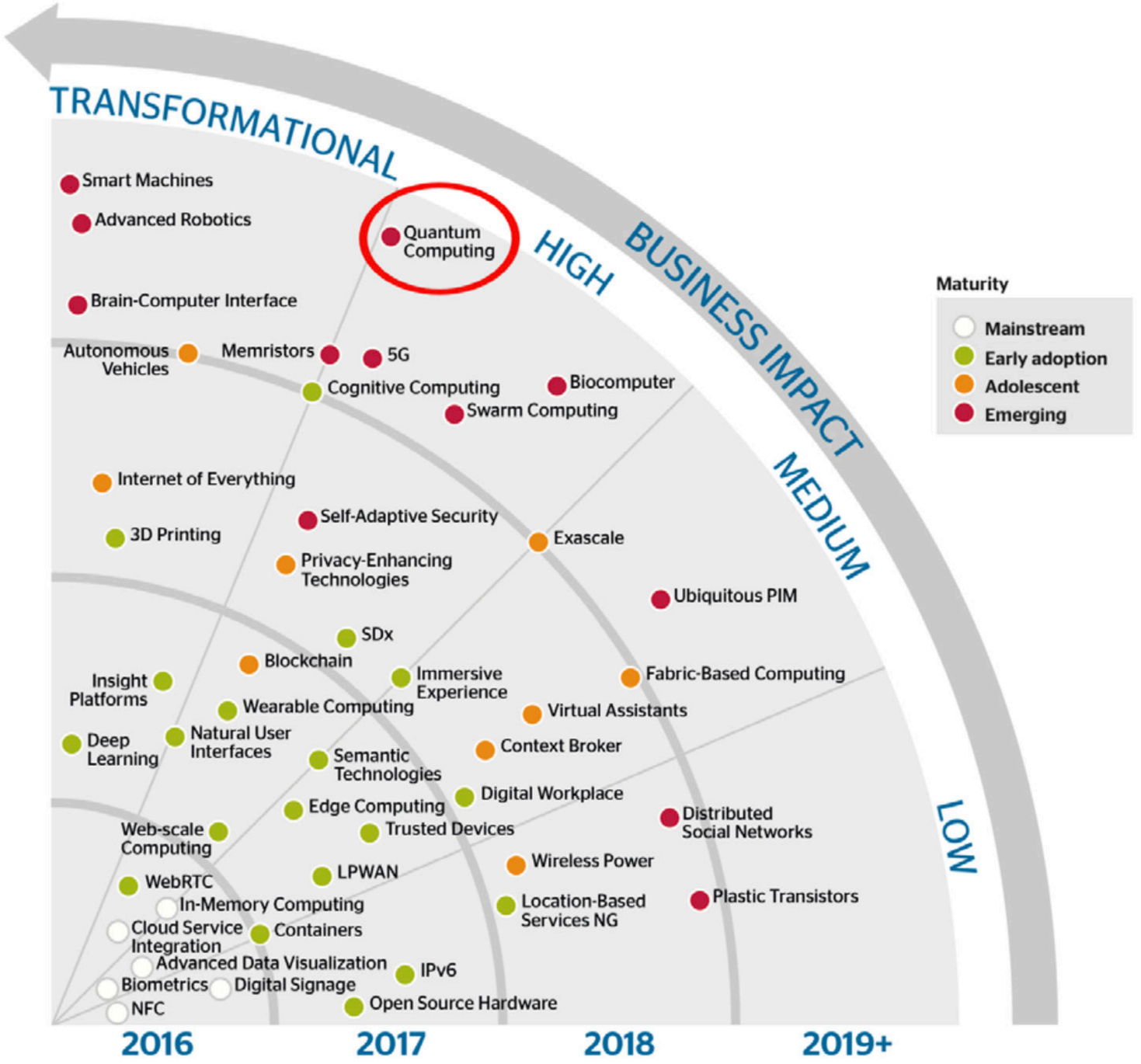
Computación Cuántica

Estado, Conceptos, Aplicaciones, y Futuro

Santiago Núñez Corrales - José Castro

José Castro

Tendencias del Mercado
Inicios



© Atos 2016. All rights reserved.

Mercado

North America
Largest Market
By Region (2019)

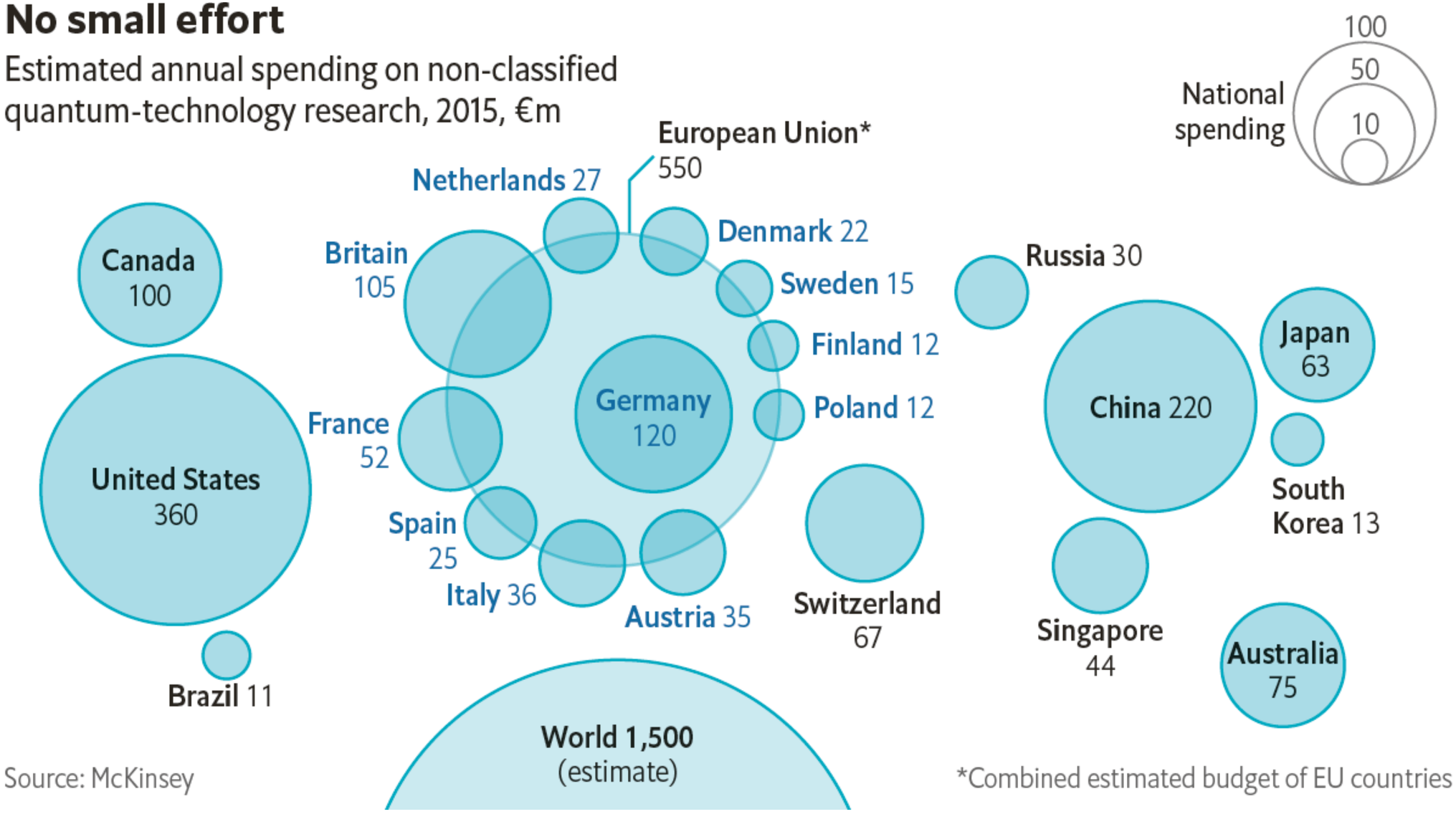
APAC
Fastest-Growing Market
By Region (2020–2030)

2019
Market Size
$89.6
million

2030
Market Size
$1,866.8
million

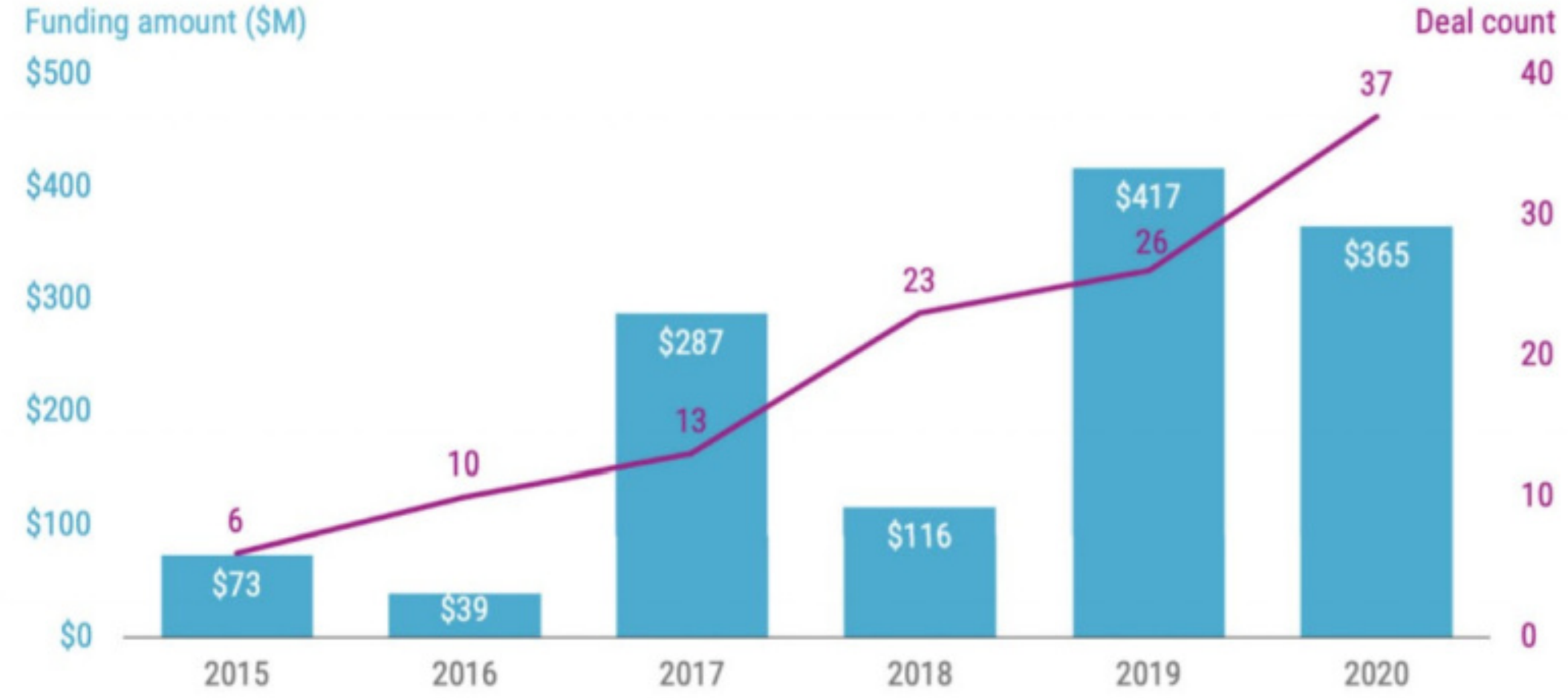
Market
Growth Rate
(2020–2030)
33.1%

Gasto anual en investigación (por país)



Quantum computing deals are on the rise

Disclosed deals & equity funding ($M), 2015 – 2020



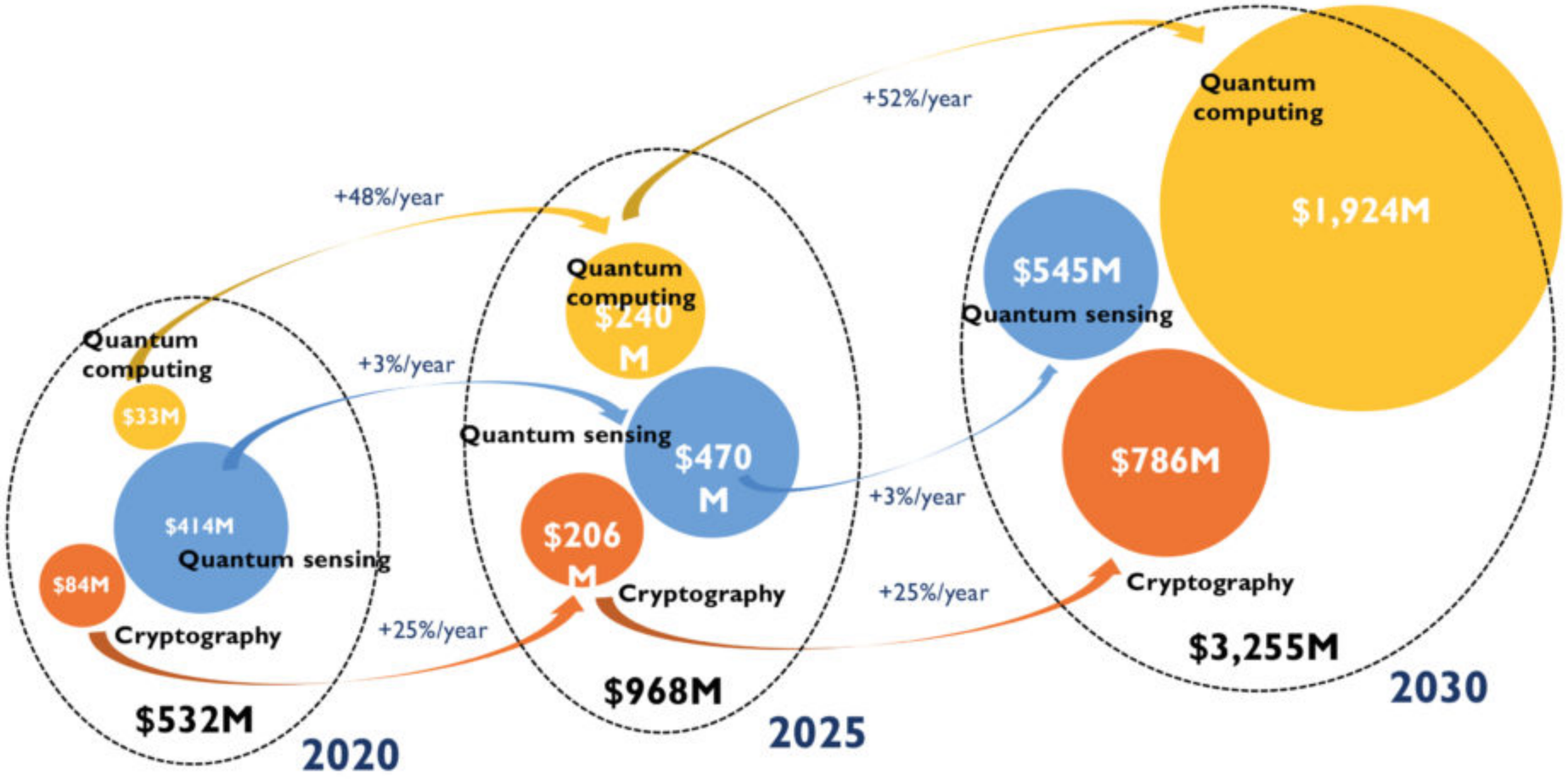
Source: cbinsights.com

CBINSIGHTS

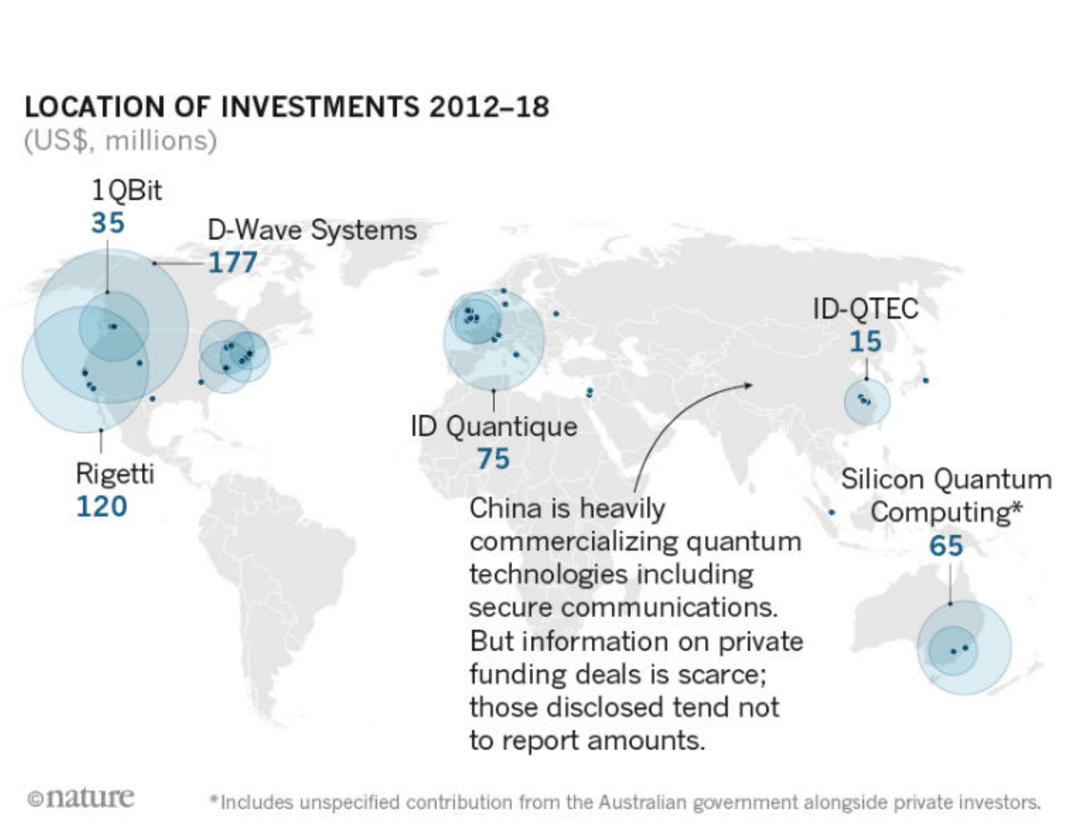
Tendencias tecnológicas

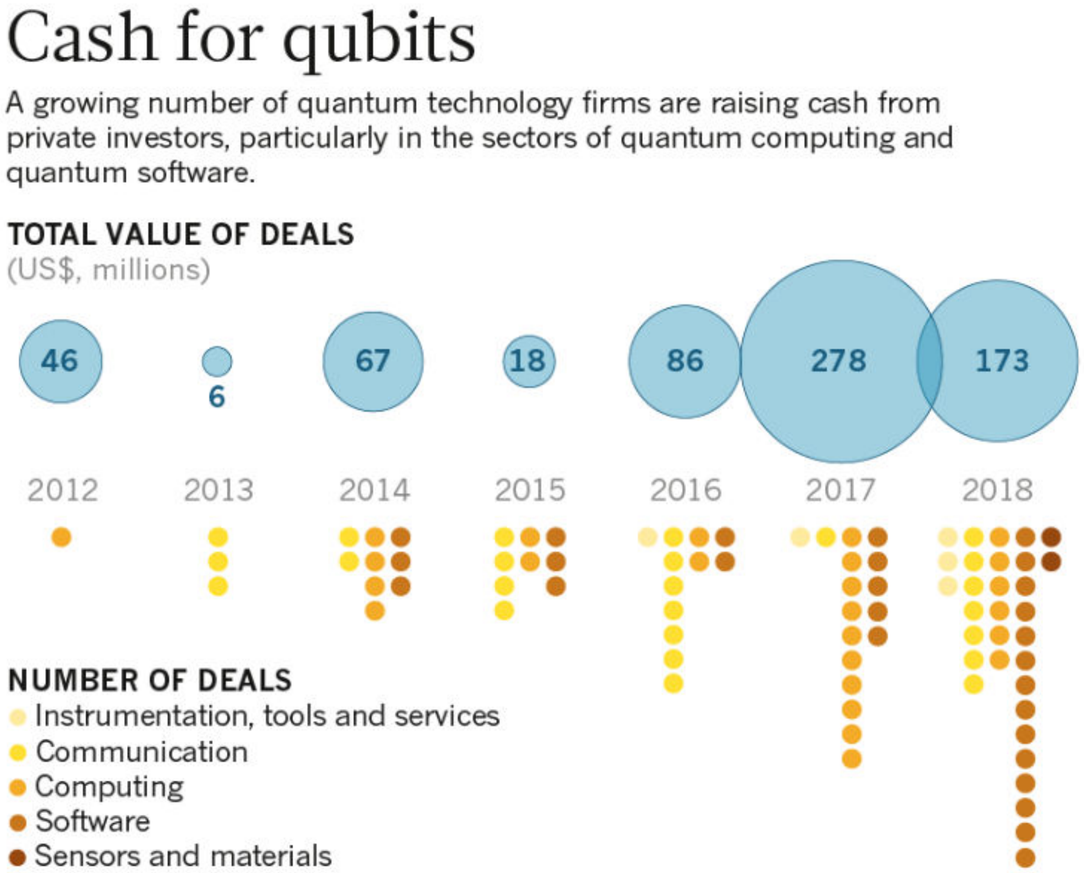
2020 – 2025 – 2030 quantum technologies forecast

(Source: Quantum Technologies report, Yole Développement, 2020)



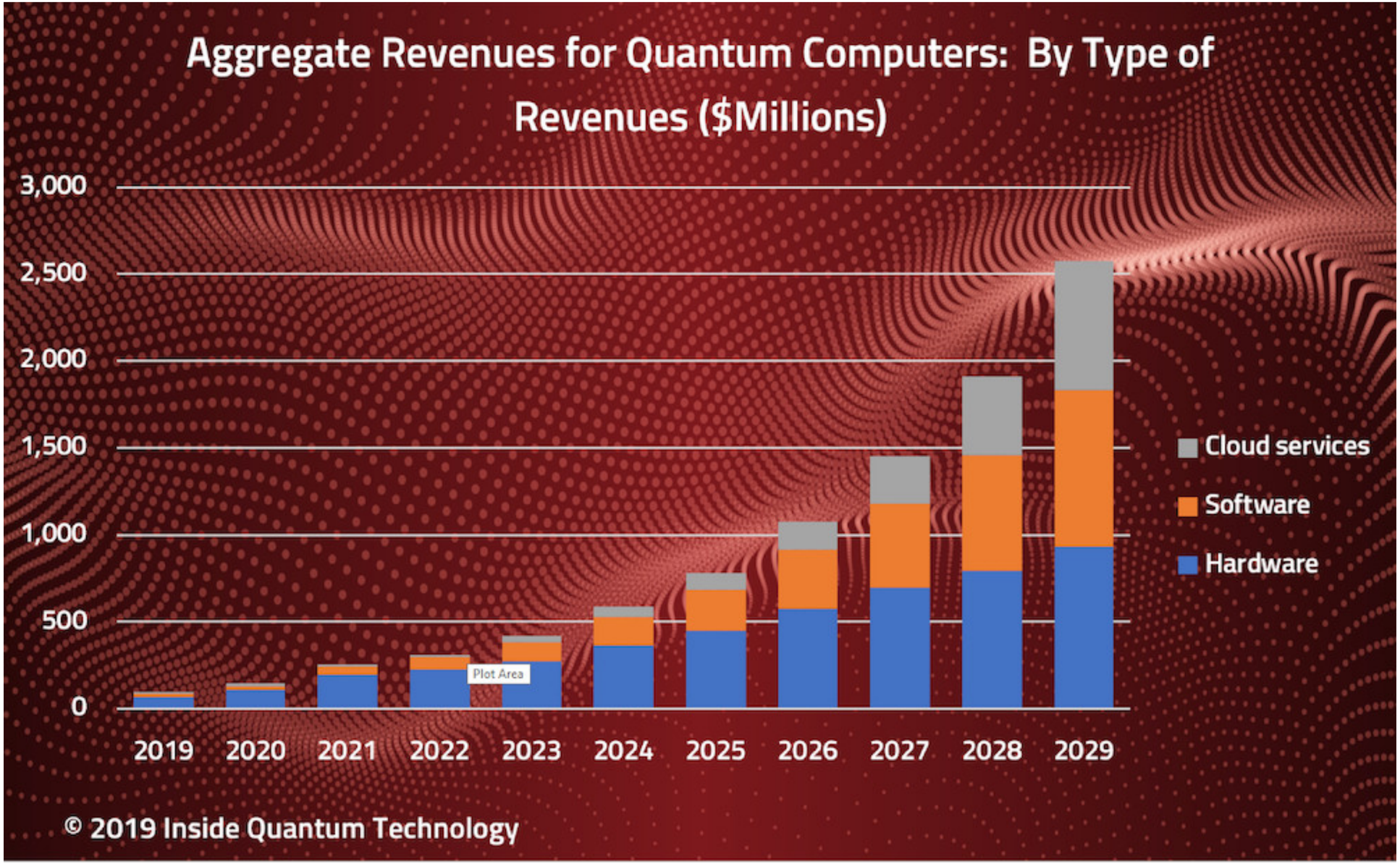
© 2020 | www.yole.fr – www.i-micronews.com





Elizabeth Gibney. **Quantum gold rush: the private funding pouring into quantum start-ups.** Nature, October 2019.

Ingresos

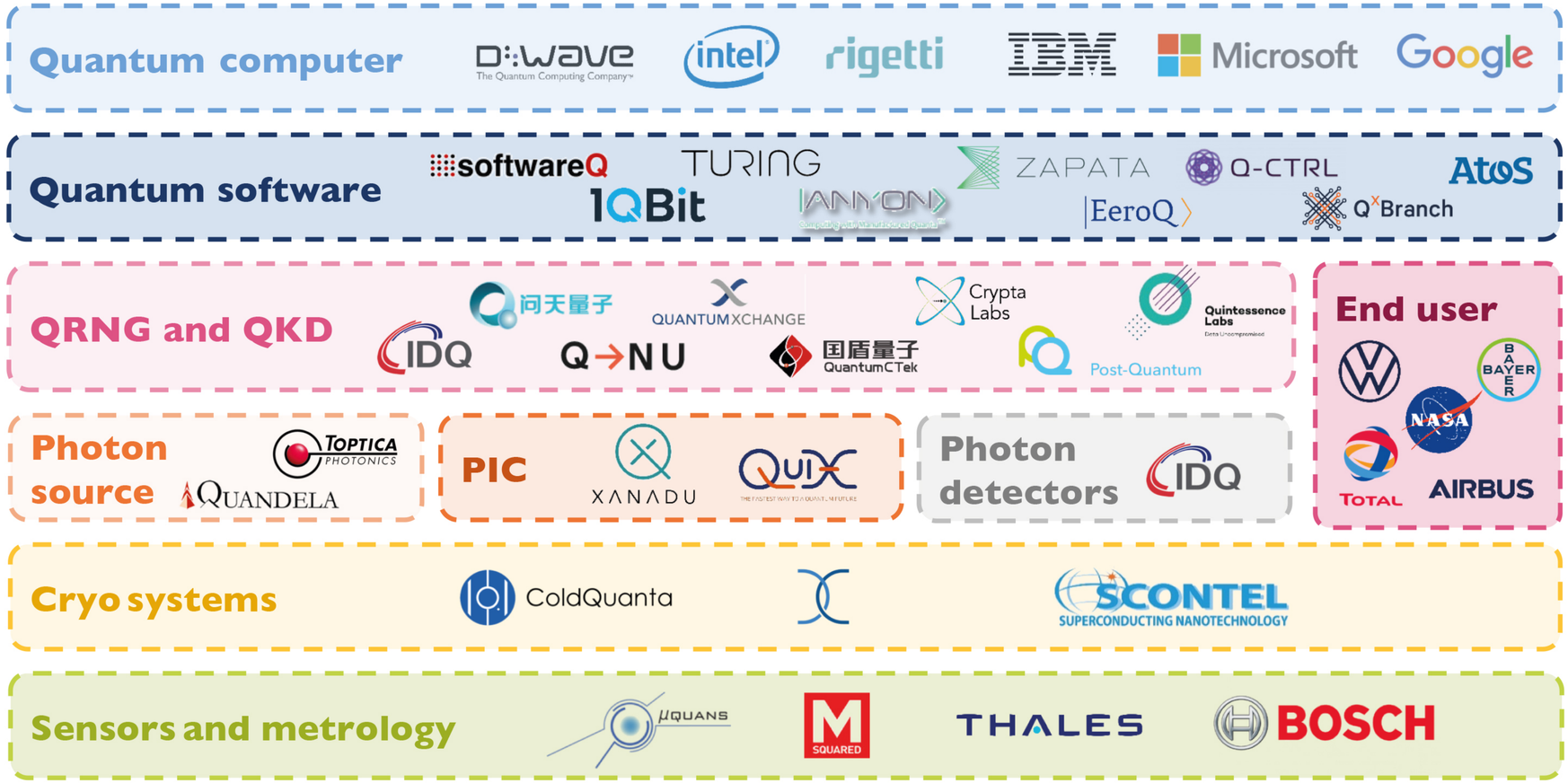

Aggregate Revenues for Quantum Computers: By Type of Revenues ($Millions)
3,000
2,500
2,000
1,500
1,000
500
0
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
Plot Area
Cloud services
Software
Hardware
© 2019 Inside Quantum Technology

Empresas


IBM
Google
id Quantique
A Quantum Leap for Cryptography
evolution
HEWLETT PACKARD
intel
Baidu 百度
Microsoft
Alibaba.com
Global trade starts here.
D:wave
The Quantum Computing Company
Atos Origin
LOCKHEED MARTIN
rigetti
HUAWEI
1QBit
TOSHIBA
Leading Innovation
Telefónica
SEQURENET
Raytheon
BBN Technologies
NEC
NTT
SK telecom
CQC
CAMBRIDGE QUANTUM COMPUTING LIMITED
Quantum Valley
INVESTMENTS
MagiQ
FUJITSU
NASA
QxBranch

Cadena de suministro

(Source: Quantum Technologies 2020 report, Yole Développement, 2020)



Non exhaustive list

PIC: Photonic Integrated Circuit - QKD: Quantum Key Distribution - QRNG: Quantum Random Number Generator

© 2020 | www.yole.fr – www.i-micronews.com

Software & Consultants

Quantum Computers

Enabling Technologies

New Funding Strategies

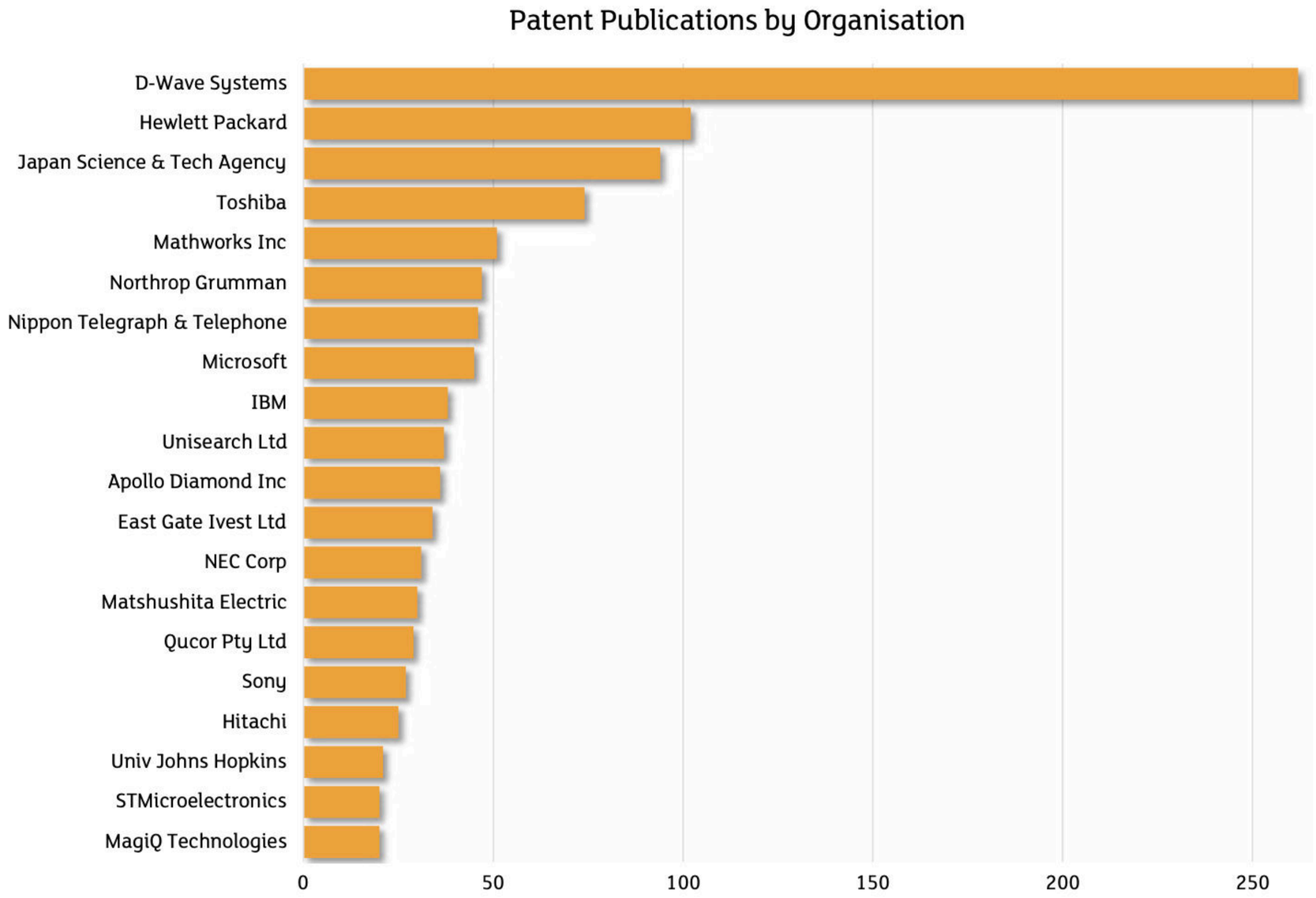
Representative list of players. A very active ecosystem!

QUANTUM WORLD ASSOCIATION

Patentes

The USA tops the list followed by the European Union, Canada, Japan and the UK.

Figure 2.3 shows the most active organisations, with D-Wave Systems (Canada) clearly leading the field, followed by Hewlett Packard, the Japan Science & Tech Agency and Toshiba.



What can quantum computers do better ?

Quantum computing could solve a range of complex aerospace problems

RESOLVING COMPLEX COMPUTATIONAL CHALLENGES

IMPROVING CRYPTOGRAPHIC ALGORITHMS

DEBUGGING MILLIONS OF LINES OF SOFTWARE CODE

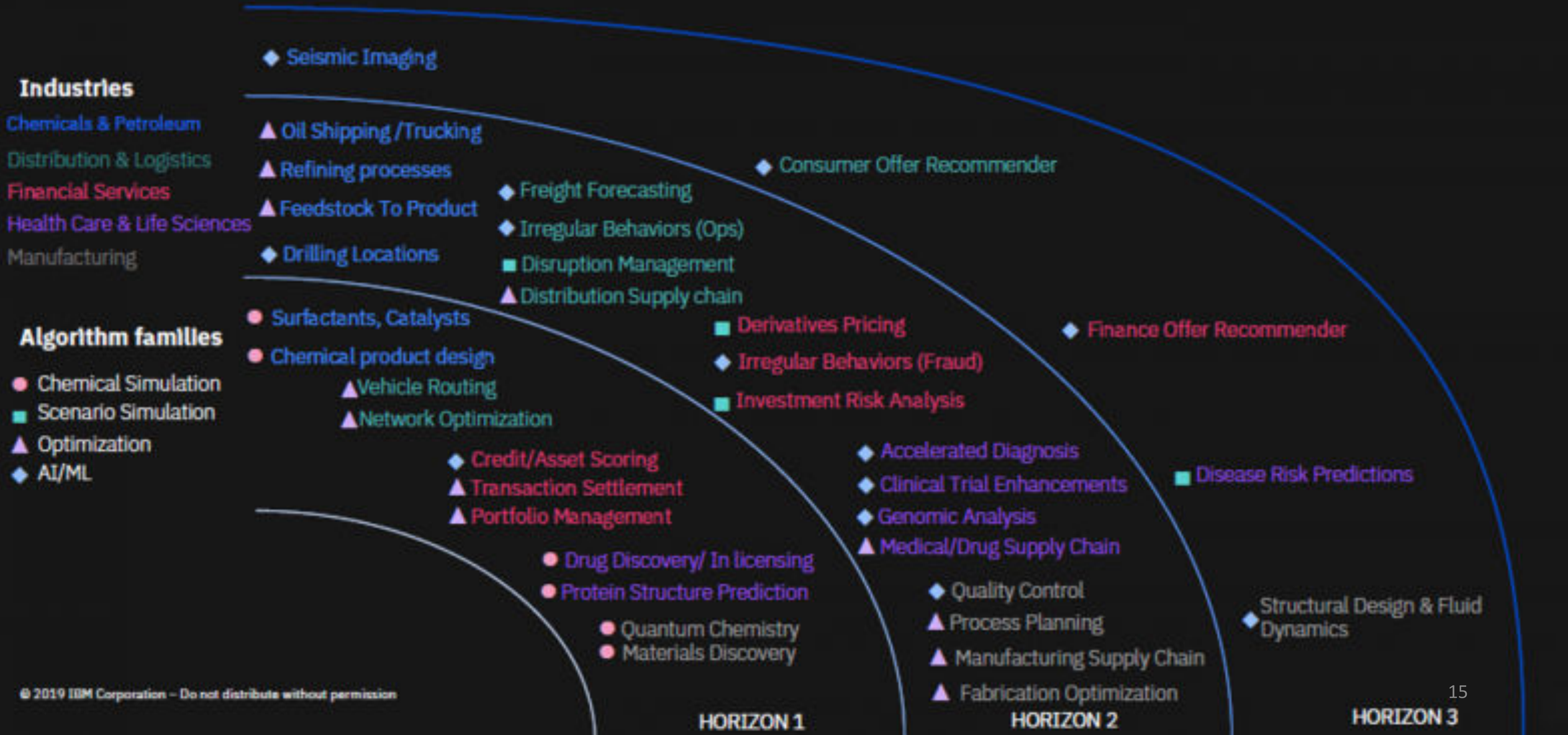
ADVANCING MACHINE LEARNING

SPEEDING UP AIRCRAFT DESIGN

MMS 20192351. August 2019.

AIRBUS

Maturity horizons are based on tangible value of Quantum Volume and potential advantage applied to a business use case



© 2019 IBM Corporation – Do not distribute without permission

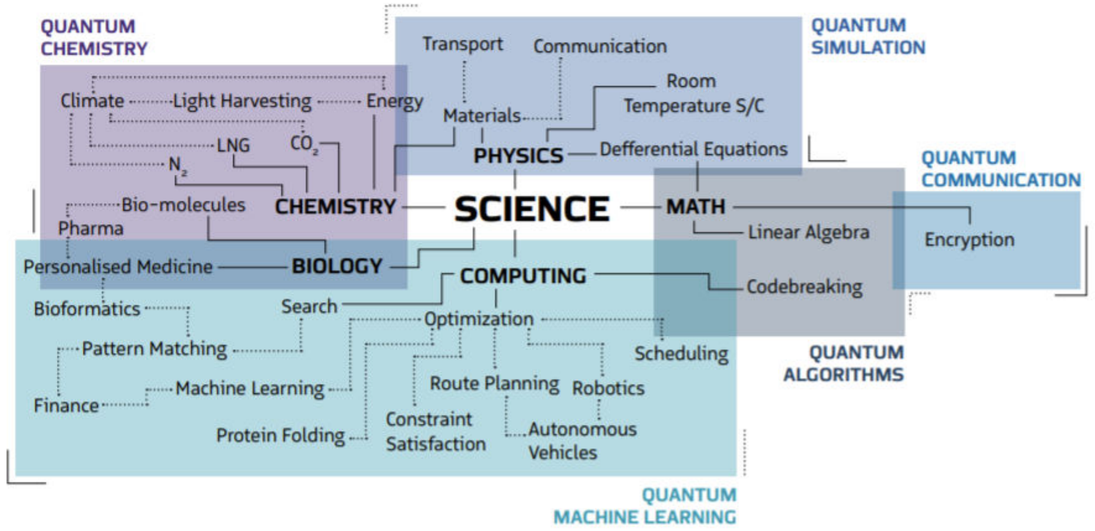
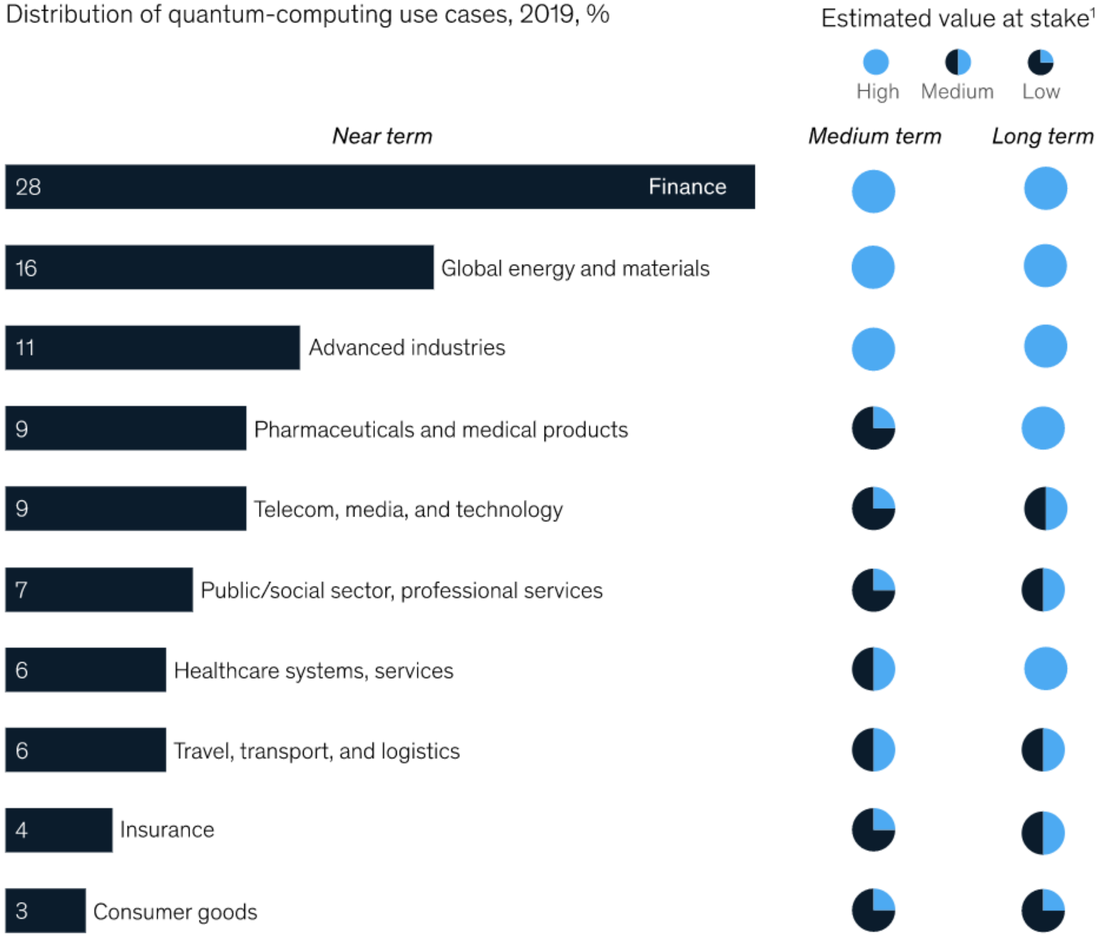


Figure 2

Potential applications for quantum computing (Source: Quantum Computing Market & Technologies – 2018-2024, Industry 4.0 Market Research,a division of HSRC, February 2018)

Who could create value with quantum computing?

Distribution of quantum-computing use cases, 2019, %

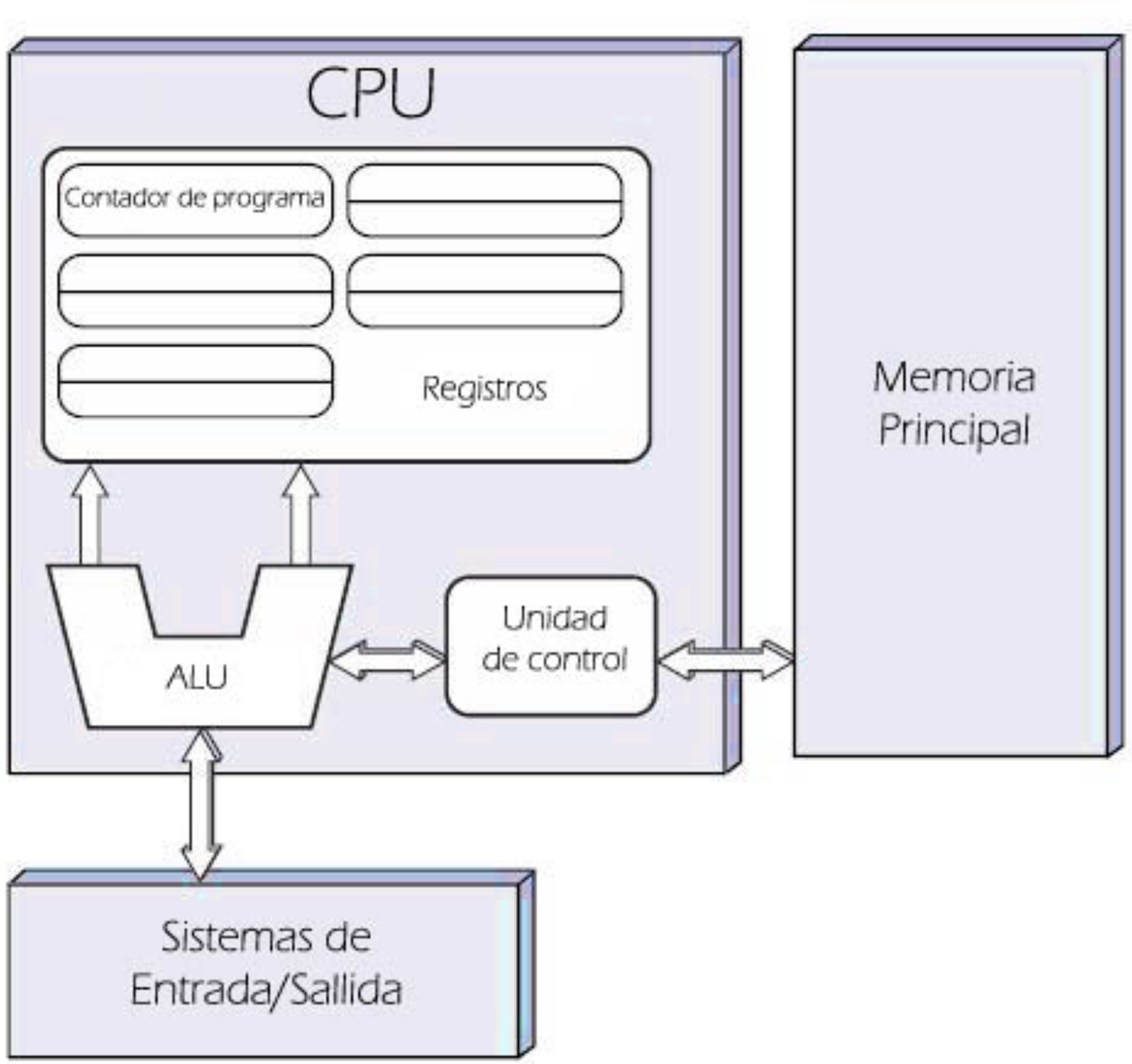


[1]Approximate timing for medium term is by the year 2025; for long term, by the year 2035. Experts consider these values at stake to be a snapshot in time. Fully developed quantum computing will lead to additional value within and shifts between industry verticals.
Source: Expert interviews; McKinsey analysis

¿Cómo funcionan?
¿qué las hace especiales?

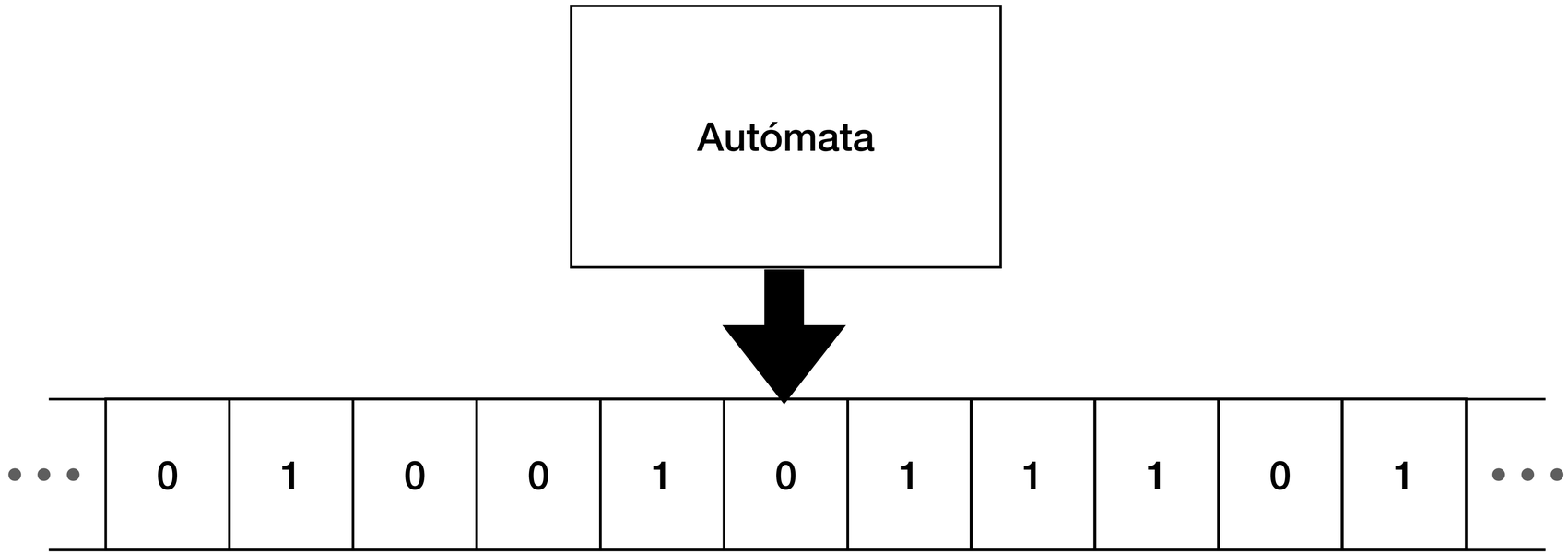
¿Qué es una computadora?

Arquitectura Von Neumann



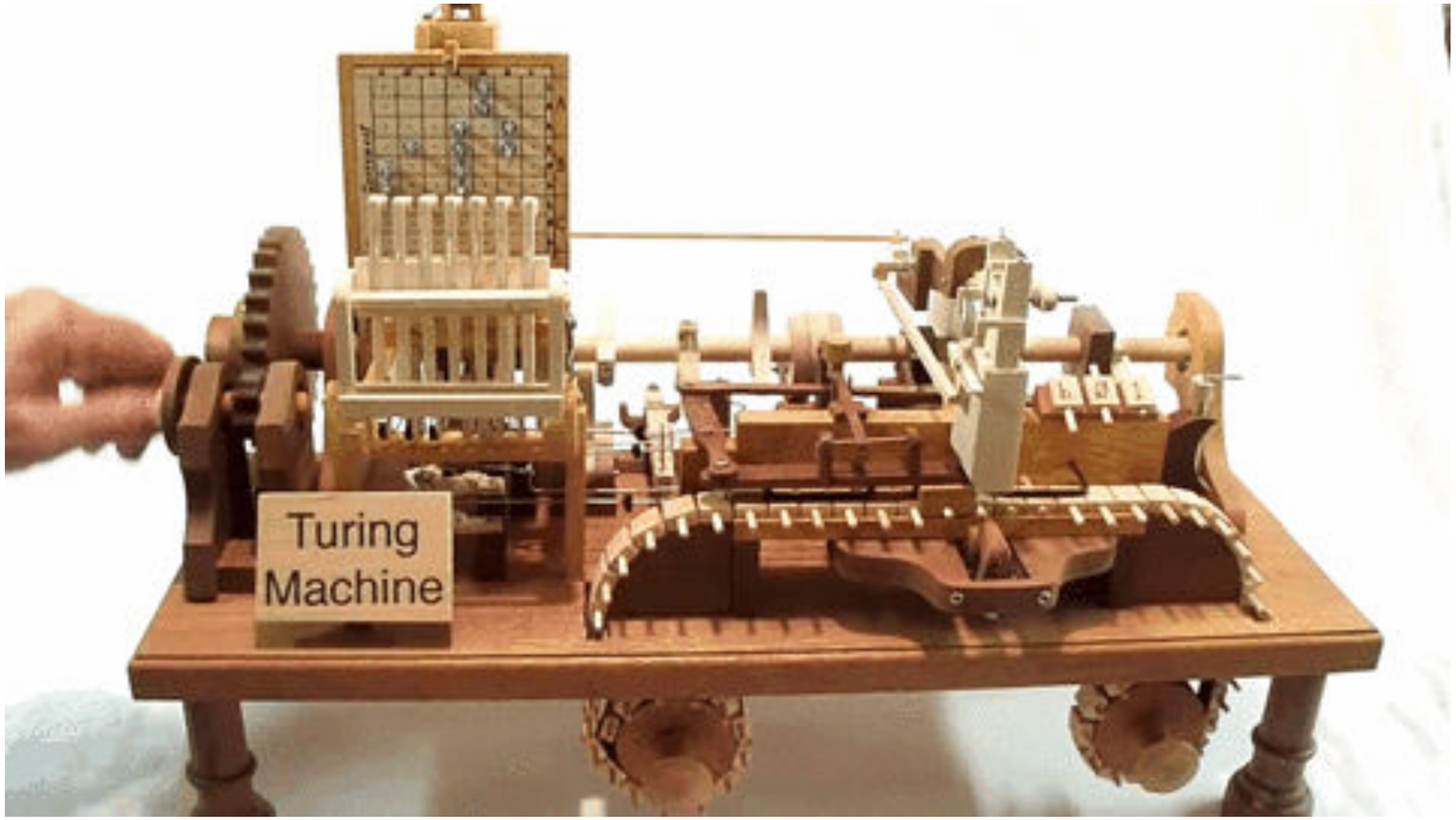
Máquina de Turing

Conceptos Básicos



Máquina de Turing

Conceptos Básicos



Máquina de Turing (máquina clásica)

Supuestos

- **Principio de Localidad:**
  - Los eventos suceden en una posición y no tienen repercusión a la distancia, se propagan a partir del punto en que suceden a puntos vecinos en unidades discretas de tiempo, o a una velocidad limitada.
- **Principio de Unicidad:**
  - Un sistema solo puede estar en un estado a la vez, no puede estar en la superposición de varios estados al mismo tiempo.
- **Principio de Objetividad:**
  - Un observador puede consultar el estado del sistema y conocerlo completamente sin interferir en el.

¿Se cumplen en Mecánica Cuántica?
Supuestos

- **Principio de Localidad:**
  - Los eventos suceden en una posición y no tienen repercusión a la distancia, se propagan a partir del punto en que suceden a puntos vecinos en unidades discretas de tiempo, o a una velocidad limitada.
- **Principio de Unicidad:**
  - Un sistema solo puede estar en un estado a la vez, no puede estar en la superposición de varios estados al mismo tiempo.
- **Principio de Objetividad:**
  - Un observador puede consultar el estado del sistema y conocerlo completamente sin interferir en el.

¿Se cumplen en Mecánica Cuántica?

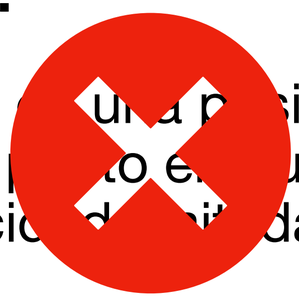
Supuestos

- **Principio de Localidad:**
  - Los eventos suceden en una posición y no tienen repercusión a la distancia, se propagan a partir del punto en que suceden a puntos vecinos en unidades discretas de tiempo, o a una velocidad limitada.
- **Principio de Unicidad:**
  - Un sistema solo puede estar en un estado a la vez, no puede estar en la superposición de varios estados al mismo tiempo.
- **Principio de Objetividad:**
  - Un observador puede consultar el estado del sistema y conocerlo completamente sin interferir en el.

¿Se cumplen en Mecánica Cuántica?

Supuestos

- **Principio de Localidad:**
  - Los eventos suceden [illegible], se propagan a partir del [illegible] discretas de tiempo, o a una velocidad [illegible].



Un estado cuántico es global, la acción en un punto pueden alterar el estado en otro lugar instantáneamente

- **Principio de Unicidad:**
  - Un sistema solo puede estar en un estado a la vez, no puede estar en la superposición de varios estados al mismo tiempo.
- **Principio de Objetividad:**
  - Un observador puede consultar el estado del sistema y conocerlo completamente sin interferir en el.

¿Se cumplen en Mecánica Cuántica?

Supuestos

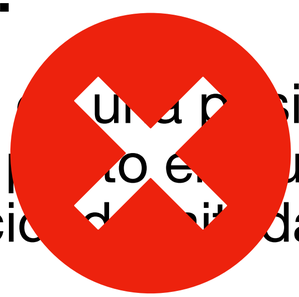
- **Principio de Localidad:**
  - Los eventos suceden [illegible] se propagan a partir del [illegible] discretas de tiempo, o a una velocidad [illegible].
- **Principio de Unicidad:**
  - Un sistema solo puede [illegible] un estado a la vez, no puede estar en la superposición de varios estados al mismo tiempo.
- **Principio de Objetividad:**
  - Un observador puede consultar el estado del sistema y conocerlo completamente sin interferir en el.

Un estado cuántico es global, la acción en un punto pueden alterar el estado en otro lugar instantáneamente

¿Se cumplen en Mecánica Cuántica?

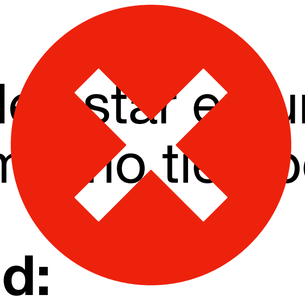
Supuestos

- **Principio de Localidad:**
  - Los eventos suceden [illegible] se propagan a partir del [illegible] discretas de tiempo, o a una veloci[illegible]da.



Un estado cuántico es global, la acción en un punto pueden alterar el estado en otro lugar instantáneamente

- **Principio de Unicidad:**
  - Un sistema solo pued[illegible] de varios estados al m[illegible]



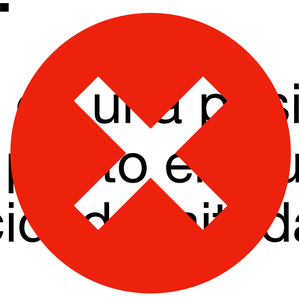
Un estado cuántico puede estar en la superposición de varios estados globales

- **Principio de Objetividad:**
  - Un observador puede consultar el estado del sistema y conocerlo completamente sin interferir en el.

¿Se cumplen en Mecánica Cuántica?

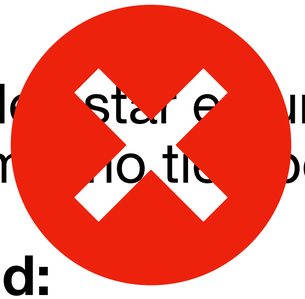
Supuestos

- **Principio de Localidad:**
  - Los eventos suceden [illegible] se propagan a partir del [illegible] discretas de tiempo, o a una veloci[illegible]da.



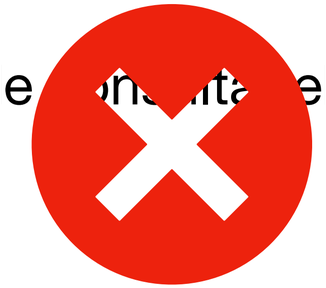
Un estado cuántico es global, la acción en un punto pueden alterar el estado en otro lugar instantáneamente

- **Principio de Unicidad:**
  - Un sistema solo pued[illegible] de varios estados al m[illegible]



Un estado cuántico puede estar en la superposición de varios estados globales

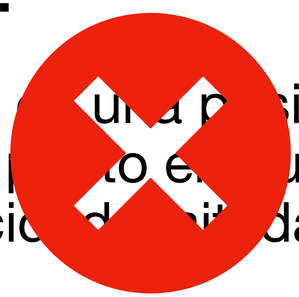
- **Principio de Objetividad:**
  - Un observador puede [illegible] el estado del sistema y conocerlo completamente sin interferir en el.



¿Se cumplen en Mecánica Cuántica?

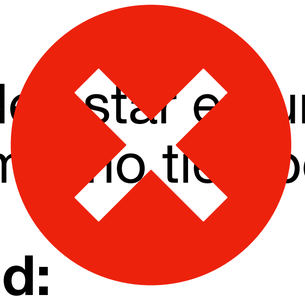
Supuestos

- **Principio de Localidad:**
  - Los eventos suceden [illegible] se propagan a partir del [illegible] discretas de tiempo, o a una velocid[illegible]da.



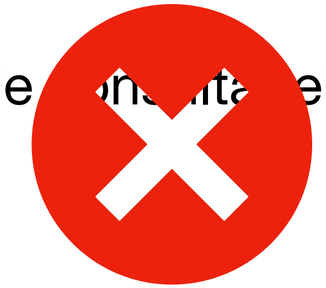
Un estado cuántico es global, la acción en un punto pueden alterar el estado en otro lugar instantáneamente

- **Principio de Unicidad:**
  - Un sistema solo puede [illegible] de varios estados al m[illegible]



Un estado cuántico puede estar en la superposición de varios estados globales

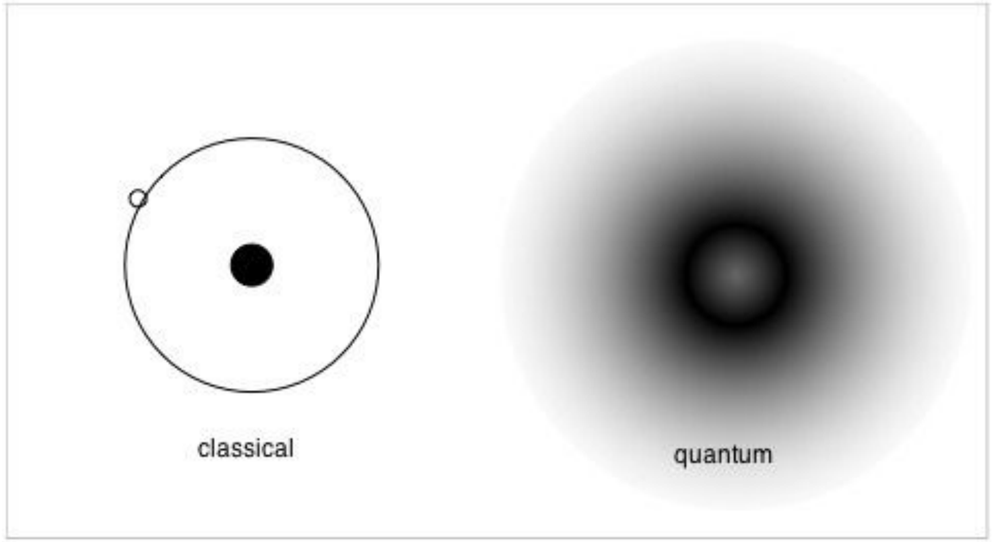
- **Principio de Objetividad:**
  - Un observador puede [illegible] interferir en el.

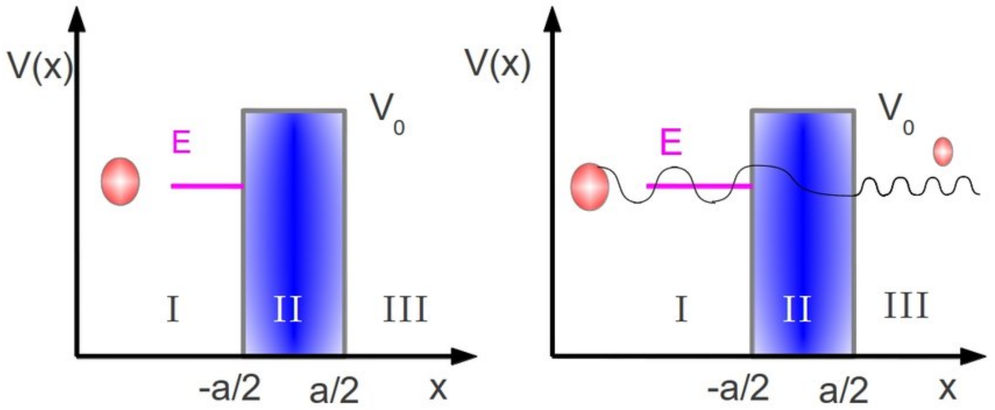


No es posible observar el estado sin alterarlo, Las reglas del sistema mientras no se observa son distintas a cuando interactuamos con el

Física clásica vs física cuántica

- Identidad definida (onda vs partícula)
- Mismas causas, mismos efectos (determinismo)
- Magnitud de efectos de proporcional a distancia (localidad)
- Medir el sistema no altera su estado (determinismo)
- El estado no se degrada al interactuar con su ambiente (coherencia)





- Identidad dual (onda y partícula)
- Una causa, múltiples posibles efectos (probabilidad)
- Causas lejanas pueden tener efectos fuertes (no-localidad)
- Medir el sistema sí altera su estado (no-determinismo)
- El estado se degrada en el tiempo al interactuar con su ambiente (decoherencia)

¿Cómo interpretamos la Mecánica Cuántica?

Filosofía

¿Cómo interpretamos la Mecánica Cuántica?

Filosofía

$$i\hbar\frac{\partial|\Psi\rangle}{\partial t} = H|\Psi\rangle$$

Ecuación determinística

Describe ondas

Pero vemos partículas

No se pusieron de acuerdo

¿Cómo interpretamos la Mecánica Cuántica?

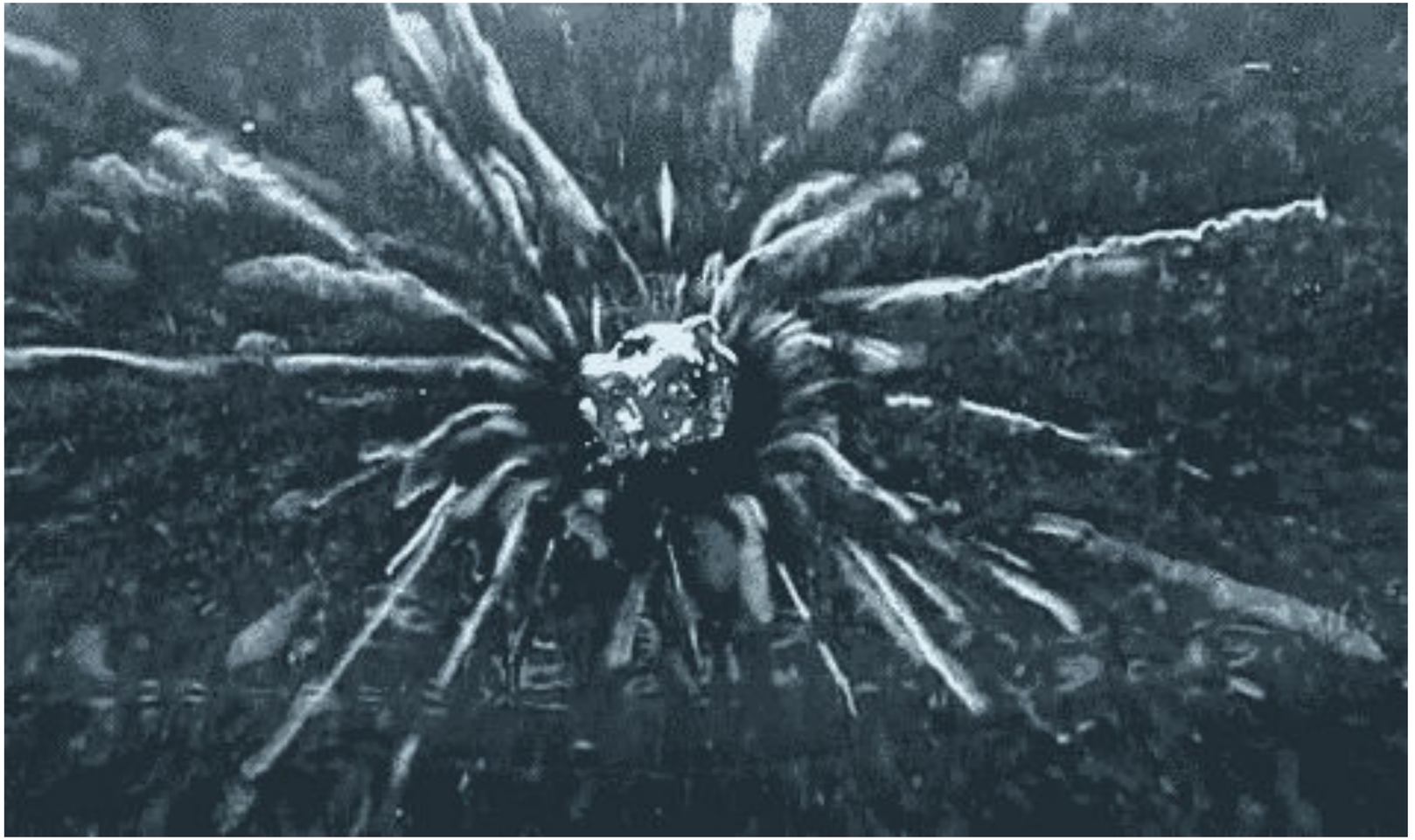
Filosofía

$$i\hbar\frac{\partial|\Psi\rangle}{\partial t} = H|\Psi\rangle$$

Ecuación determinística

Describe ondas

Pero vemos partículas



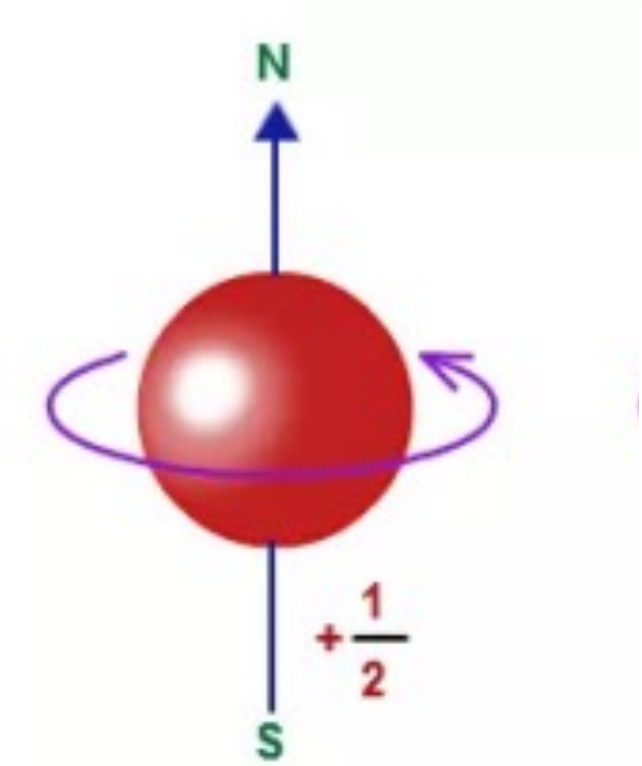
Qbit

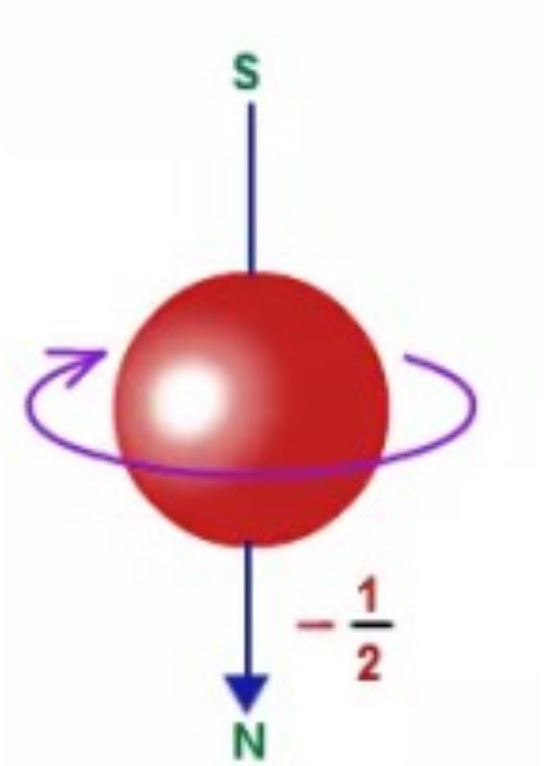
Bases

- Polarización de la luz
  - Vertical - Horizontal
- Orbita de un electrón dentro de un átomo
  - Orbita externa - Interna
- Spin de una partícula
  - Up - Down

Qbit

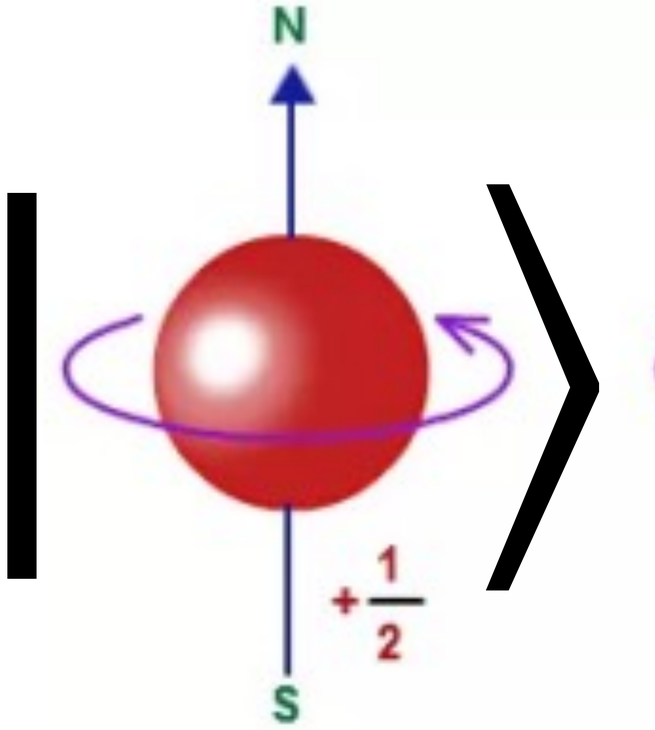
Spin

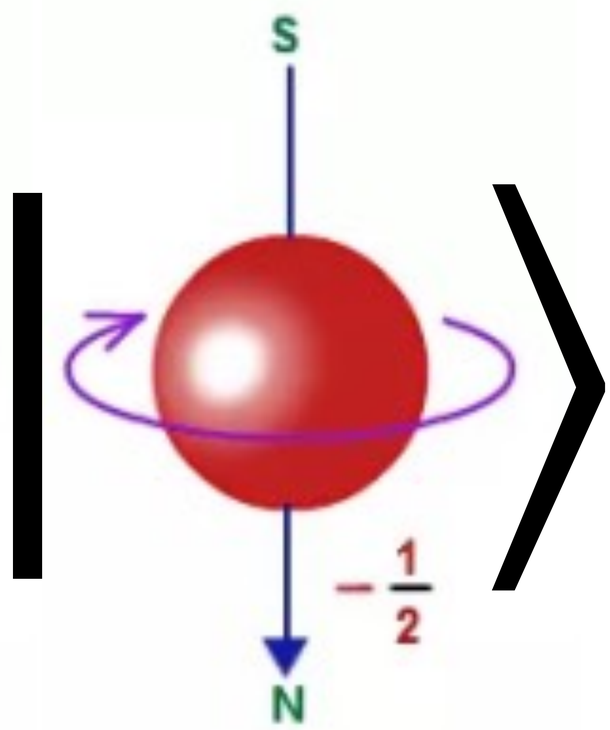




Qbit

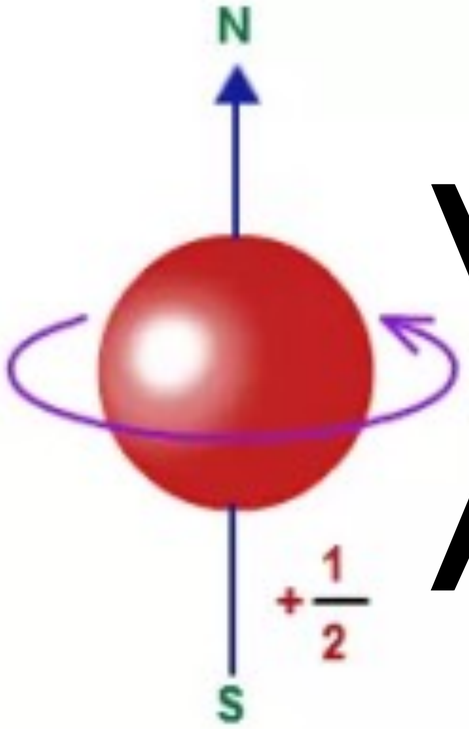
Notación de Dirac

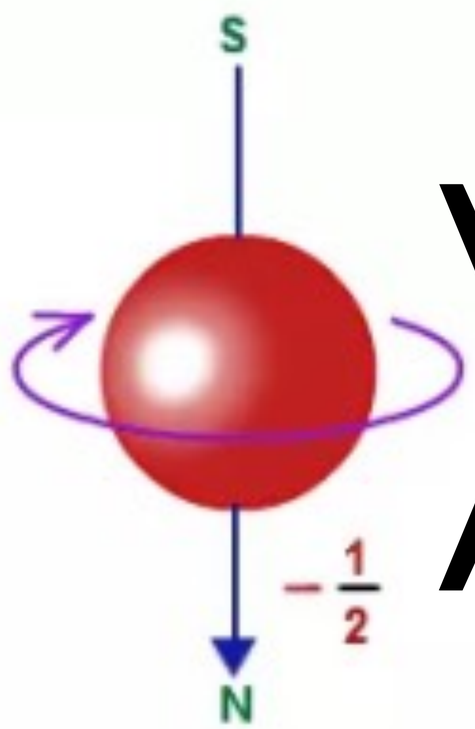




Qbit

superposición

$$\alpha|$$ 

$$\rangle + \beta|$$ 

$$\rangle$$

$$\alpha, \beta \in \mathbb{C}, \qquad \alpha^2 + \beta^2 = 1$$

Qbit

etiquetas 0 y 1

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

Qbit

etiquetas + y -

$$\alpha|+\rangle+\beta|-\rangle$$

Qbit

ortogonalidad

$$\alpha|+\rangle+\beta|-\rangle$$

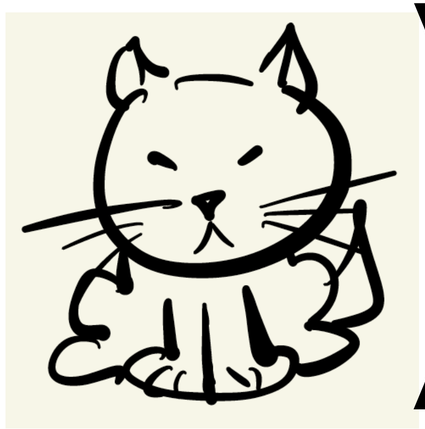
$$|+\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

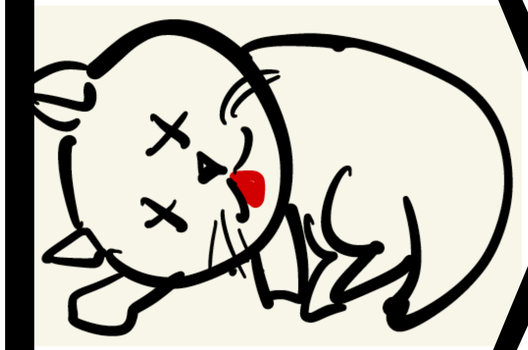
$$|-\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Qbit

superposición de estados complejos

$$\alpha|\ \rangle + \beta|\ \rangle$$





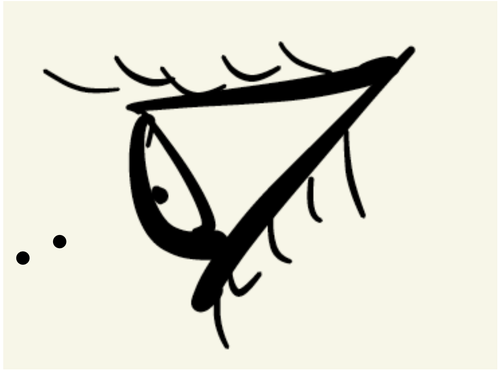
Qbit

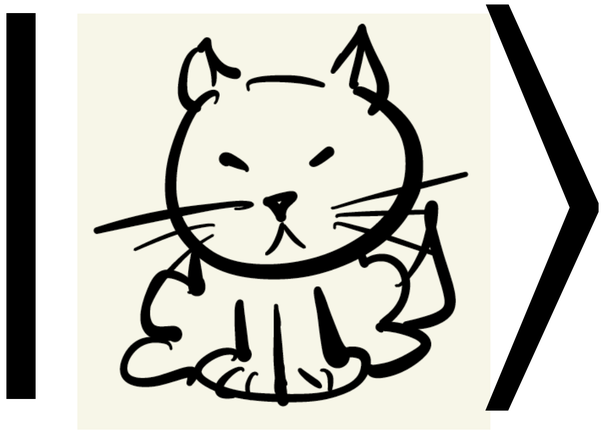
observación

$$\alpha|\ \rangle + \beta|\ \rangle$$

Qbit

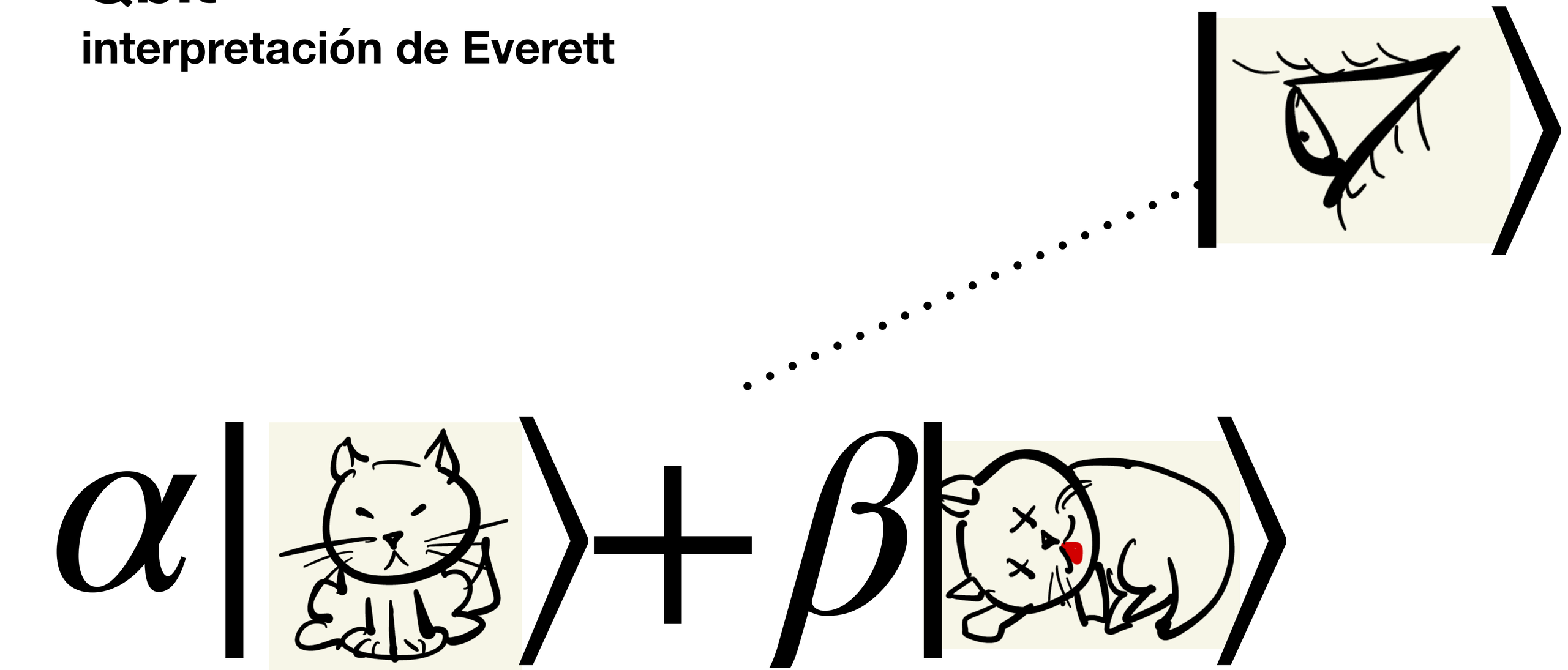
colapso





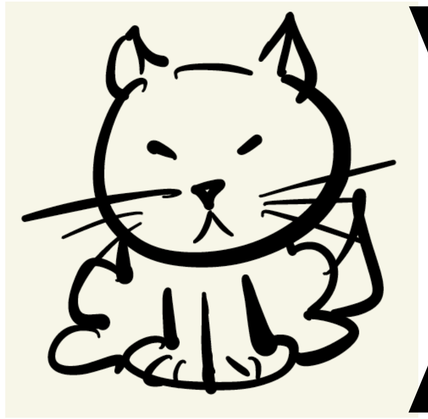
Qbit

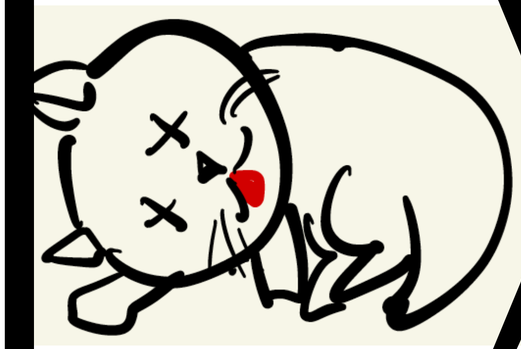
interpretación de Everett



Qbit

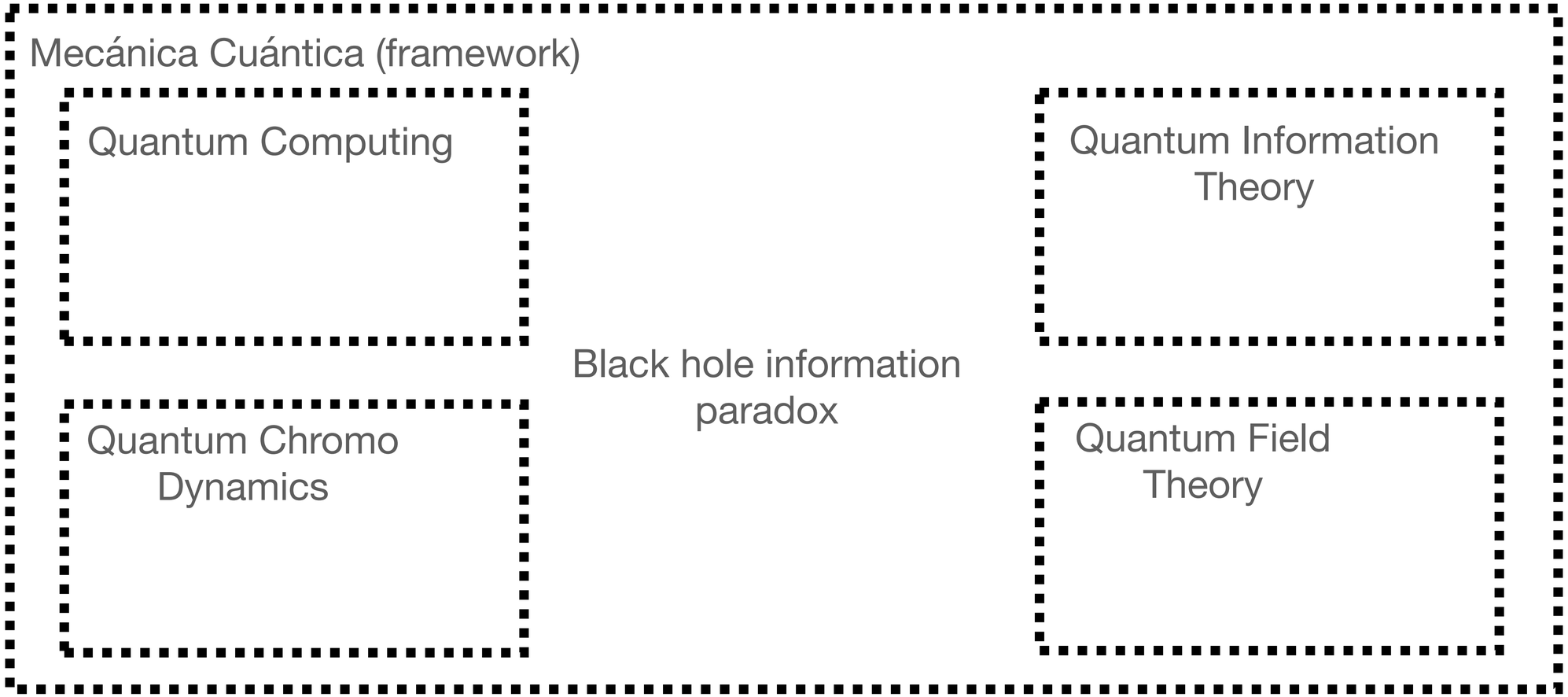
interpretación de Everett

$$\alpha \left| \text{  } \right\rangle \otimes \left| \text{  } \right\rangle$$

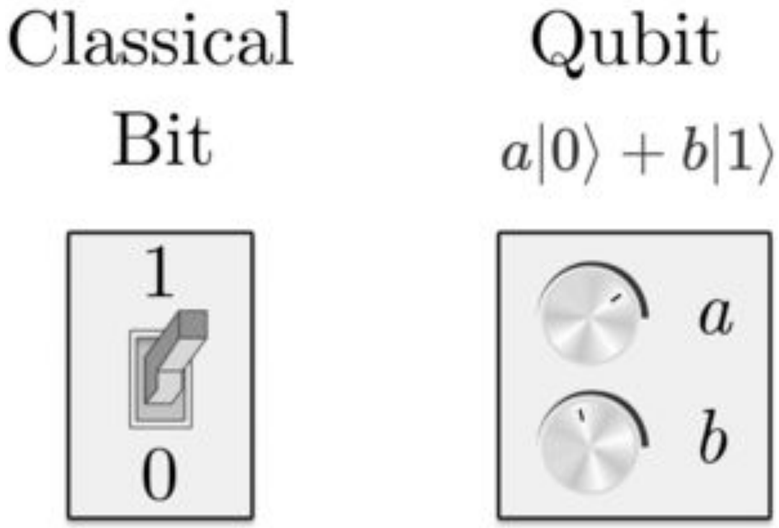
$$+ \beta \left| \text{  } \right\rangle \otimes \left| \text{  } \right\rangle$$

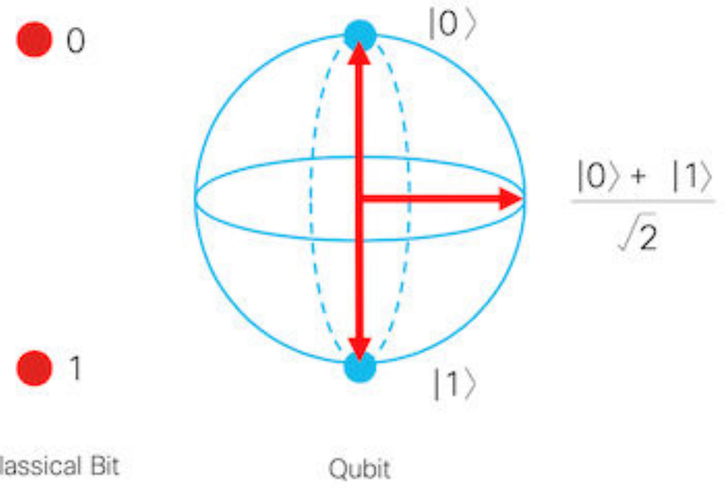
Panorama (¿qué tan complicado es?)

Bases

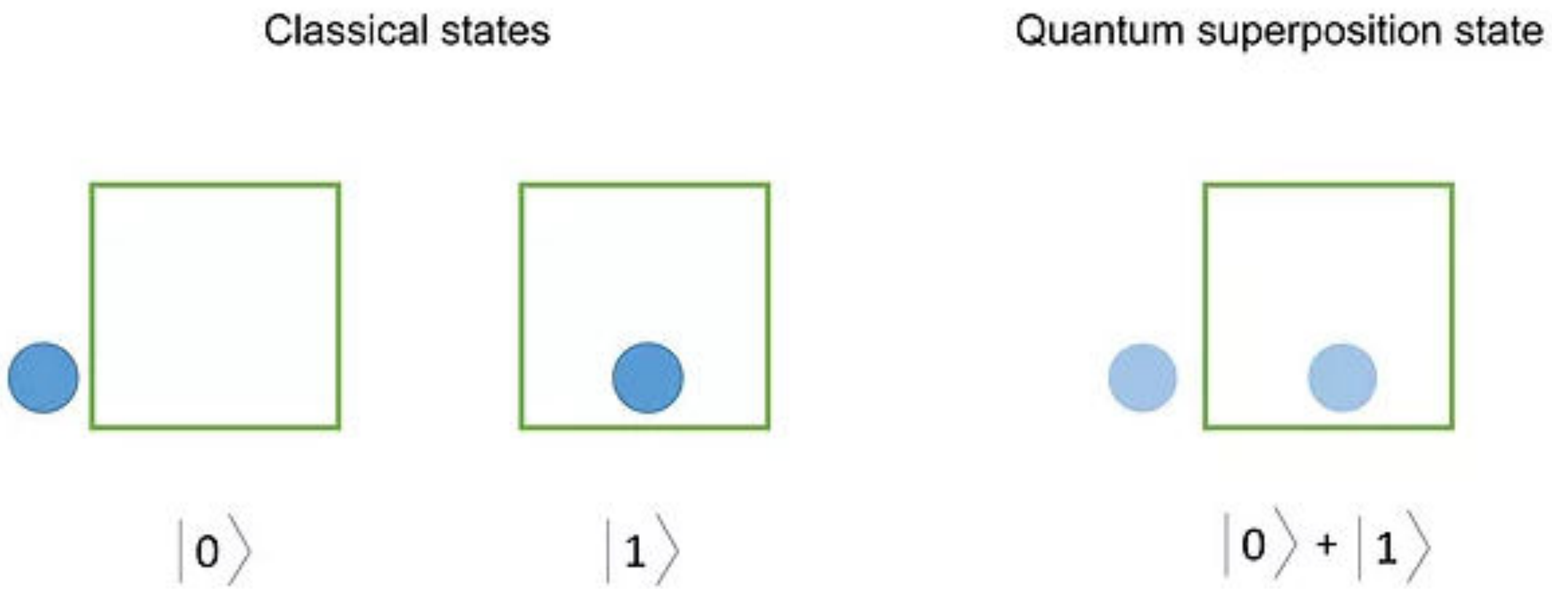


Estados clásicos vs estados cuánticos

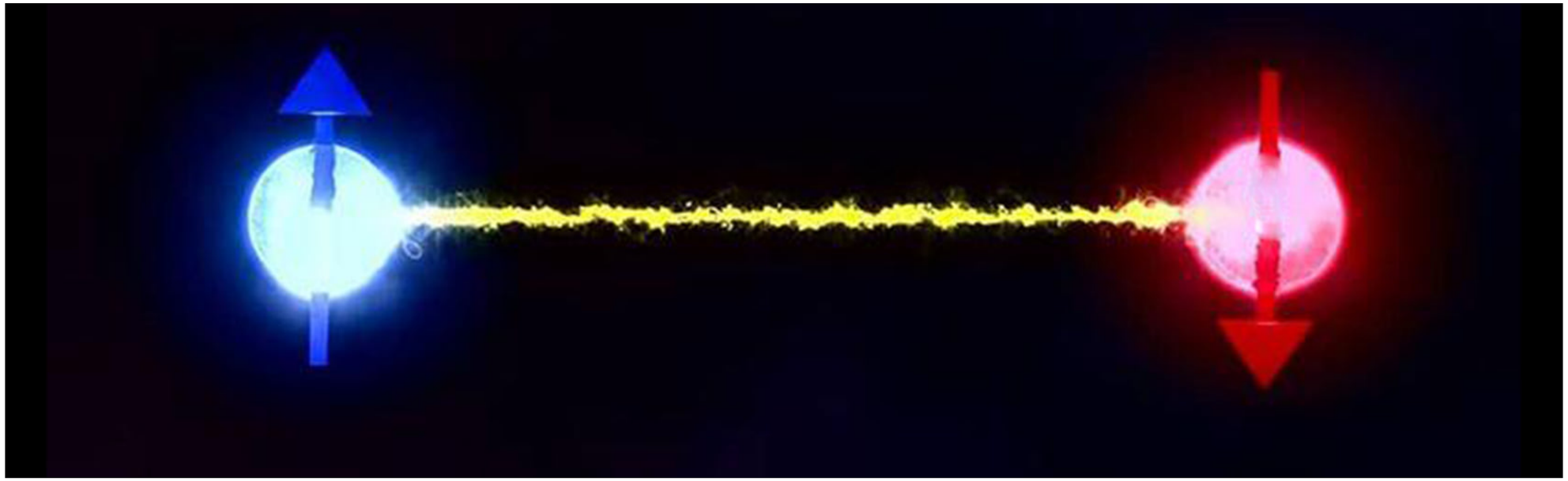




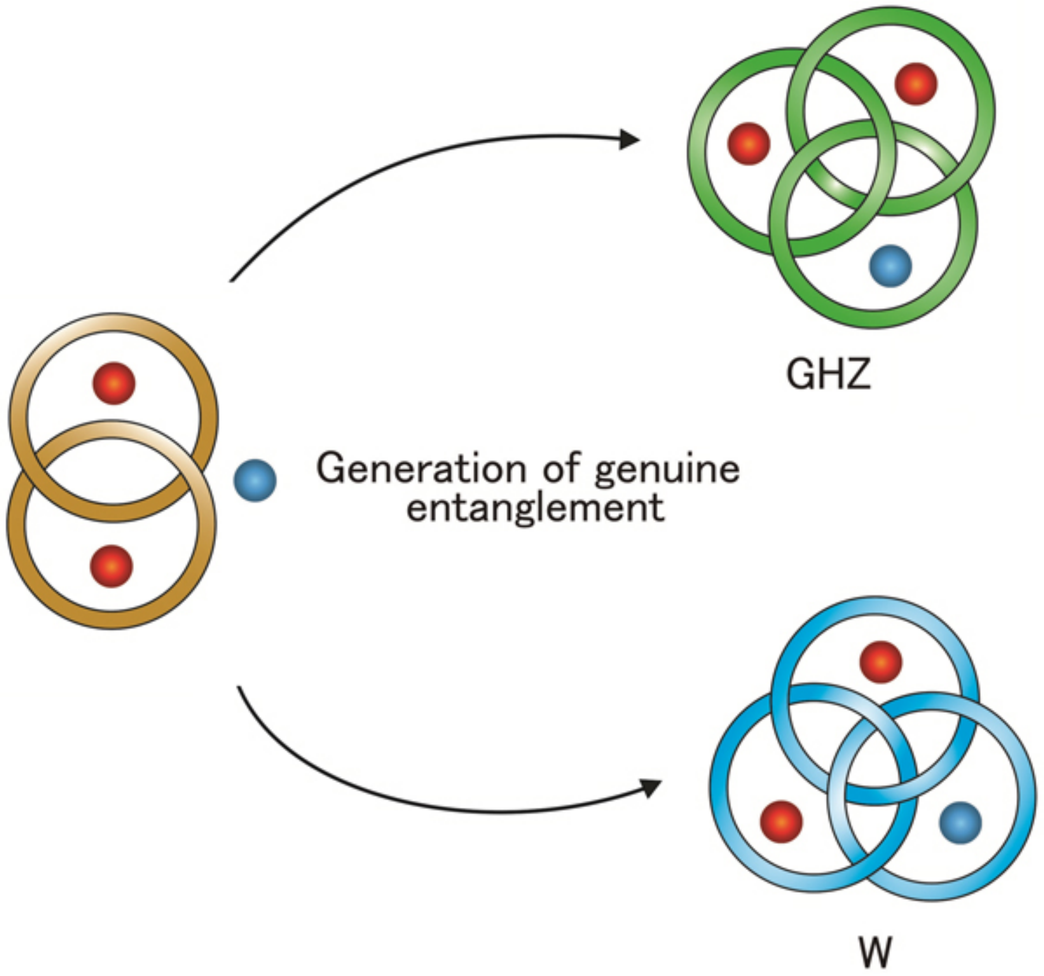
Superposición cuántica



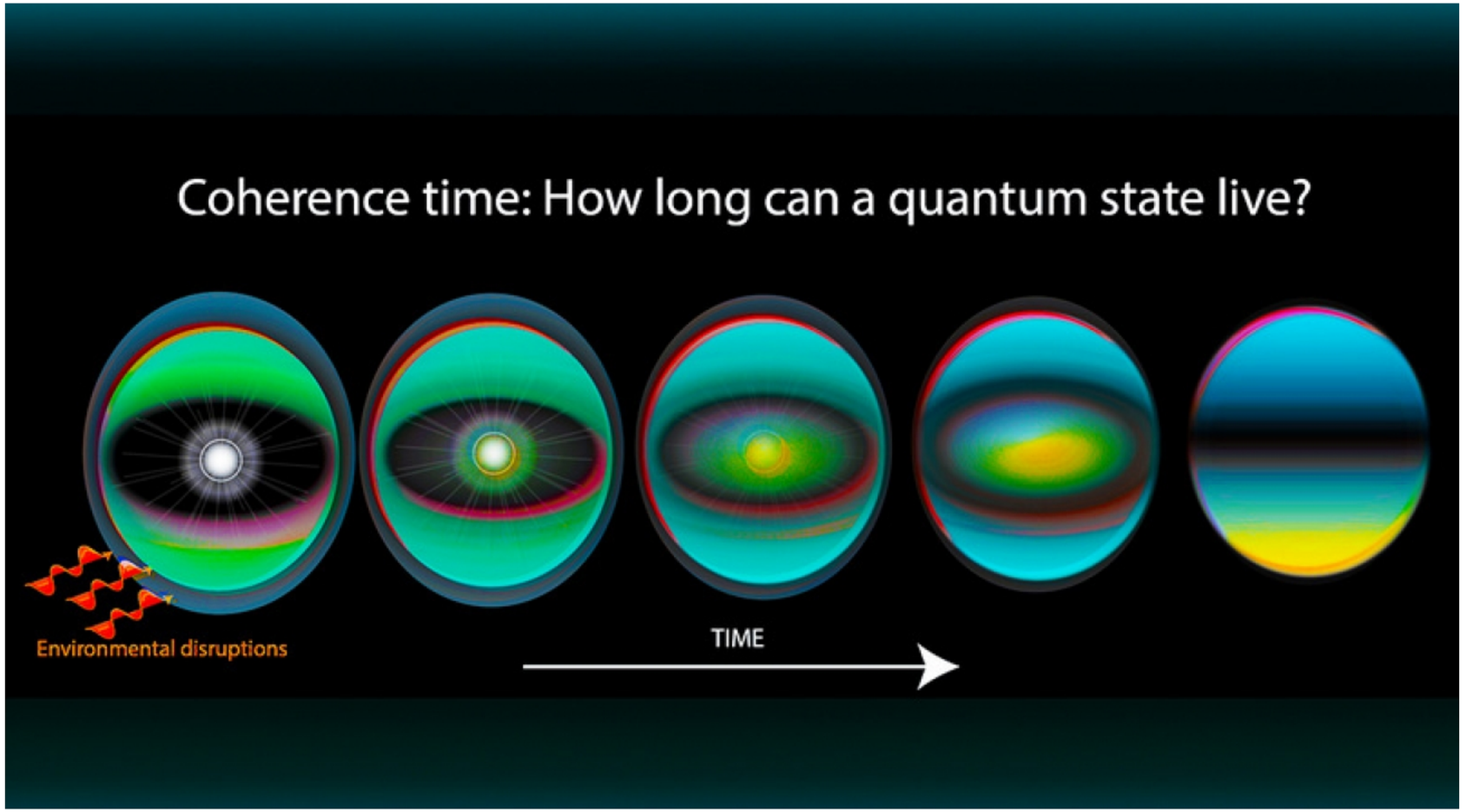
El efecto Einstein-Podolski-Rosen



Enmarañamiento (Entanglement)



Decoherencia



https://www.nist.gov/topics/physics/introduction-new-quantum-revolution/strange-world-quantum-physics

Matemáticamente hablando

Computación

- Máquinas de Turing y Von Newmann
  - Algebra de Bool (no electrónica!)

    $(p + \neg q) \cdot r \equiv t$

    $p, q, r, t \in \{0,1\}$

    $+ = \wedge$ (and)

    $\cdot = \vee$ (or)

    $\neg =$ not

- Computación Cuántica
  - Algebra Lineal con variable compleja (no física cuántica!)

    $$\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \ \alpha, \beta \in \mathbb{C}$$

    $$\alpha = a + ib, \ a, b \in \mathbb{R}, \ i = \sqrt{-1}$$

  - No puede haber disipación de energía, compuertas son reversibles

Matemáticamente hablando

Computación cuántica

- Estados = vectores (de números complejos)
- 1 Qubit (vector de 2 elementos)
- 2 Qubits (vector de 4 elementos)
- 3 Qubits (vector de 8 elementos

  ⋮

- n Qubits (vector de 2^n elementos)

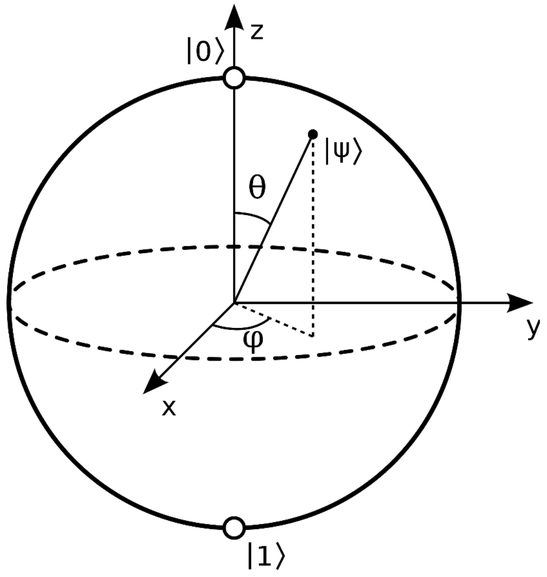
- Operaciones = matrices (de números complejos)
- 1 Qubit (mat. de 2x2 elementos)
- 2 Qubits (mat. de 4x4 elementos)
- 3 Qubits (mat. de 8x8 elementos)

  ⋮

- n Qubits (mat de $2^n \times 2^n$ ele.)

Matrices de Pauli

Operadores en 1 QuBit



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

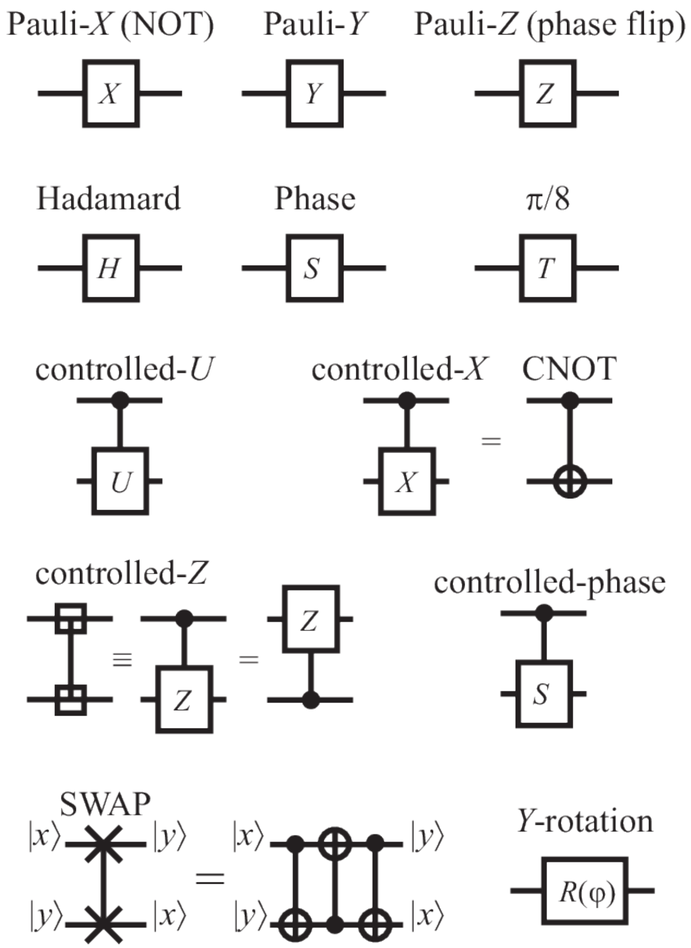
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

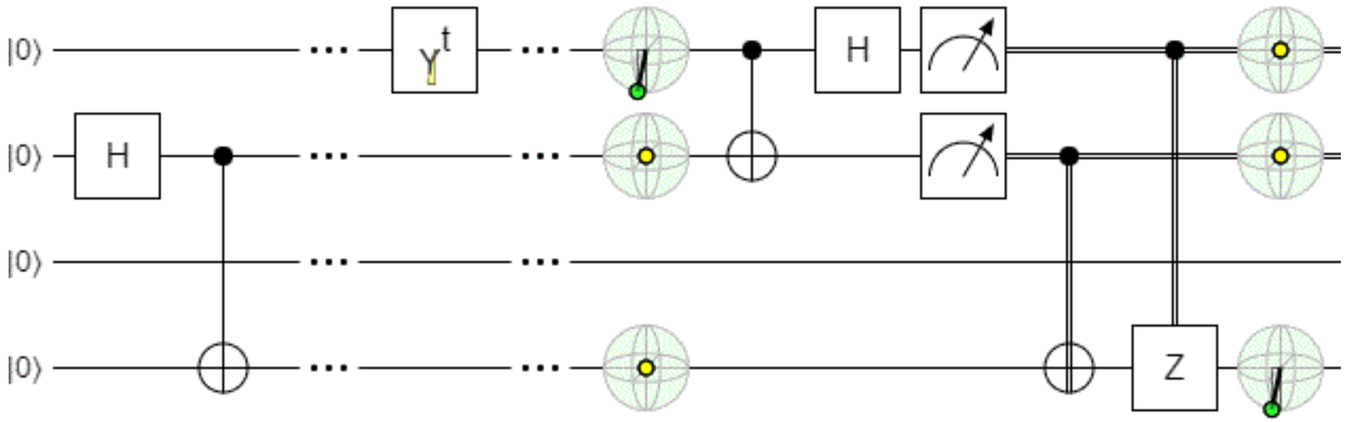
$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

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

$$\hat{\sigma}_z|+\rangle = |+\rangle$$
$$\hat{\sigma}_z|-\rangle = -|-\rangle$$
$$\hat{\sigma}_x|+\rangle = |-\rangle$$
$$\hat{\sigma}_x|-\rangle = |+\rangle$$
$$\hat{\sigma}_y|+\rangle = i|-\rangle$$
$$\hat{\sigma}_y|-\rangle = -i|+\rangle$$

Compuertas cuánticas





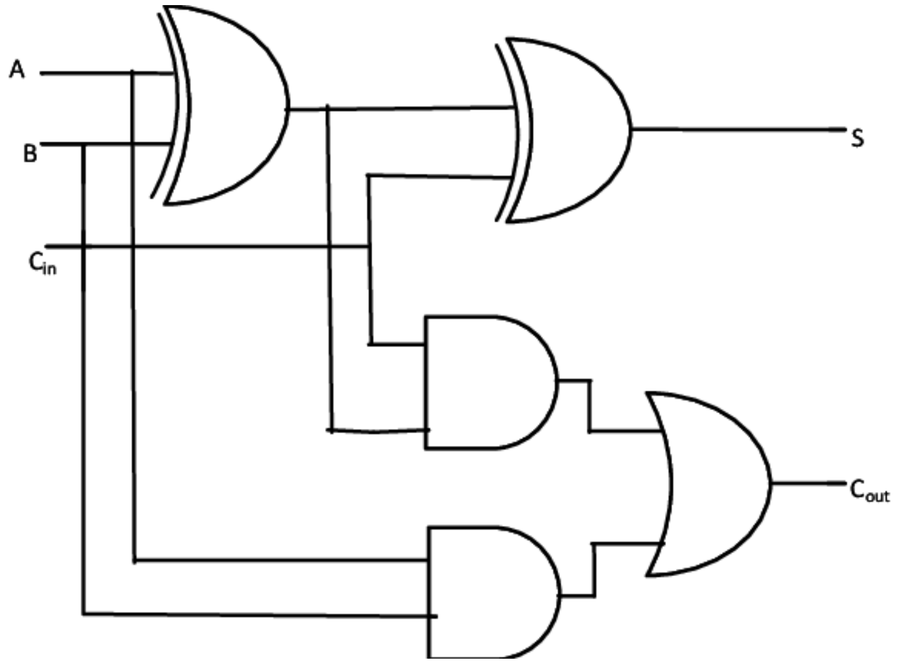
Compuertas Cuánticas

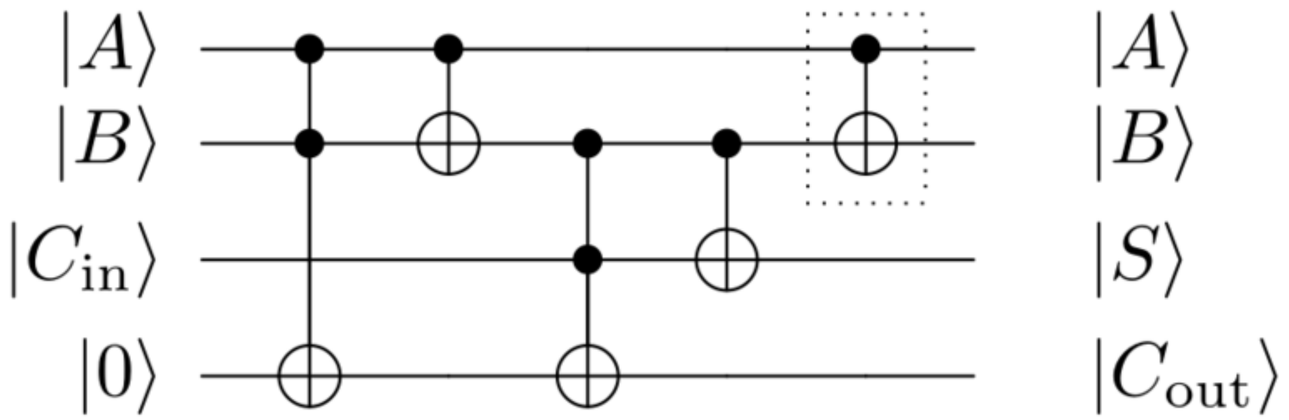
Compuertas Cuánticas

Consideraciones

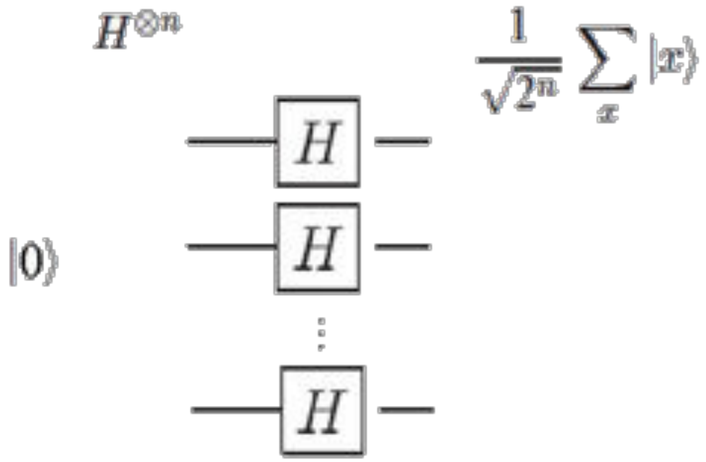
- La mayoría de los algoritmos cuánticos y paquetes de desarrollo se especifican a nivel de las compuertas
- Esto es cercano a un “ensamblador”, no es idóneo, la comunidad reconoce la necesidad de desarrollar herramientas para poder especificar/compilar a más alto nivel

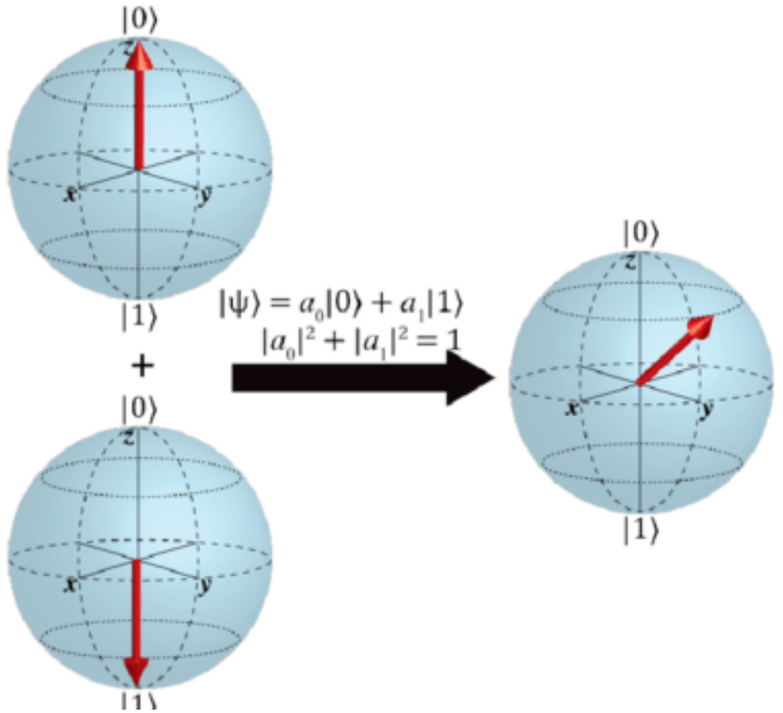
Sumador clásico vs sumador cuántico





El poder de la superposición

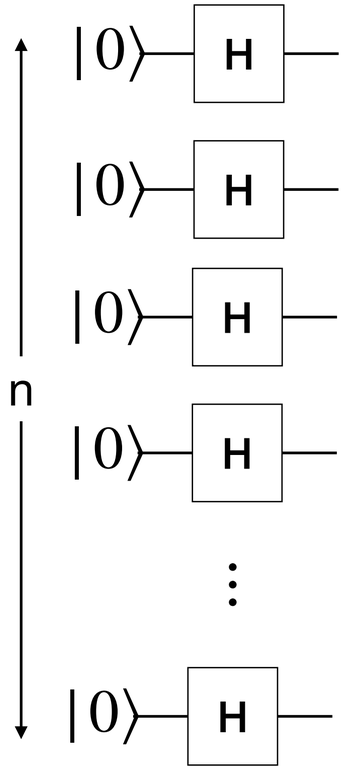




- La superposición nos permite explorar múltiples posibles soluciones de forma simultánea
- Cuando los problemas tienen estructura interna que permite hacer una “consulta global”, se obtiene eficiencia exponencial.

Paralelismo Cuántico

Memoria de n qbits

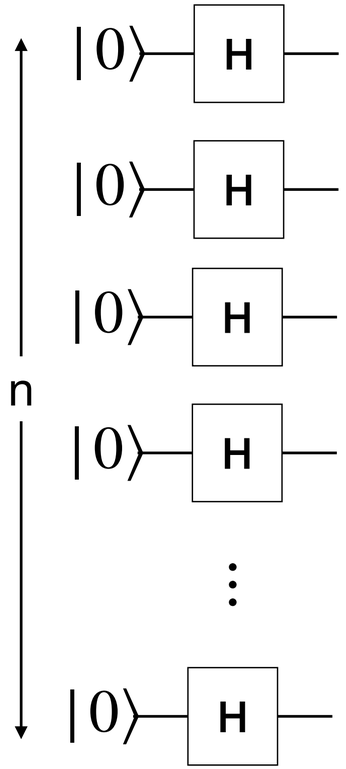


$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

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

Paralelismo Cuántico

Memoria de n qbits



$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

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

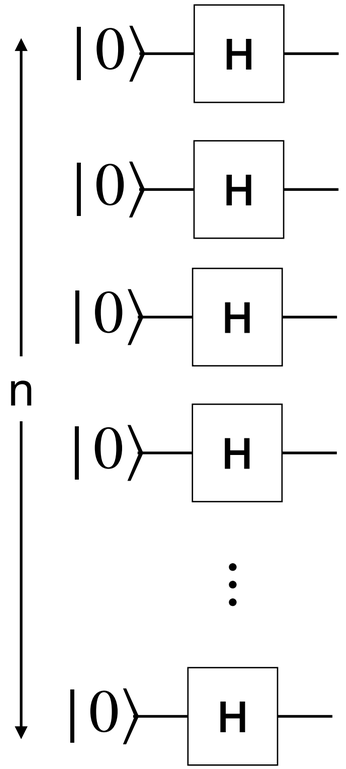
Por linealidad, si le aplicamos M a esto …

$$= M\left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \right)$$

$$= \quad M \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

Paralelismo Cuántico

Memoria de n qbits



$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

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

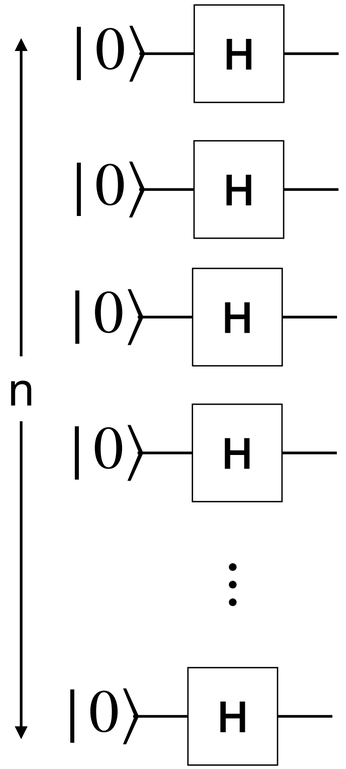
Por linealidad, si le aplicamos M a esto …

$$= M\left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} M|i\rangle$$

Paralelismo Cuántico

Memoria de n qbits



$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

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

Por linealidad, si le aplicamos M a esto …

$$= M\left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} M|i\rangle$$

aplica M a todas las distintas configuraciones de memoria al mismo tiempo

Paralelismo Cuántico

Memoria de n qbits

GENIAL! leamos el resultado

$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} M\,|\,i\rangle$$

aplica M a todas las distintas configuraciones de memoria al mismo tiempo

Paralelismo Cuántico

Memoria de n qbits

GENIAL! leamos el resultado

$$= \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} M\,|\,i\rangle$$

aplica M a todas las distintas configuraciones de memoria al mismo tiempo

Paralelismo Cuántico

Memoria de n qbits

GENIAL! leamos el resultado

$M\,|\,i\rangle$

Desaparecen todos menos 1!

aplica M a todas las distintas configuraciones de memoria al mismo tiempo

Paralelismo Cuántico

caveats

- Solo ciertos algoritmos pueden aprovechar el paralelismo cuántico
  - Hay que conocer la matemática (algebra lineal) que hay detrás para saber cuales son
  - Tiene que existir algún tipo de interferencia o patrón entre las distintas soluciones para que el paralelismo funcione
  - Los algoritmos terminan siendo probabilísticos (probabilidad alta de obtener la solución correcta)

Ejemplo: la transformada rápida de Fourier

$$x[k] = \sum_{n=0}^{N-1} x[n] e^{\frac{-j2\pi kn}{N}}$$

$$x[k] = \sum_{r=0}^{\frac{N}{2}-1} x[2r] e^{\frac{-j2\pi k(2r)}{N}} \quad + \quad x[k] = \sum_{r=0}^{\frac{N}{2}-1} x[2r+1] e^{\frac{-j2\pi k(2r+1)}{N}}$$

$$x[k] = \sum_{r=0}^{\frac{N}{2}-1} x[2r] e^{\frac{-j2\pi k(2r)}{N}} \quad + \quad x[k] = e^{\frac{-j2\pi k}{N}} \sum_{r=0}^{\frac{N}{2}-1} x[2r+1] e^{\frac{-j2\pi k(2r)}{N}}$$

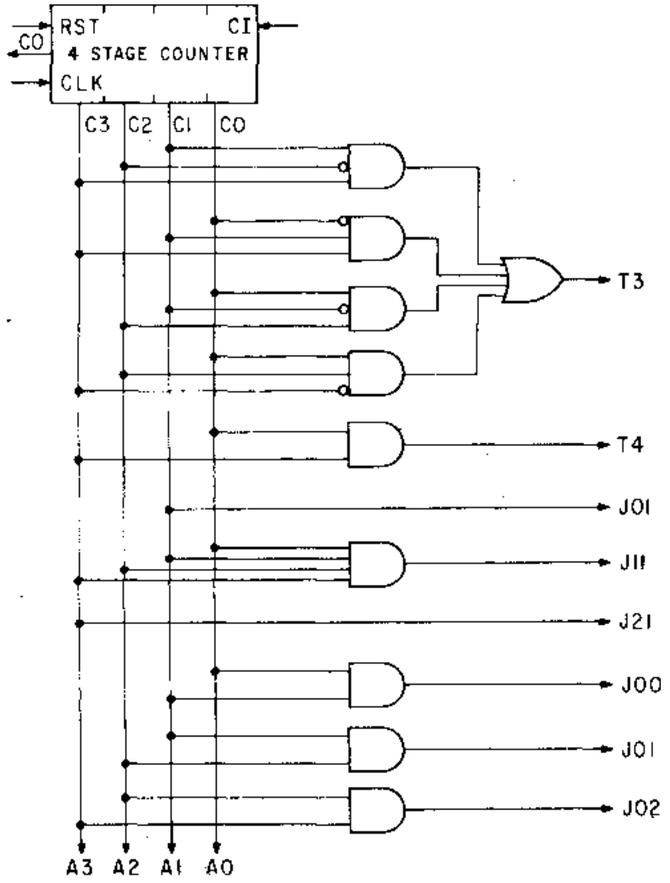
$$x[k] = \sum_{r=0}^{\frac{N}{2}-1} x[2r] e^{\frac{-j2\pi k(r)}{N/2}} \quad + \quad x[k] = e^{\frac{-j2\pi k}{N}} \sum_{r=0}^{\frac{N}{2}-1} x[2r+1] e^{\frac{-j2\pi k(r)}{N/2}}$$

$$x[k] = x_{even}[k] \; + \; e^{\frac{-j2\pi k}{N}} x_{odd}[k]$$

Ejemplo: la transformada rápida de Fourier

```
for (s = 0 ; s < log2N ; s++)
  for (i = 0 ; i < N/(2^(s+1)) ; i++)
          C = wr[idx];  S = wi[idx];
          for (j = i ; j < N ; j + = N/2^s)
               tmpr = aar[idx] - aar[idx+N/2^(s+1)];
               tmpi = aai[idx] - aai[idx+N/2^(s+1)];
               aar[idx] = aar[idx] + aar[idx+N/2^(s+1)];
               aai[idx] = aai[idx] + aai[idx+N/2^(s+1)];
               aar[idx+N/2^(s+1)] = tmpr*C - tmpi*S;
               aai[idx+N/2^(s+1)] = tmpr*S + tmpi*C;
          idx = idx + 2^s;
```

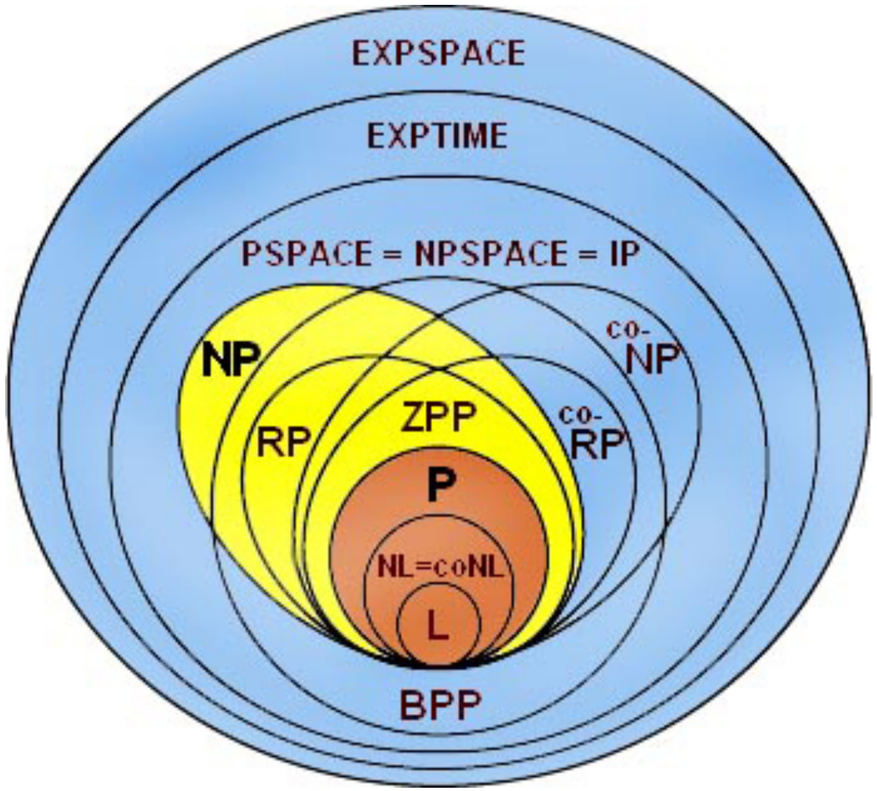
Ejemplo: la transformada rápida de Fourier

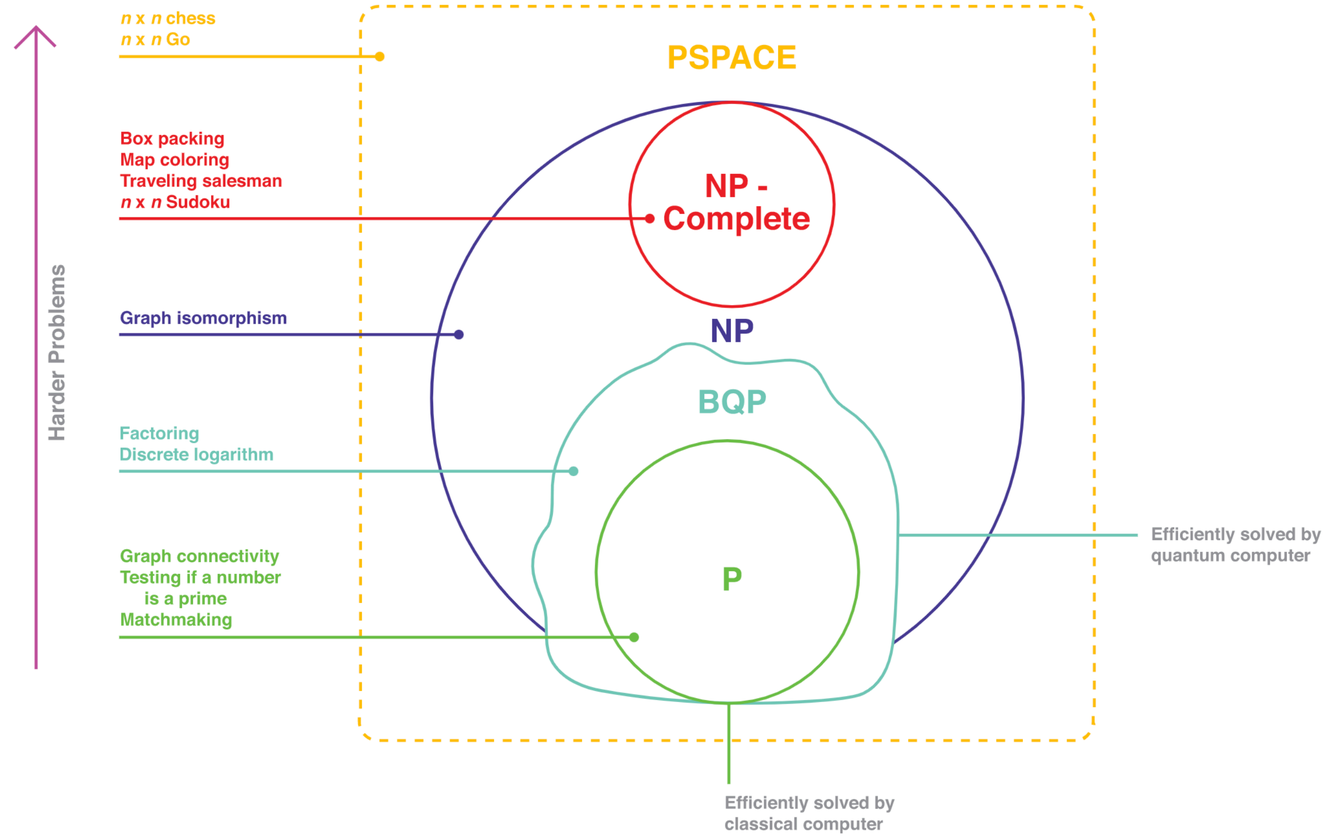


Algunos algoritmos cuánticos

Algoritmo	Utilidad	Impacto en actividades humanas
Factorización entera (Shor)	Descubrir factores primos en tiempo polinomial en vez de exponencial	Fuerza a repensar toda la infraestructura de llave pública-privada basada en RSA
Búsqueda no estructurada (Grover)	Encontrar elementos en conjuntos de datos grandes	Búsqueda en Big Data, estrategias automáticas en FinTech
Álgebra lineal cuántica	Resolver sistemas de ecuaciones lineales que representan múltiples tipos de pregunas	Logística, machine learning, ingeniería en general
QKD (quantum key distribution)	Compartir llaves criptográficas de manera 100% segura	Impacto fuerte y pronto en la seguridad informática y sistema bancario

Complejidad computacional clásica y cuántica



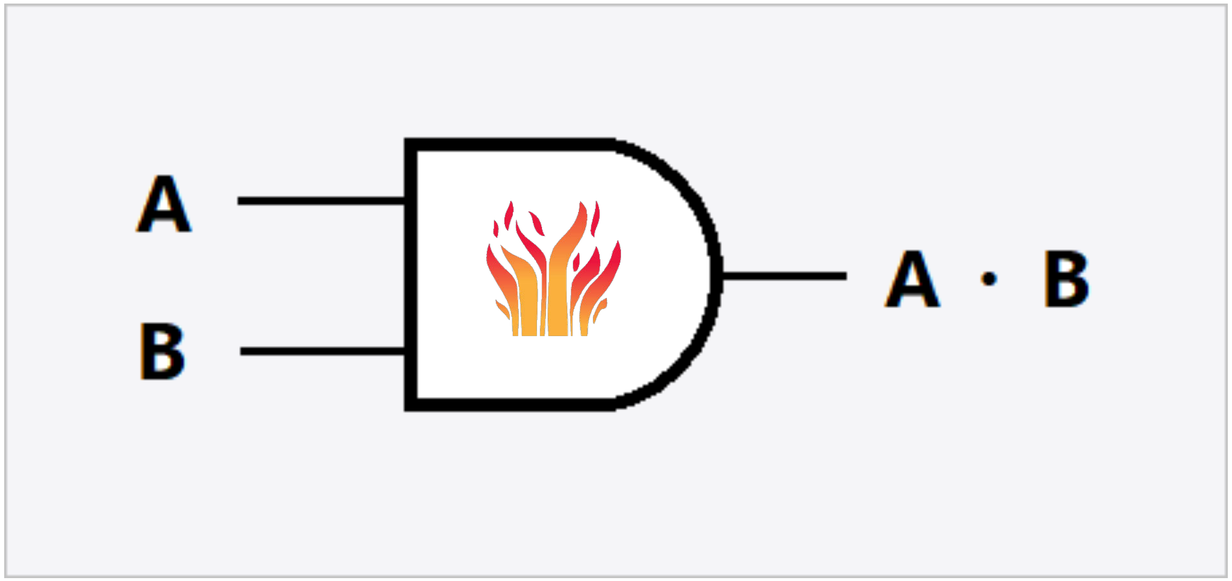


De vuelta a compuertas lógicas

A = 1

B = 0

A . B = 0

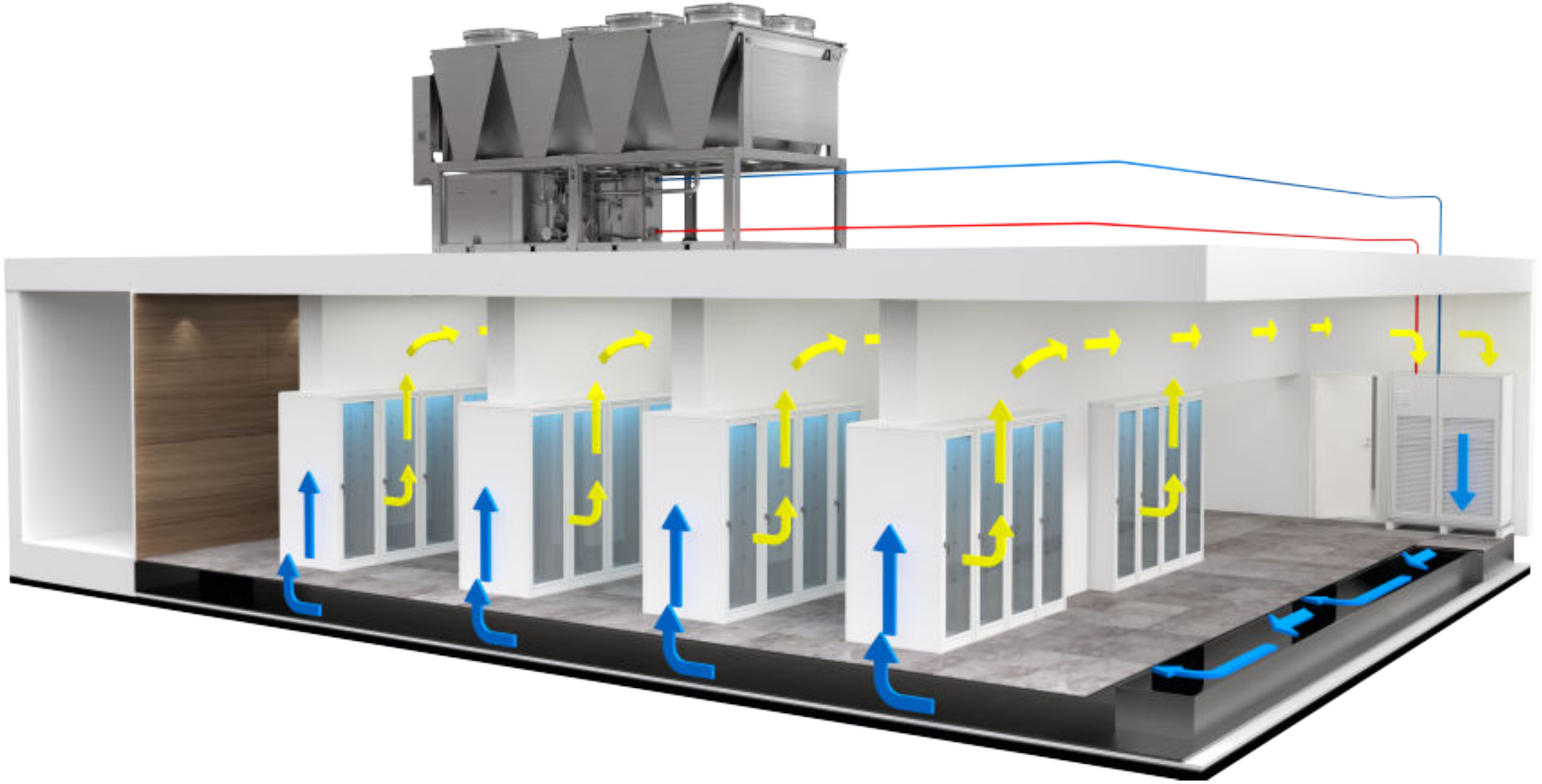


A = 0 A = 1 A = 0

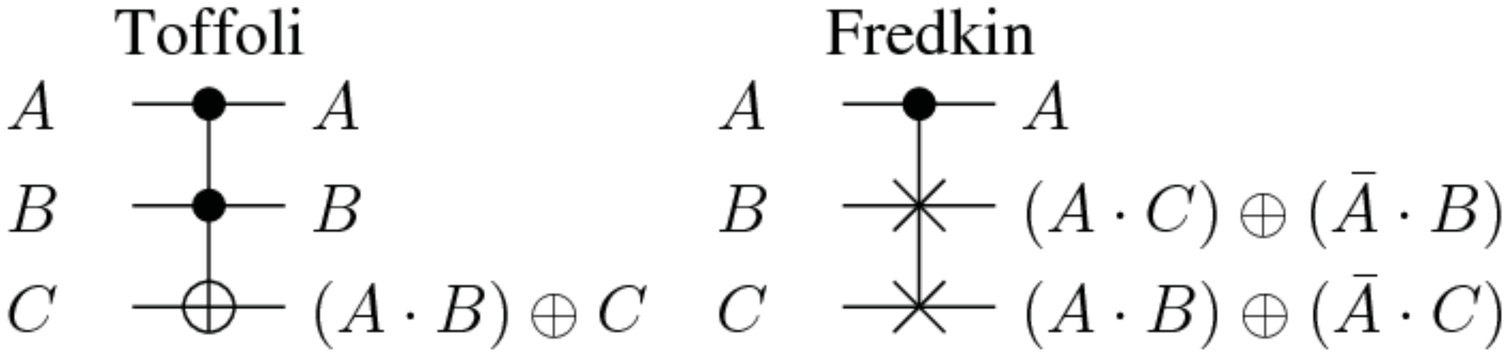
B = 0 B = 0 B = 1

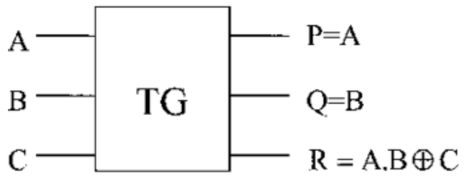
El modelo de hardware que utilizamos es irreversible:
perdemos información útil y producimos calor.

Landauer, R. (1961). **Irreversibility and heat generation in the computing process**. *IBM journal of research and development*, *5*(3), 183-191.

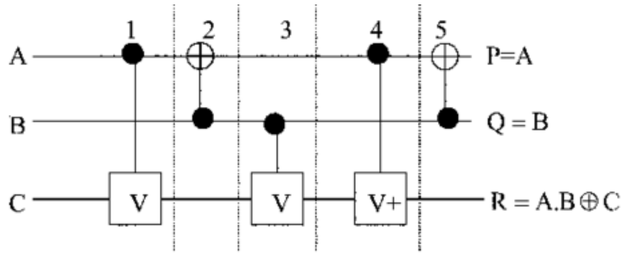


La solución: compuertas reversibles

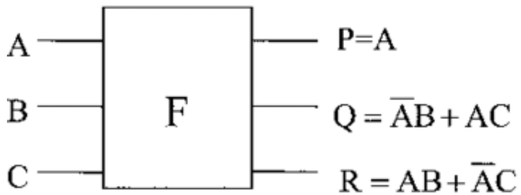




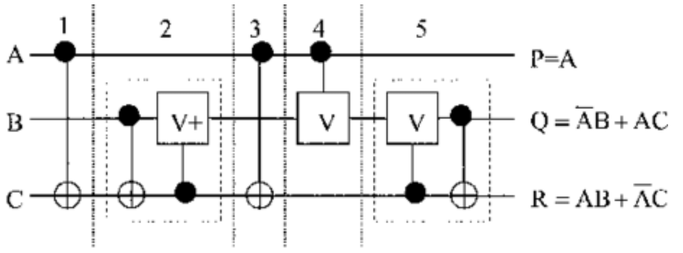
(a) Toffoli Gate



(b) Quantum implementation of the Toffoli Gate

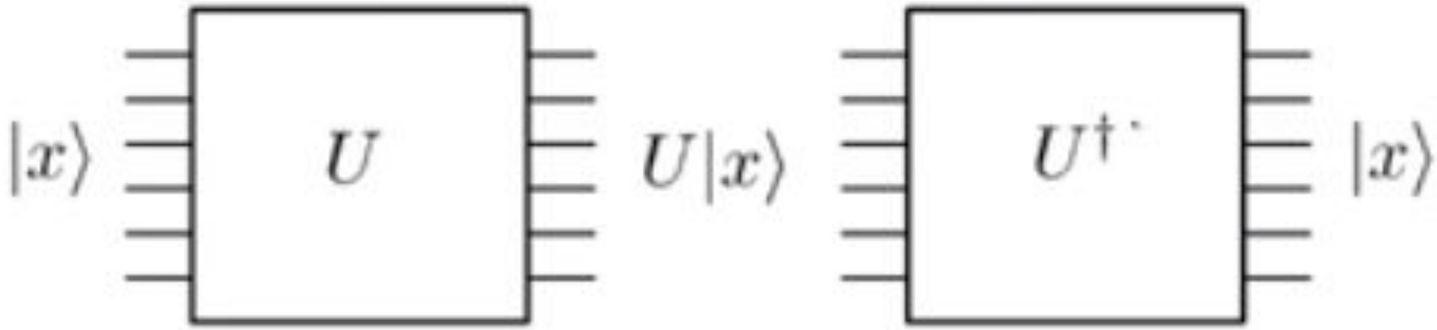


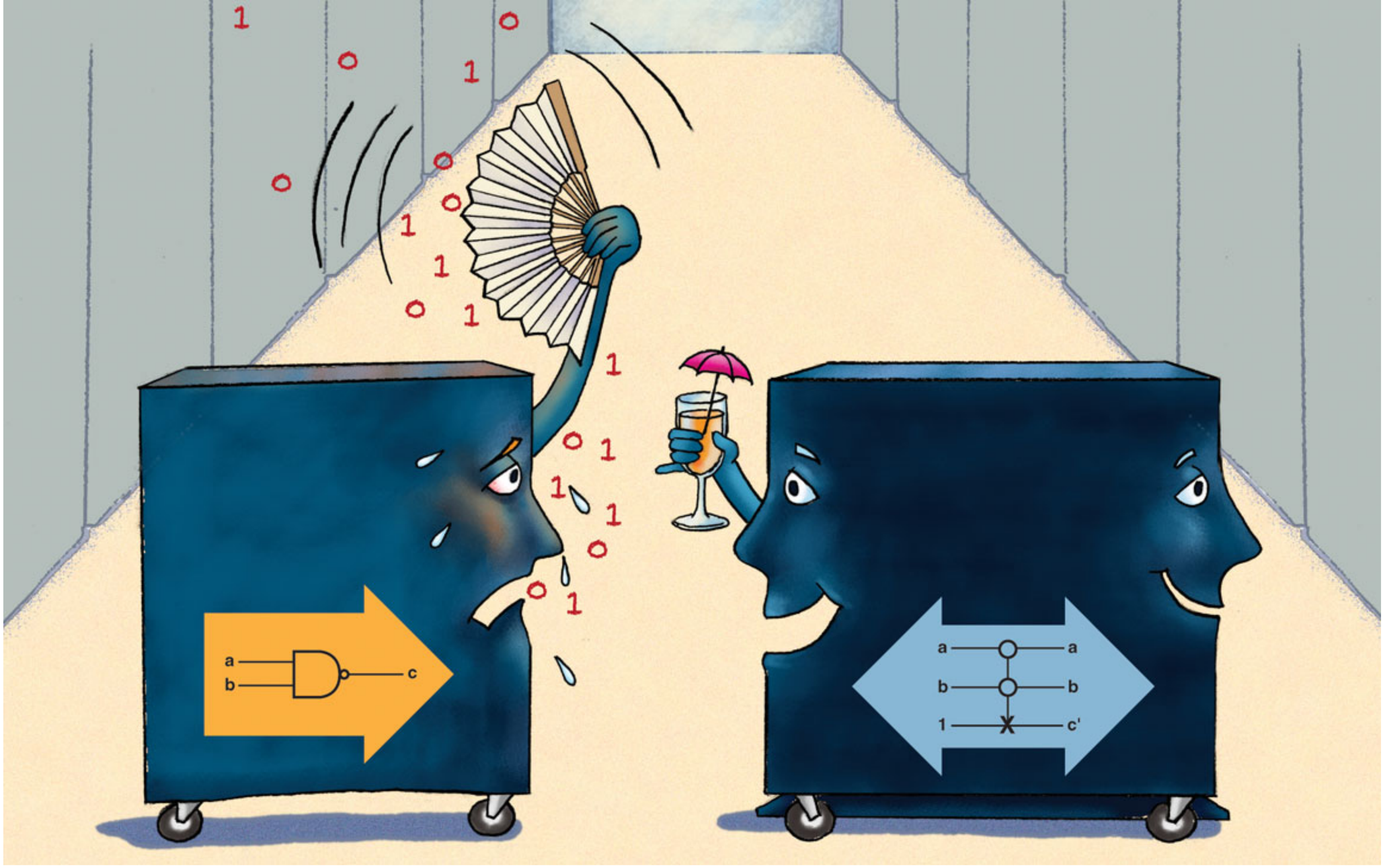
(a) Fredkin Gate



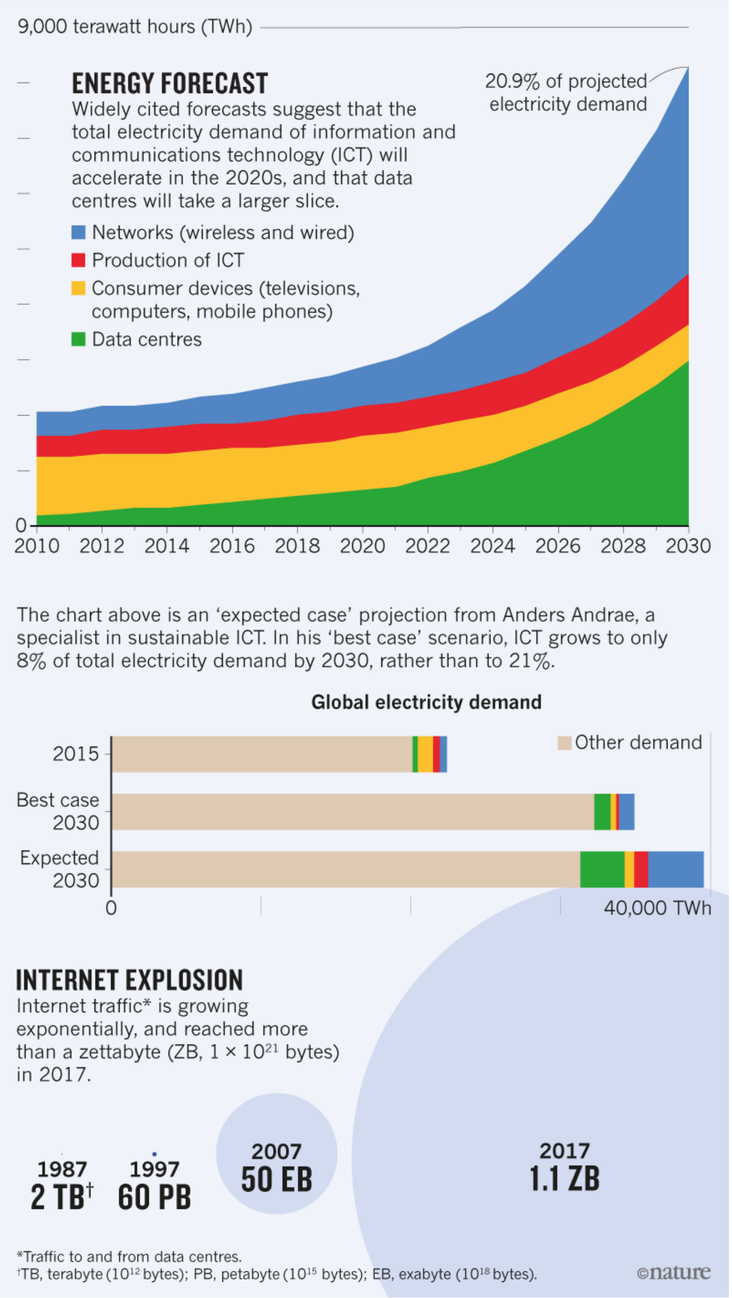
(b) Quantum representation of the Fredkin Gate

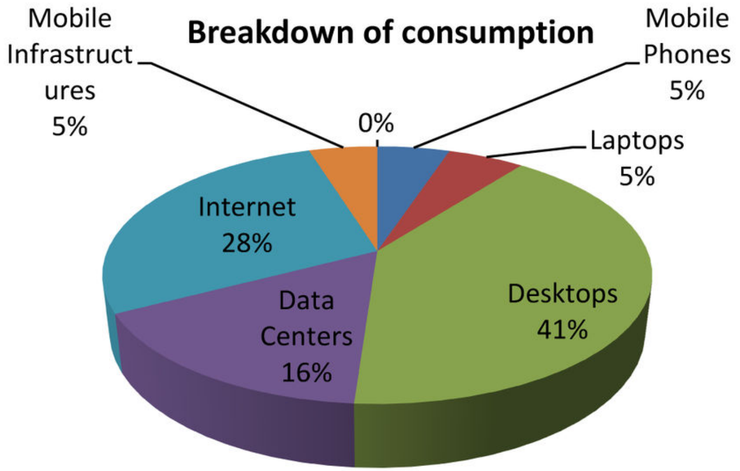
¡Todas las compuertas cuánticas son reversibles (excepto medición)!

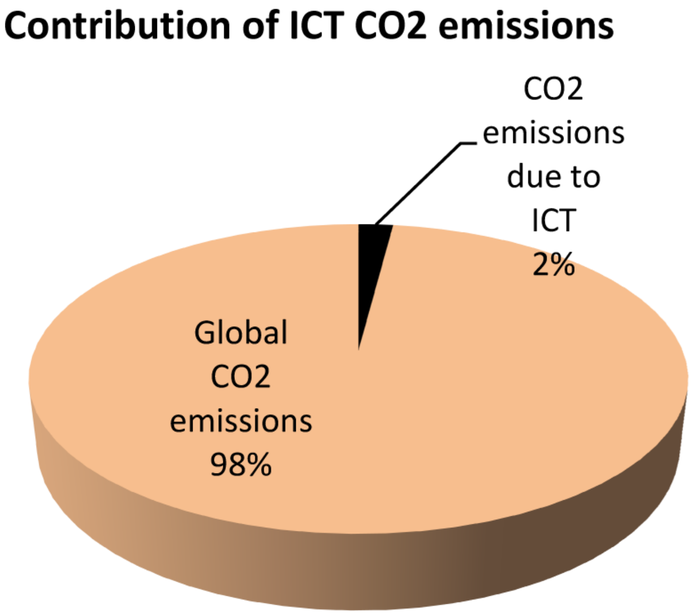




https://www.americanscientist.org/article/computers-that-can-run-backwards







Somavat, P., & Namboodiri, V. (2011). **Energy consumption of personal computing including portable communication devices.** *Journal of Green Engineering*, *1*(4), 447-475.

Energía y TIC: quantum como respuesta

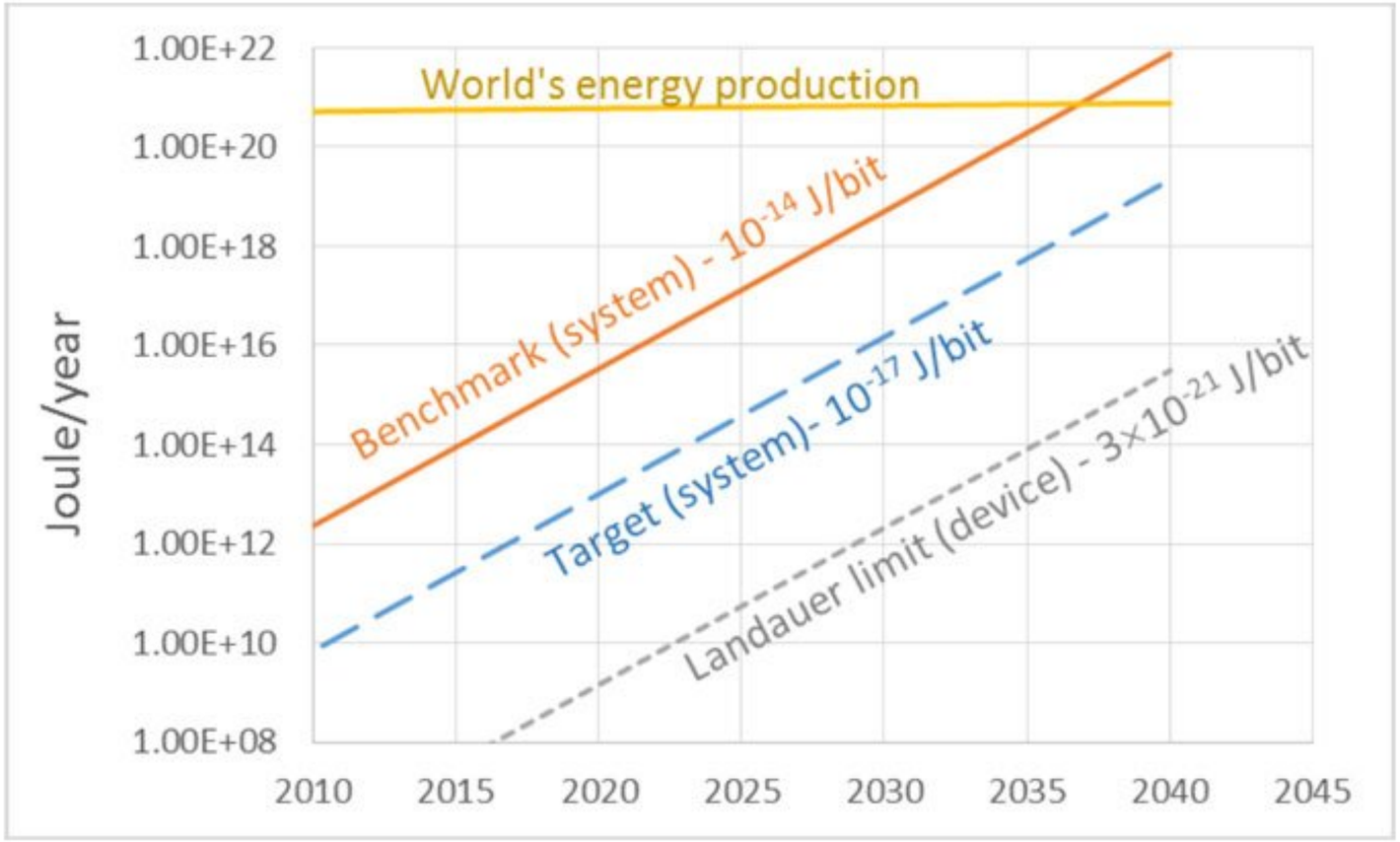
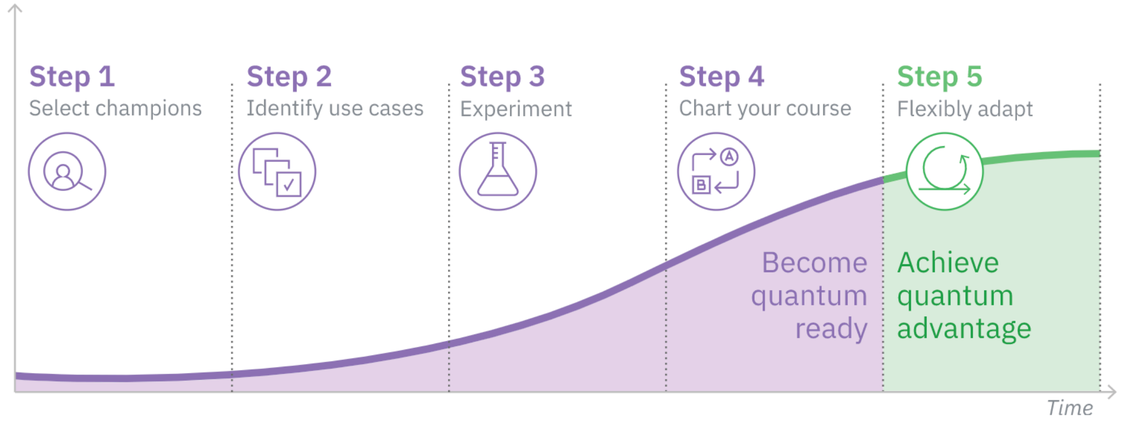
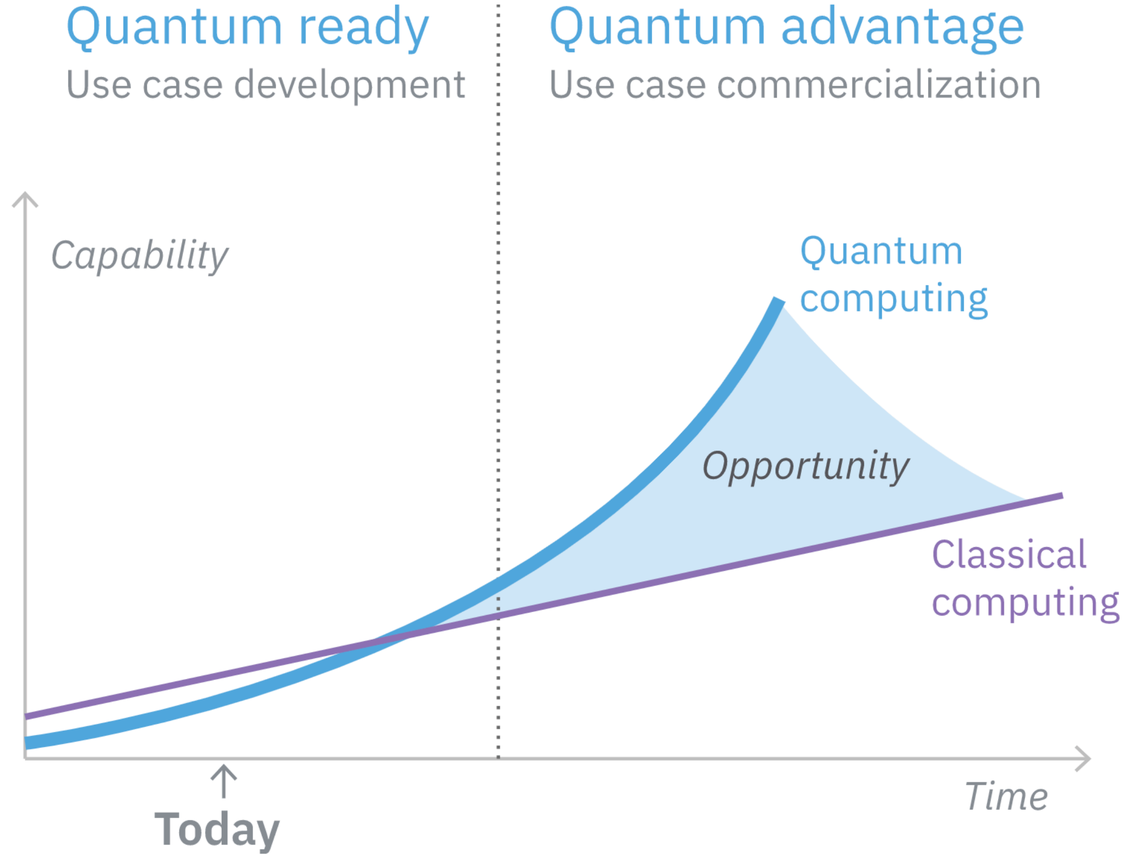


Fig. A8. Total energy of computing.

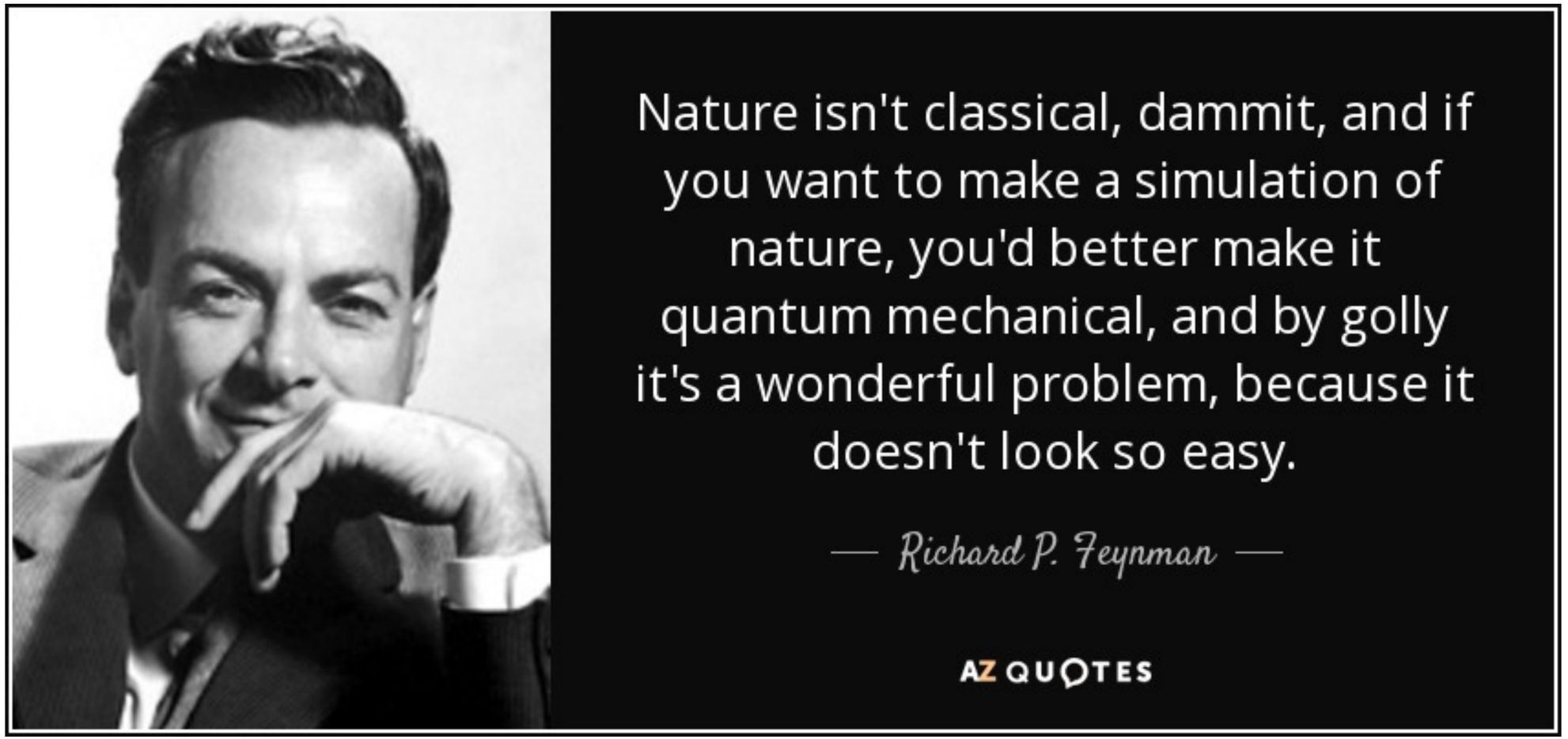
Drechsler, R., & Wille, R. (2012). **Reversible circuits: Recent accomplishments and future challenges for an emerging technology.** In *Progress in VLSI Design and Test* (pp. 383-392). Springer, Berlin, Heidelberg.

Type of scaling	Time to solve problem				
Classical algorithm with exponential runtime	10 secs	2 mins	330 years	3300 years	Age of the universe
Quantum algorithm with polynomial runtime	1 min	2 mins	10 mins	11 mins	~24 mins





¿Para qué nos sirve una computadora cuántica?



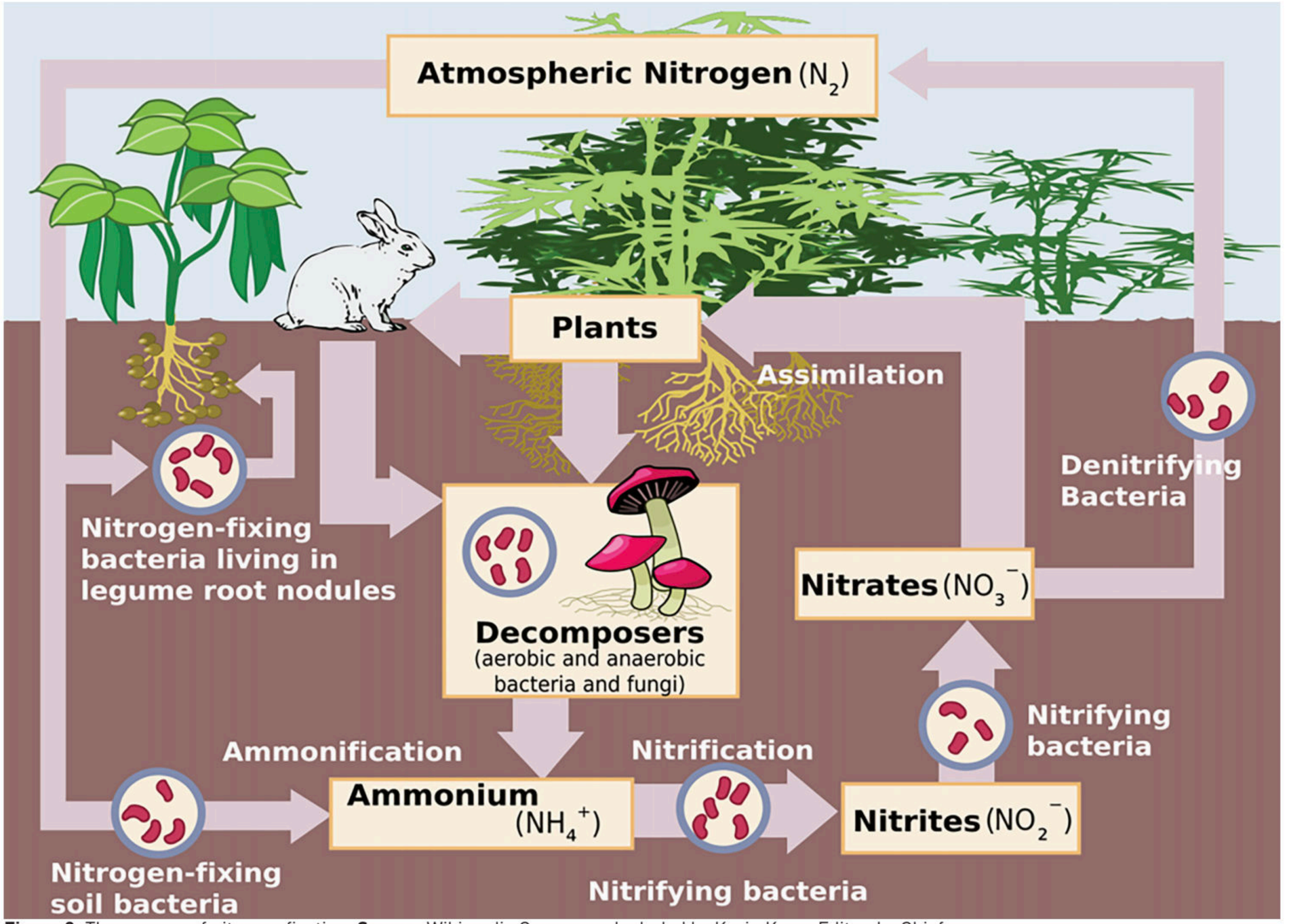
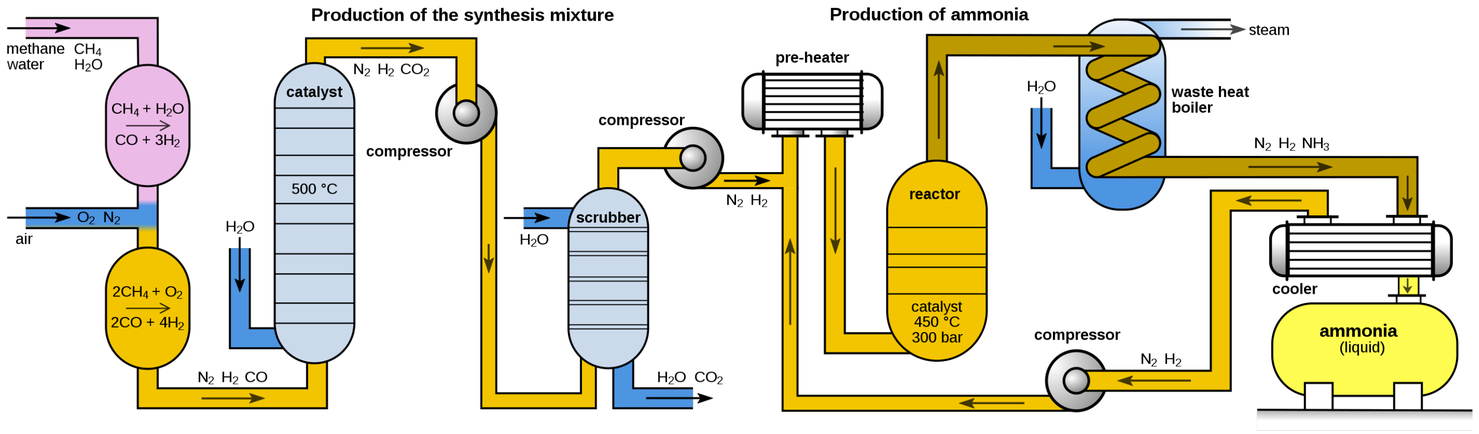
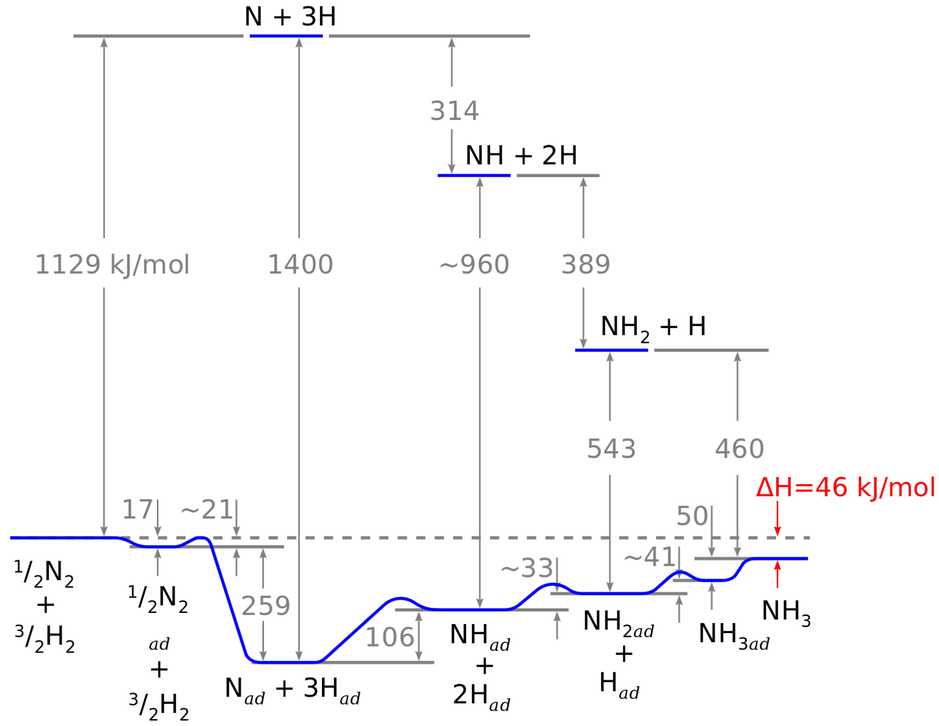


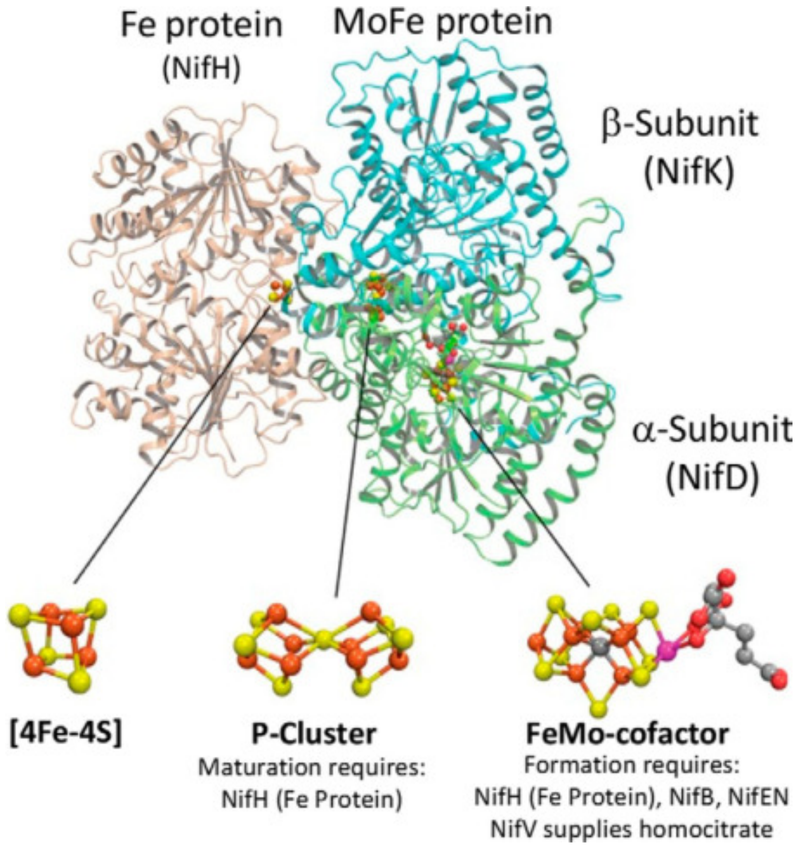
Figure 2: The process of nitrogen fixation. **Source:** Wikimedia Commons. Included by Kevin Kang, Editor-In-Chief

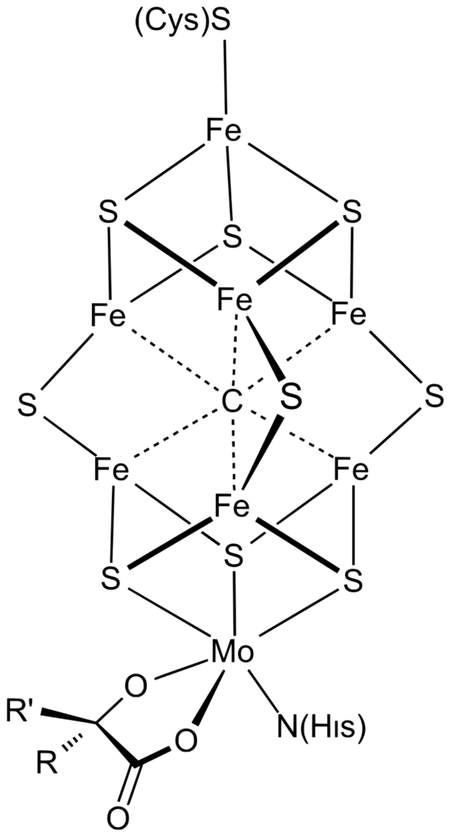
Haber-Bosch (61% eff.): 2% de la energía global, 5% del gas natural global, 450°C a 200 atms.

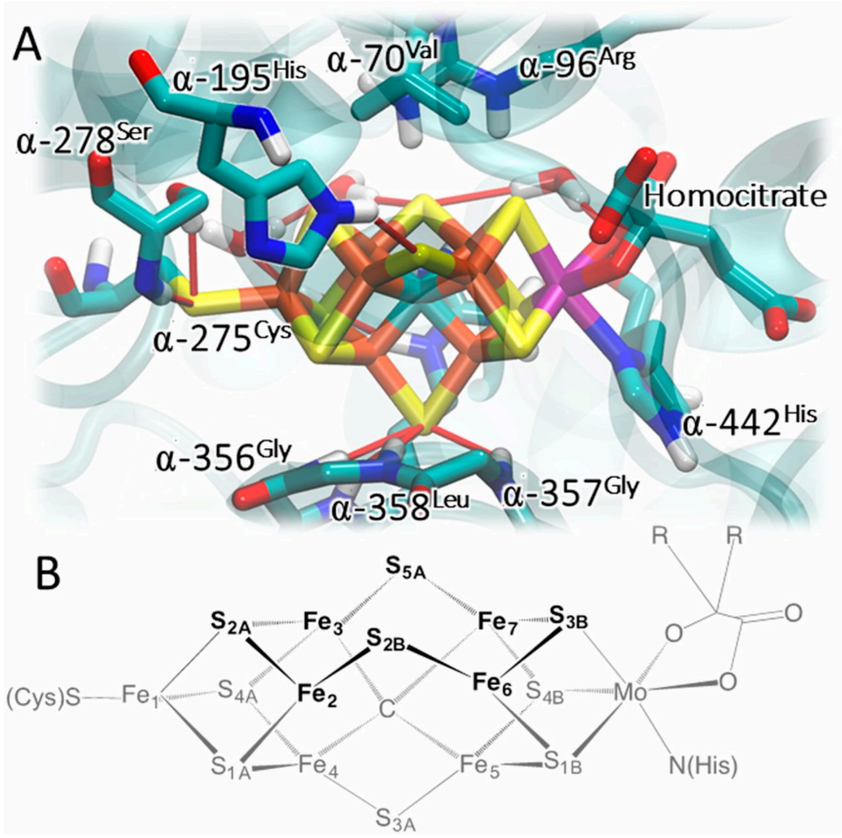
$$\mathrm{N_2 + 3\,H_2 \longrightarrow 2\,NH_3} \quad \Delta H^\circ = -91.8\ \mathrm{kJ/mol}$$





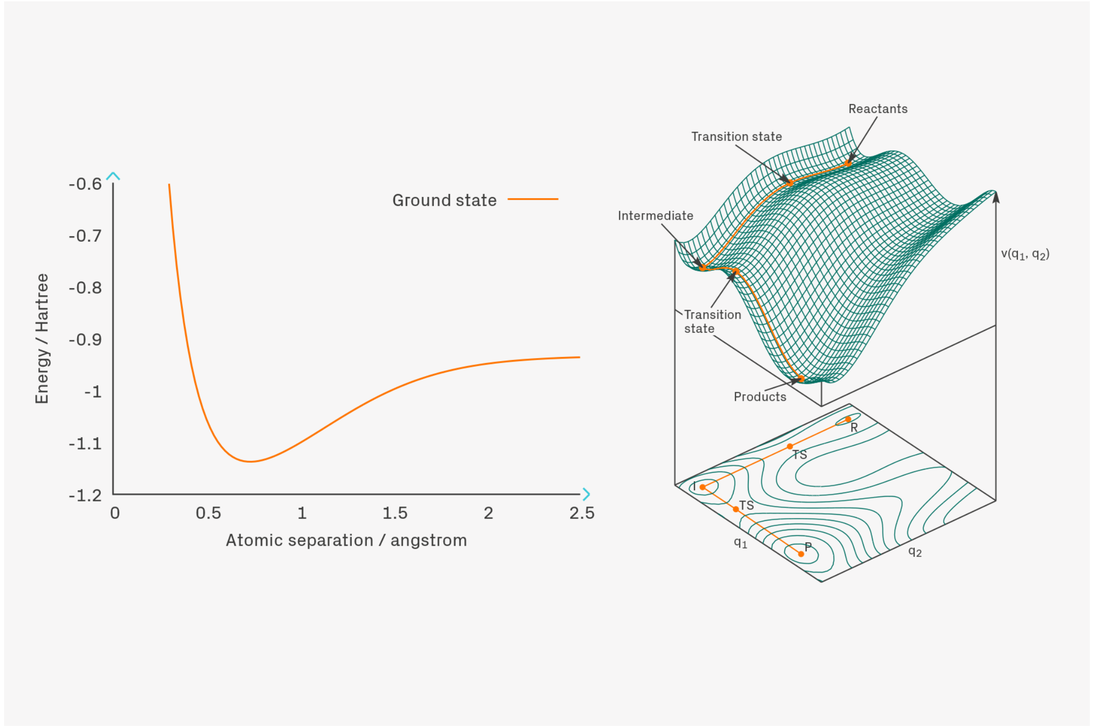


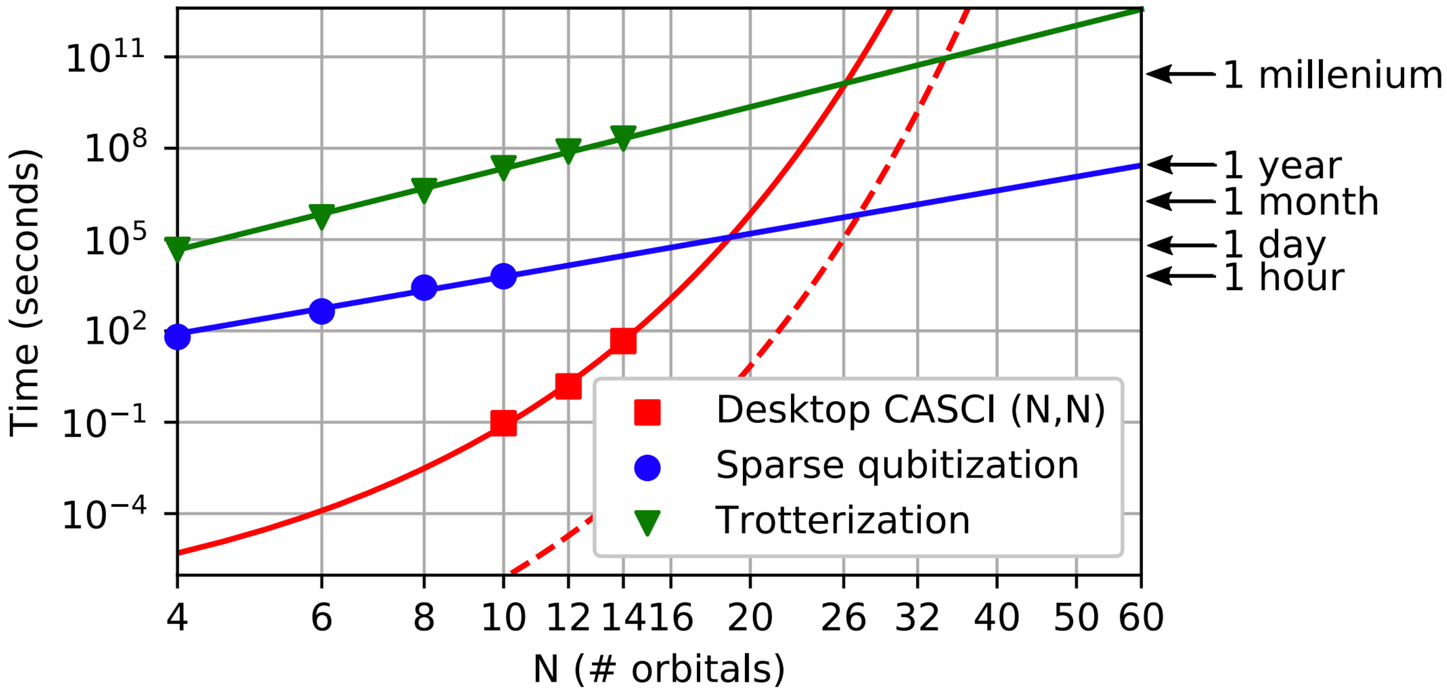




Raugei, S., Seefeldt, L. C., & Hoffman, B. M. (2018). **Critical computational analysis illuminates the reductive-elimination mechanism that activates nitrogenase for N2 reduction.** *Proceedings of the National Academy of Sciences*, *115*(45), E10521-E10530.

Química cuántica asistida por QC



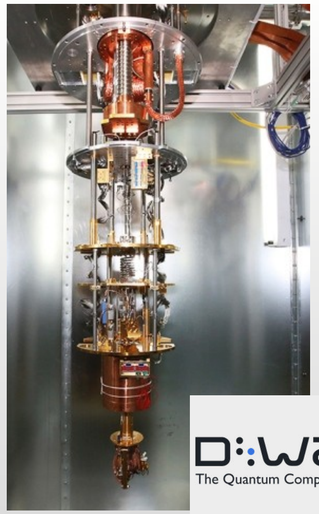


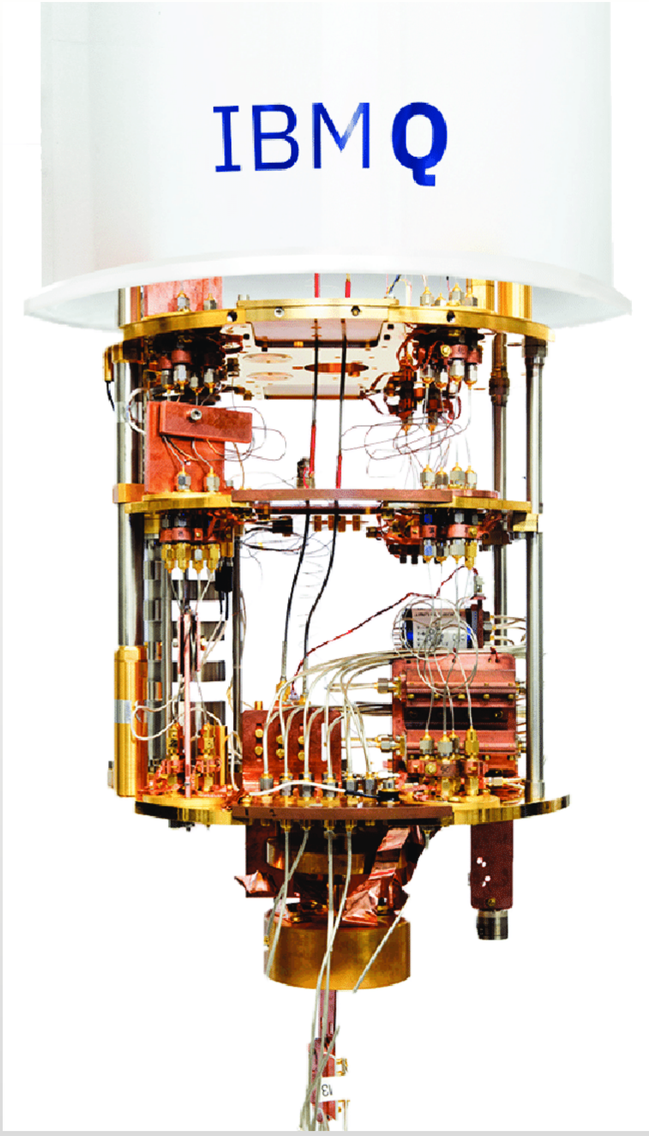
Elfving, V. E., Broer, B. W., Webber, M., Gavartin, J., Halls, M. D., Lorton, K. P., & Bochevarov, A. (2020). **How will quantum computers provide an industrially relevant computational advantage in quantum chemistry?**. *arXiv preprint arXiv:2009.12472*.

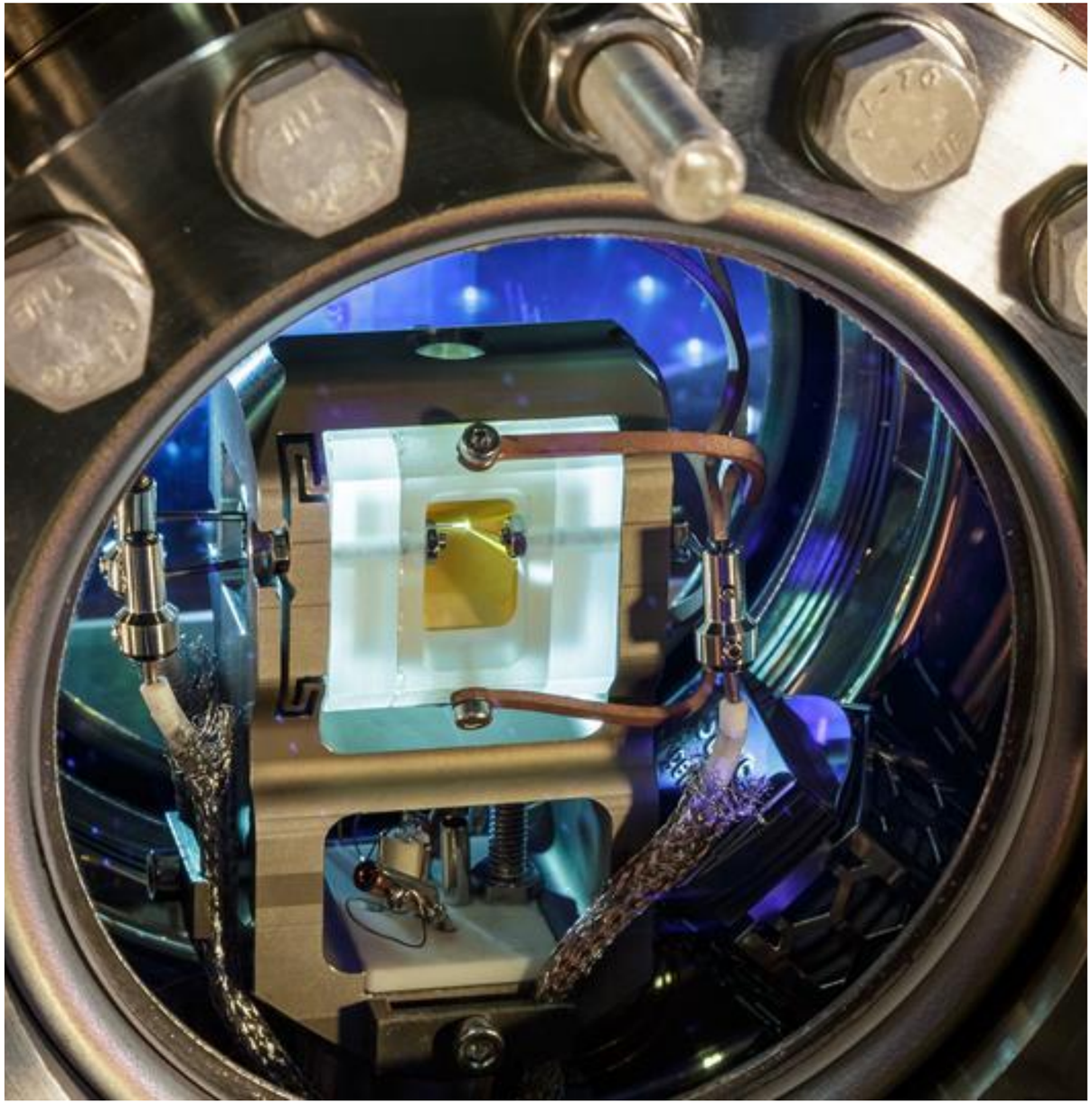
Como se programa una computadora cuántica

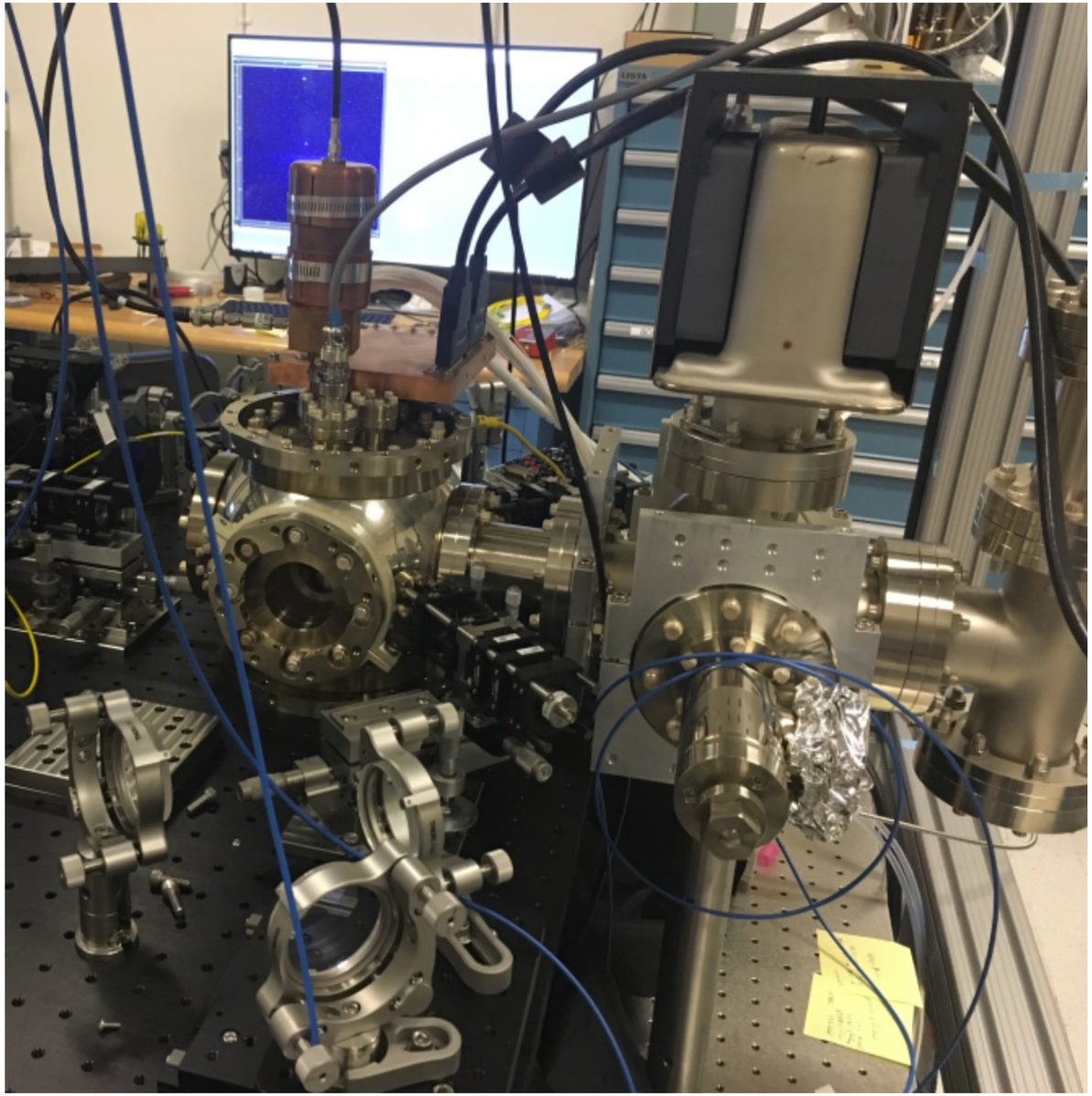

Google


rigetti

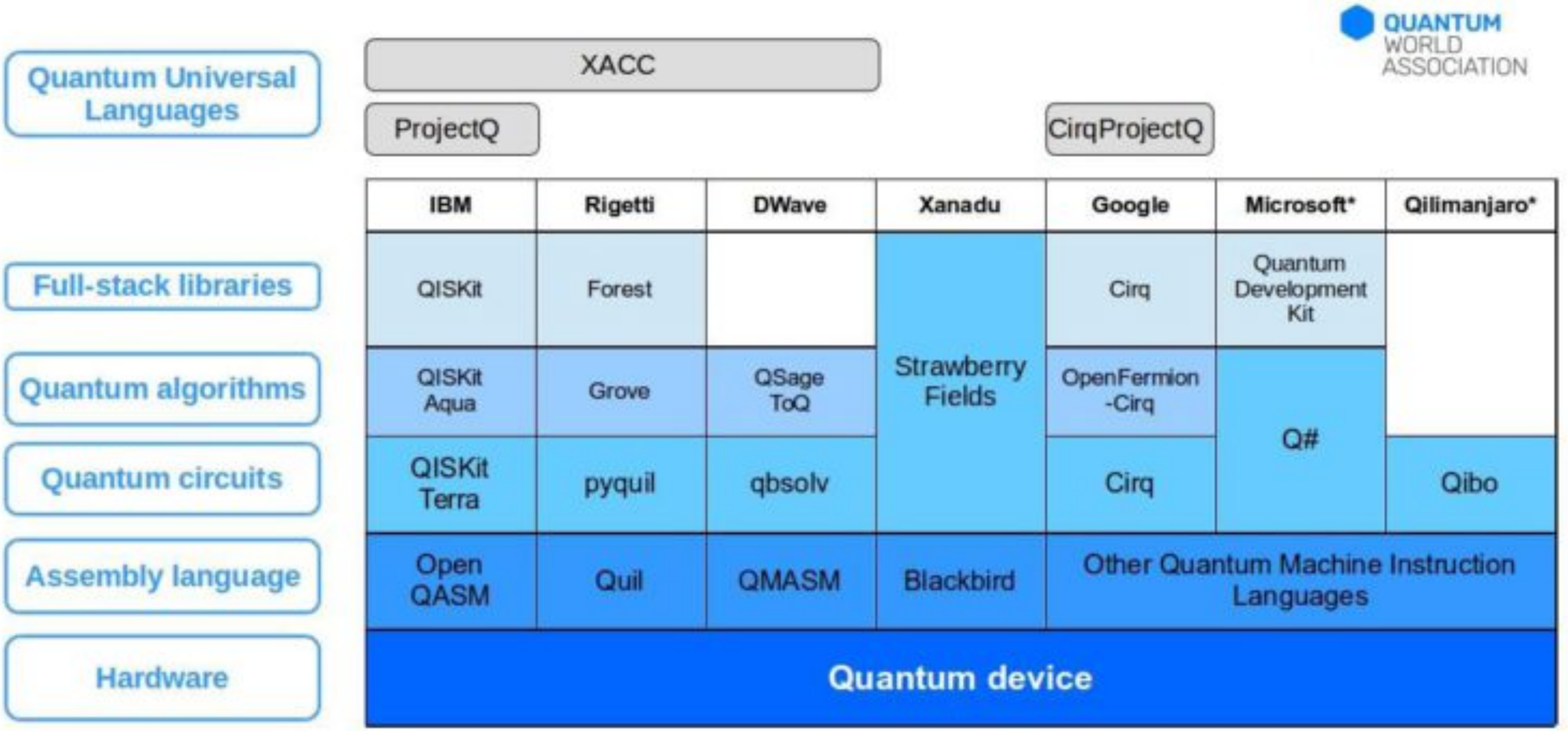

D:wave
The Quantum Computing Company™


IBMQ





Quantum Computing Programming Languages



* Hardware under development. Quantum programs are run on their own simulators.

"Quantum Language" is refered with no distinction both as a quantum equivalence of a programming language and as a library to write quantum programs supported by some well-known classical programming language.

© Alba Cervera-Lierta for the QWA (2018)

Qiskit

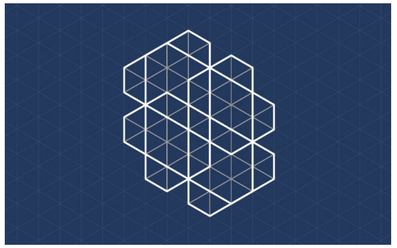
```python
from collections import OrderedDict
from qiskit_chemistry import FermionicOperator
from qiskit_chemistry.drivers import PySCFDriver, UnitsType

# Use PySCF, a classical computational chemistry software package, to compute the one- an
# two-body integrals in molecular-orbital basis, necessary to form the Fermionic operator
driver = PySCFDriver(atom='H .0 .0 .0; H .0 .0 0.735', unit=UnitsType.ANGSTROM,
                     charge=0, spin=0, basis='sto3g')
molecule = driver.run()
num_particles = molecule.num_alpha + molecule.num_beta
num_spin_orbitals = molecule.num_orbitals * 2

# Build the qubit operator, which is the input to the VQE algorithm in Aqua
ferOp = FermionicOperator(h1=molecule.one_body_integrals, h2=molecule.two_body_integrals)
map_type = 'PARITY'
qubitOp = ferOp.mapping(map_type)
qubitOp = qubitOp.two_qubit_reduced_operator(num_particles)
num_qubits = qubitOp.num_qubits

# set the backend for the quantum computation
from qiskit import Aer
backend = Aer.get_backend('statevector_simulator')

# setup a classical optimizer for VQE
from qiskit_aqua.components.optimizers import L_BFGS_B
optimizer = L_BFGS_B()

# setup the initial state for the variational form
from qiskit_chemistry.aqua_extensions.components.initial_states import HartreeFock
init_state = HartreeFock(num_qubits, num_spin_orbitals, num_particles)

# setup the variational form for VQE
from qiskit_aqua.components.variational_forms import RYRZ
var_form = RYRZ(num_qubits, initial_state=init_state)

# setup and run VQE
from qiskit_aqua.algorithms import VQE
algorithm = VQE(qubitOp, var_form, optimizer)
result = algorithm.run(backend)
print(result['energy'])
```

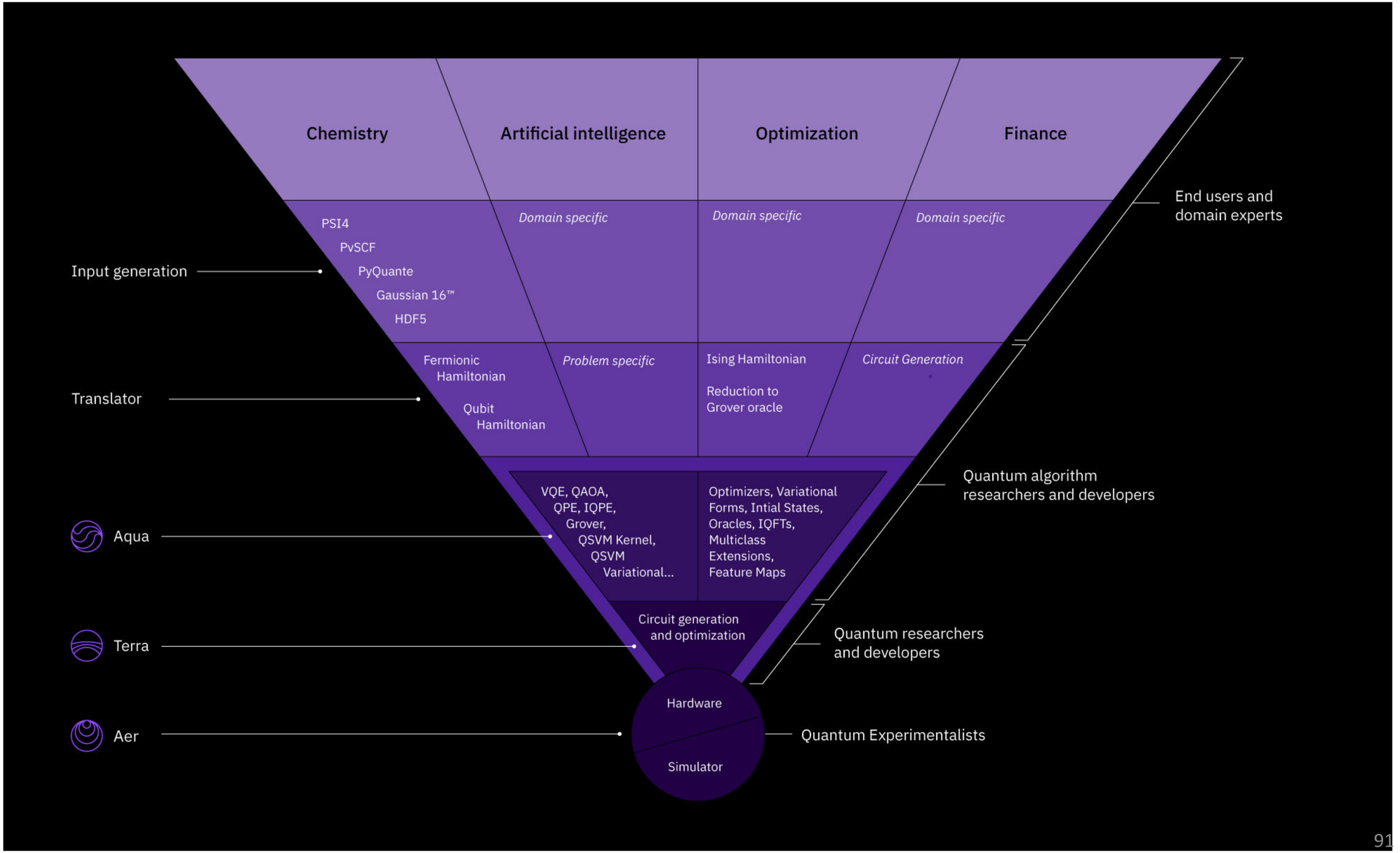
aqua_chemistry_experiment.py hosted with ❤️ by GitHub view raw

Microsoft

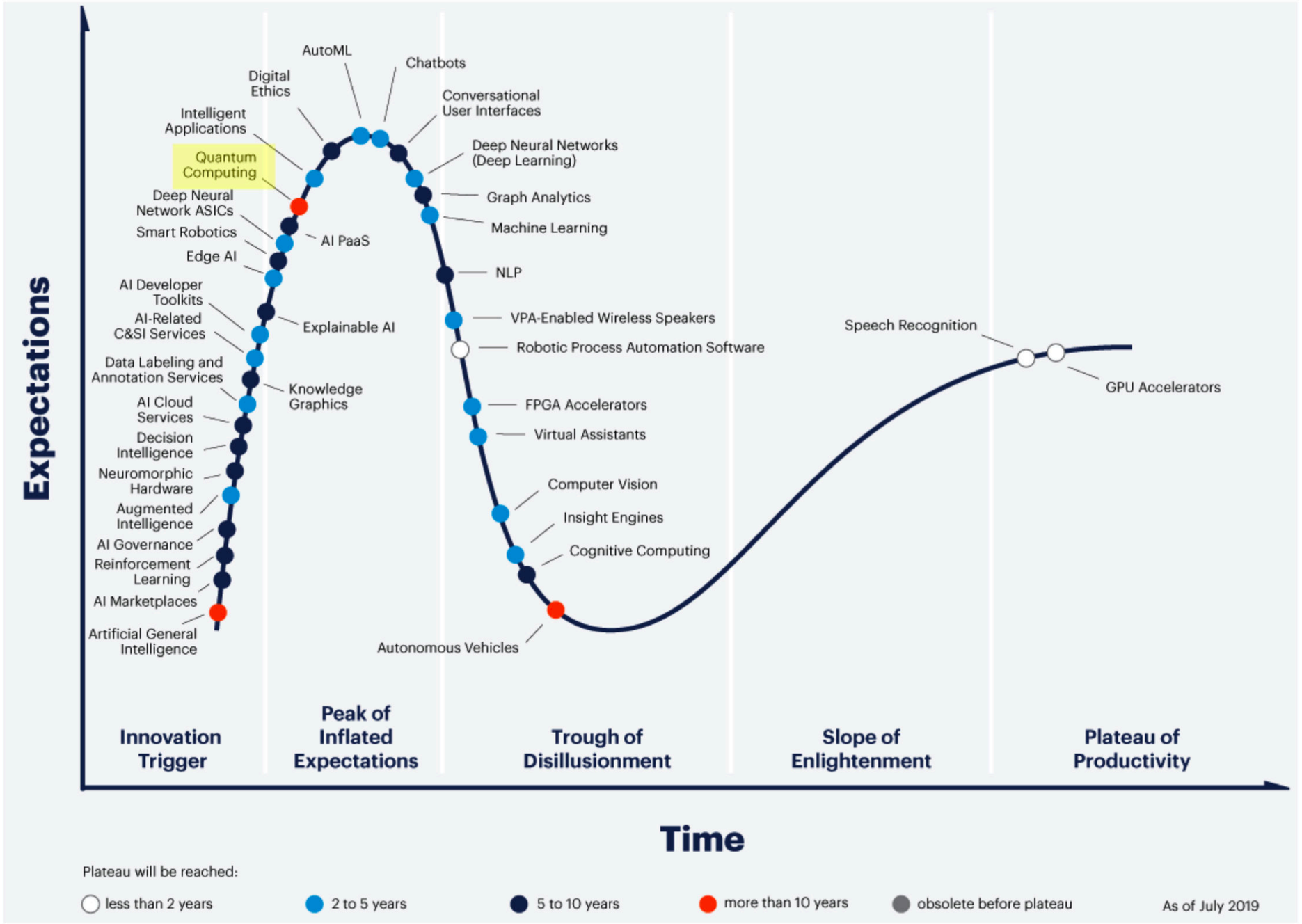
Q# Copy

```
operation TestBellState(count : Int, initial : Result) : (Int, Int) {

    mutable numOnes = 0;
    use qubit = Qubit();
    for test in 1..count {
        SetQubitState(initial, qubit);
        let res = M(qubit);

        // Count the number of ones we saw:
        if res == One {
            set numOnes += 1;
        }
    }

    SetQubitState(Zero, qubit);



    // Return number of times we saw a |0> and number of times we saw a |1>
    Message("Test results (# of 0s, # of 1s): ");
    return (count - numOnes, numOnes);
}
```

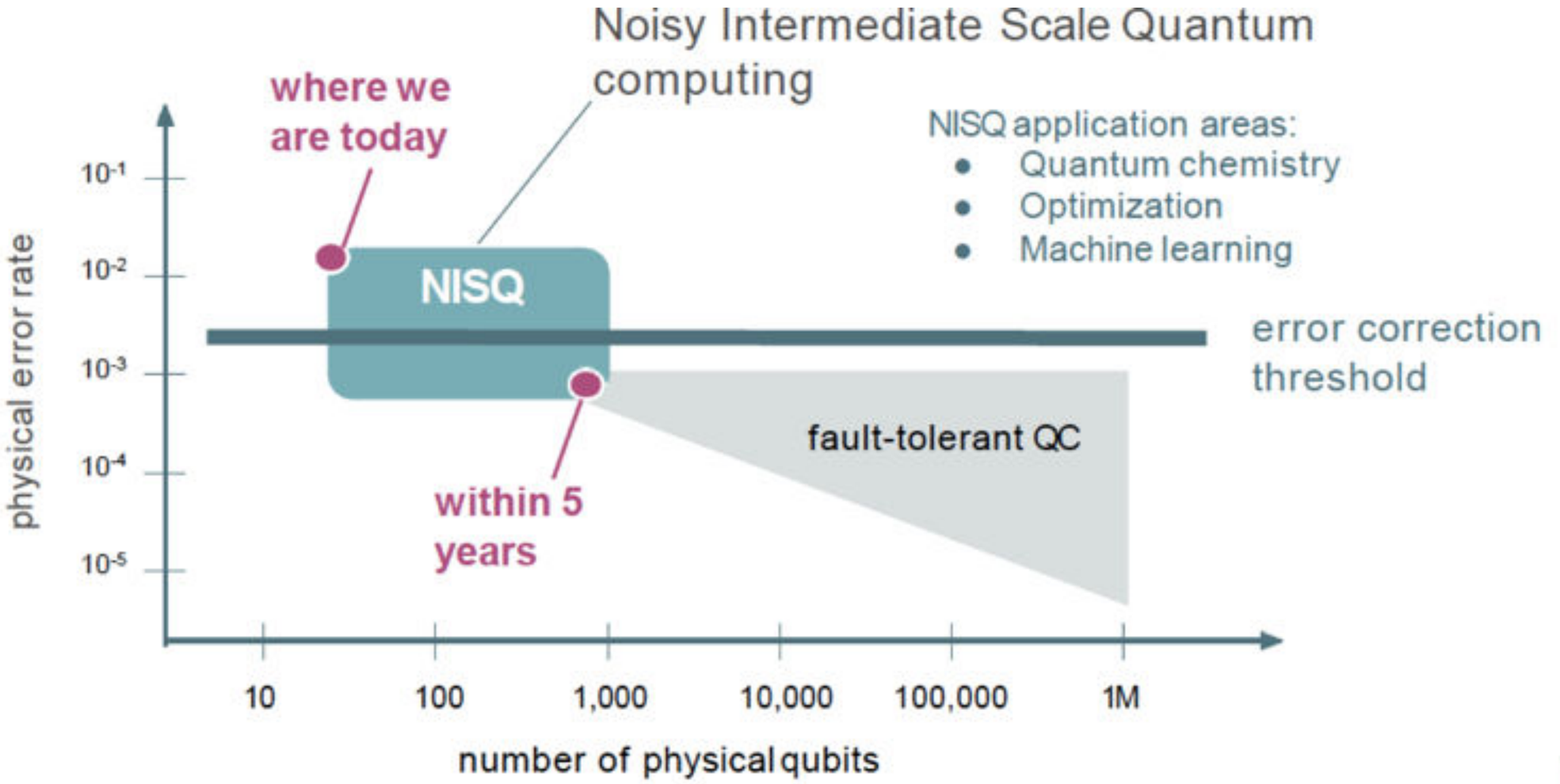



Chemistry
Artificial intelligence
Optimization
Finance
End users and domain experts
PSI4
PyQuante
PySCF
Gaussian 16™
HDF5
Domain specific
Domain specific
Domain specific
Input generation
Translator
Fermionic Hamiltonian
Qubit Hamiltonian
Problem specific
Ising Hamiltonian
Reduction to Grover oracle
Circuit Generation
Quantum algorithm researchers and developers
VQE, QAOA, QPE, IQPE, Grover, QSVM Kernel, QSVM Variational...
Optimizers, Variational Forms, Intial States, Oracles, IQFTs, Multiclass Extensions, Feature Maps
Aqua
Circuit generation and optimization
Terra
Quantum researchers and developers
Hardware
Simulator
Aer
Quantum Experimentalists

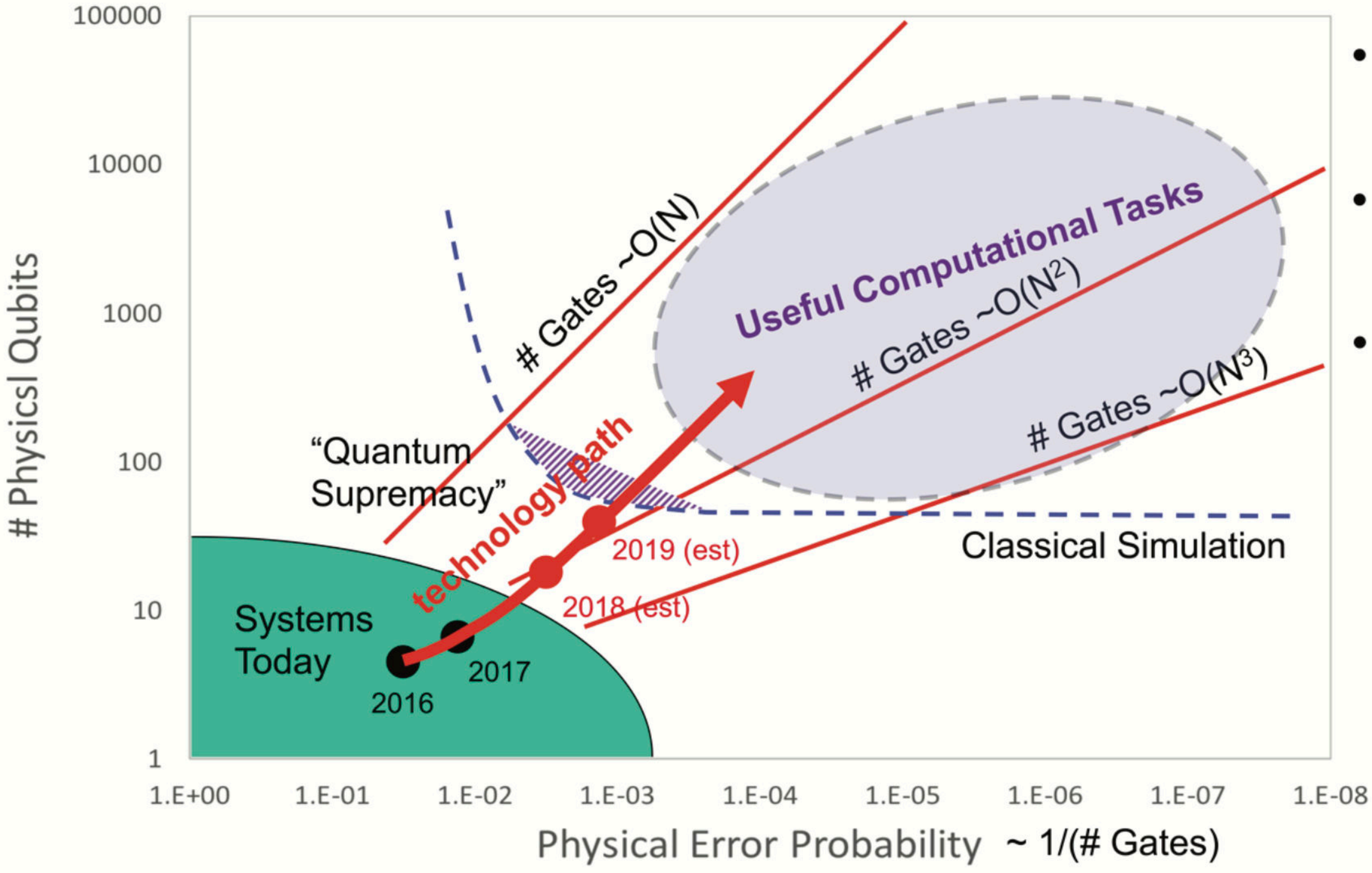
Futuro:
¿será una tecnología realista?



The 2019 Gartner Hype Cycle for Artificial Intelligence, with quantum computing highlighted in yellow. Credit: Gartner

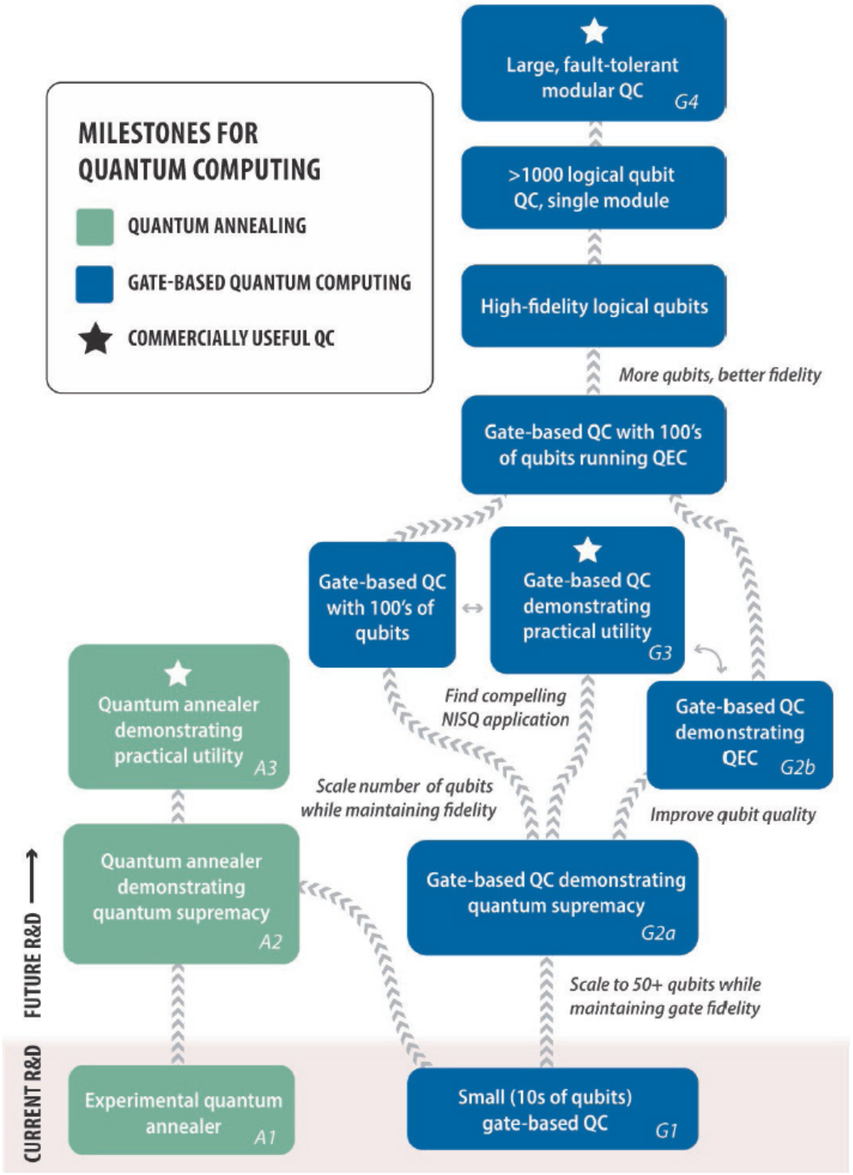


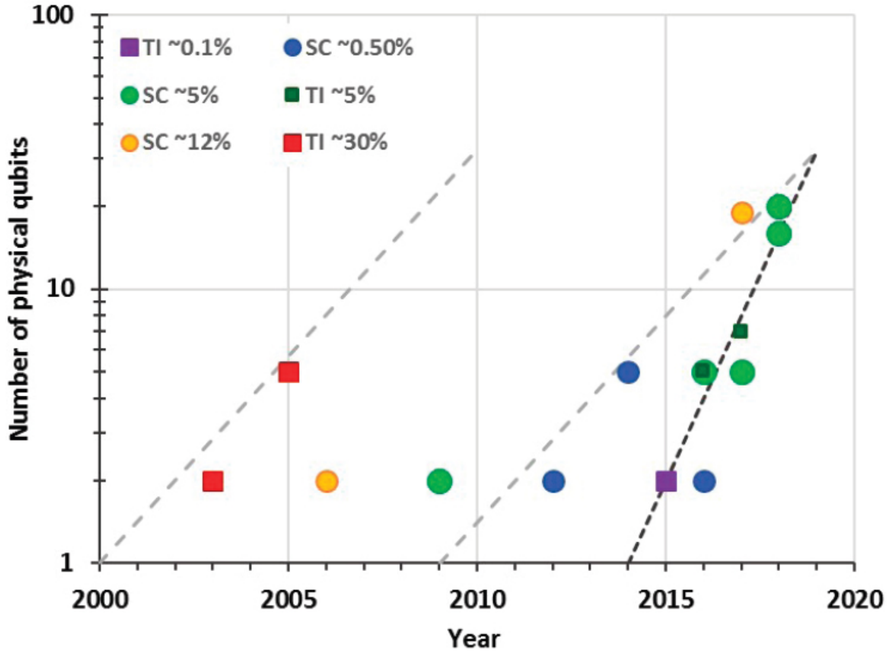
"Quantum computing in the NISQ era and beyond" Preskill, 2018 https://arxiv.org/abs/1801.00862

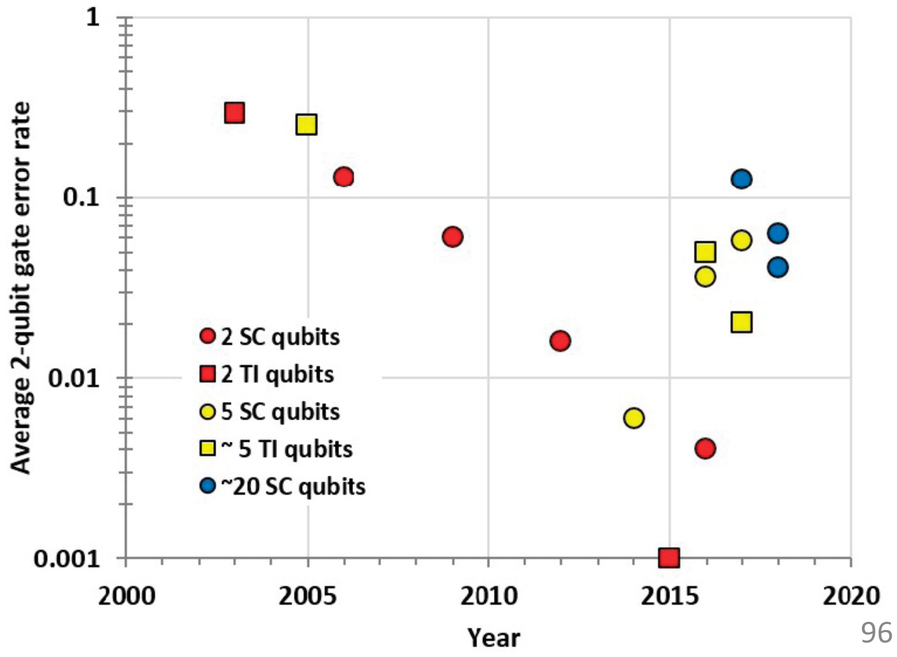


- First, reach a fault-tolerant qubit
- Then scale up in numbers
- Interesting computational tasks beyond classical simulation limit

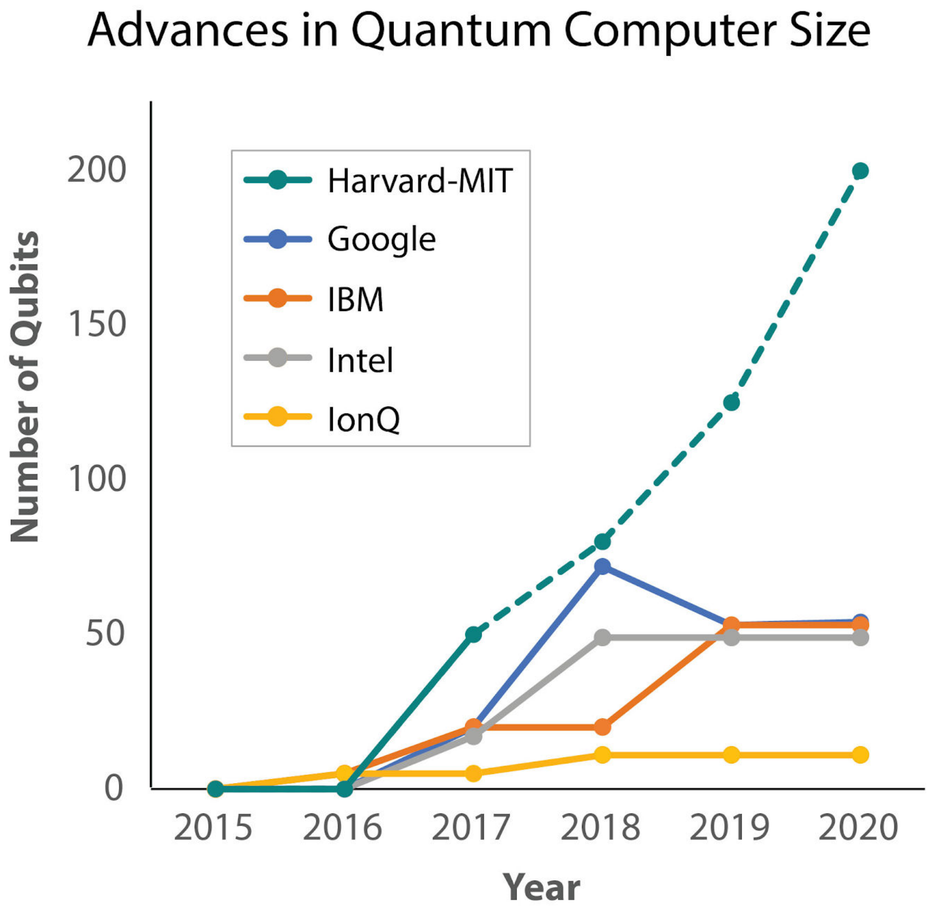
Martonosi, M., & Roetteler, M. **Next steps in quantum computing: computer science's role**. *arXiv preprint arXiv:1903.10541*. 2019.







National Academies of Sciences, Engineering, and Medicine. *Quantum computing: progress and prospects*. National Academies Press. 2019.

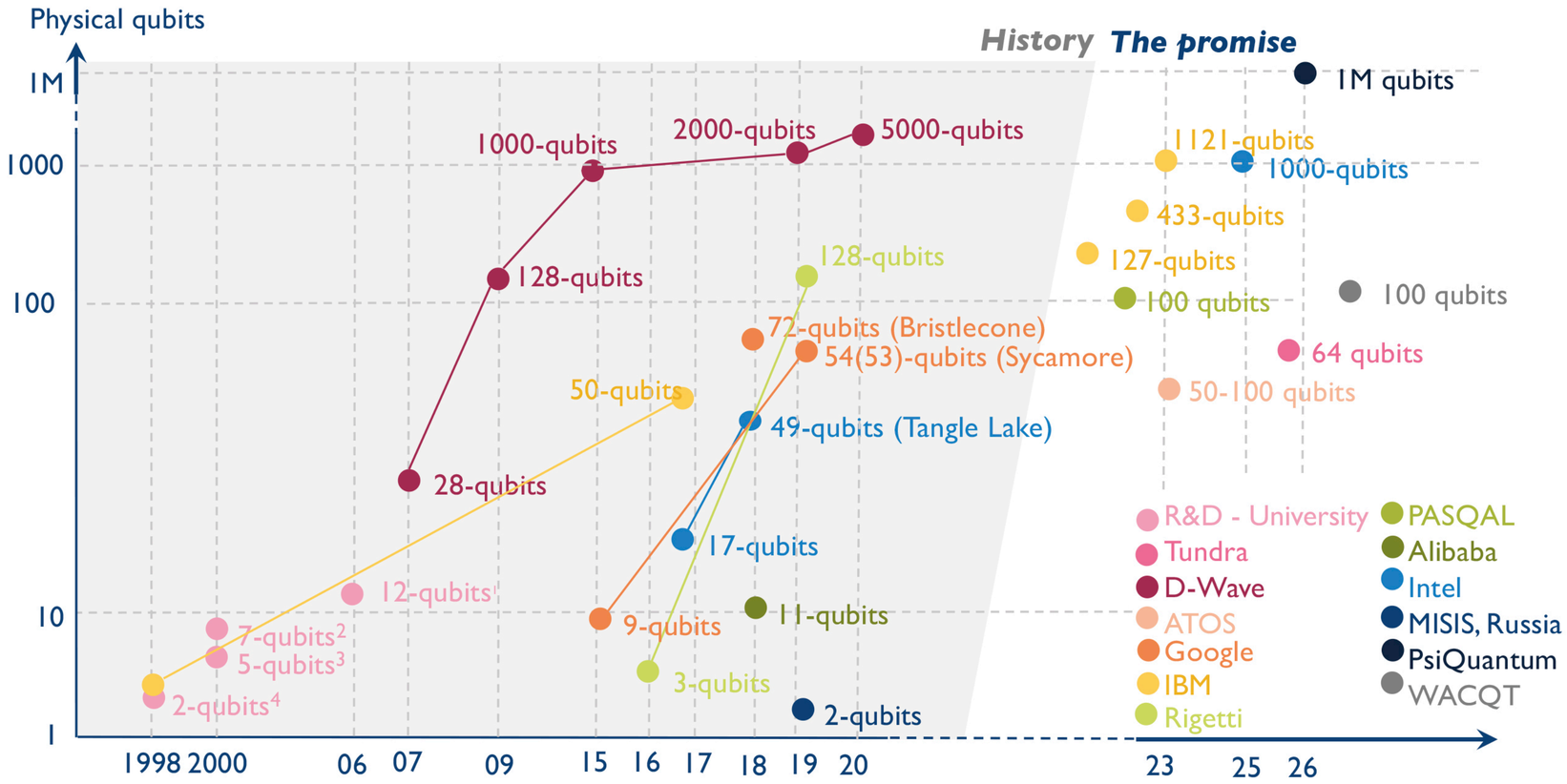


System	Type	Number of Qubits	Qubit Stability	System Flexibility
Google	Superconducting circuits	54		Medium
IBM	Superconducting circuits	53		Medium
Intel	Superconducting circuits	49		Medium
IonQ	Trapped Ions	11		High
Harvard-MIT	Ultracold Atoms	50		Low

Insa Mohr. **Searching for the Holy Grail of Quantum Computing.** October 2020

1998-2026 Physical qubit roadmap for quantum computer

(Source: Quantum Technologies 2021 report, Yole Développement, 2021)



[1] (Institute for Quantum Computing, Perimeter Institute for Theoretical Physics, MIT)
[2] (Los Alamos National lab)
[3] (TU Munich)
[4] (Oxford University, IBM, UC Berkeley, Stanford, MIT)

Puntos clave

Estamos a 5 años de contar con hardware cuántico con poder computacional suficiente para disrupción industrial a gran escala

Aún es un ambiente pre-competitivo en materia de innovación, gran ecualizador de oportunidades

Innovar en QC puede ocurrir más fácilmente a nivel de software, algoritmos y aplicaciones (una oportunidad para Costa Rica y socios país)

Aún cuando se requieren fundamentos de física, personas con formación en álgebra lineal y software pueden introducirse bien en este campo

¿Qué podemos hacer en Costa Rica?

estrategia

- No estamos a nivel para participar en desarrollo de hardware
- Posiblemente en aplicaciones, si preparamos a la gente en las bases del area
- El area también requiere herramientas de alto nivel, como compiladores, no son fáciles, pero CR tiene el conocimiento en la industria en esa area
- Si en estos 5 años no preparamos gente en el momento del boom no estaremos listos

¿Qué podemos hacer en CR?
estrategia

- La formación para programar/entender computación cuántica es algebra lineal en variable compleja
  - Similar a los programas que ya se están dando en ciencia de datos en varias universidades
  - Ya hay gente entonces que ha recorrido parte del camino
- La matemática necesaria está a nivel de un estudiante de bachillerato universitario
- Muchas universidades norteamericanas ya dan cursos de computación cuántica para sus estudiantes de bachillerato
- Es razonable dar electivas e ir preparando gente para que de aquí a 5 años estemos en mejores condiciones de absorber un boom