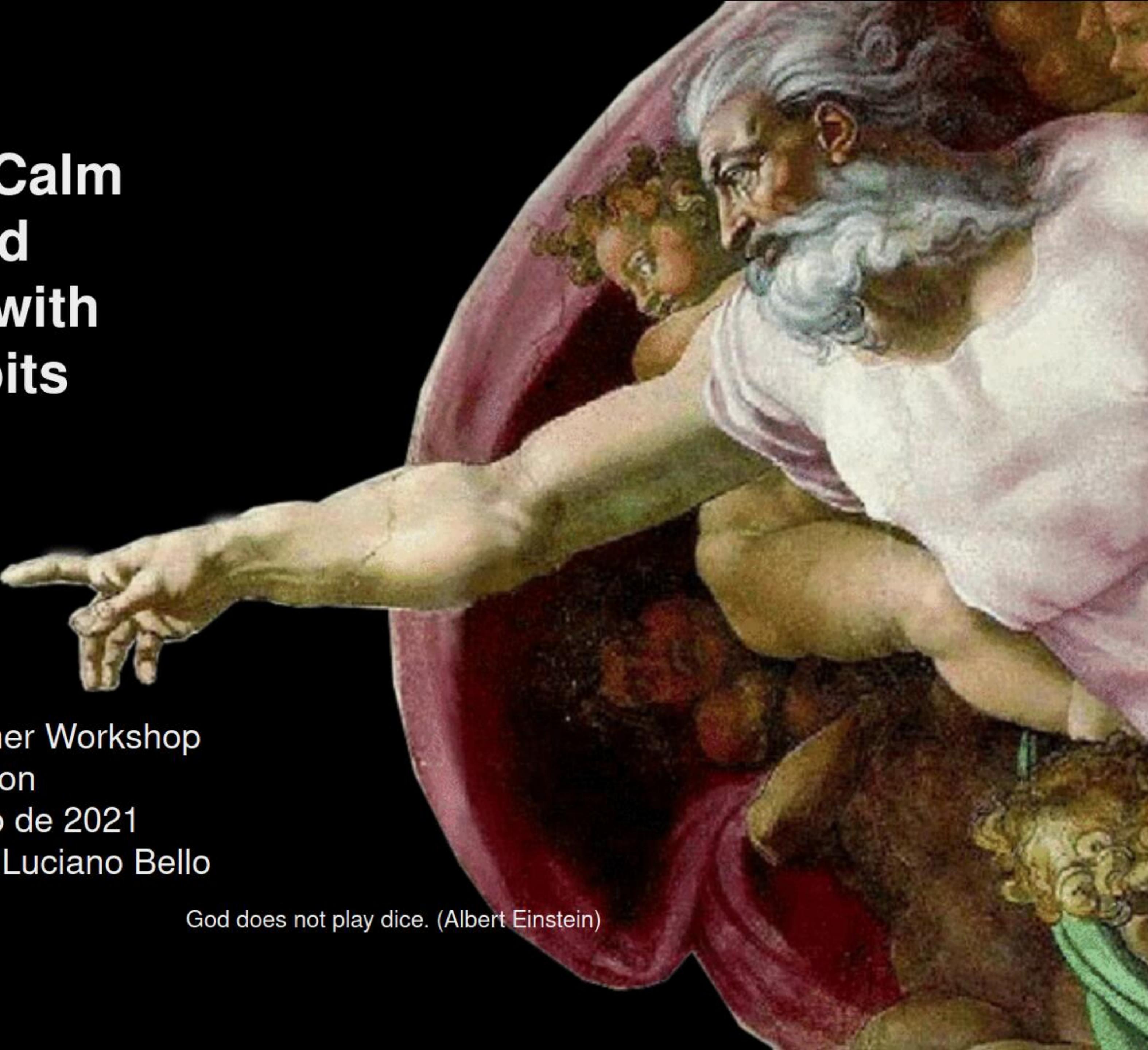
# Keep Calm and Play with Qubits

## II



Ekoparty Summer Workshop  
Version  
27 de Enero de 2021  
Carlos Benitez - Luciano Bello

God does not play dice. (Albert Einstein)





## Carlos Benitez

Ing. y Mg. de la UTN FRBA

- Investigador en procesamiento de señales acústicas submarinas
- Primer Lab en Seguridad Informática (Si6) y primer SOC Defensa
- Asesor técnico de la Subsecretaría de Ciberdefensa
- Docente de posgrado y consultor en ciberseguridad
- Co-fundador de Platinumciber
- Formador y mentoring de equipos
- SOC, Ethical Hacking y Análisis y Gestión de Riesgos
- Quantum Computing enthusiast



## Luciano Bello

Ing. de la UTN FRBA

- PhD de Chalmers (Suecia)
- Desarrollador Senior en IBM Research
- Doctor en seguridad basada en lenguajes
- Python coder
- Desarrollador de Software Libre en Debian
- Diseñador de lenguajes formales
- Infosec enthusiast
- Geocacher

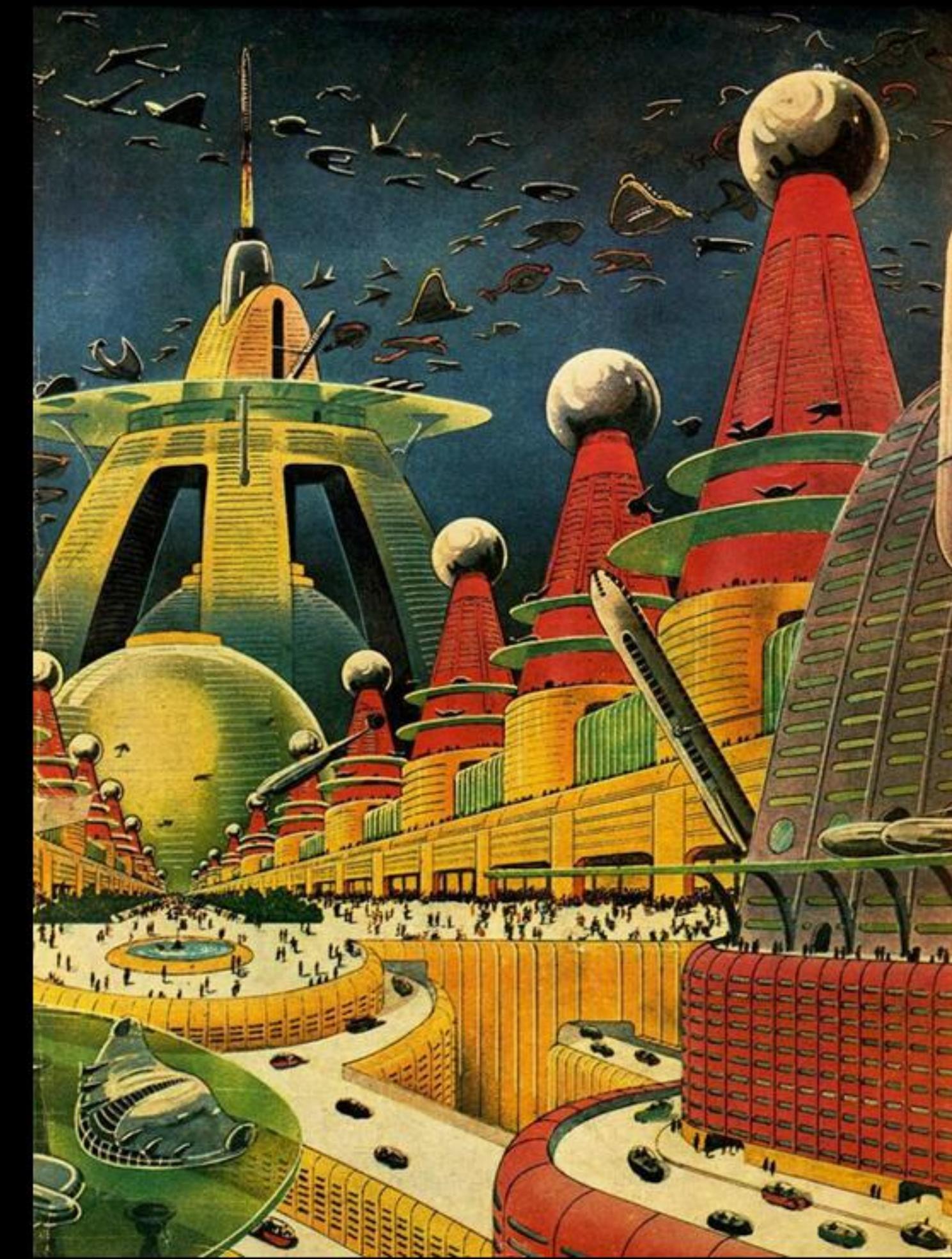
# Who we are?

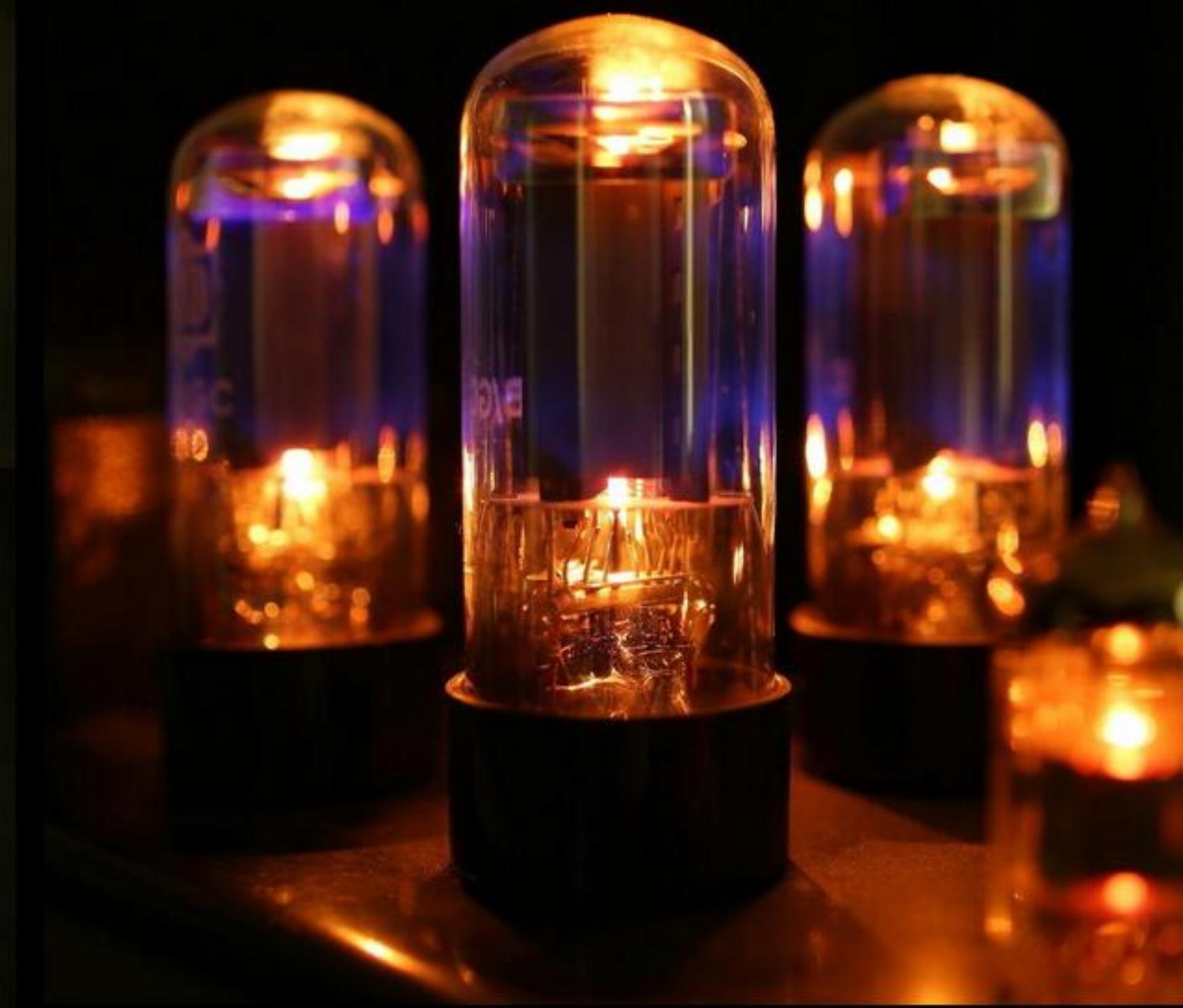
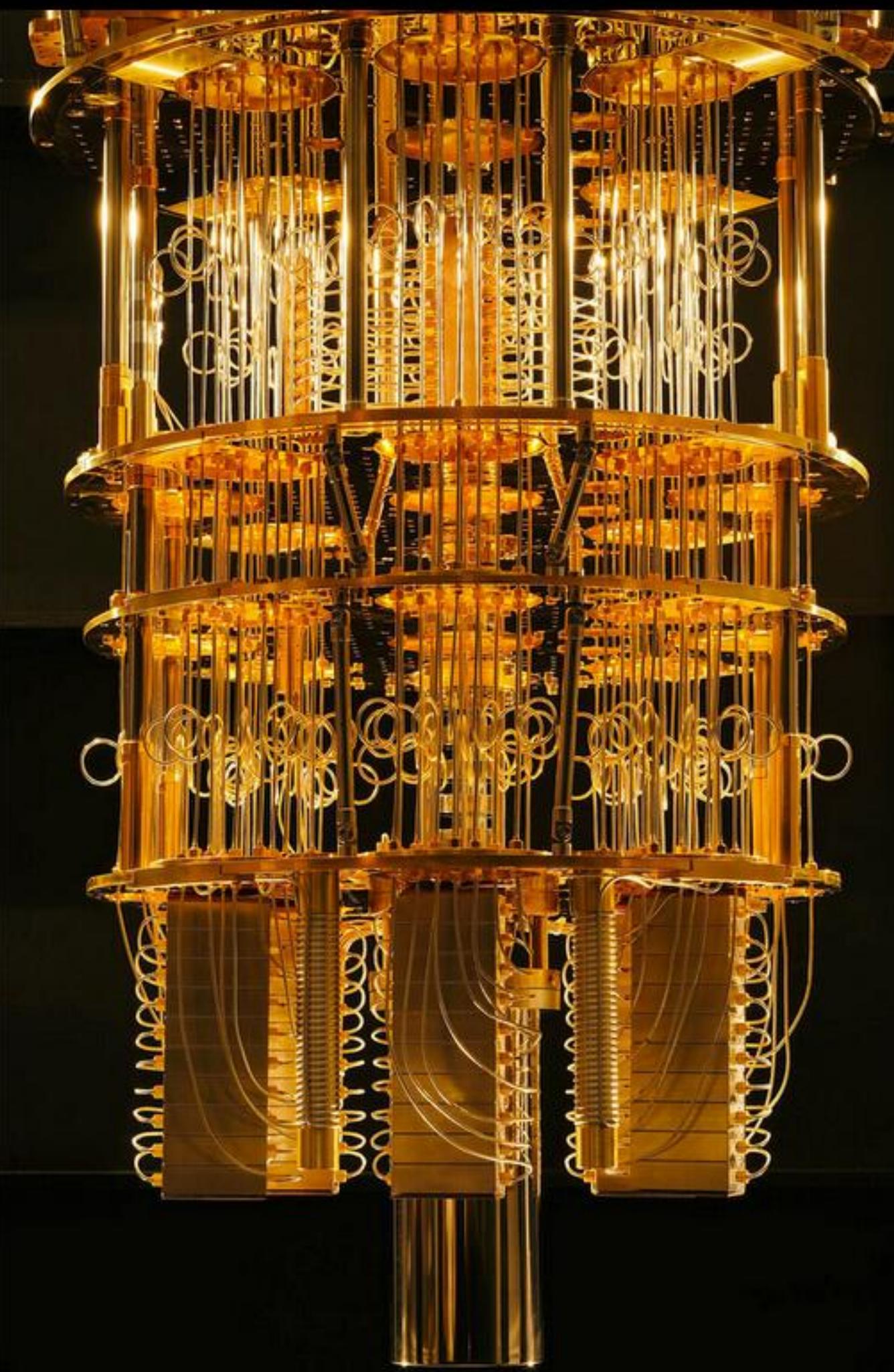
# Disclaimer

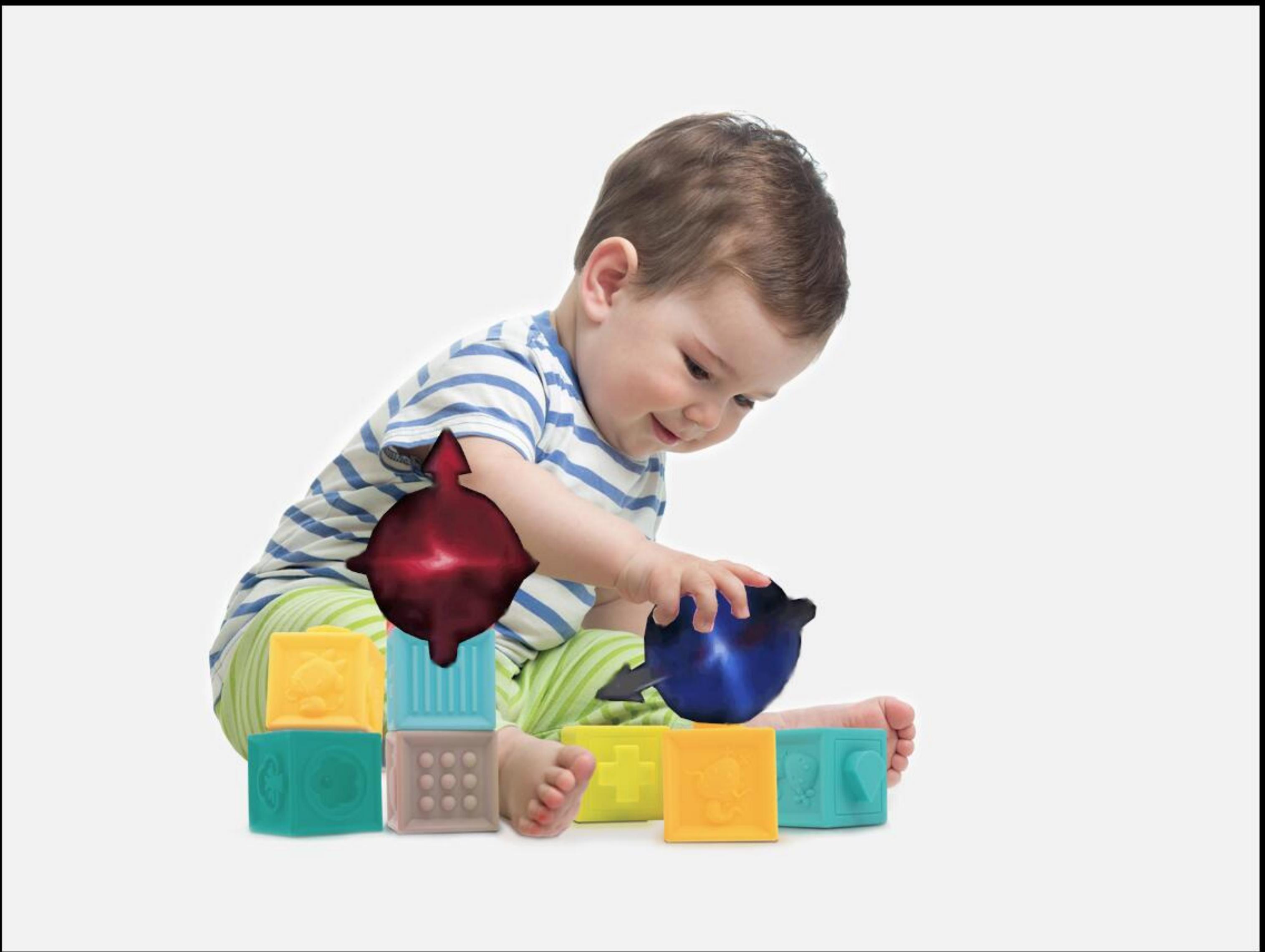
Los conceptos vertidos en este trabajo corren por exclusiva cuenta de los autores; corresponden a sus propias opiniones y experiencia personal y de ningún modo representan a las empresas u organismos a los que pertenecen.

A  
PREVIOUSLY

...on Keep Calm...









¿Qué es la  
computación cuántica?

Paradigma de computación  
que utiliza propiedades cuánticas  
para resolver cálculos matemáticos

¿Qué es la computación cuántica?

mecánico ~~cuántica~~

física ~~cuántica~~

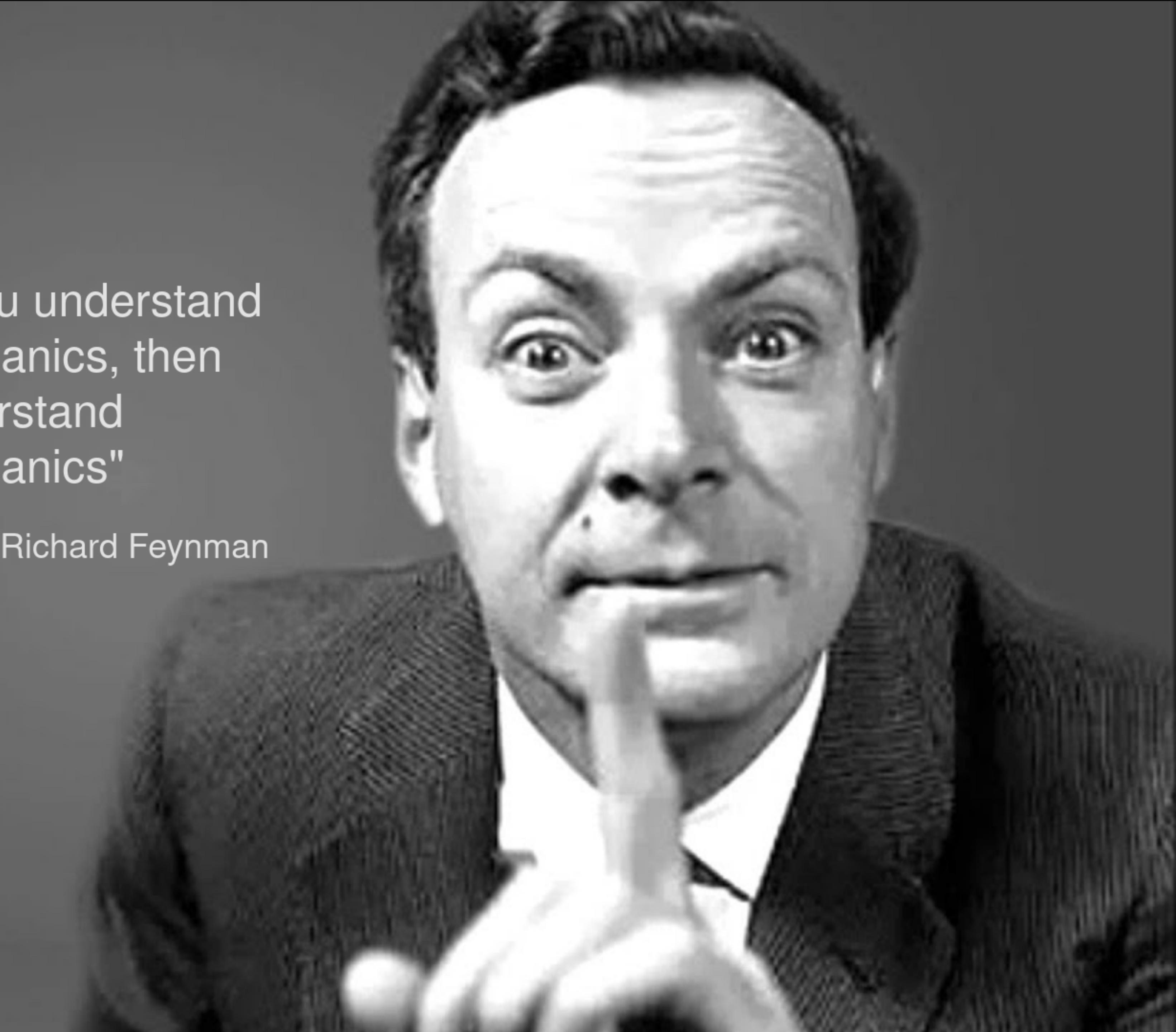
criptografía ~~cuántica~~

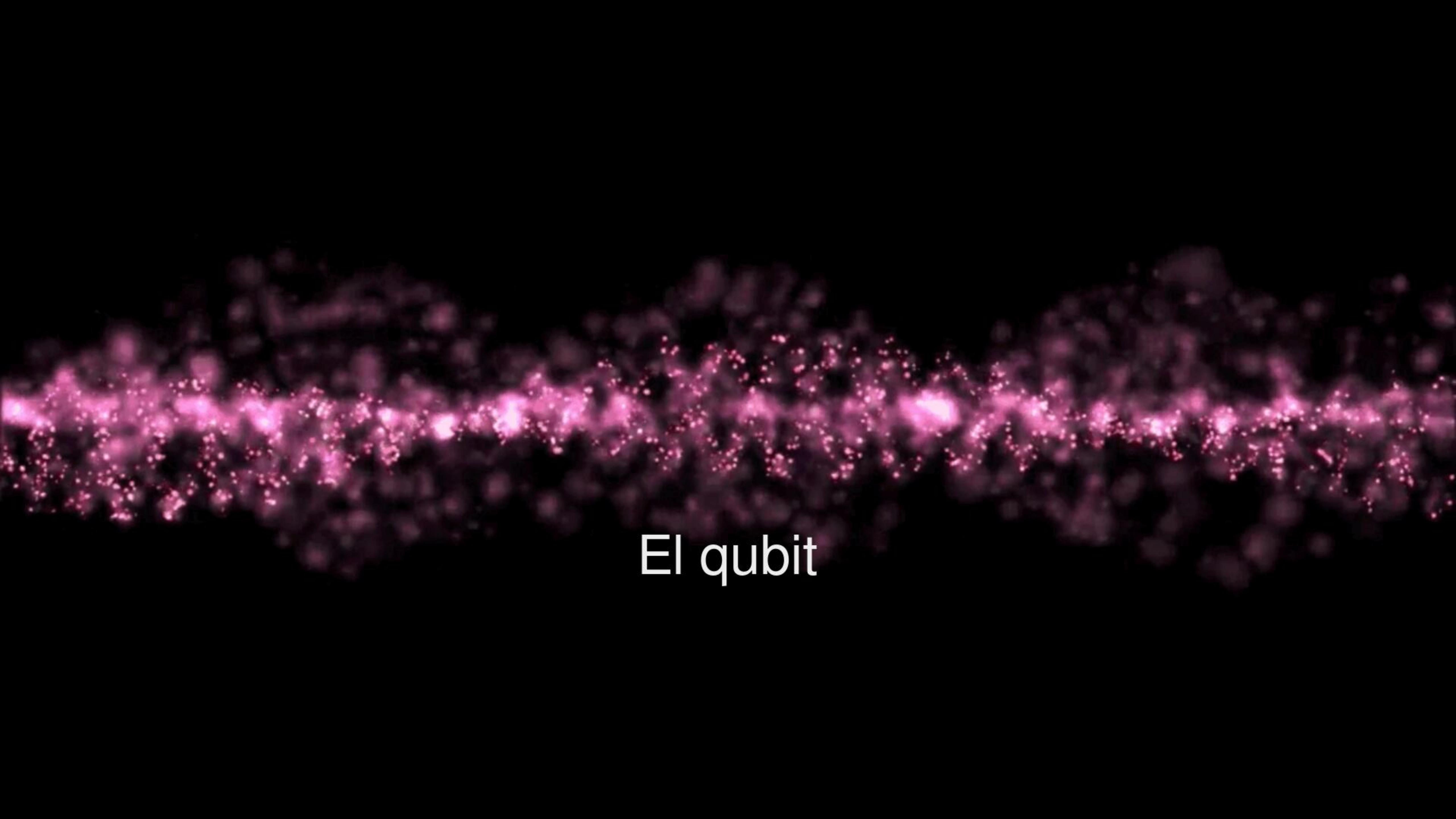
criptografía ~~post-cuántica~~

¿Qué NO ES la computación cuántica?

"If you think you understand quantum mechanics, then you don't understand quantum mechanics"

Richard Feynman

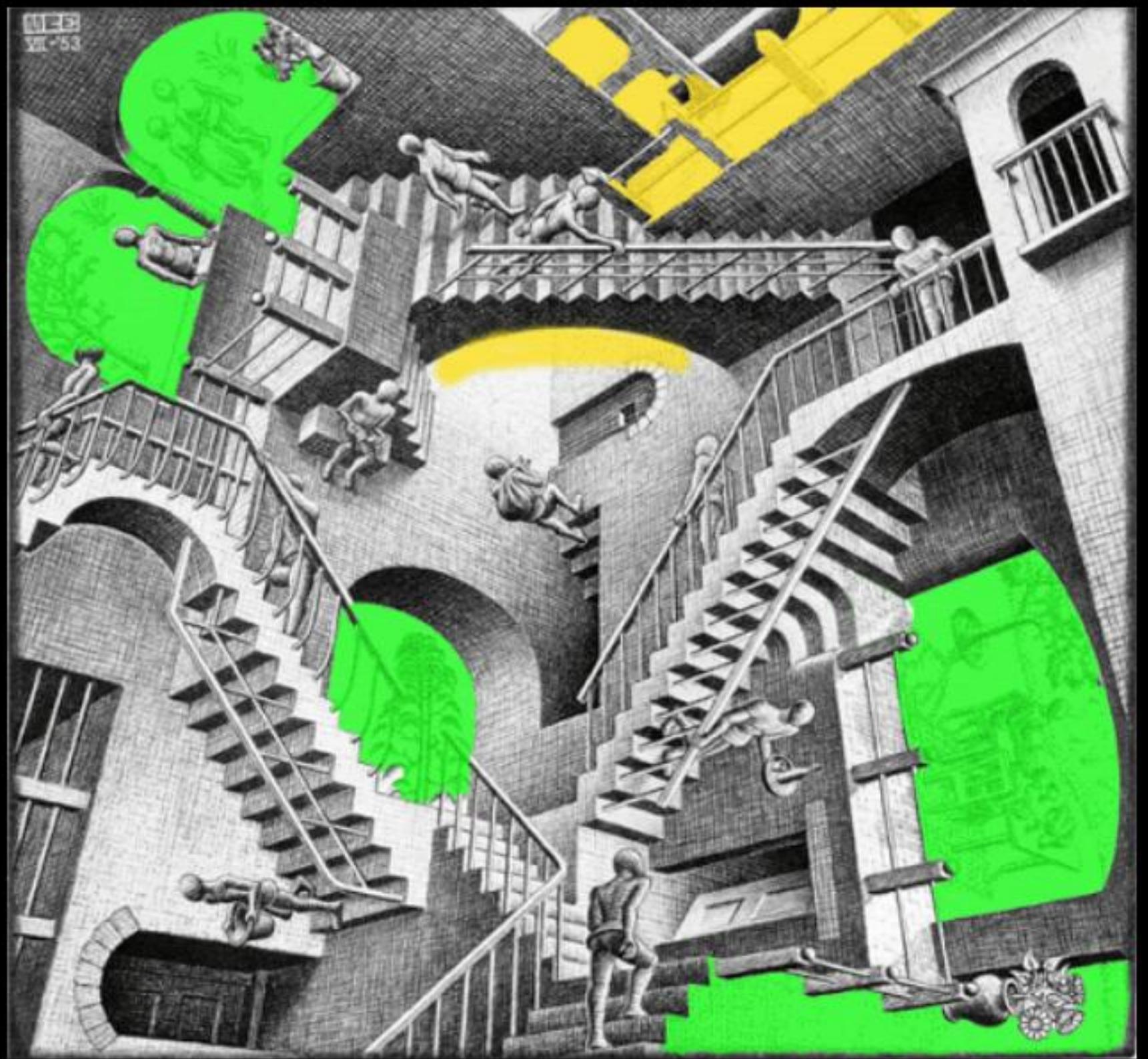




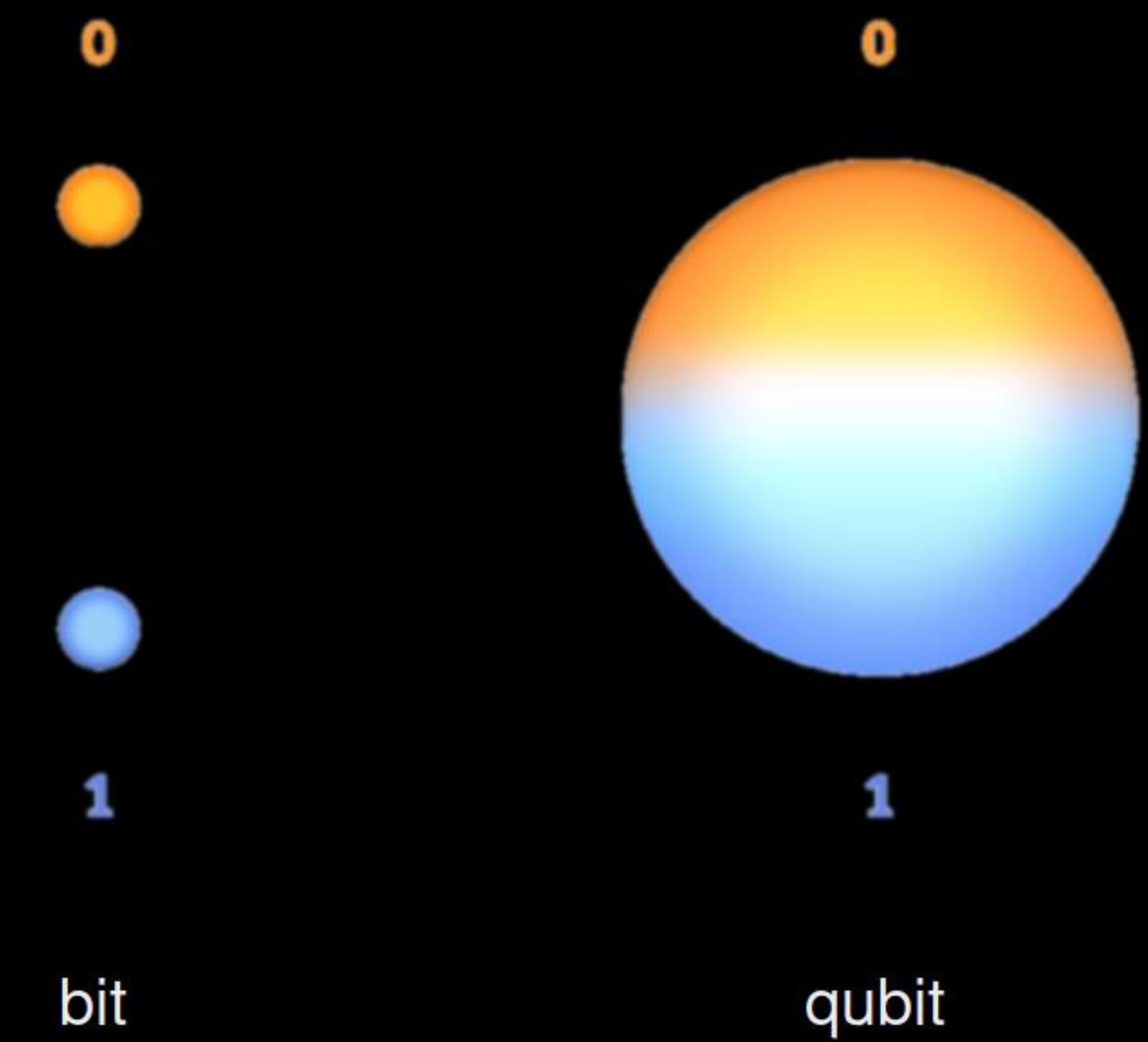
El qubit

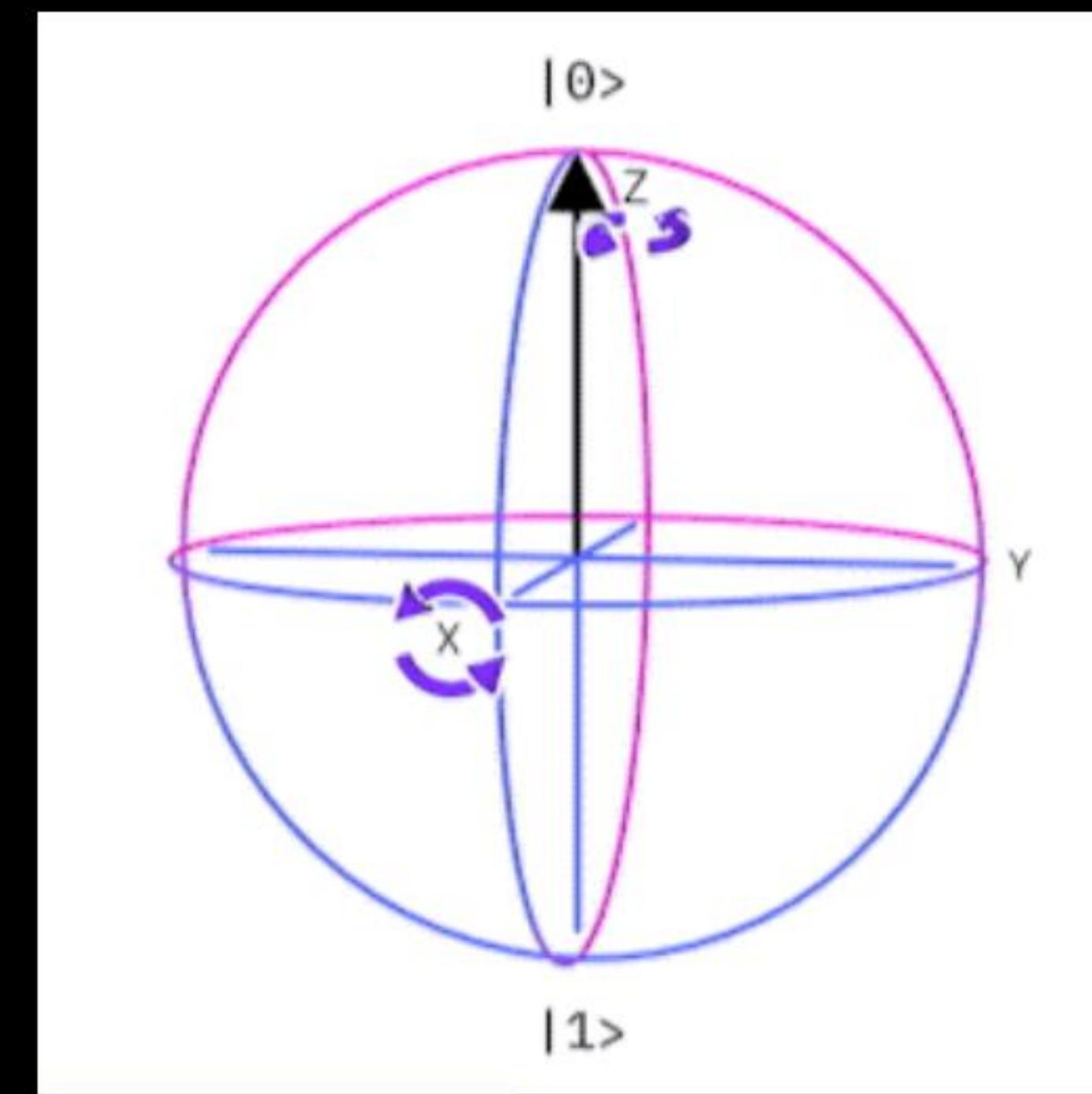


bit



qubit

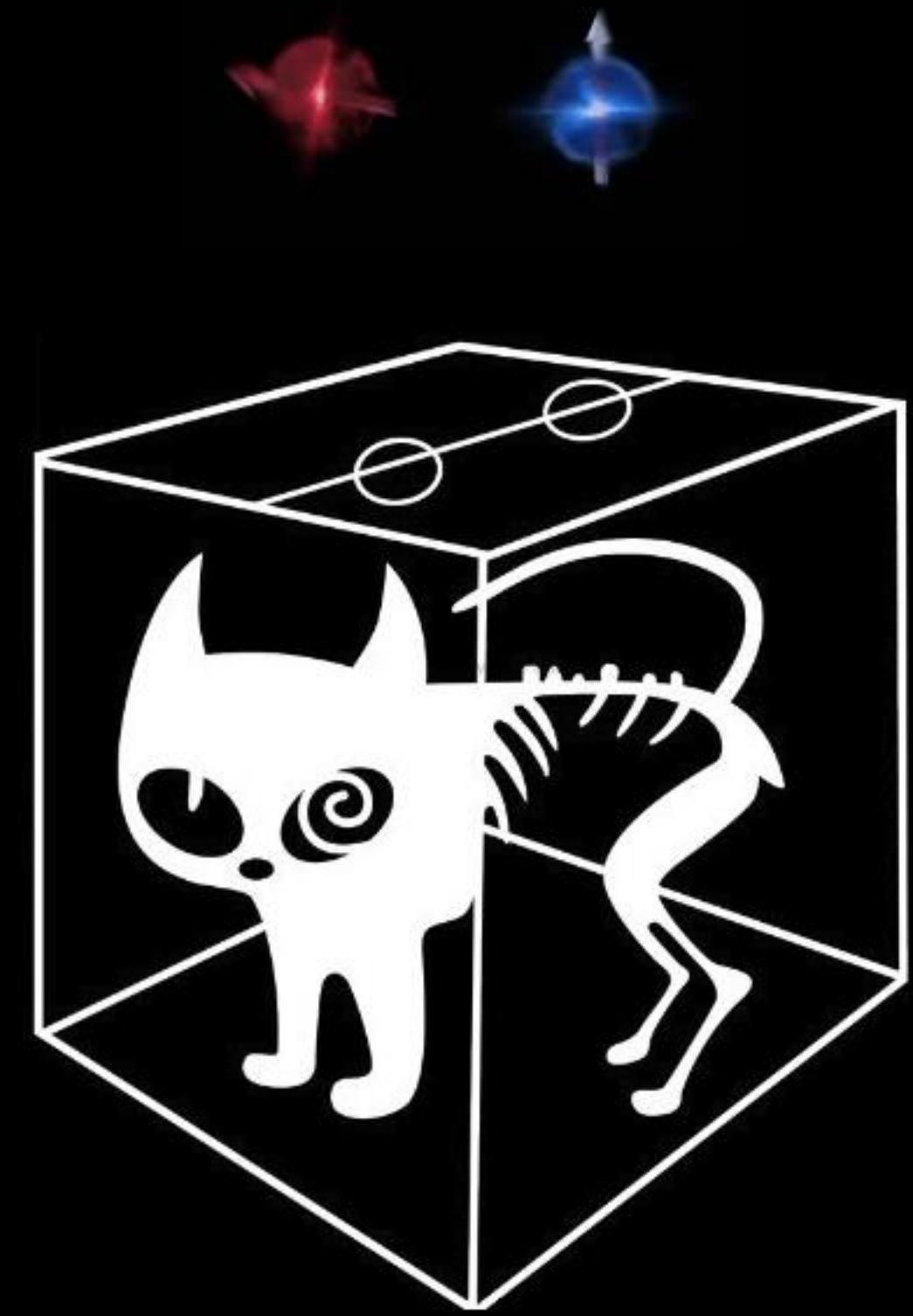




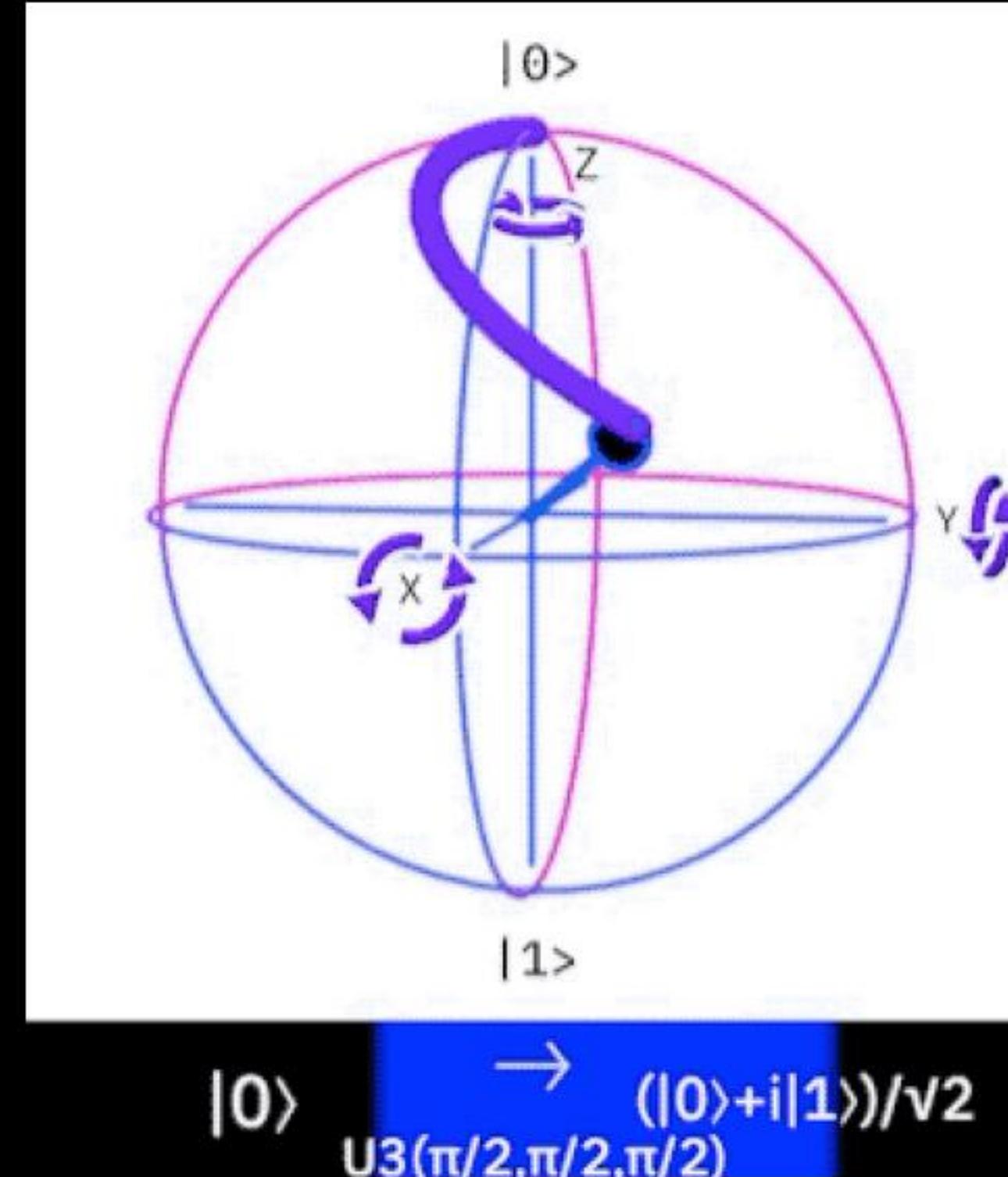
Esfera de Bloch



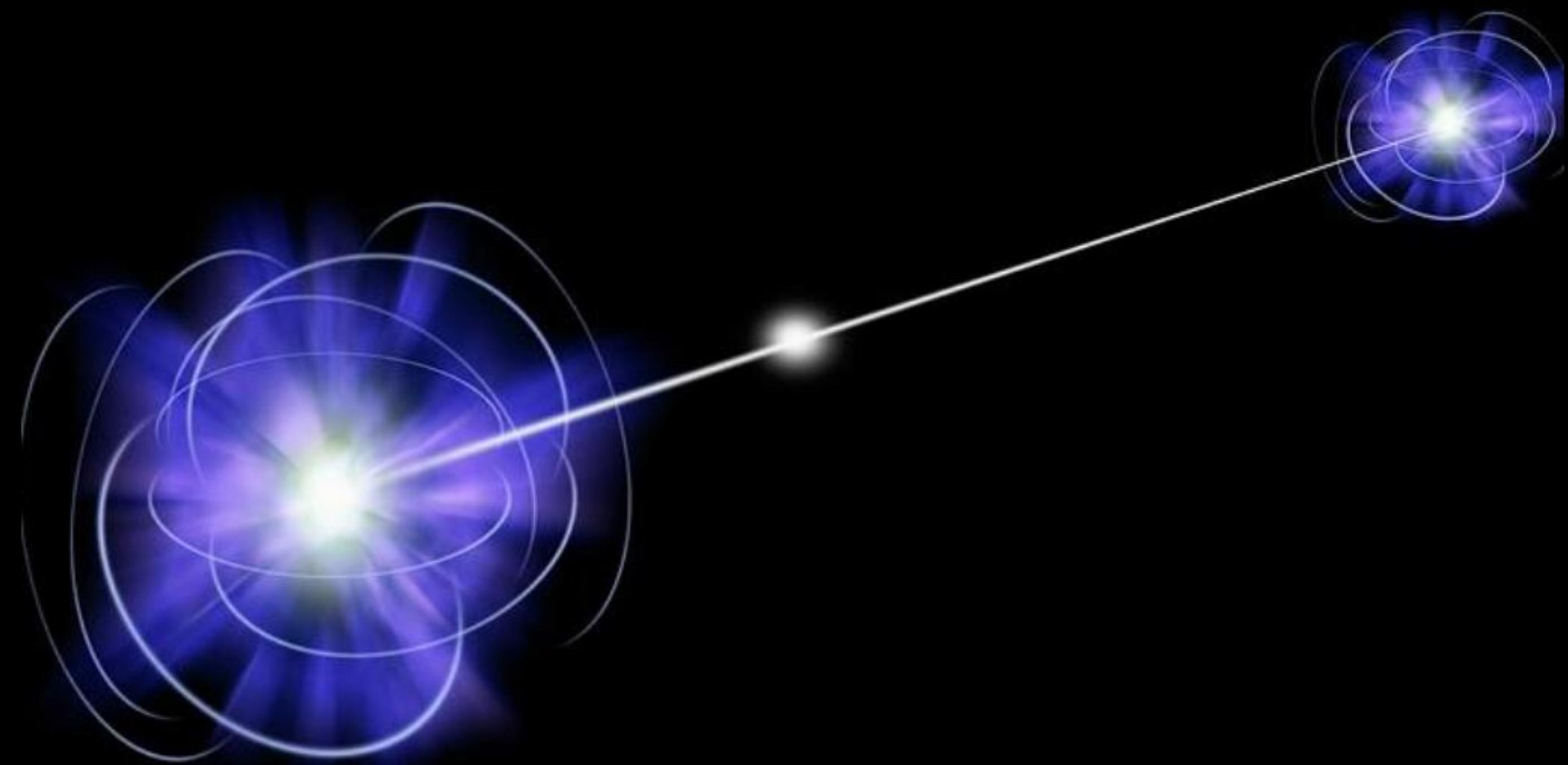
# Propiedades de los qubits



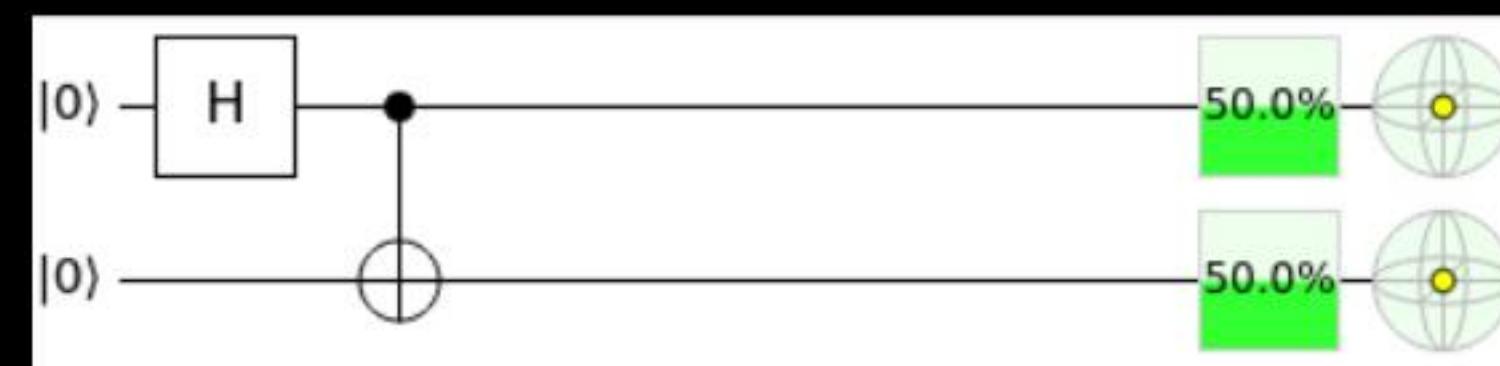
Propiedad #1: Superposición



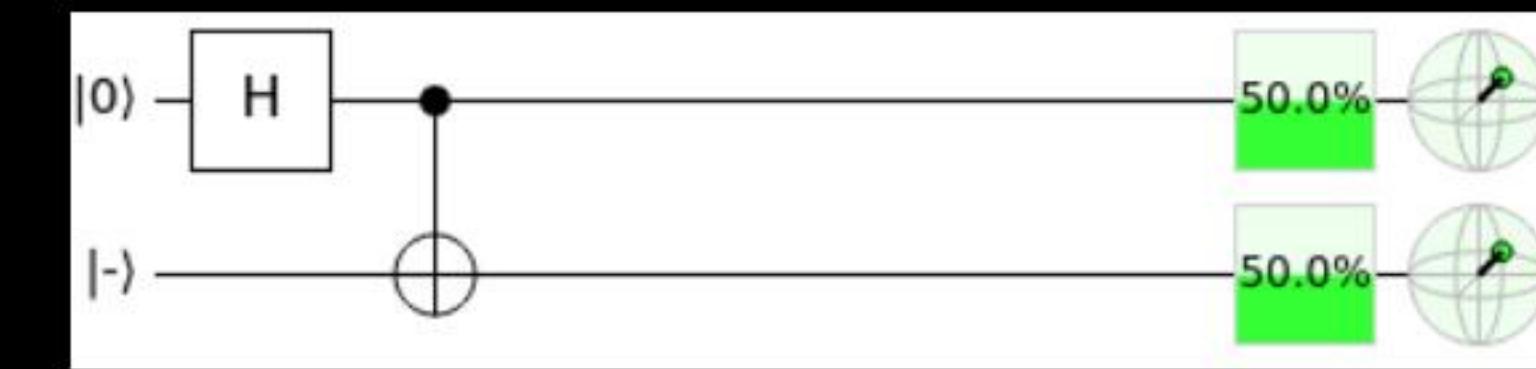
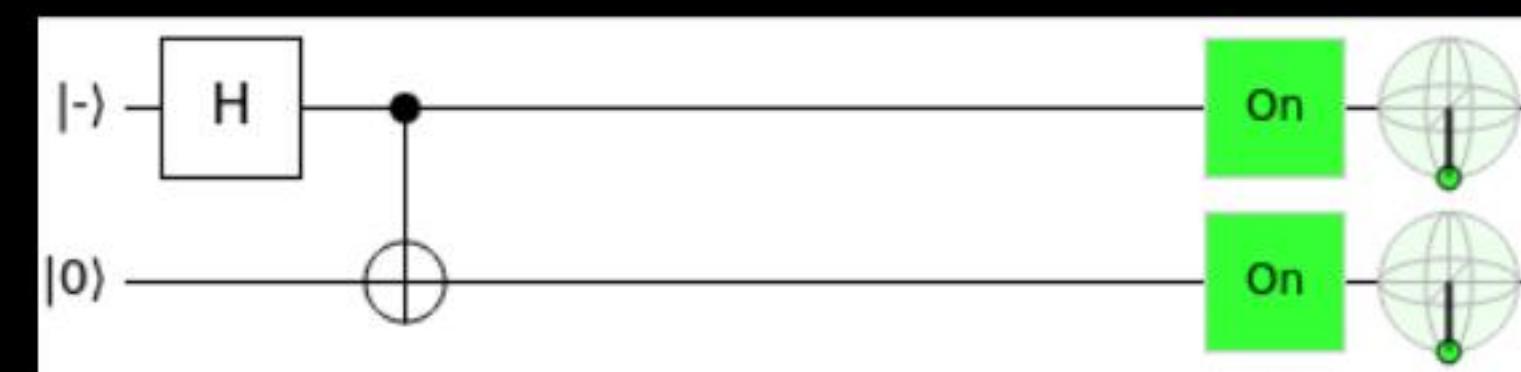
Propiedad #1: Superposición



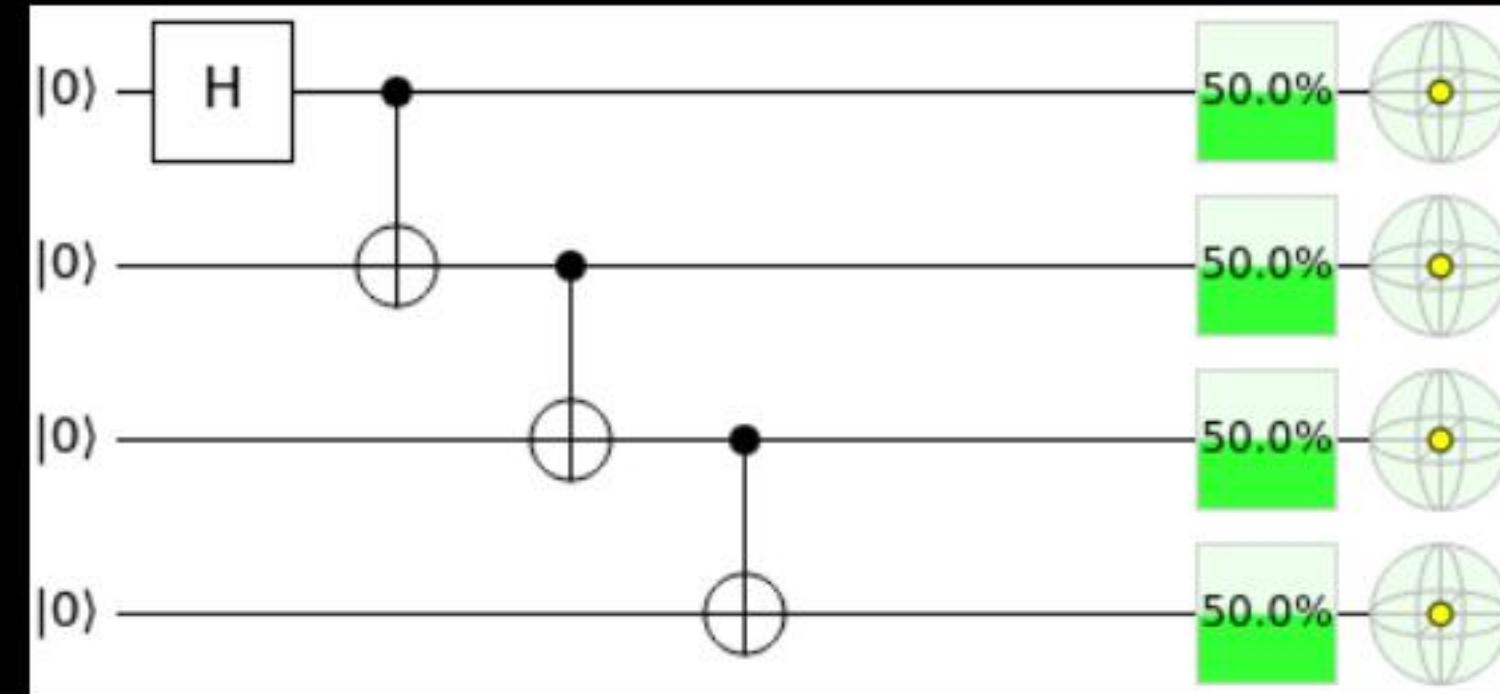
Propiedad #2: Entrelazamiento (Entanglement)



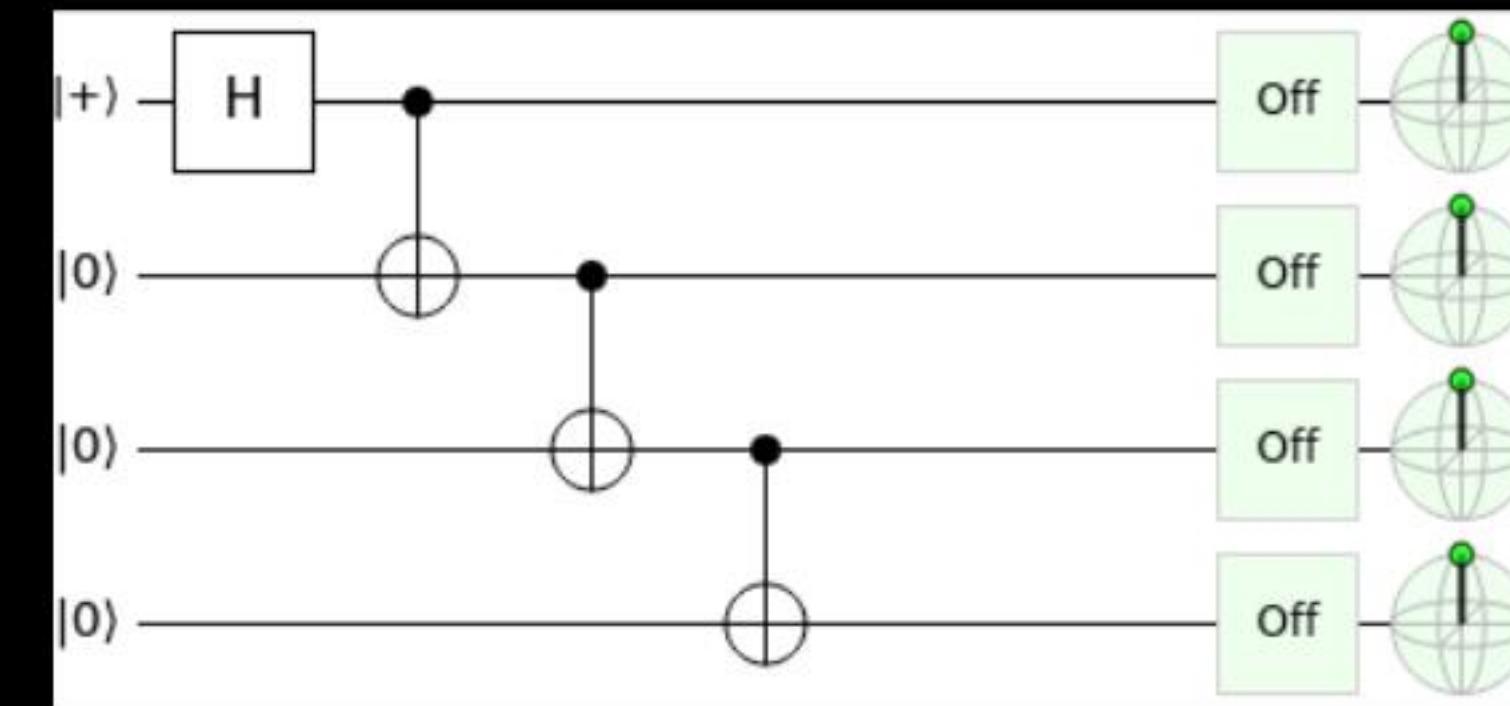
Bell State



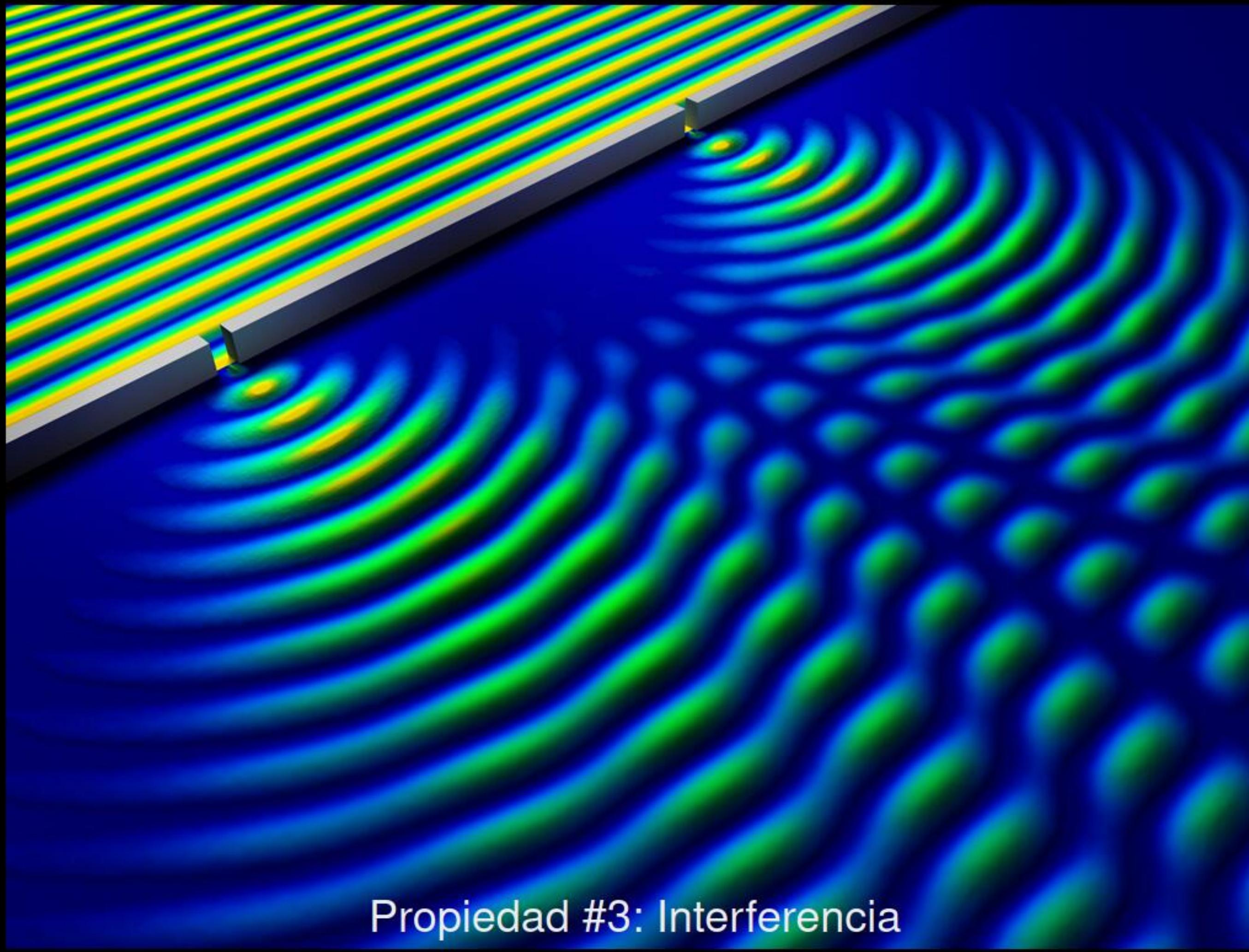
Propiedad #2: Entrelazamiento (Entanglement)



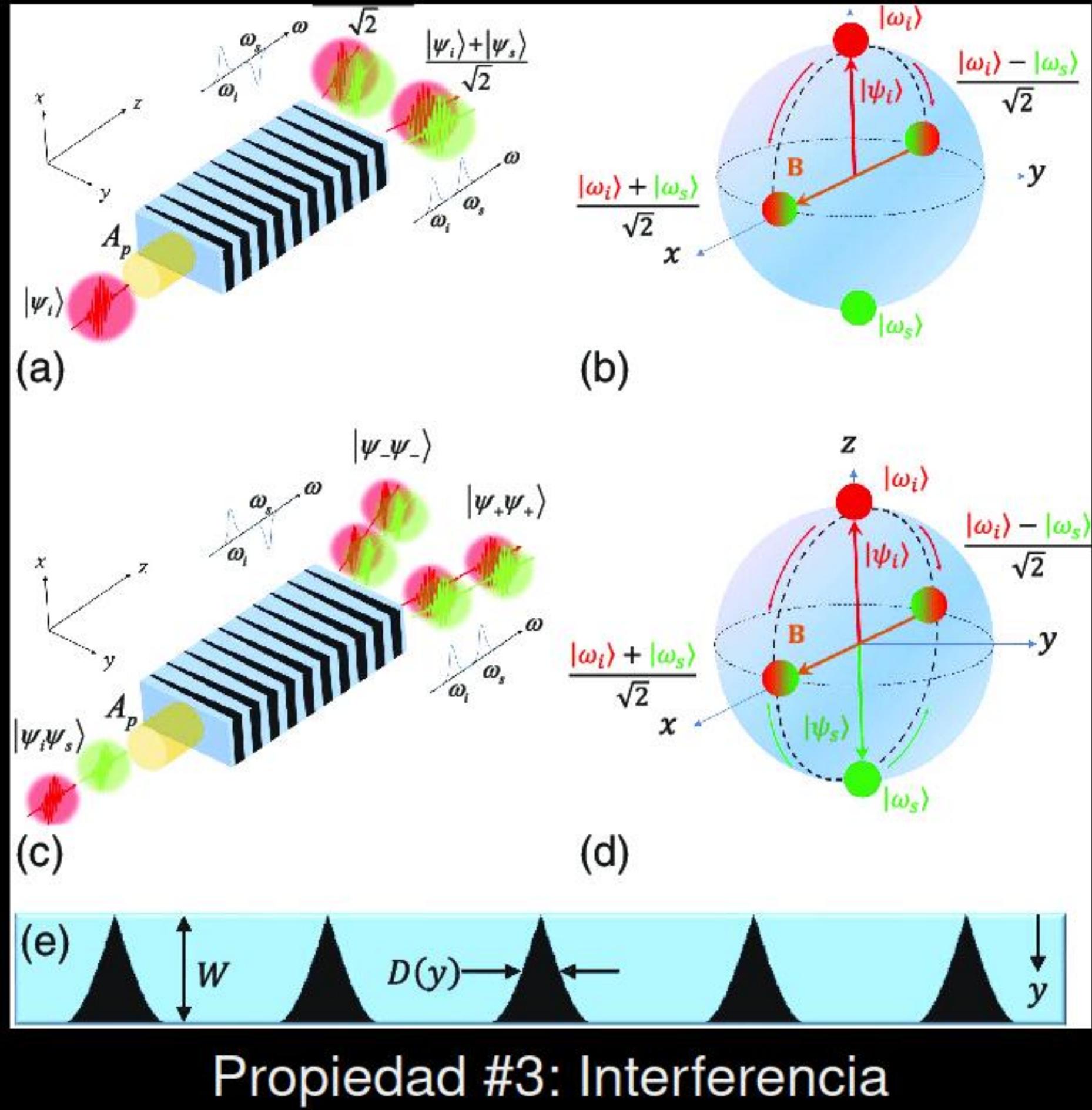
GHZ State



Propiedad #2: Entrelazamiento (Entanglement)

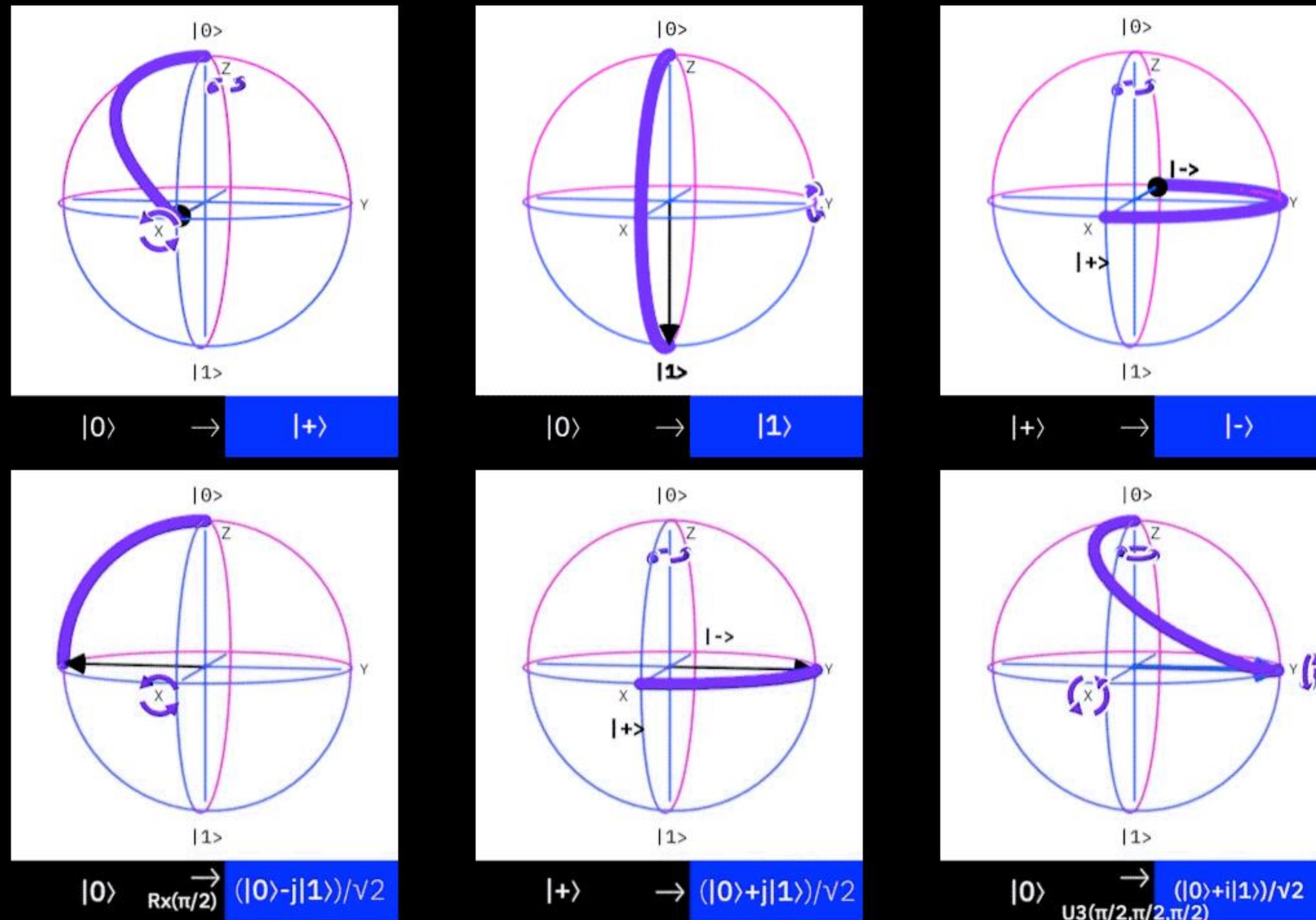


Propiedad #3: Interferencia



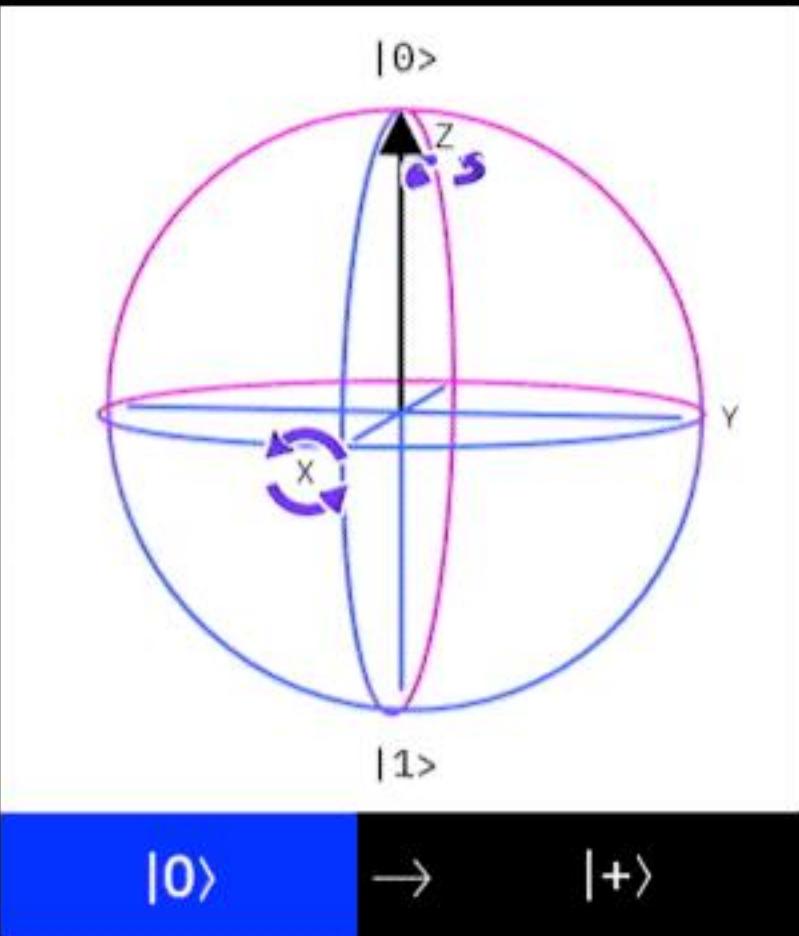


# Operaciones con qubits



Operaciones sobre un qubit

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

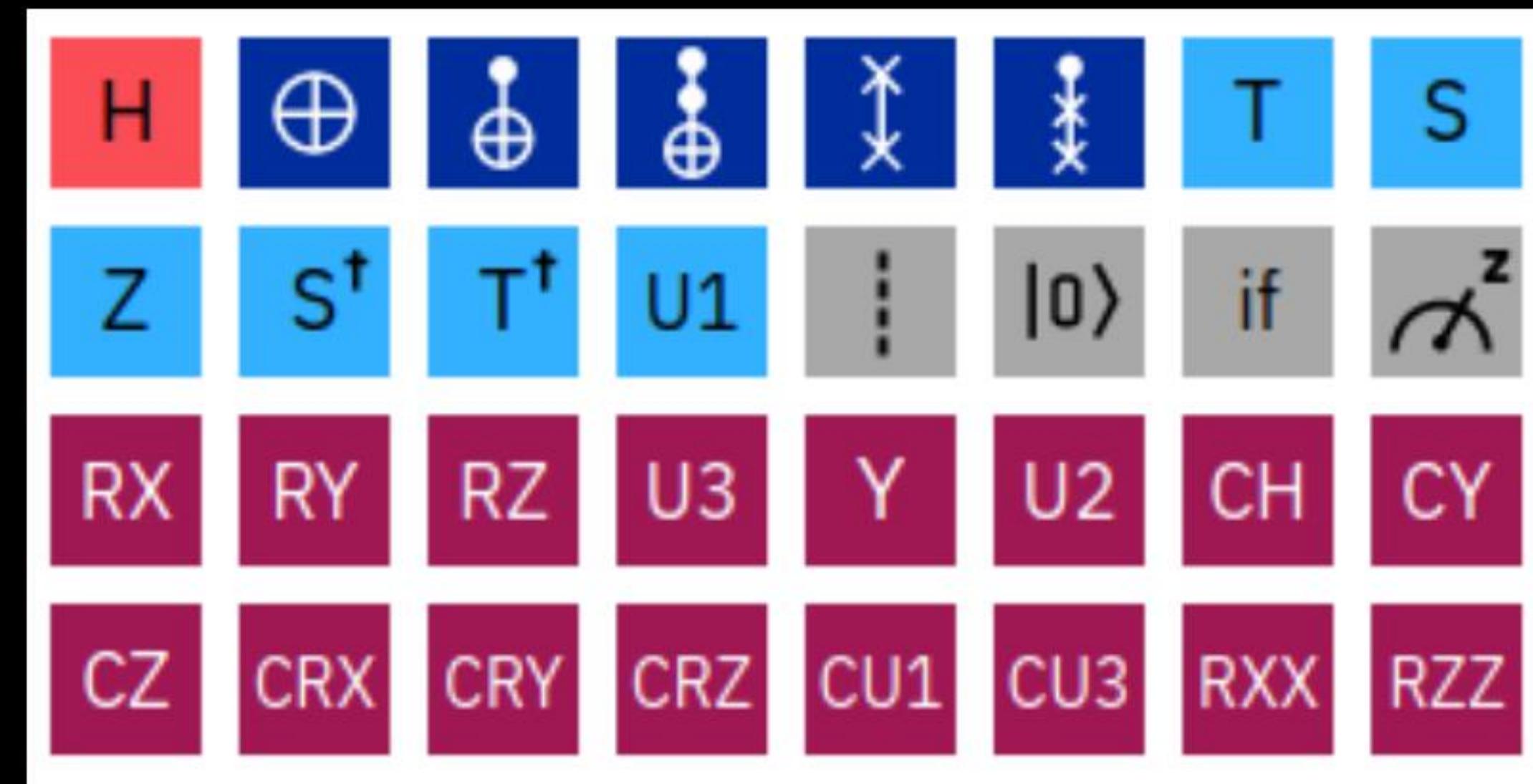


$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



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

Rotaciones como productos de matrices



Compuertas

Menu Export Clear Circuit Clear ALL Undo Redo Make Gate Version 2.3

**Toolbox**

Probes	Displays	Half Turns	Quarter Turns	Eighth Turns	Spinning	Formulaic	Parametrized	Sampling	Parity
		Z Swap	S S <sup>-1</sup>	T T <sup>-1</sup>	Z <sup>t</sup> Z <sup>-t</sup>	Z <sup>f(t)</sup> R <sub>z(f(t))</sub>	Z <sup>A/2^n</sup> Z <sup>-A/2^n</sup>		[Z] par
		Y	Y <sup>1/2</sup> Y <sup>-1/2</sup>	Y <sup>1/4</sup> Y <sup>-1/4</sup>	Y <sup>t</sup> Y <sup>-t</sup>	Y <sup>f(t)</sup> R <sub>y(f(t))</sub>	Y <sup>A/2^n</sup> Y <sup>-A/2^n</sup>		[Y] par
		H	X <sup>1/2</sup> X <sup>-1/2</sup>	X <sup>1/4</sup> X <sup>-1/4</sup>	X <sup>t</sup> X <sup>-t</sup>	X <sup>f(t)</sup> R <sub>x(f(t))</sub>	X <sup>A/2^n</sup> X <sup>-A/2^n</sup>		[X] par

|0> —————— use controls ——————|0>

drag gates onto circuit

Off Off

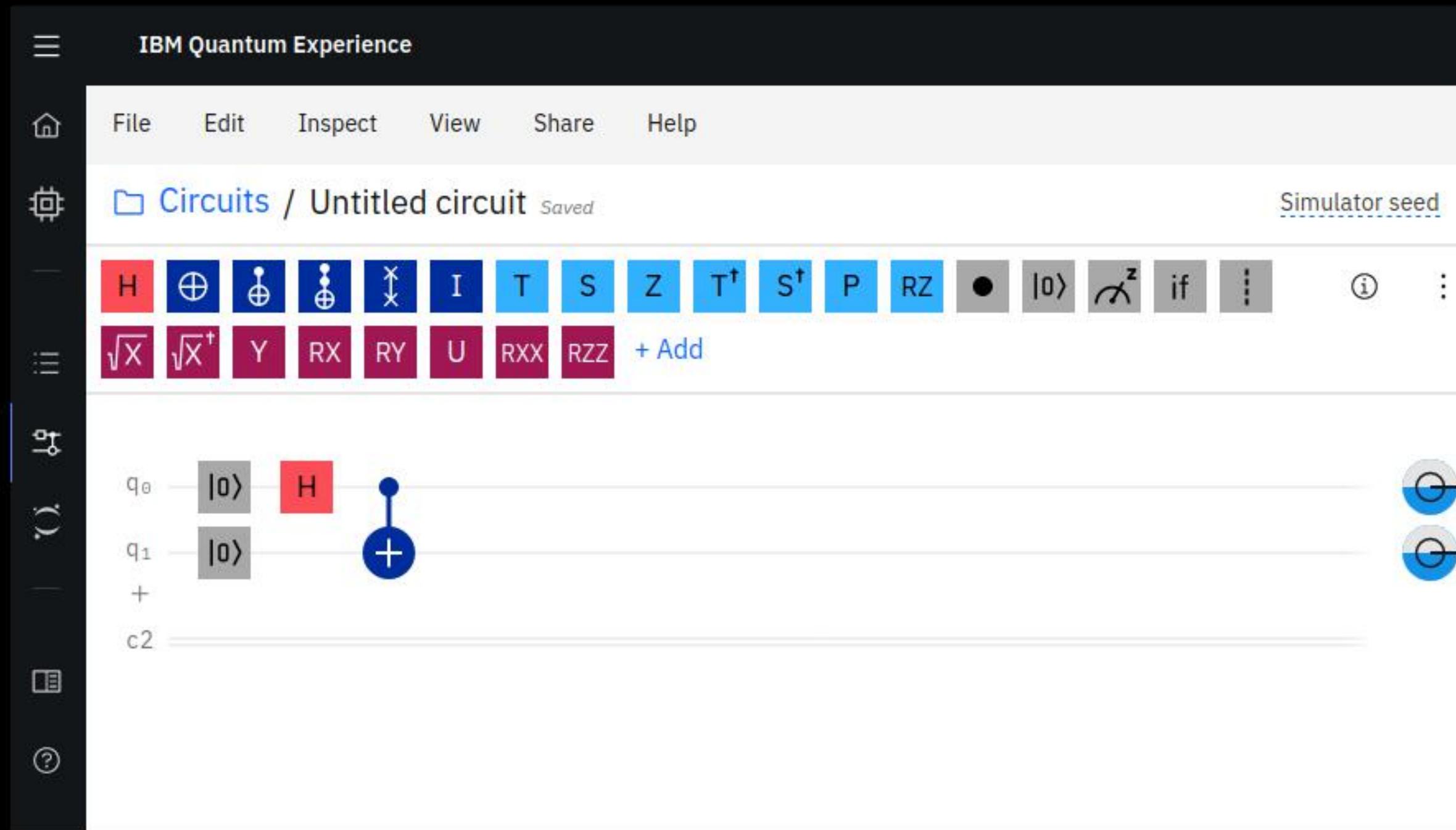
Local wire states (Chance/Bloch) |0> |1> Final amplitudes

**Toolbox<sub>2</sub>**

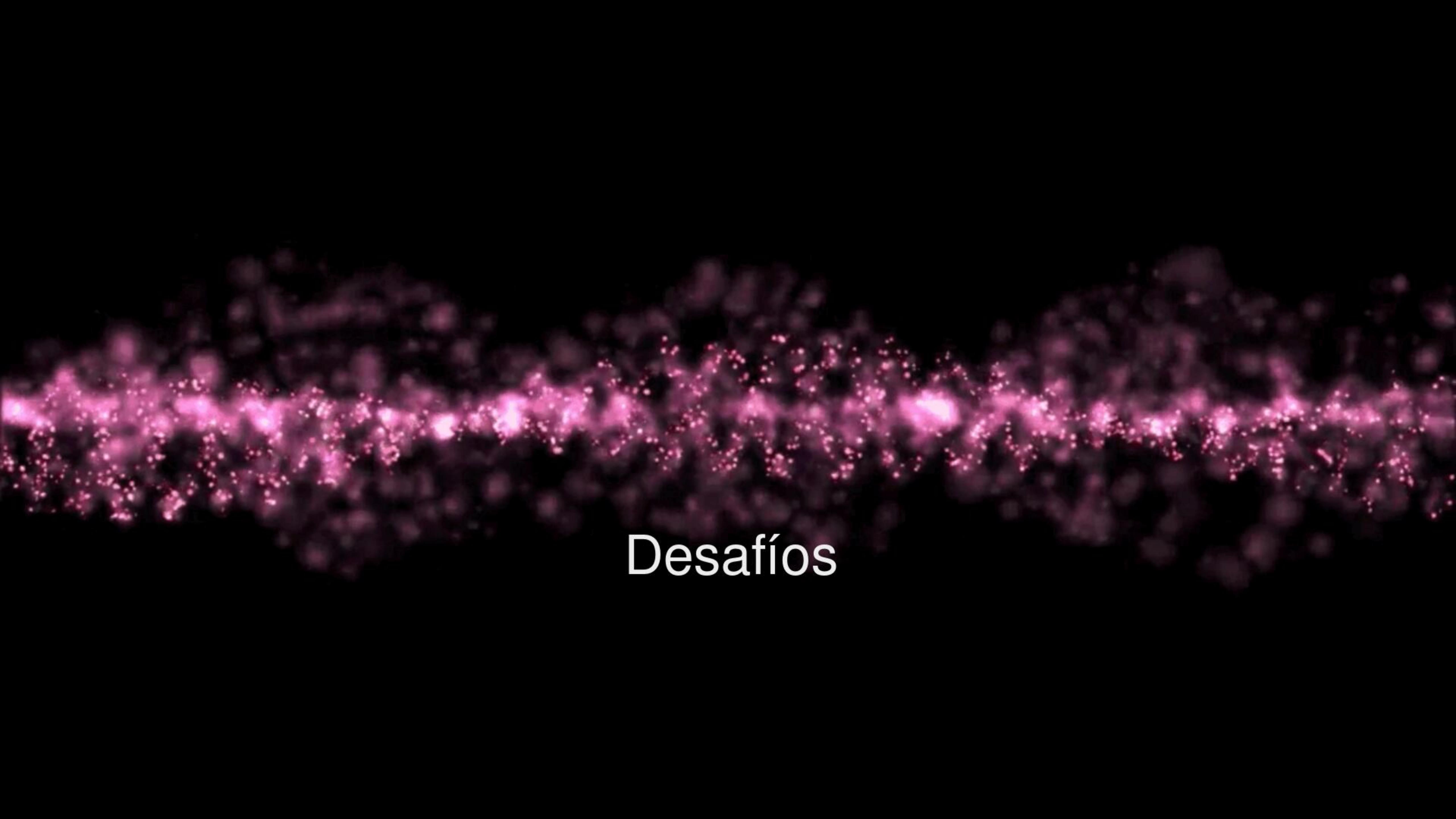
$\ominus$ $\oplus$	$+[t]$ $-[t]$	QFT QFT <sup>†</sup>	input A A = # default	+1 -1	$\oplus A < B$ $\oplus A > B$	+1 -1 mod R	... 0
$\oslash$ $\otimes$	Reverse	Grad <sup>1/2</sup> Grad <sup>-1/2</sup>	input B B = # default	+A -A	$\oplus A \leq B$ $\oplus A \geq B$	+A -A mod R	-
$ +\rangle\langle + $ $ -\rangle\langle - $		Grad <sup>t</sup> Grad <sup>-t</sup>	input R R = # default	+AB -AB	$\oplus A = B$ $\oplus A \neq B$	$\times A$ $\times A^{-1}$ mod R	i -i
$ i\rangle\langle i $ $  -i\rangle\langle -i $	Order	Frequency	Inputs	$\times A$ $\times A^{-1}$	Compare	$\times B$ $\times B^{-1}$ mod R	$\sqrt{i}$ $\sqrt{-i}$

X/Y Probes Order Frequency Inputs Arithmetic Compare Modular Scalar Custom Gates

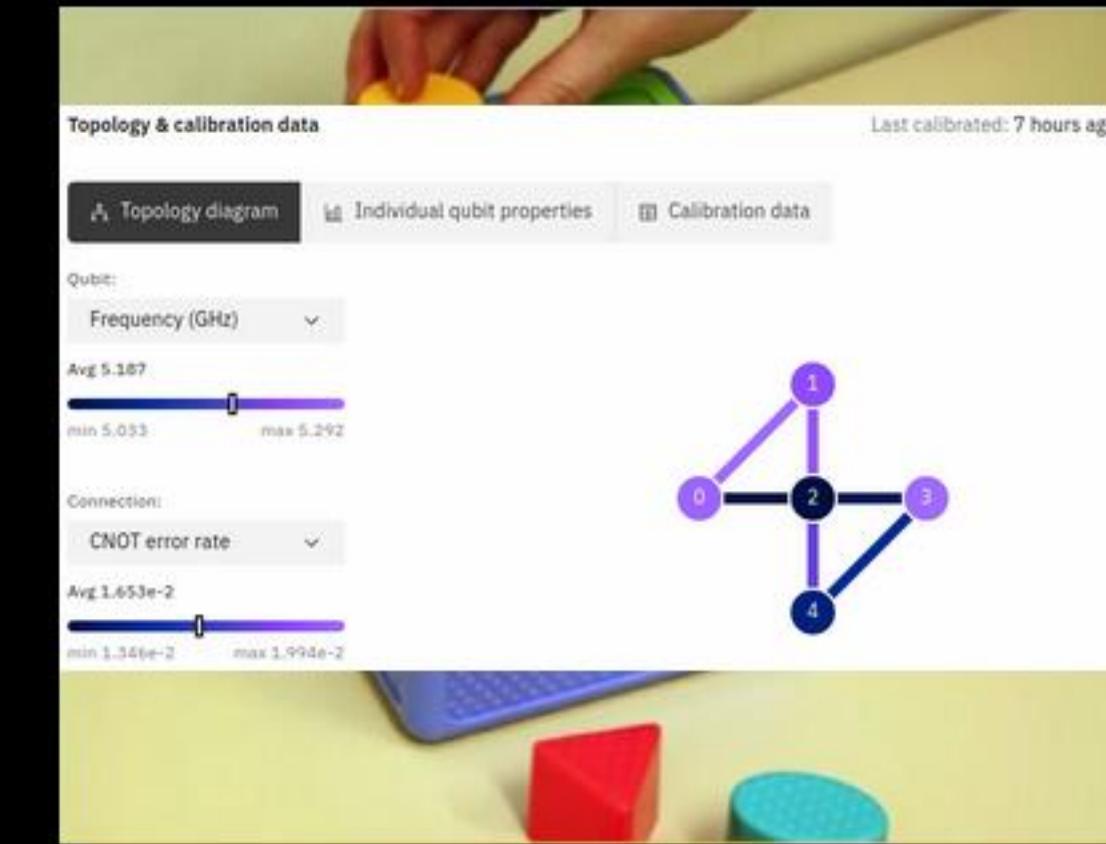
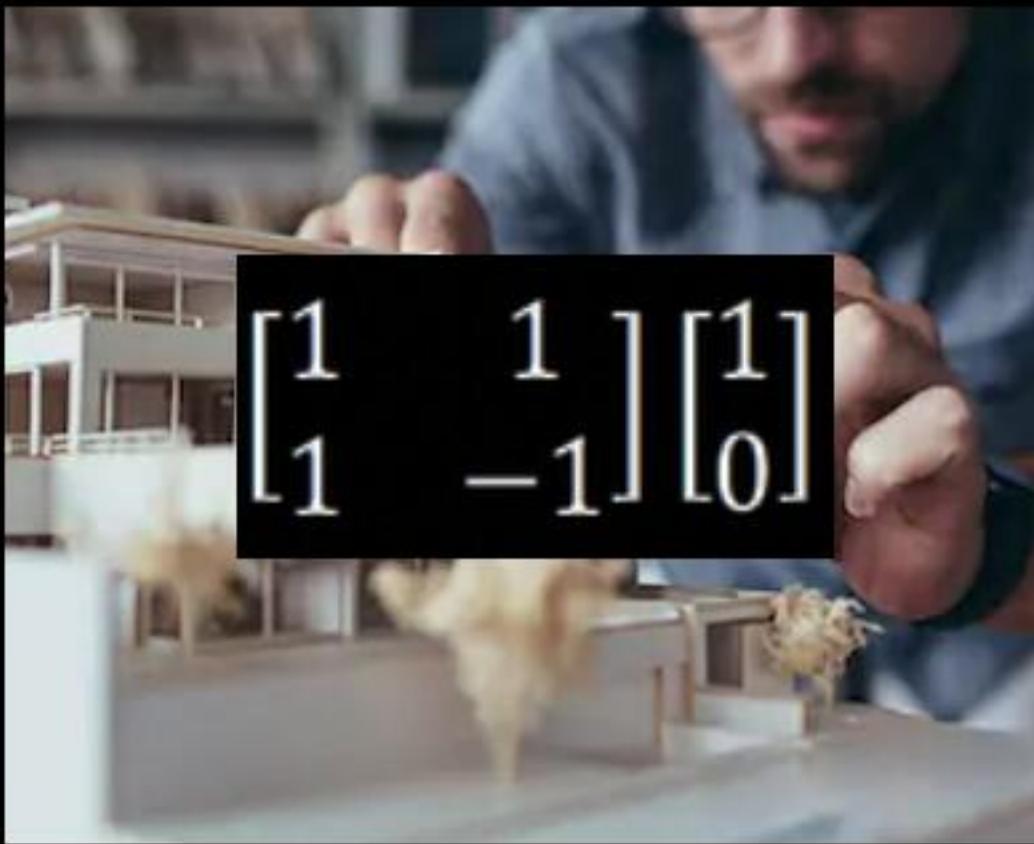
<https://algassert.com/quirk>



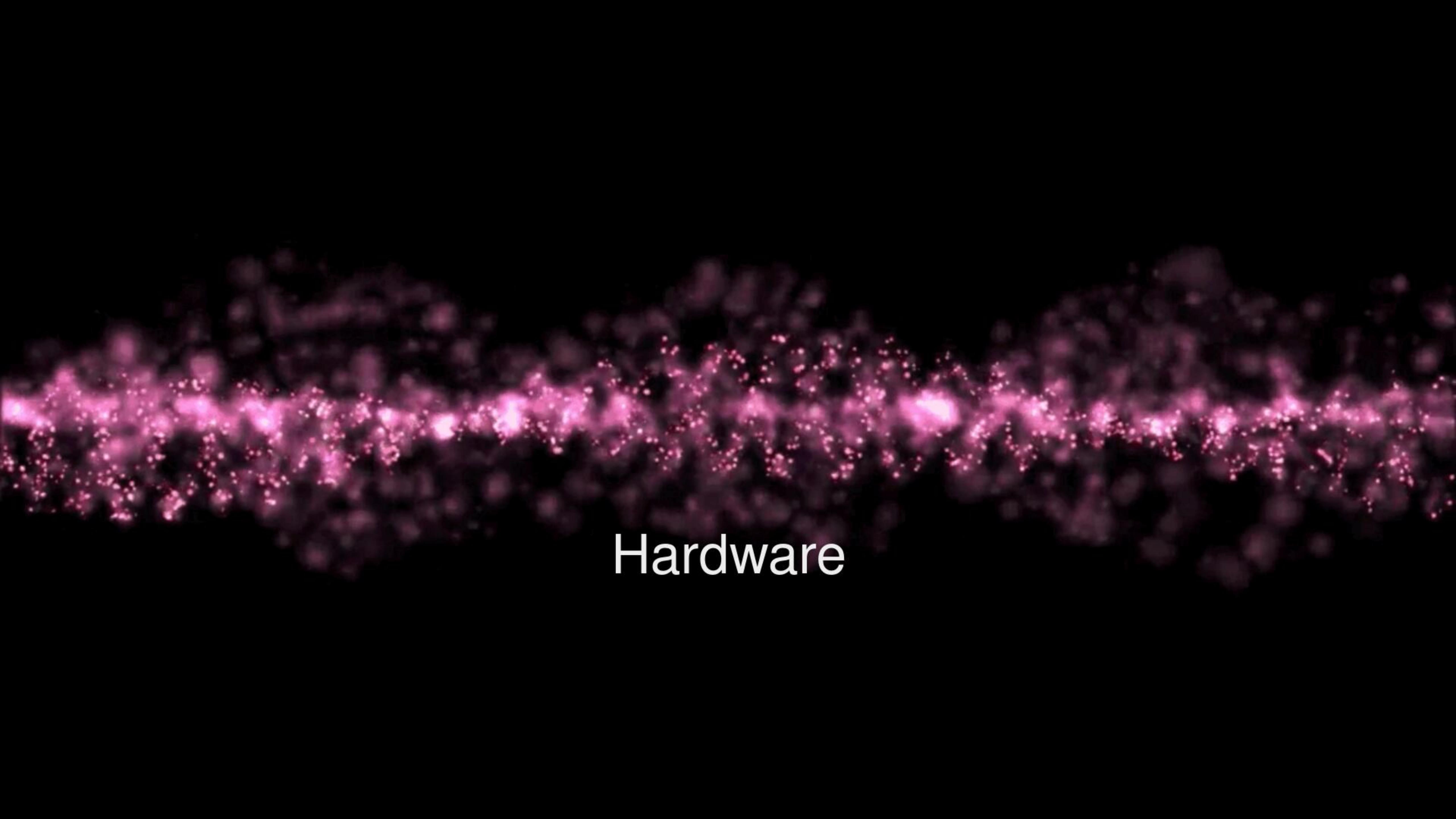
<https://quantum-computing.ibm.com/composer>



Desafíos



## Desafíos

The background of the image is black. A horizontal band of glowing pink particles, resembling a comet's tail or a starburst, stretches across the middle of the frame. The particles are concentrated in the center and taper off towards the edges.

Hardware

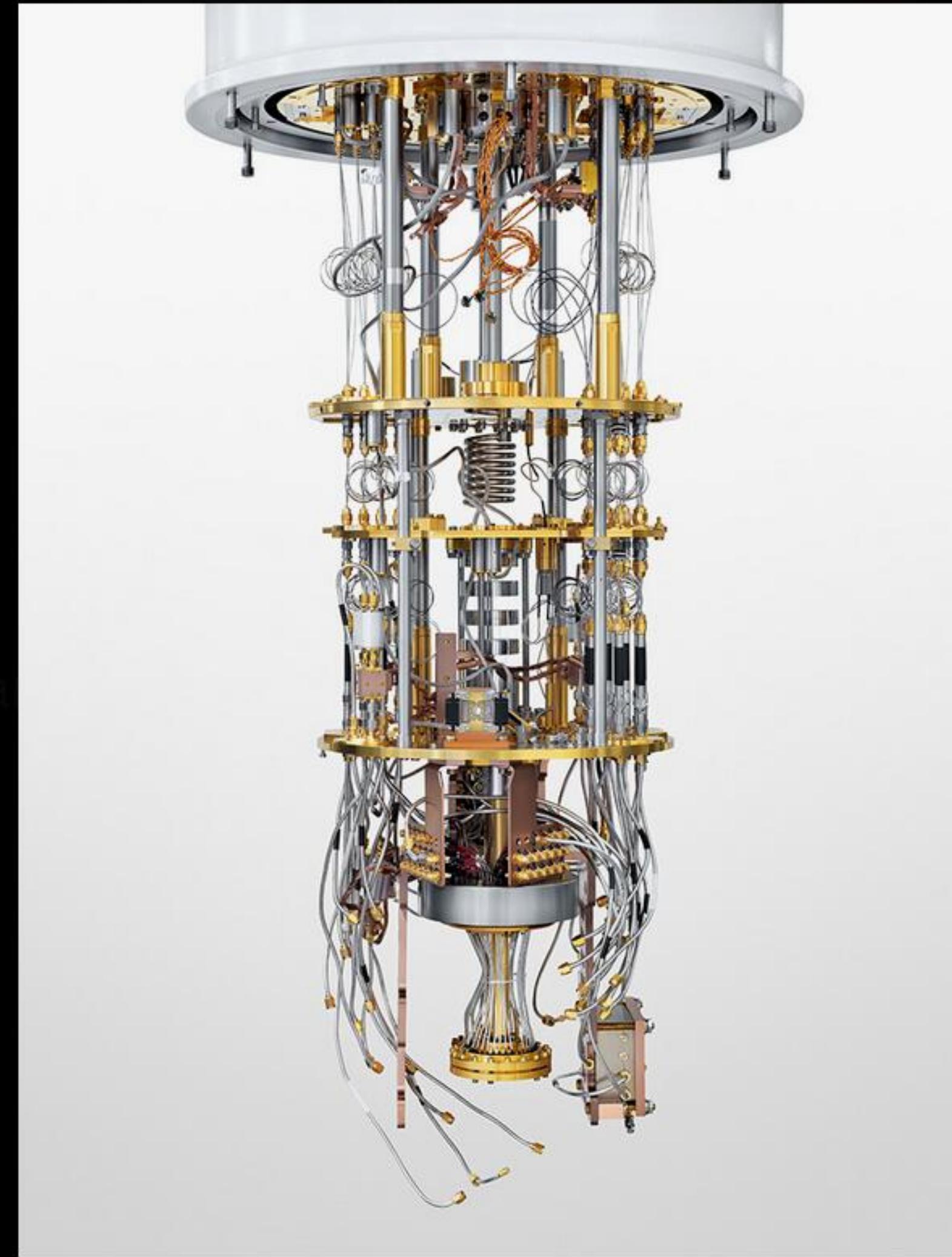


Computadoras clásicas

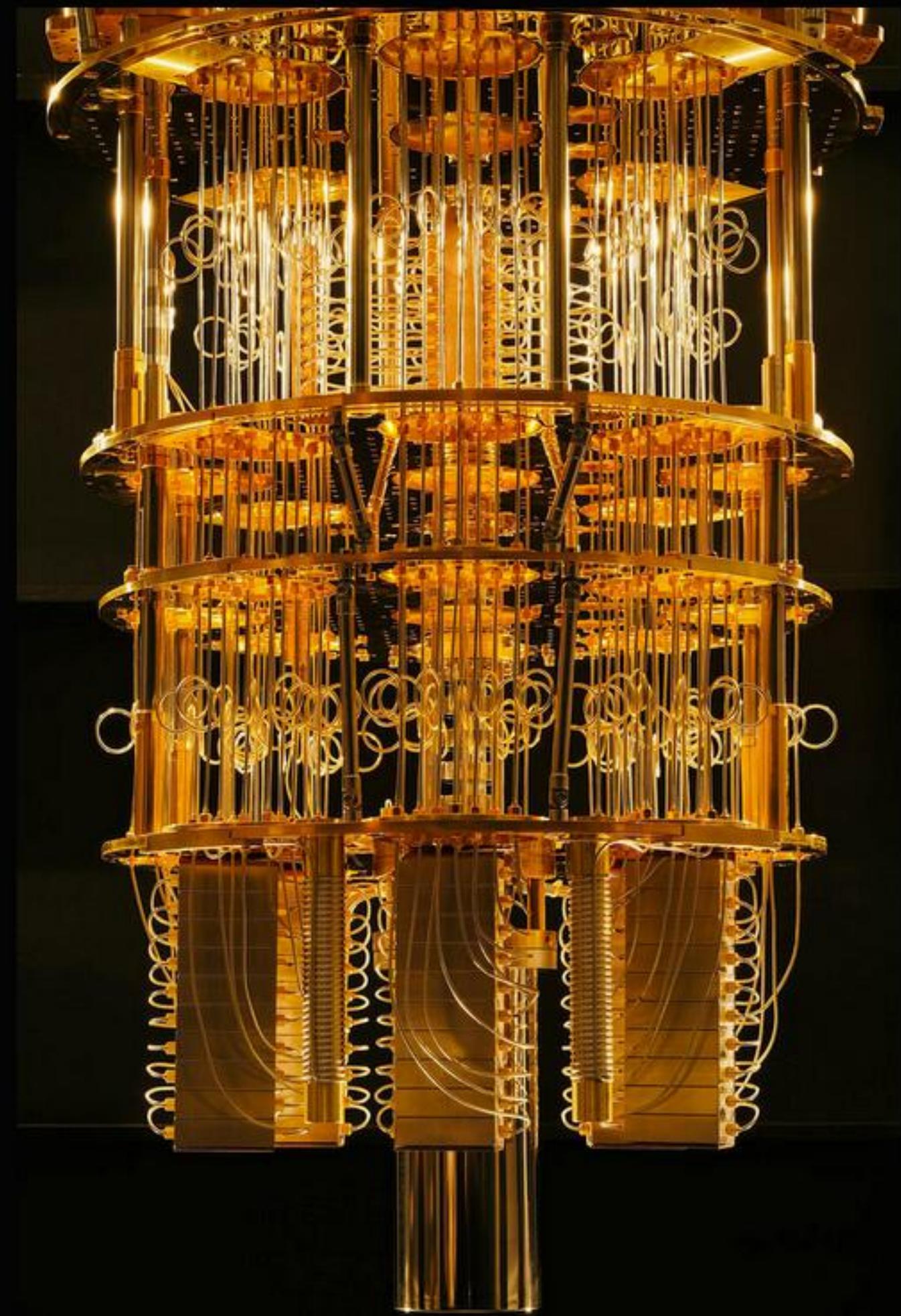


Google Sycamore

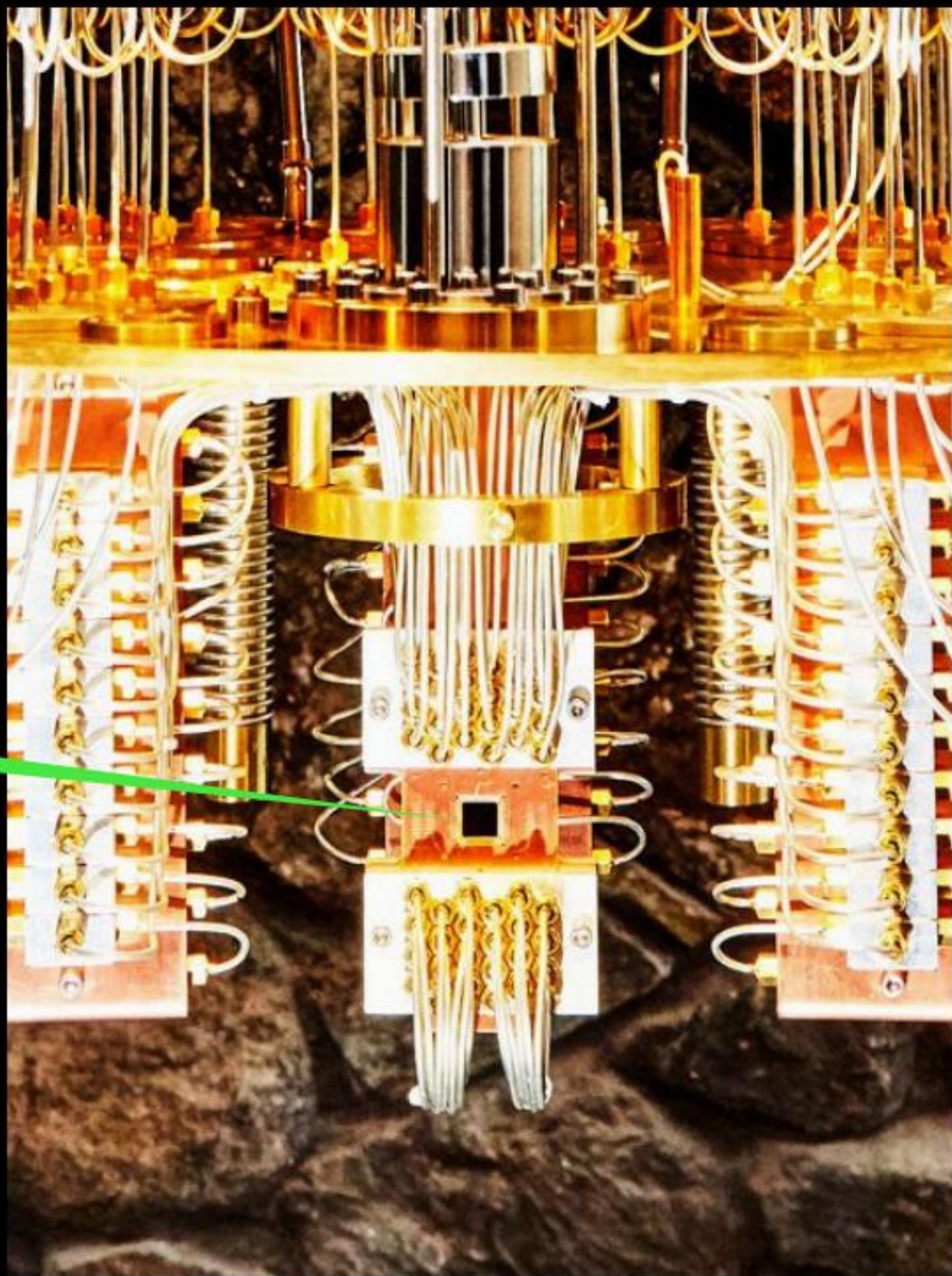
Rigetti  
e Syca

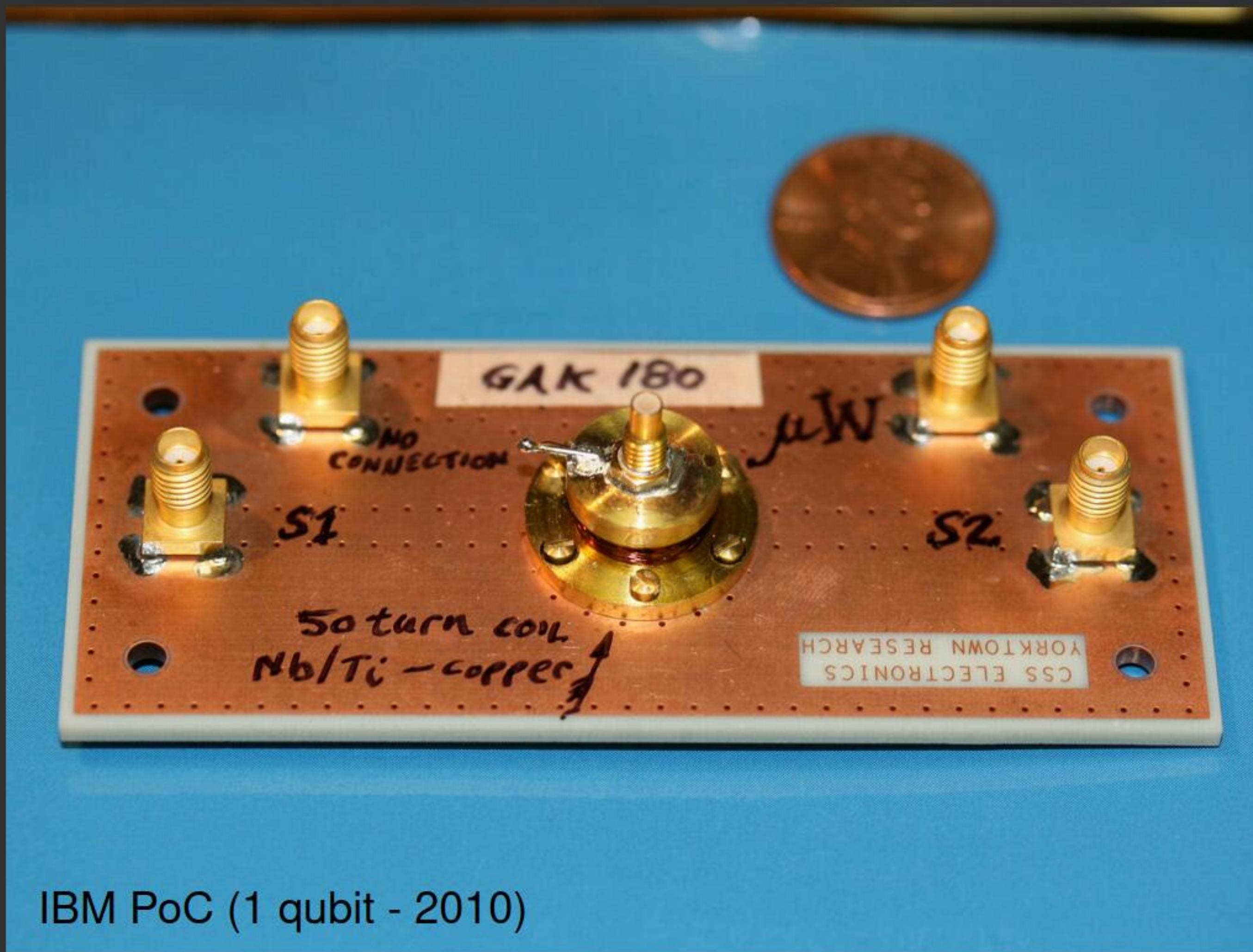


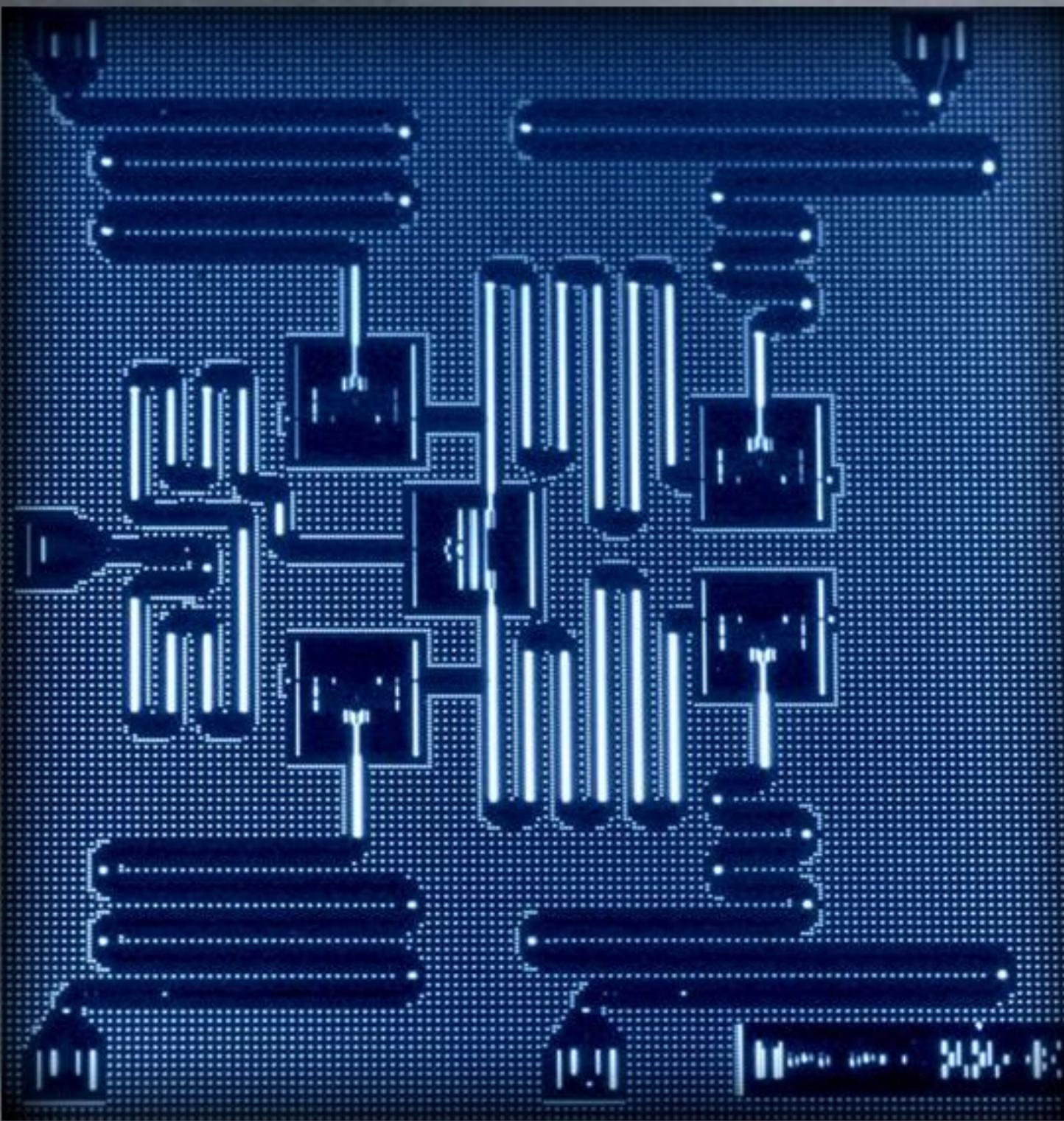
IBM Q 53



IBM Q 53  
(chip)





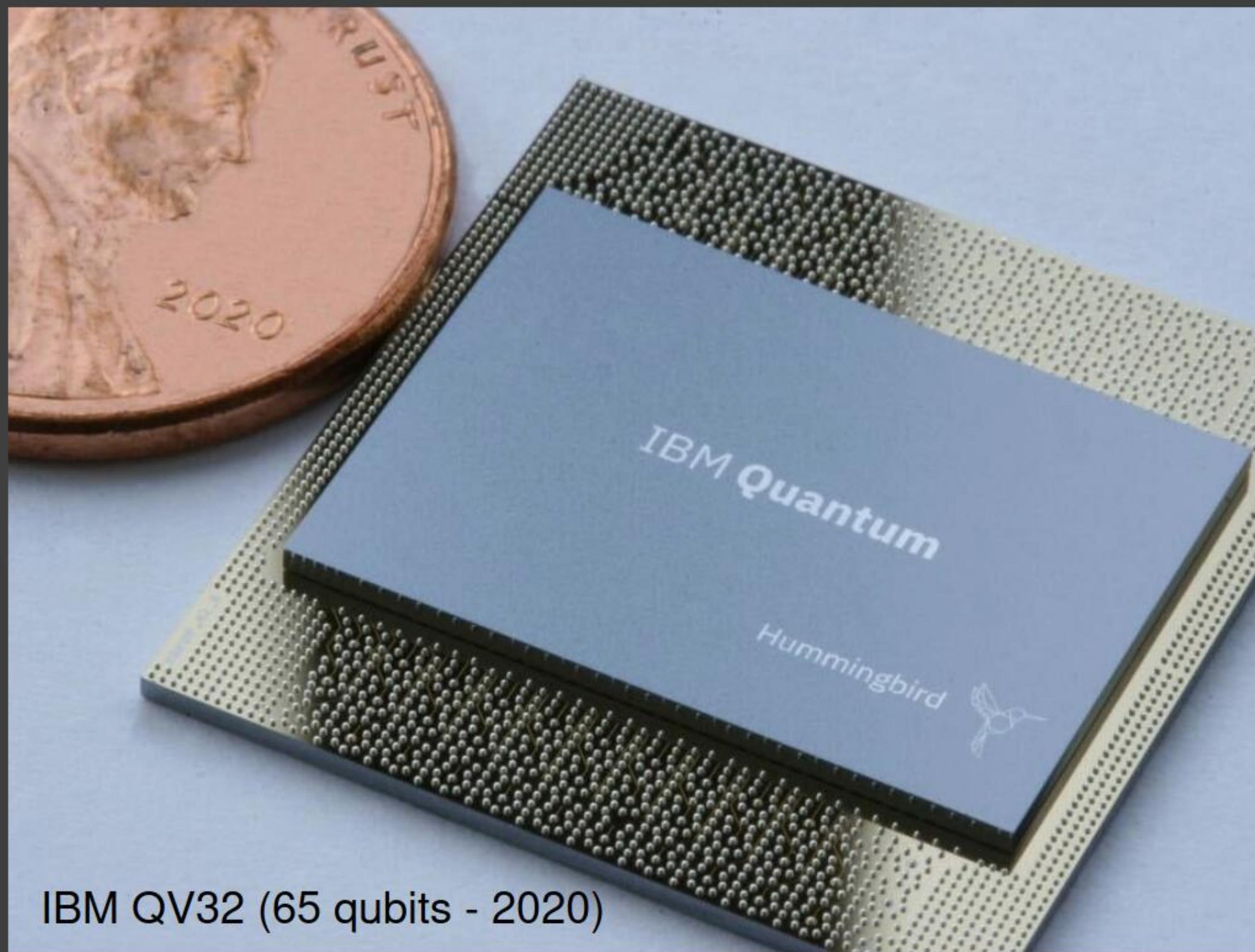


Procesador cuántico de IBM en la nube  
(5 qubits - 2015)



Superconductor

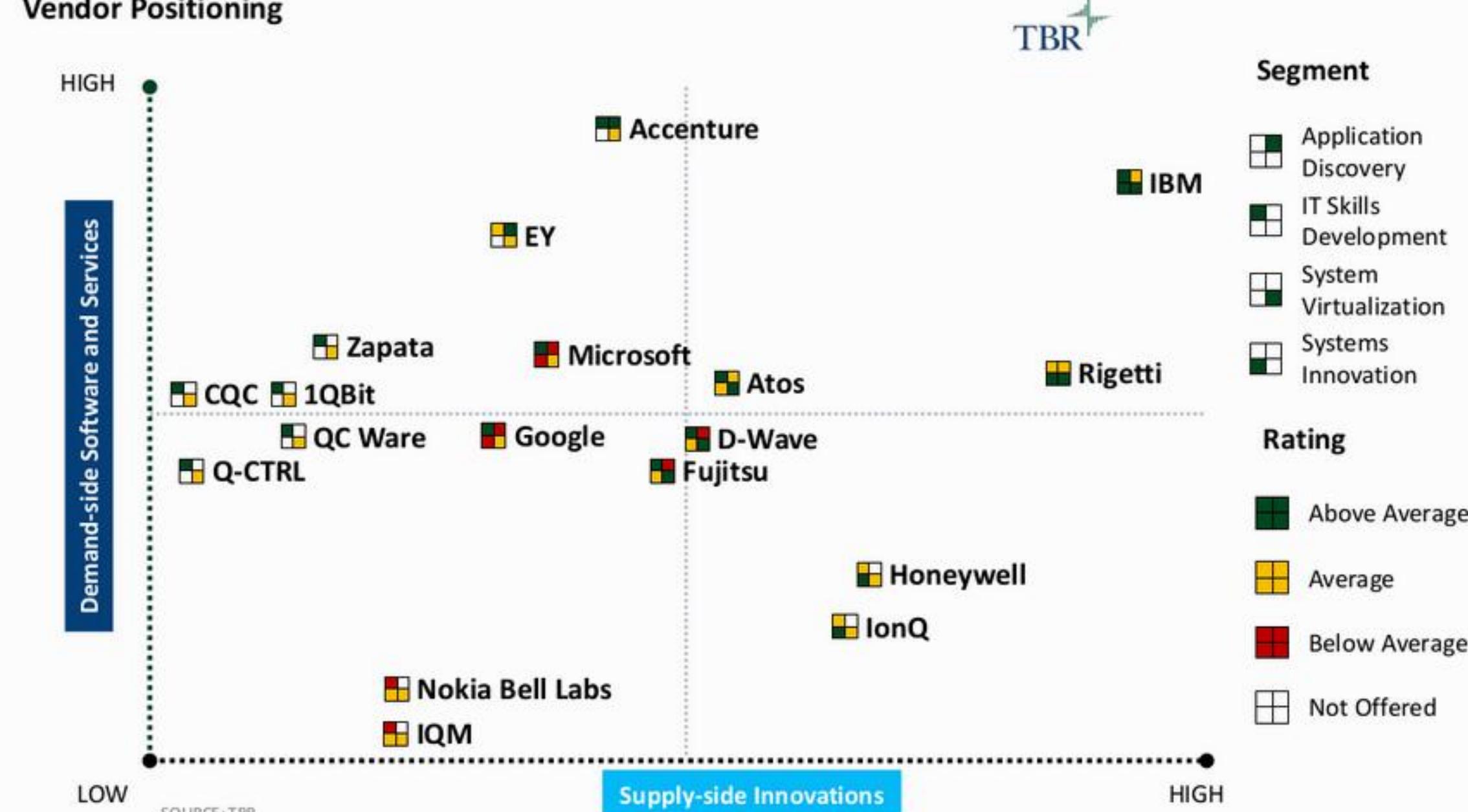




IBM QV32 (65 qubits - 2020)

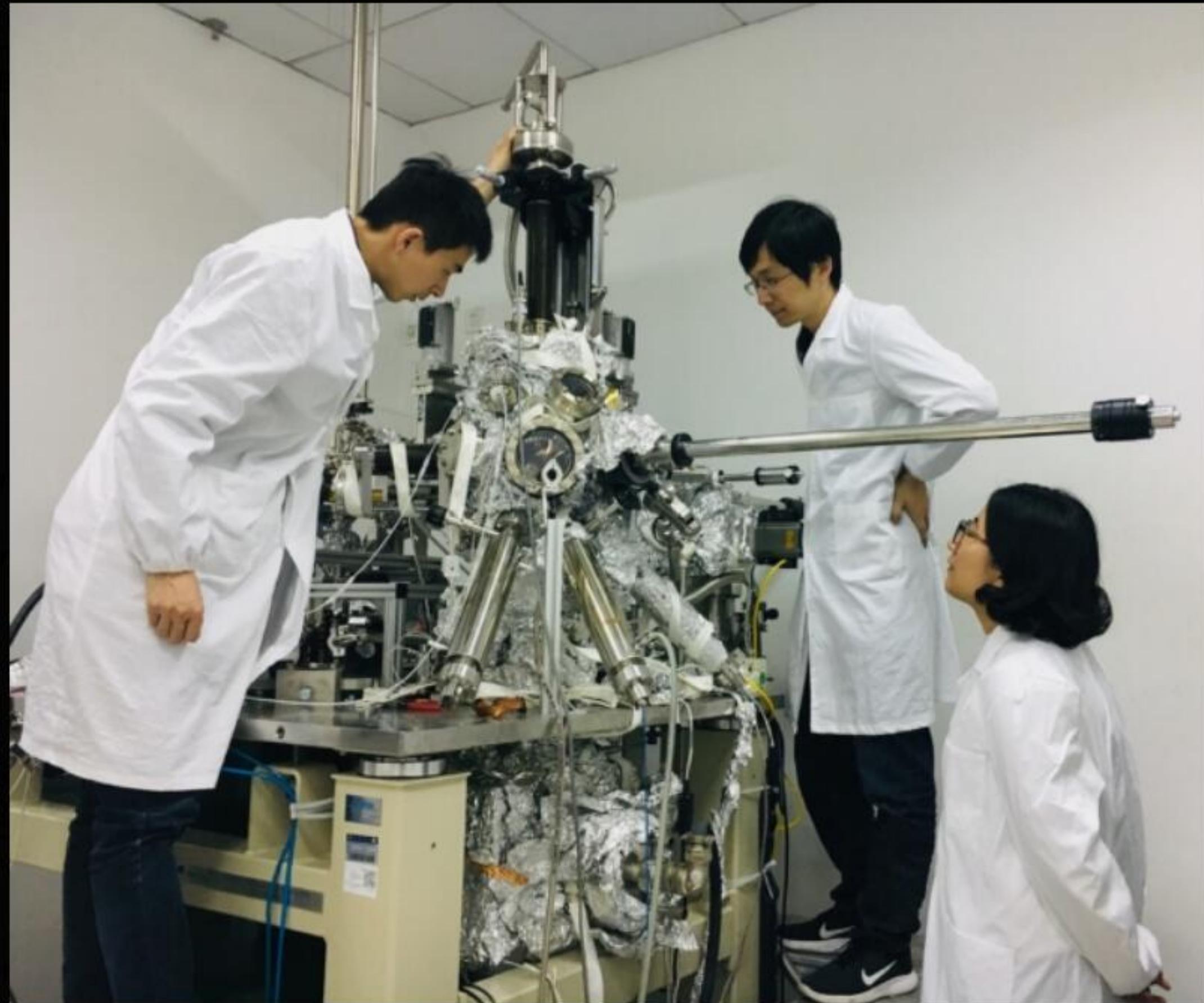
**Few vendors compete across the 4 elements of the quantum stack,  
though many have development initiatives for the future**

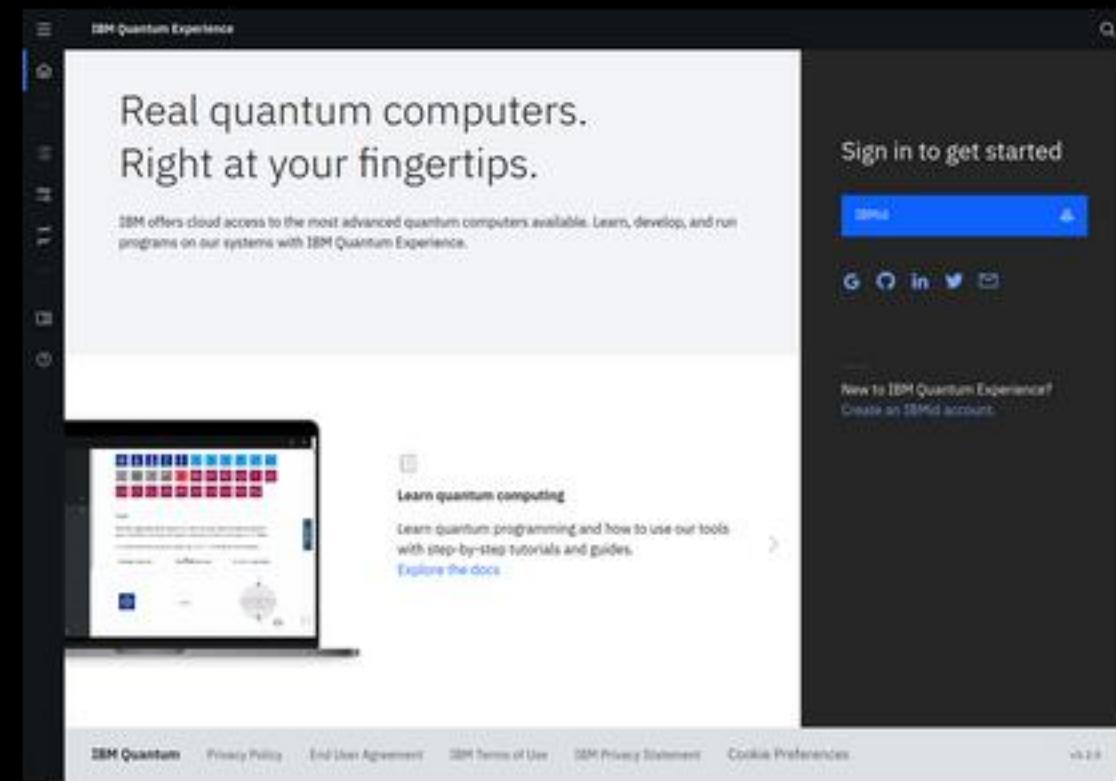
Vendor Positioning



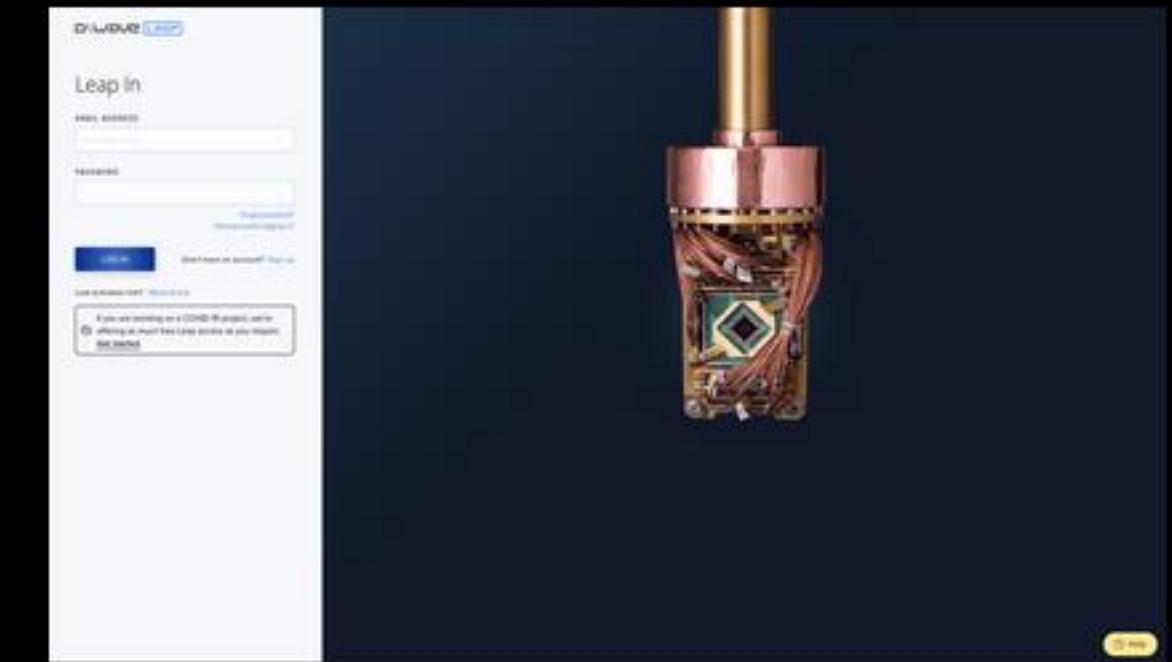
# Institute of Physics of the Chinese Academy of Sciences

Creative Summary: Our  
Few vendors come  
though many have  
Vendor positioning

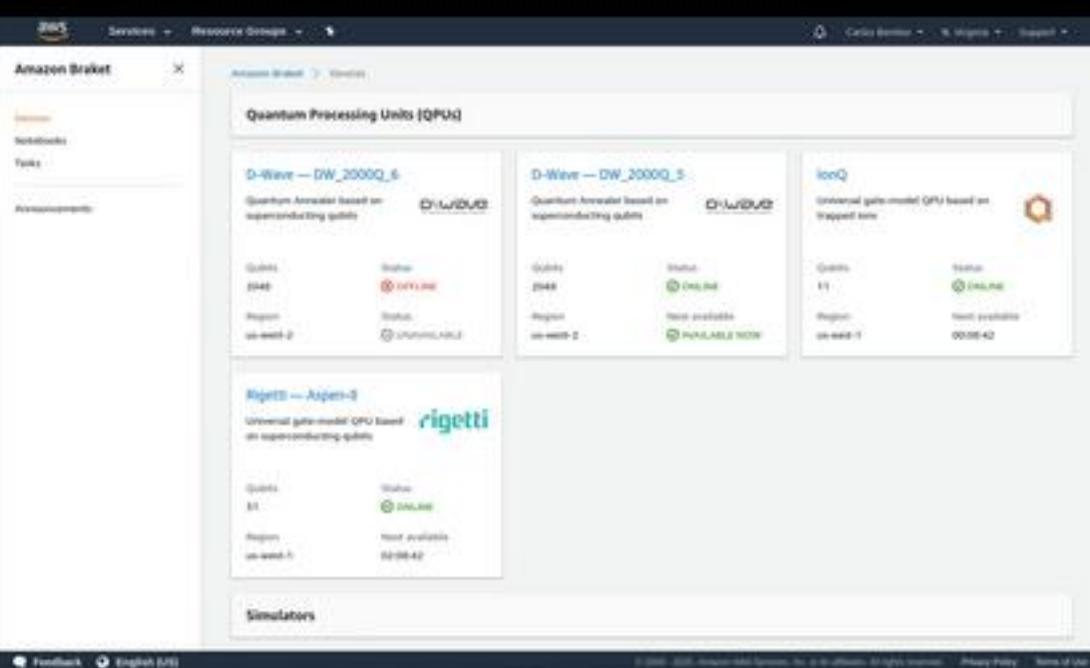




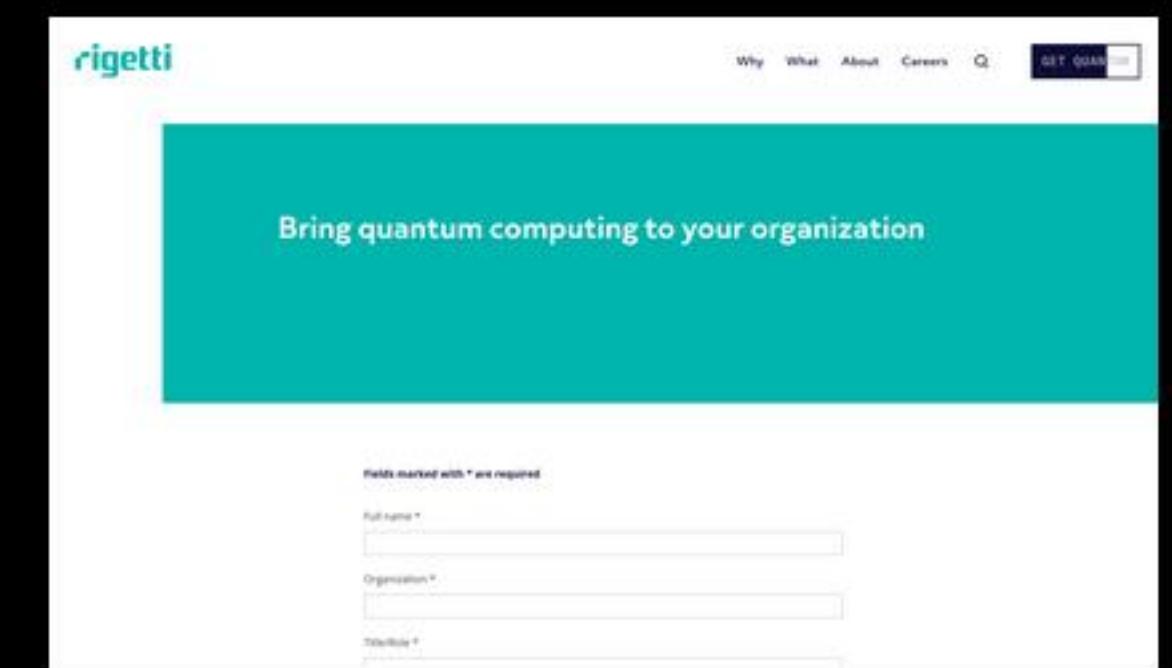
<https://quantum-computing.ibm.com/>



<https://cloud.dwavesys.com/leap/login/>



<https://console.aws.amazon.com/braket/home>

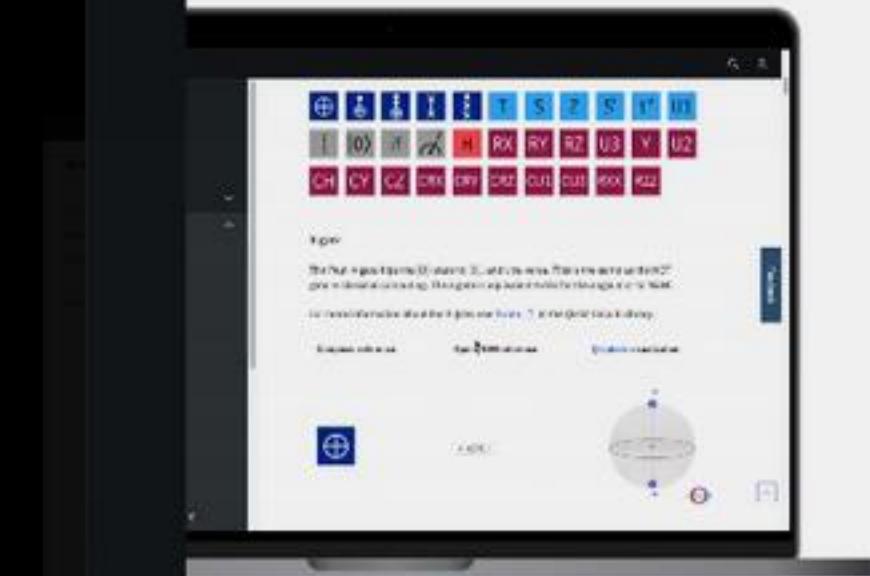


<https://www.rigetti.com/get-quantum>

IBM Quantum Experience

Real quantum computers.  
Right at your fingertips.

IBM offers cloud access to the most advanced quantum computers available. Learn, develop, and run programs on our systems with IBM Quantum Experience.



Learn quantum computing

Learn quantum programming and how to use our tools with step-by-step tutorials and guides.

Explore the docs >

Sign in to get started

IBMid

G O in Twitter Email

New to IBM Quantum Experience?  
Create an IBMid account.

https://quantum-computing.ibm.com/

IBM Quantum Privacy Policy End User Agreement IBM Terms of Use IBM Privacy Statement Cookie Preferences v3.2.0



KEEP  
CALM  
AND  
PLAY WITH  
QUBITS

## Referencias

- <https://github.com/1ucian0/talks/tree/main/ekoparty0121>
- <https://algassert.com/quirk>
- <https://qiskit.org/textbook>
- <https://quantum-computing.ibm.com/>
- <https://spectrum.ieee.org/computing/hardware/quantum-computers-strive-to-break-out-of-the-lab>
- <https://www.ibm.com/quantum-computing/technology/systems/>
- <https://quantum-computing.ibm.com/support/guides/introduction-to-quantum-circuits>
- <https://quantum-computing.ibm.com/support/guides/getting-started-with-circuit-composer>
- <https://github.com/Qiskit/qiskit-iqx-tutorials>
- <https://www.dwavesys.com/tutorials/background-reading-series/introduction-d-wave-quantum-hardware>
- <https://nbviewer.jupyter.org/github/mett29/Shor-s-Algorithm/blob/master/Shor.ipynb>
- <https://www.youtube.com/watch?v=5xsyx-aNCIM>
- [https://github.com/1ucian0/qiskit-presentations/tree/master/2019-06-20\\_Techsauce\\_workshop](https://github.com/1ucian0/qiskit-presentations/tree/master/2019-06-20_Techsauce_workshop)
- <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/>
- [http://www-2.unipv.it/dottorati/scienzeetecnologie/fisica/n/web\\_PhD/attachments/section/19/Quantum%20Computing%20Tavernelli%2014-02-2019.pdf](http://www-2.unipv.it/dottorati/scienzeetecnologie/fisica/n/web_PhD/attachments/section/19/Quantum%20Computing%20Tavernelli%2014-02-2019.pdf)
- [https://my.tbri.com/external/2q20/bench/quantumcompml/tbr\\_quantum\\_ml\\_2q20\\_cbq.pdf](https://my.tbri.com/external/2q20/bench/quantumcompml/tbr_quantum_ml_2q20_cbq.pdf)

# ¡muchas gracias!

**Luciano Bello**

bel<at>zurich.ibm.com  
@microluciano

**Carlos Benitez**

carlos<at>platinumciber.com  
<https://cybersonthestorm.com>  
@ch4r1i3b

Not only does God play dice, but... he sometimes throws them where they cannot be seen. (Stephen Hawking)

