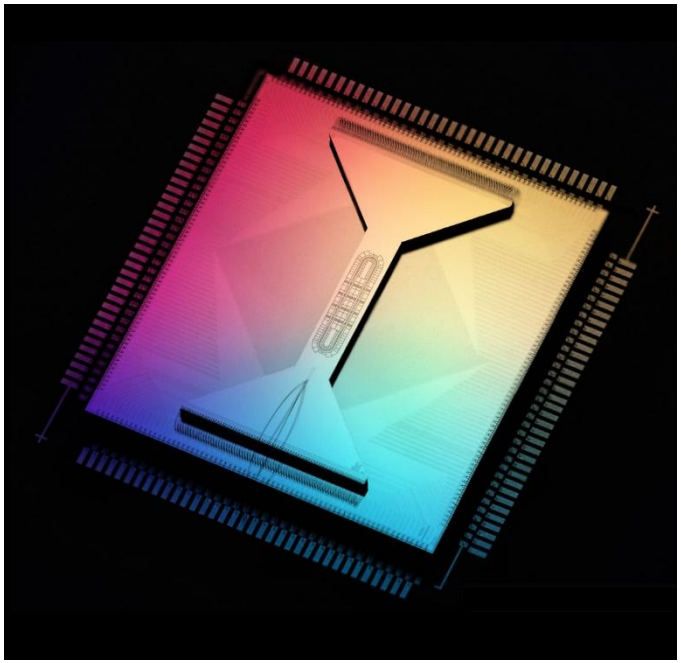
# PHYS-541 - Quantum Computing

**Vincenzo Savona**

***EPFL Center for Quantum Science and Engineering***



Trapped-ion quantum processor: Quantinuum


Superconducting quantum computer: IBM

# PHYS-541 - Quantum Computing

| | |
|---|---|
| Teacher: | *Vincenzo Savona* |
| Assistants: | *Sara Alves, David Linteau, Shao Hen Chiew* |
| Dates: | Thursdays 11.9 – 18.12.2025 |
| Time: | Course 13:15 – 16:00 |
| | Exercises 16:15 – 18:00 |
| Location: | BS 260 |
| Material: | see moodle (PHYS-541) |
| Sources: | M. A. Nielsen & I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge, 2011) |
| | John Preskill, *Lecture Notes on Quantum Information and Computation* http://theory.caltech.edu/~preskill/ph219/ph219_2019-20 |

In October 2019, Google announced **quantum supremacy**:

A programmable, general-purpose engineered quantum device could perform a computational task much faster than any existing supercomputer would do

Nature **574**, 505 (2019)

**Scope of the course:**
**Acquire the skills needed to understand this result**

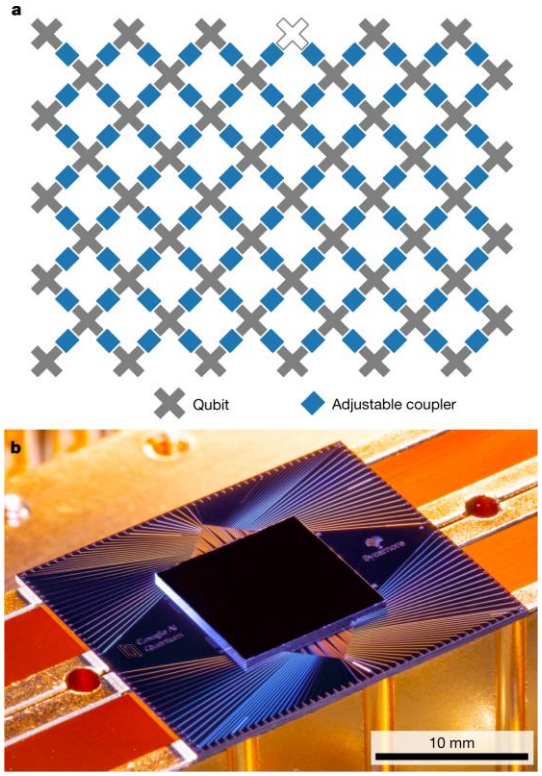
Notion of quantum information

Paradigm of digital quantum computing

Notion of classical and quantum computational complexity

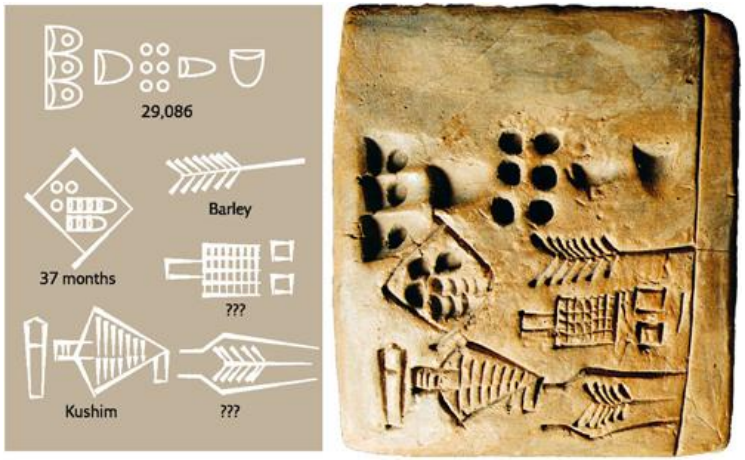
Notion of errors in a quantum computation

Quantum circuits and algorithms



# The physical nature of information

Information is physical

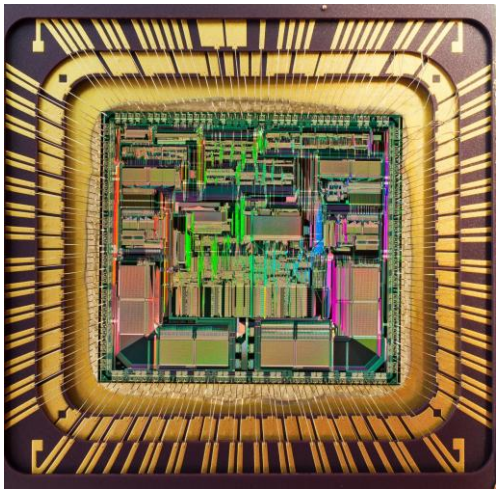



“Kushim” clay tablet (3400 – 3000 BC)

“Quipu” (3000 – 2000 BC)

# The physical nature of information

Information is physical



Current information devices are described by the **laws of classical physics**

Everyday phenomena obey the **laws of non-relativistic quantum mechanics**

**Quantum superposition** and **entanglement** are not used in classical devices

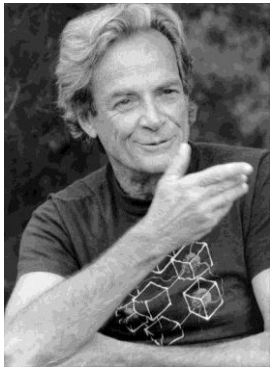
Can these properties result in a more efficient computation paradigm?

# The idea of quantum computing

Time-dependent Schrödinger equation:

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

Quantum many-body systems are in general computationally untreatable: resources scale exponentially with the size of the system



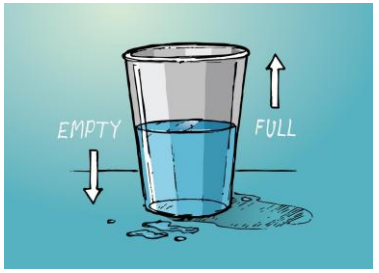
**"… nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."**

Richard Feynman
*Simulating physics with computers* (1981)

A resource, not a limitation!

Nature executes this specific "computational" task exponentially faster than classical computers

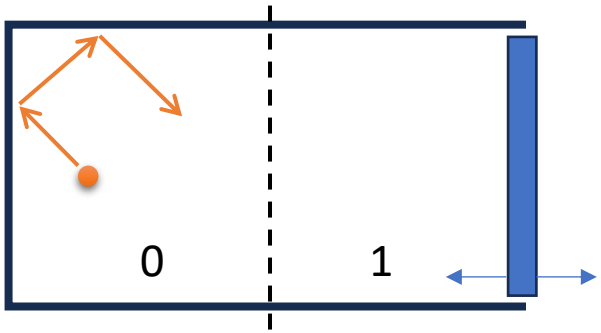
If we could map a computational task onto $|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$ efficiently, we would have a great computational advantage



# How we got there

In the 70's, physicists studied the physics of information

Charles H. Bennett, Richard P. Feynman: Physical limit of heat produced by computation




1 bit of information

1 gas molecule in a box, movable wall

Left = 0 , Right = 1

Erase the stored information by moving (slowly) the wall to the left

Now the state is 0, no matter what it was before erasing

Thermodynamics! Isothermal reversible process at temperature T

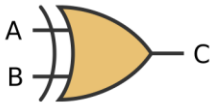
Change of entropy: twice smaller volume of configuration space $\Delta S = -k_B \ln 2$

Heat absorbed by the system: $Q = T\Delta S = -k_B T \ln 2$

**Heat is emitted!** (work done on the moving wall)

# Thermodynamics of computation

An elementary logic gate (XOR) has the same loss of information $\Delta S = -k_B \ln 2$




| A | B | C |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

The minimal dissipated heat (thermodynamics) is $Q = k_B T \ln 2$

Today, consumer electronics still dissipates more than this fundamental limit

Possible solution: reversible logic gates! $\Delta S = 0$

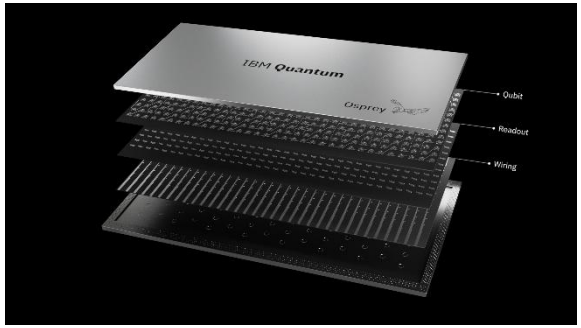
Example: Toffoli gate $(a,\, b,\, c) \rightarrow (a,\, b,\, c \oplus a \wedge b)$

Other possible solution: **Unitary time-evolution of a state of a quantum mechanical system**

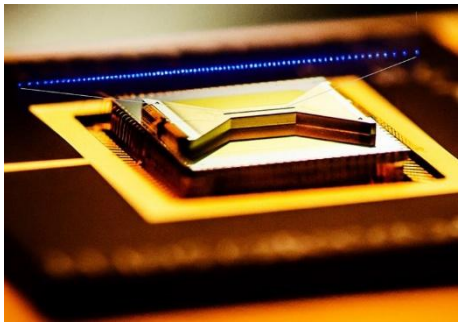
Unitary quantum operations on quantum states are a **new computation paradigm**

# Many candidate quantum computing platforms

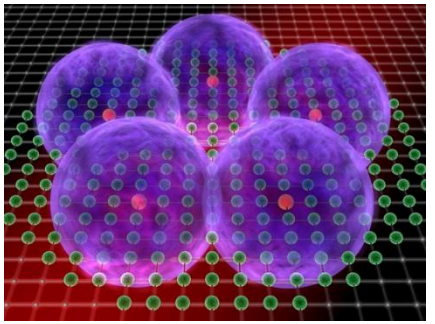
Superconducting circuits



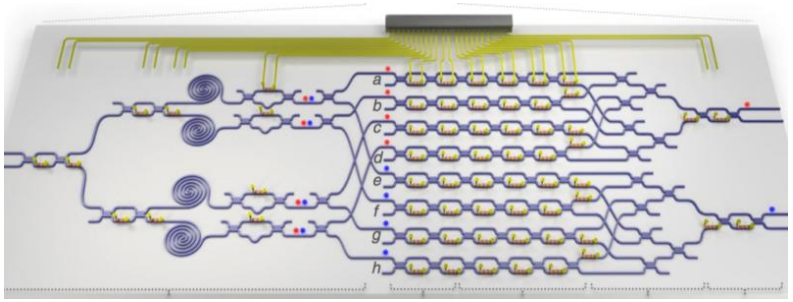

Trapped ions



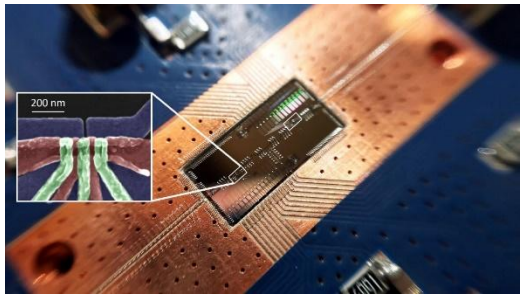
Rydberg atoms



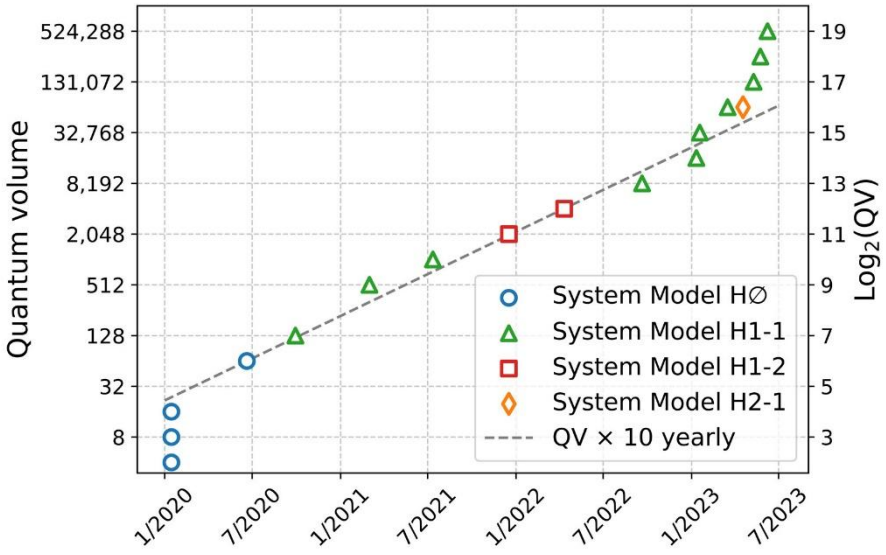
Integrated photonics



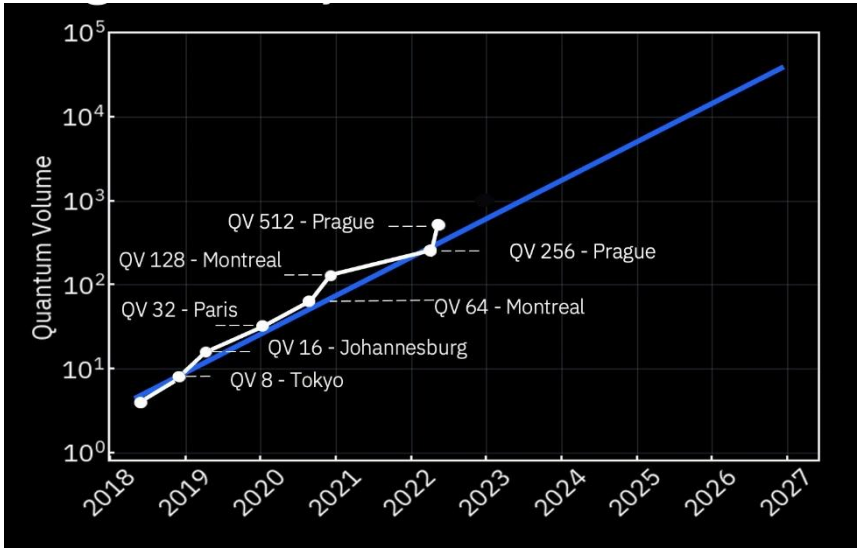

Electron (or hole) spin



# Advances in quantum computing




QUANTINUUM



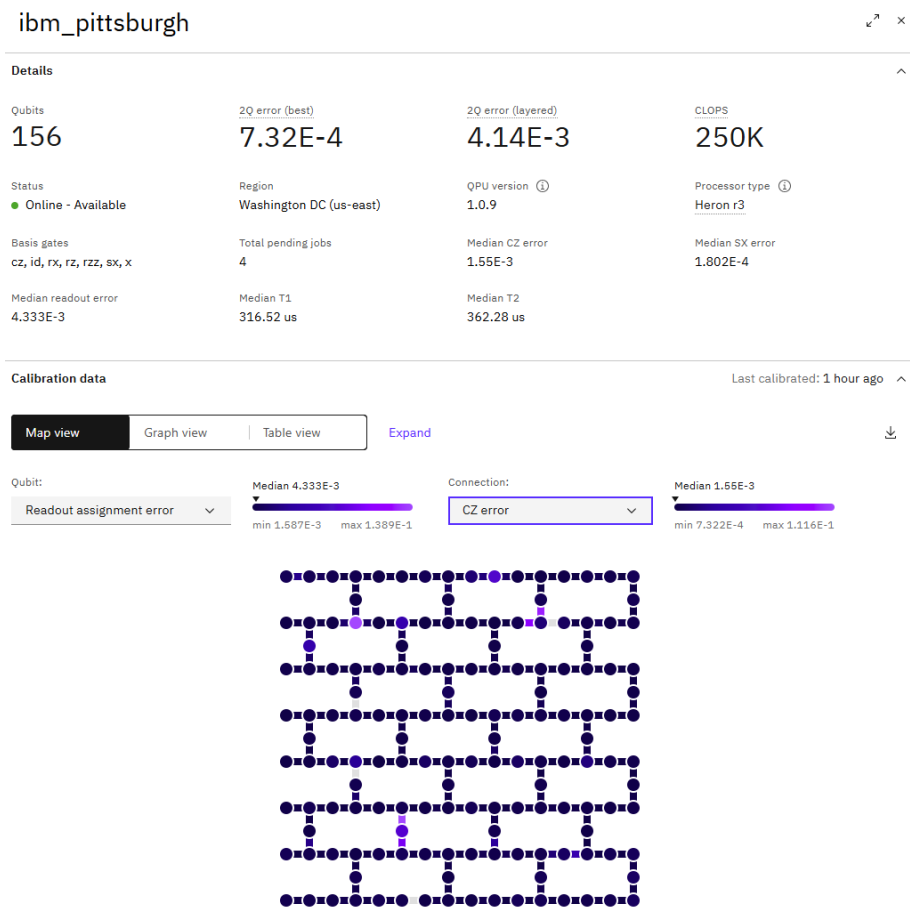

IBM

| | QUANTINUUM QCCD | SUPERCONDUCTING | NEUTRAL ATOM |
|---|---|---|---|
| QUBIT TYPE | Ion (charged atom) | Transmon | Neutral Atom |
| ARCHITECTURE | Quantum Charge-coupled Device | Fixed 2D grid | Neutral atom tweezer array |
| IDENTICAL QUBITS | Yes | No | Yes |
| CONNECTIVITY | All-to-all | Nearest-neighbor | All-to-all |
| MID-CIRCUIT MEASUREMENT AND RE-USE (DEMONSTRATED) | Yes | Yes | Yes |
| QUANTUM VOLUME [1] [2] | 8,388,608 | 512 | Not published |
| 2 QUBIT GATE ERROR RATE [3] [4] [5] | $0.9 \times 10^{-3}$ | $1.4 \times 10^{-3}$ | $4.8 \times 10^{-3}$ |
| 1 QUBIT GATE ERROR RATE [6] [7] [8] | $0.199 \times 10^{-4}$ | $3.5 \times 10^{-4}$ | $2.2 \times 10^{-4}$ |
| STATE PREP AND MEASUREMENT (SPAM) ERROR (%) [9] [10] [11] | 0.15 | 0.67 | 0.6 |
| COHERENCE TIME (μS) [12] [13] [14] | ~1,000,000 | <100 | ~1,000,000 |
| LOGICAL ERROR RATE PER ERROR CORRECTION ROUND (%) (DEMONSTRATED) [12] [13] [14] | 0.022 | 0.143 | 4.9 |
| 2 QUBIT GATE TIME (μS), INCLUDING TRANSPORT OVERHEADS [15] [16] [17] | ~2000 | 0.068 | ~3 |
| CONDITIONAL LOGIC? [18] [19] [20] | Yes | Yes | Yes |
| PARAMETERIZED ANGLE GATES [20] [21] | Yes | Yes | No |
| REAL-TIME DECODING [22] [23] | Yes | Yes | No |

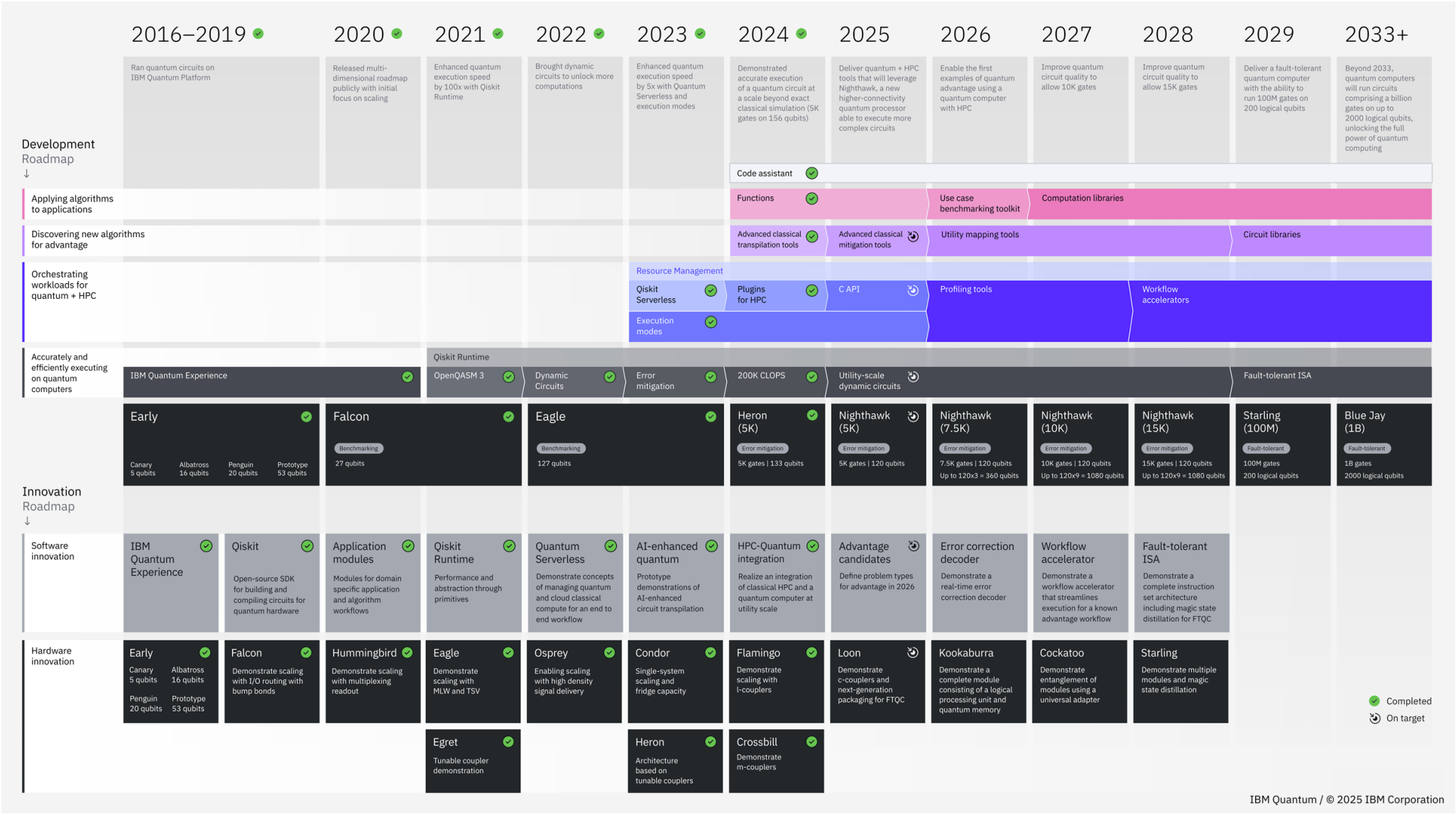
QUANTINUUM

READ THE BLOG

TABLE 1. Leading commercial spec for each listed architecture or demonstrated capabilities on commercial hardware.



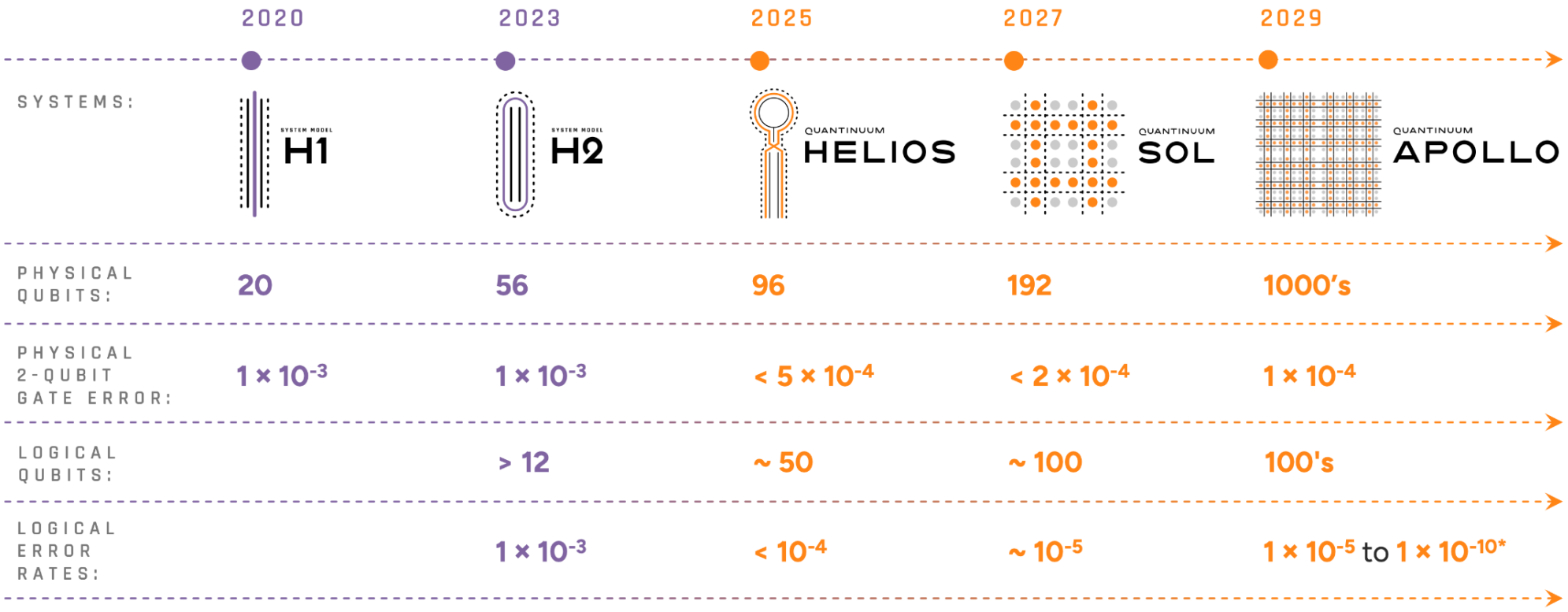
# Advances in quantum computing



# Advances in quantum computing

## Development roadmap

QUANTINUUM

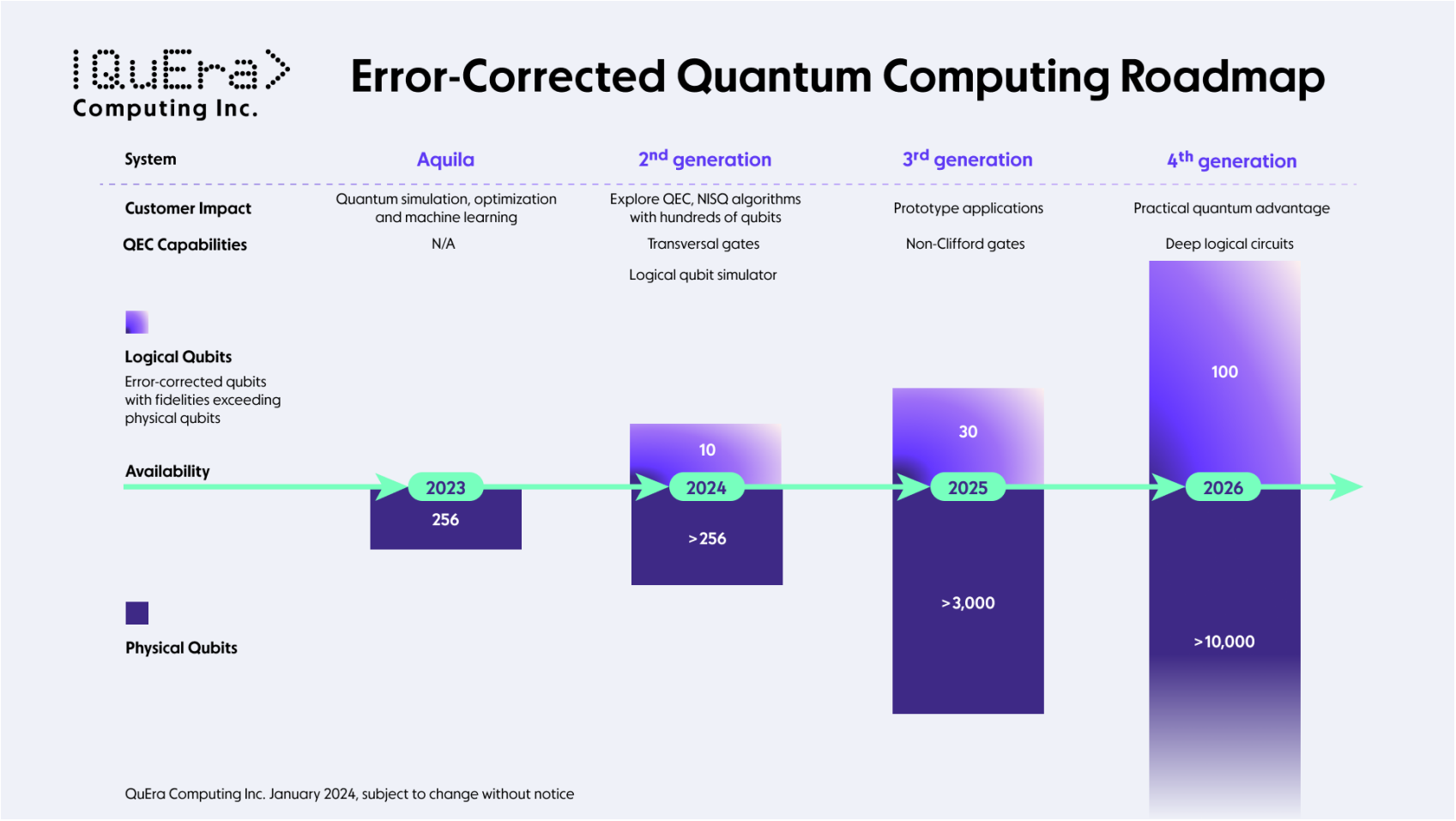




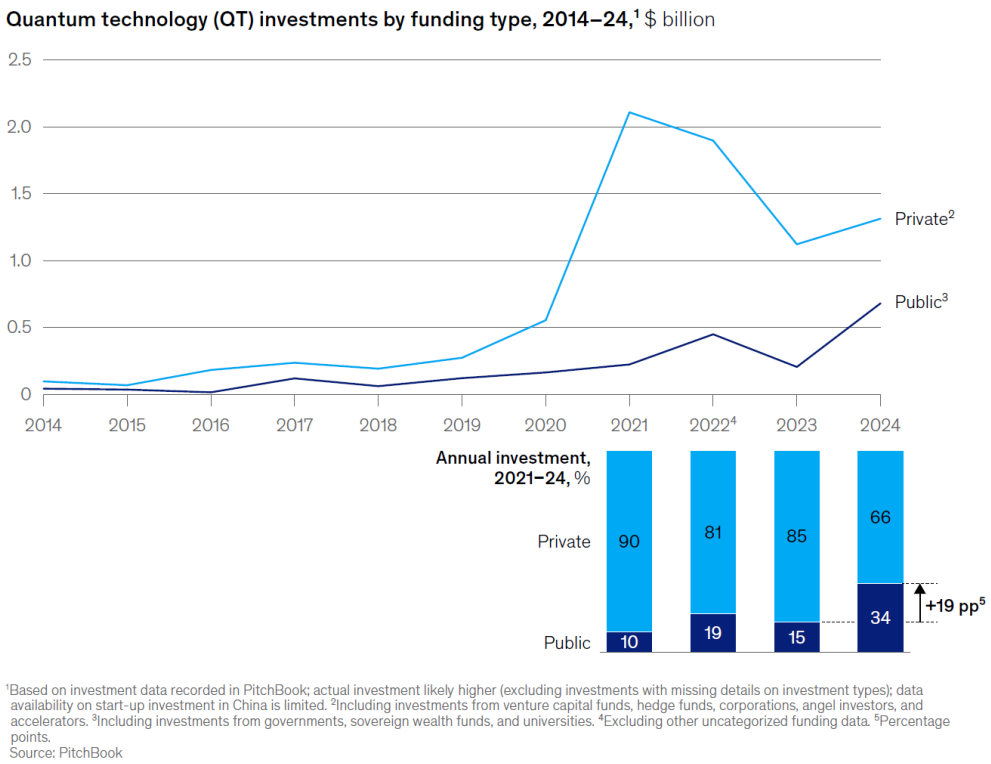

*analysis based on recent literature in new, novel error correcting codes predict that error could be as low as 1E-10 in Apollo (ref: arXiv:2403.16054, arXiv:2308.07915)

# Advances in quantum computing

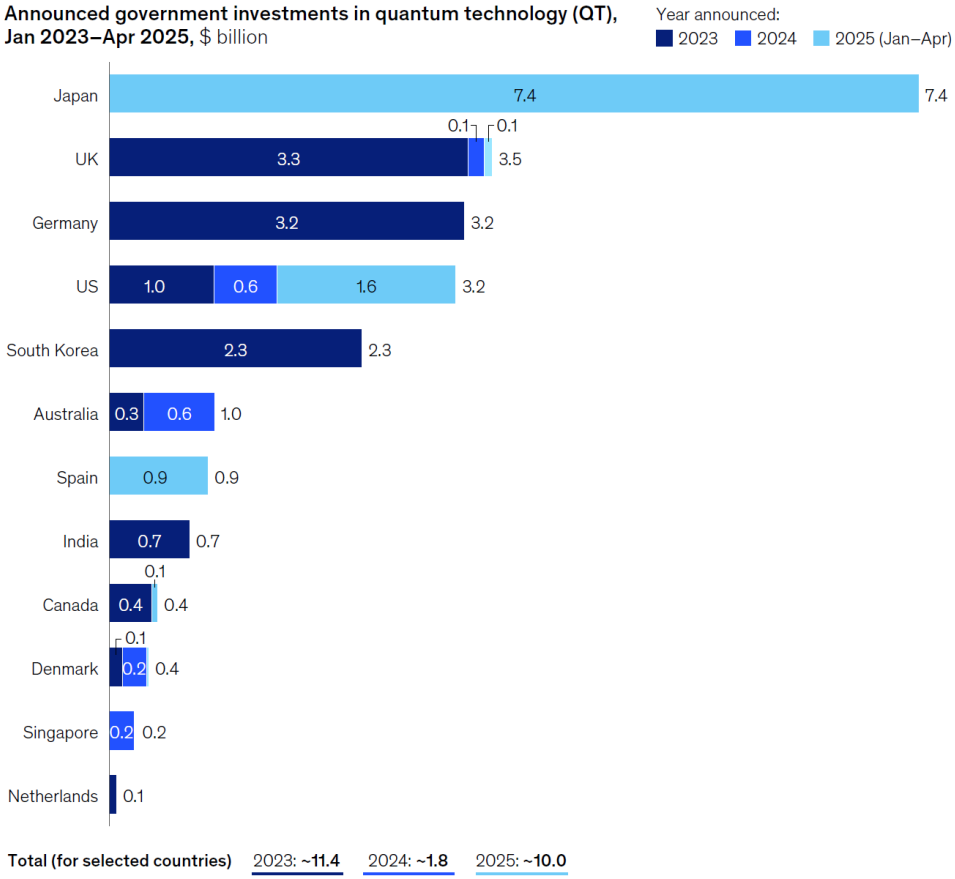
QuEra neutral-atom (Rydberg) quantum computer



# Private and public investment in quantum technology



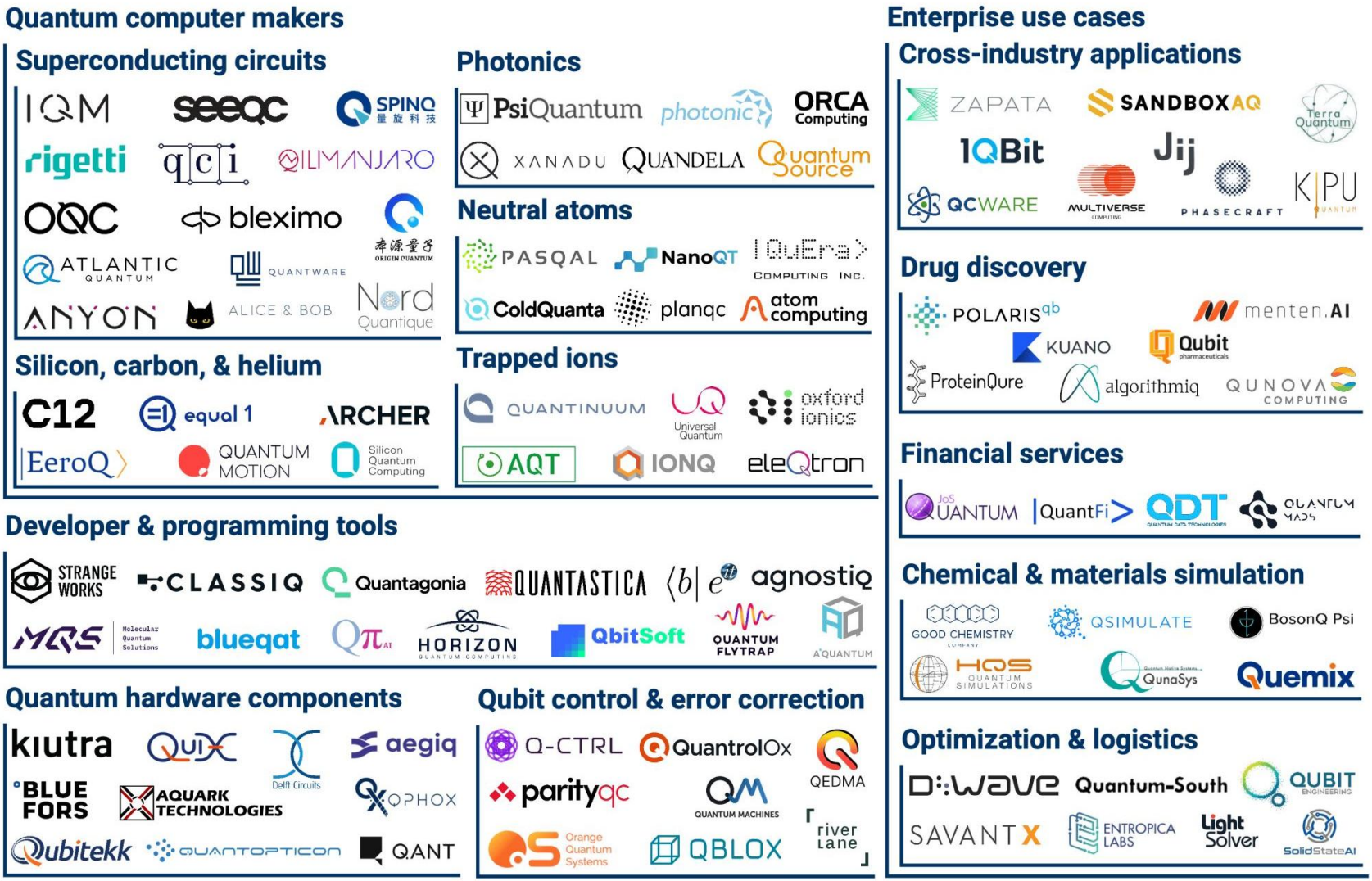

[1]Based on investment data recorded in PitchBook; actual investment likely higher (excluding investments with missing details on investment types); data availability on start-up investment in China is limited. [2]Including investments from venture capital funds, hedge funds, corporations, angel investors, and accelerators. [3]Including investments from governments, sovereign wealth funds, and universities. [4]Excluding other uncategorized funding data. [5]Percentage points.
Source: PitchBook




Note: Figures may not sum, because of rounding. Limited transparency on commercial activity in China; numbers excluding the $136 billion announced investment toward emerging technologies due to unclarity of relevance for QT; the ~$15 billion investment is not shown here because it was announced before 2023. Numbers also excluding $680 million in Swedish investments toward research and innovation, and US–Swedish investment of $40 million toward next-generation networks, AI, quantum technology, and educational science within STEM areas. Also excluding Saudi Arabia's $6.4 billion investment in 2022 toward future tech because no breakdown for quantum technology is present; excluding Qatar's (QIA) and Bpifrance's investment in Alice & Bob in 2025 due to missing breakdown of investment. Japan's investment is not exclusively directed toward quantum technology (includes next-generation chip design as well).
Source: Press search

Quantum Technology Monitor Report
McKinsey & Company 2025

# A growing ecosystem



# What can a quantum computer do?

A widespread concept is that of **“quantum parallelism”**

$$|\psi\rangle = |\text{cat}_1\rangle + |\text{cat}_2\rangle + \ldots + |\text{cat}_N\rangle$$

A single quantum register can apparently store **exponentially more information** than a classical one

One operation on the quantum register will be carried out **“in parallel”** on all stored items

**This simple picture of quantum parallelism is not useful**. A **readout** of the quantum register is a **quantum measurement**. It will **return a random item** and destroy the remaining information through **state collapse**

$$|\psi\rangle = |\text{cat}_1\rangle + |\text{cat}_2\rangle + \ldots + |\text{cat}_N\rangle$$

readout

$$|\psi\rangle = |\text{cat}_2\rangle$$

**Need for algorithms that use quantum superposition to take advantage of quantum parallelism**

# What can a quantum computer do?

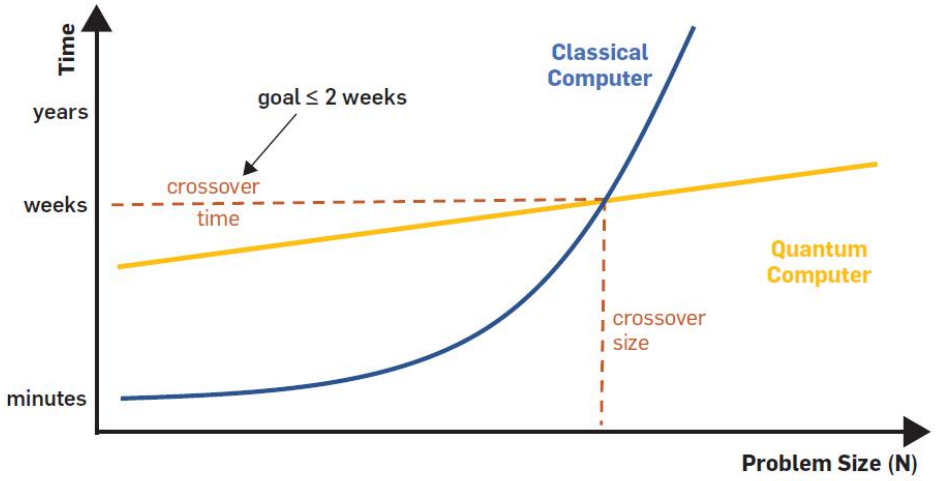
Quantum computers can solve **some** computational problems **better** than conventional computers

**some:** A quantum computer is not a universal tool

Among problems with **quantum advantage**, many have very high societal benefit

**better:** **Quantum advantage** is not just “faster”

It is about how **computational time** scales with **problem size**



# A quantum algorithm zoo

https://quantumalgorithmzoo.org/

Today there are **hundreds of useful quantum algorithms** ready for future quantum hardware

**Quantum Phase estimation (1995).**

**Estimate an eigenvalue of a unitary operator** with error $\varepsilon$, using $O(\log(1/\varepsilon))$ qubits and $O(1/\varepsilon)$ operations. Used as a primitive in many algorithms, like Shor or HHL. **Simulate energy levels of complex Hamiltonians efficiently.**

**Quantum Amplitude estimation / amplification (2000).**

Estimate or amplify one component in a given quantum state. Useful primitive in several algorithms, like e.g. Grover's algorithm or Quantum accelerated Monte Carlo sampling.

**Quantum Fourier Transform (1994).**

Compute discrete Fourier transform of $2^n$ amplitudes with complexity $O(n^2)$. Primitive ubiquitous in many computational tasks, from Shor to data science.

# A quantum algorithm zoo

https://quantumalgorithmzoo.org/

Today there are **hundreds of useful quantum algorithms** ready for future quantum hardware

**Shor's algorithm (1994)**.

Compute a prime factor of a n-qubit integer with $O(n^2 \log(n) \log(\log(n)))$ gates. Best known classical algorithm requires $\exp(O(n^{1/3} \log(n)^{2/3}))$ time

**Grover's algorithm (1996).**

Search an unstructured database of N entries with $O(N^{1/2})$ gates. Best classical algorithm requires time O(N). There's proof that $O(N^{1/2})$ is optimal according to quantum mechanics. Evidence that quantum computers can't solve NP-complete problems.

**Digital quantum simulation (1996).**

Compute $U = e^{-iHt}$ on n qubits with $O(n^3 \log(n))$ gates. Classical algorithms are exponential.

# A quantum algorithm zoo

https://quantumalgorithmzoo.org/

Today there are **hundreds of useful quantum algorithms** ready for future quantum hardware

**Quantum solution of linear systems of equations (HHL algorithm) (2008).**

Estimate (a measurement on) **the solution of a linear system of N equations** with O(log(N)) complexity. Ubiquitous applications: electromagnetic scattering, linear differential equations, finite element simulations, least-square fitting, machine learning and data science.

**Quantum-accelerated Monte Carlo sampling (2015).**

Sample a function of a random variable (st.d. $\sigma$) with accuracy $\varepsilon$, using $O(\sigma/\varepsilon)$ samples, instead of $O(\sigma^2/\varepsilon^2)$. Ubiquitous use in science, and finance (risk analysis, derivative pricing)

# How to deal with errors

Digital electronics is subject to errors (cosmic rays!). **Today's error rate is $10^{-10}$ errors/bit/hour**

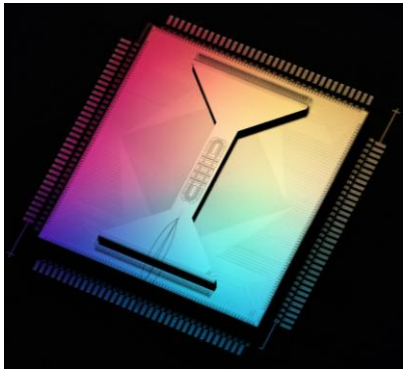
https://en.wikipedia.org/wiki/ECC_memory

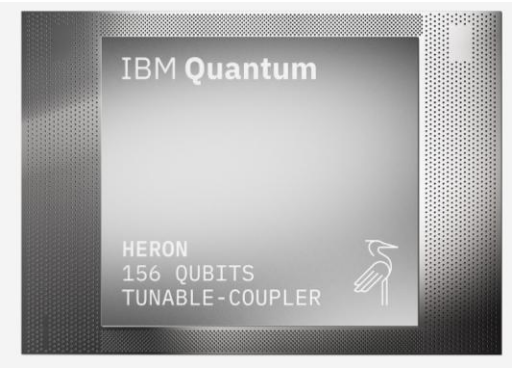
**Errors in digital electronics are not corrected!**

https://arstechnica.com/gadgets/2021/01/linus-torvalds-blames-intel-for-lack-of-ecc-ram-in-consumer-pcs/

In quantum computers errors are an issue for two reasons

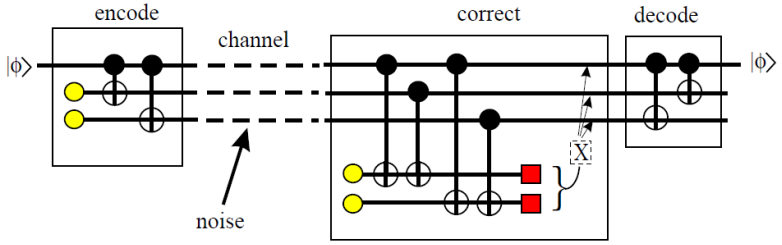
1. Error rates. One-qubit gate: $1x10^{-4}$; two-qubit gate: $1x10^{-3}$; one-qubit readout: $5x10^{-3}$ (as of 2025)
2. Error correction requires information readout, which is a destructive process because of collapse. Need an agnostic error correction scheme





# How to deal with errors: two roads

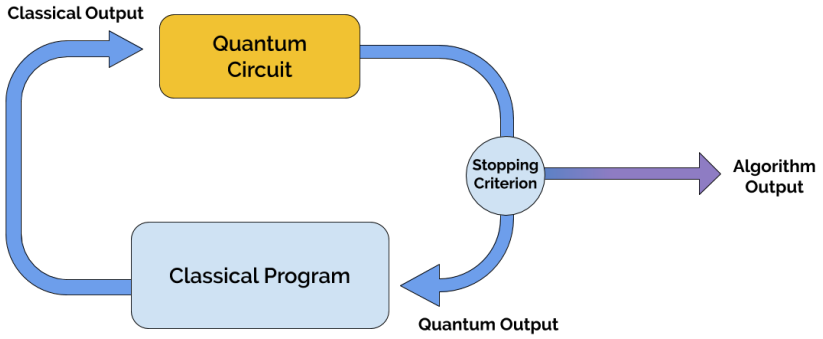
**Fault-tolerant quantum computing**: **Correct errors** with Quantum Error Correction Codes (QECC)




Timescale to achievement: decades

**Hybrid algorithms on Noisy Intermediate-Scale Quantum (NISQ) hardware: Do not correct errors.**

Make quantum subroutines as short ("shallow") as possible. Combine with classical processing. Estimate result from statistical inference of noisy output. Use error mitigation schemes.




Timescale to achievement: years

*Noisy intermediate-scale quantum algorithms*, Rev. Mod. Phys. 94, 015004 (2022)
*Variational quantum algorithms*, Nature Reviews Physics 3, 625 (2021)

# Hybrid variational quantum algorithms

Among the most important Variational Quantum Algorithms are:

**The Variational Quantum Eigensolver (2014).**

Estimate the ground state energy of a quantum system using a parametrized representation of the quantum state. Holds great promise for the simulation of molecules and materials.

**The Quantum Approximate Optimization Algorithms (2014).**

Finds an approximate solution to a discrete unconstrained optimization problem. It is a digital version of the quantum annealing process. Many applications in industrial processes, transportation, climate, medicine, etc.

**The Quantum Variational Dynamics (2017).**

Estimate the time evolution of a quantum state governed by a given Hamiltonian, using a parametrized representation of the state.

# Lots of Promises

Article | Open access | Published: 14 June 2023

## Evidence for the utility of quantum computing before fault tolerance

Youngseok Kim, Andrew Eddins, Sajant Anand, Ken Xuan Wei, Ewout van den Berg, Sami Rosenblatt, Hasan Nayfeh, Yantao Wu, Michael Zaletel, Kristan Temme & Abhinav Kandala

*Nature* **618**, 500–505 (2023) | Cite this article

IBM

## Demonstration of Algorithmic Quantum Speedup for an Abelian Hidden Subgroup Problem

Phattharaporn Singkanipa[1,2], Victor Kasatkin[3,2], Zeyuan Zhou[4], Gregory Quiroz[4,5], and Daniel A. Lidar[6,7]

Show more

Phys. Rev. X **15**, 021082 – **Published 5 June, 2025**

DOI: https://doi.org/10.1103/PhysRevX.15.021082

arXiv > quant-ph > arXiv:2503.20870

**Quantum Physics**

*[Submitted on 26 Mar 2025 (v1), last revised 11 Apr 2025 (this version, v2)]*

## Digital quantum magnetism at the frontier of classical simulations

QUANTINUUM

# The flagship quantum computing problem: factoring

arXiv > quant-ph > arXiv:2505.15917v1

Quantum Physics

[Submitted on 21 May 2025]

**How to factor 2048 bit RSA integers with less than a million noisy qubits**

Craig Gidney

Article | Open access | Published: 16 August 2021

**Demonstration of Shor's factoring algorithm for N = 21 on IBM quantum processors**

Unathi Skosana & Mark Tame

*Scientific Reports* **11**, Article number: 16599 (2021) | Cite this article

2025/1237 (PDF)

Last updated: 2025-09-07

**Replication of Quantum Factorisation Records with an 8-bit Home Computer, an Abacus, and a Dog**

Attacks and cryptanalysis

*Peter Gutmann and Stephan Neuhaus*

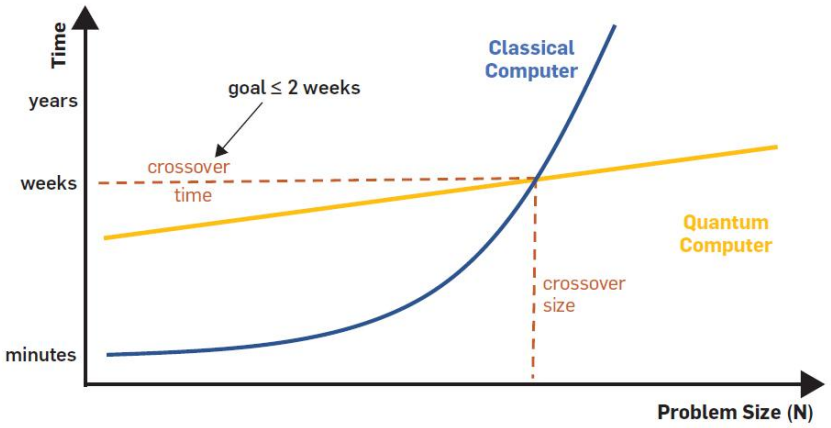
Hide abstract -

This paper presents implementations that match and, where possible, exceed current quantum factorisation records using a VIC-20 8-bit home computer from 1981, an abacus, and a dog. We hope that this work will inspire future efforts to match any further quantum factorisation records, should they arise.

Cryptology ePrint Archive (2025)

# Truth is in the middle

Upper bound on the n. of operations for a quantum algo to crossover in two weeks




We determine the number of operations that can be afforded per function call (see the accompanying figure) for a quantum computer to show an advantage over a classical computer using a quantum algorithm with quadratic, cubic, and quartic quantum speedup. The number of oracle calls required to reach the crossover point with a quadratic, cubic, and quartic speedup is computed using the relative runtimes of a single oracle evaluation, and the total runtime of $10^6$ seconds is then used to compute how many basic operations can be afforded in each oracle call. Since we make optimistic assumptions for a future quantum computer, we ignore overheads of reversible arithmetic for quantum computing and limit the classical computer to a single chip that can be manufactured today. The actual crossover operation counts will be significantly smaller. A similar analysis for quantum algorithms with exponential speedups yields promising operation budgets for all datatypes.

**Maximum number of operations for practical**

| Operation type | quadratic speedup | cubic speedup | quartic speedup |
|---|---|---|---|
| 16-bit floating point | 0.2 | 45,800 | 2,800,000 |
| 32-bit integer | 0.003 | 1,630 | 130,000 |
| Binary (logical) | 68 | 12,500,000 | 712,000,000 |

Quantum practicality requires algorithms with **at least $N^4$ speedup and small input data**

Candidate tasks: **Simulations of quantum chemistry and materials**

> *"Innovations in chemistry and material science are estimated to have an impact on 96% of all manufactured goods, which impact 100% of humanity"*
>
> Matthias Troyer, Microsoft

*Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage*

T. Hoefler, T. Häner, M. Troyer, Commun. of the ACM **66**, 82 (2023)

# Recent breakthroughs in quantum error correction

Article | Published: 29 April 2024

## Constant-overhead fault-tolerant quantum computation with reconfigurable atom arrays

Qian Xu, J. Pablo Bonilla Ataides, Christopher A. Pattison, Nithin Raveendran, Dolev Bluvstein, Jonathan Wurtz, Bane Vasić, Mikhail D. Lukin, Liang Jiang & Hengyun Zhou

*Nature Physics* **20**, 1084–1090 (2024) | Cite this article

nature

https://doi.org/10.1038/s41586-025-09367-3

Accelerated Article Preview

## Experimental demonstration of logical magic state distillation

arXiv > quant-ph > arXiv:2506.00579

Quantum Physics

*[Submitted on 31 May 2025]*

## Observation of a Fault Tolerance Threshold with Concatenated Codes

Grace M. Sommers, Michael Foss-Feig, David Hayes, David A. Huse, Michael J. Gullans

Article | Open access | Published: 09 December 2024

## Quantum error correction below the surface code threshold

Google Quantum AI and Collaborators

*Nature* **638**, 920–926 (2025) | Cite this article

# Outline

1. General introduction
2. A short overview of quantum mechanics
3. The paradigm of digital quantum computing
4. Universal quantum gates and the Solovay-Kitaev theorem
5. Deutsch and Deutsch-Jozsa algorithms
6. Shor's factoring algorithm
7. Grover's search algorithm
8. Overview of other algorithms
9. The theory of open quantum systems and noisy quantum channels
10. Errors and quantum error correction
11. Fault-tolerant quantum error correction
12. Hybrid quantum algorithms: the variational quantum eigensolver
13. Hybrid quantum algorithms: the quantum approximate optimization algorithm
14. Hybrid quantum algorithms: the variational quantum dynamics simulation
15. Current challenges in quantum computing: an outlook.

# Public investment in quantum computing