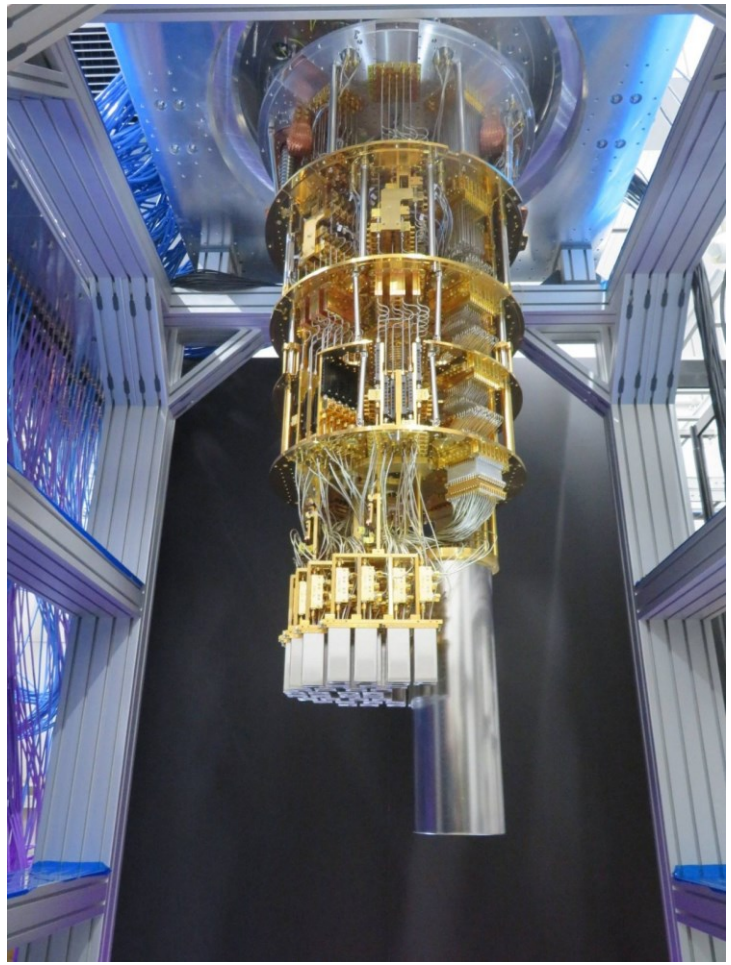
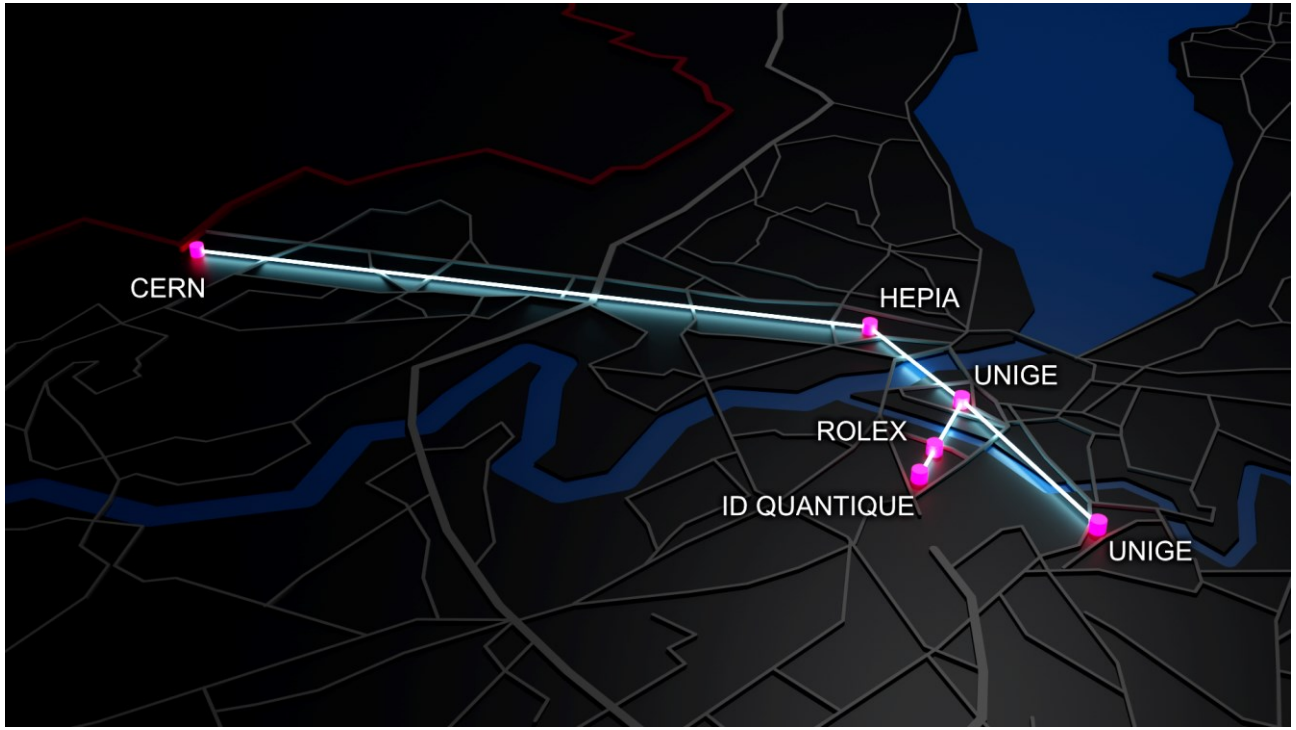
What is Quantum Computing ?

March 2026



quantum computer from
Fujitsu and Riken Institute
(April 2025)

Actualité !



Geneva Quantum Network (illustration Xavier Ravinet, October 2025)

Nobel Prize in Physics 2025

Ill. Niklas Elmehed © Nobel Prize Outreach

John Clarke

Prize share: 1/3

Ill. Niklas Elmehed © Nobel Prize Outreach

Michel H. Devoret

Prize share: 1/3

Ill. Niklas Elmehed © Nobel Prize Outreach

John M. Martinis

Prize share: 1/3

The Nobel Prize in Physics 2025 was awarded jointly to John Clarke, Michel H. Devoret and John M. Martinis "for the discovery of macroscopic quantum mechanical tunnelling and energy quantisation in an electric circuit"

Royal Swedish Academy of Sciences (October 2025)

Sommaire

Introduction

Quantum computing…

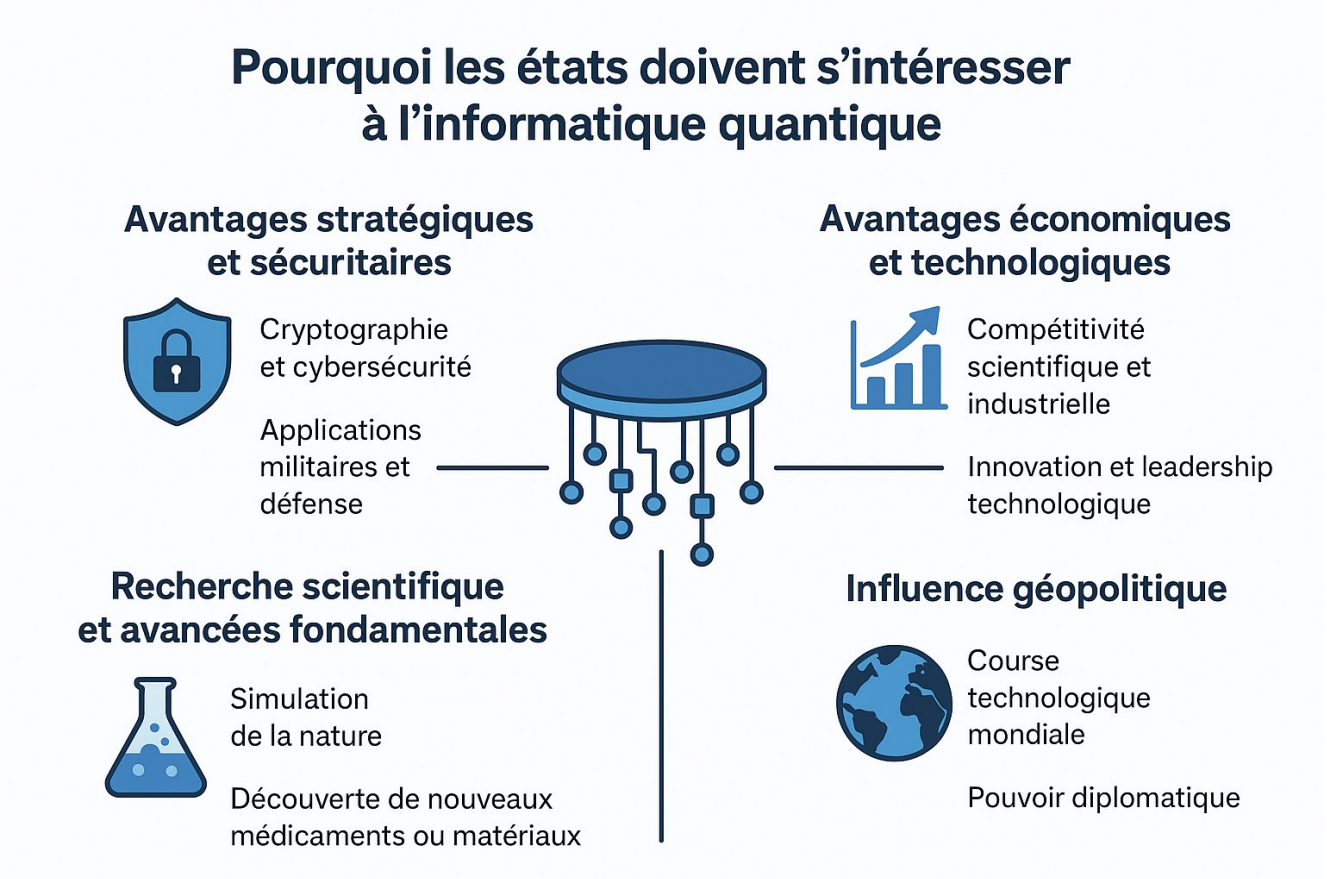
❑ Why do I care ?

Technology watch, 20 years of research in mathematical physics, currently writing a monograph on quantum mechanics with a professor from Nagoya University

❑ Why should organisations care ?

National security agencies (NCSC in the UK, NIST in the US, etc.) estimate that quantum computers could be able of breaking current encryption systems by 2035. But there is much more :

illustration ChatGPT (in French, September 2025)



Introduction

What is Quantum Computing ?

Quantum computing is a branch of computer science that relies on the principles of quantum mechanics to encode and process information.

Unlike classical computing, which uses bits (0 or 1), it uses qubits governed by the laws of quantum mechanics.

→ Will make possible to solve certain problems beyond the capabilities of classical computers.

Fundamental principles

A qubit («quantum bit») is the unit of information in quantum computing. It can be in the states $|0\rangle$, $|1\rangle$, or in a superposition

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

with α and β complex amplitudes, $|\alpha|^2 + |\beta|^2 = 1$.

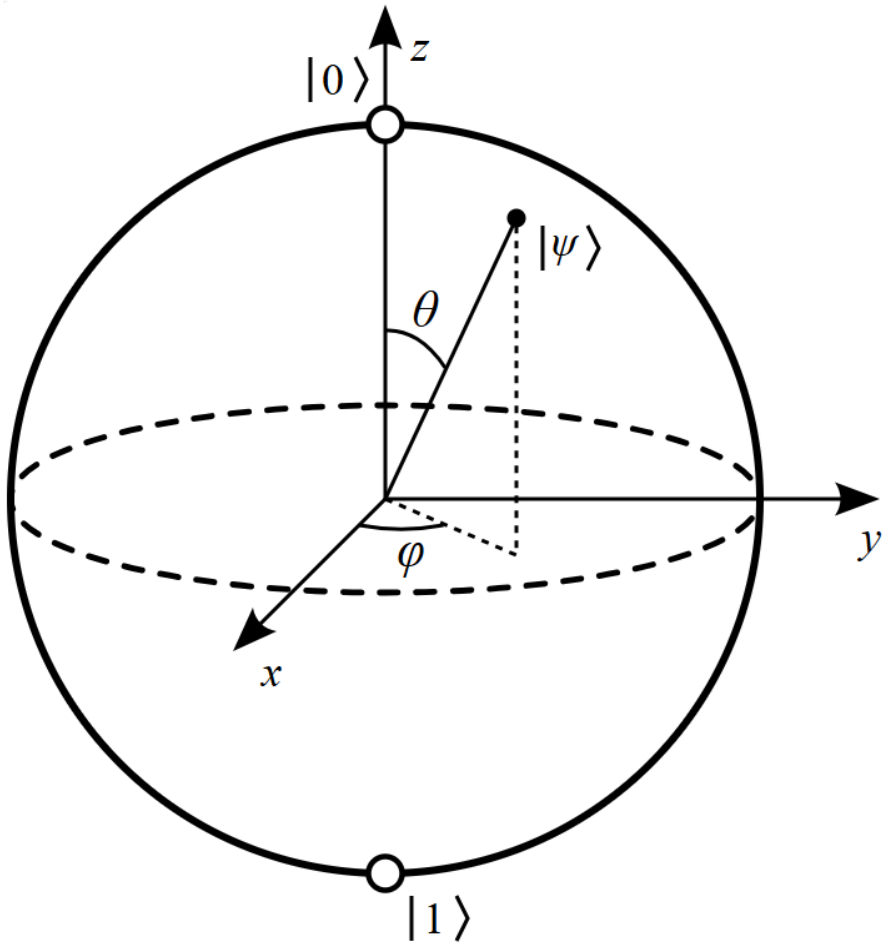
($|\psi\rangle$ can be represented as a point on a sphere of radius 1 called the « Bloch sphere»)

Several approaches to manufacturing qubits :

- ❑ Supraconductor Qubits (Google, IBM, Rigetti, Intel)
- ❑ Trapped ions (IonQ, Quantinuum)
- ❑ Spin qubits (Intel, Silicon Quantum Computing)
- ❑ Photonic qubits (Xanadu)

Not yet clear which technologies will prevail…

Bloch sphere (Wikipedia, September 2025)



Fundamental principles

The principles of quantum mechanics used in quantum computing are (among others) :

❑ **Superposition and interference of wave functions**
(qubits can be in superposition of several states simultaneously)

For example : $\left(\frac{1}{2}|0\rangle + \frac{1}{4}|1\rangle\right) + \frac{1}{4}|0\rangle = \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$

❑ **Entanglement of wave functions**
(qubits can be correlated «instantly», even at a distance)

For example : $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ (famous example called «Bell state»)

❑ **Collapse of wave functions during a measurement**
(the classical state of a quantum system is determined when it is measured/observed)

For example : $\frac{1}{2}|0\rangle + \sqrt{\frac{3}{4}}|1\rangle \longrightarrow$  $\longrightarrow |1\rangle$

Fundamental principles

Quantum logic gates («quantum gates») are the equivalent of classical logic gates such as AND, OR, NOT, etc., but they operate on qubits rather than bits.

Quantum gates...

- ❑ transform the state of qubits in a quantum circuit
- ❑ perform reversible transformations (unlike classical gates, which can be irreversible)
- ❑ are represented mathematically by unitary matrices (which guarantees reversibility + conservation of the norm of wave functions)

Fundamental principles

Unitary matrices stem from the Schrödinger equation in finite dimension...

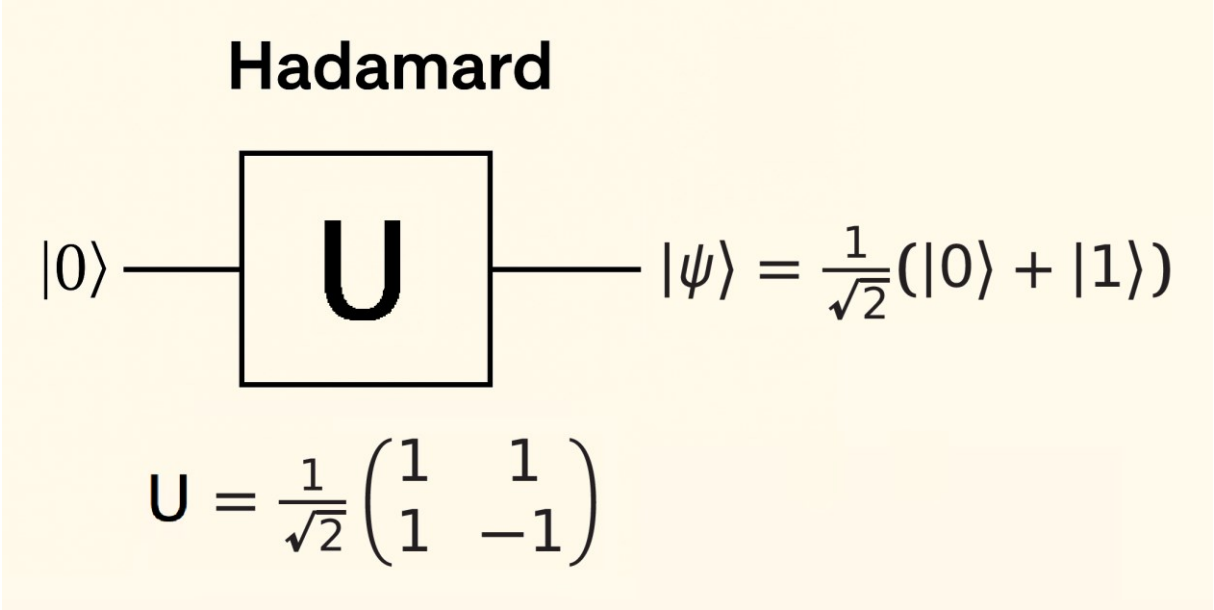
$$i\frac{\mathrm{d}}{\mathrm{dt}}|\psi(t)\rangle = H|\psi(t)\rangle \iff |\psi(t)\rangle = \mathrm{e}^{-itH}|\psi(0)\rangle \quad (H = \text{hermitian matrix})$$

... and in discrete time $t = n$:

$$|\psi(n)\rangle = (\mathrm{e}^{-iH})^n|\psi(0)\rangle \iff |\psi(n)\rangle = U^n|\psi(0)\rangle \quad (U = \text{unitary matrix})$$

Fundamental principles

Example of quantum gate :

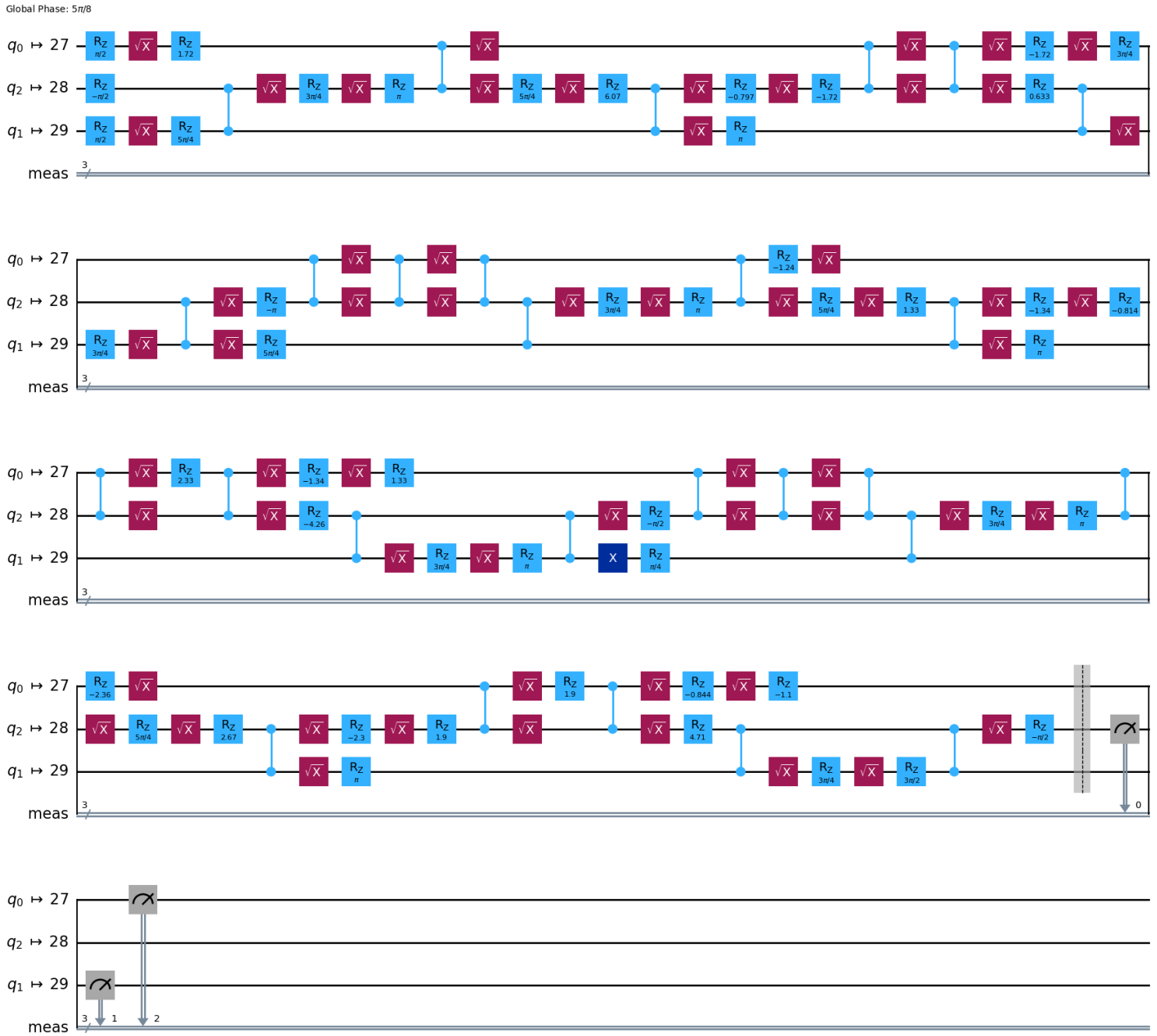


Fundamental principles

Example of a 3-qubit circuit run on the «ibm_sherbrooke» quantum computer on May 7, 2025.

Programming and diagram created using the open-source Python library Qiskit, introduced by IBM Research in 2017.

(diagram to be read like a musical score...)



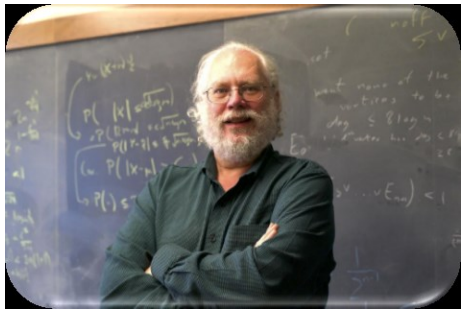
Applications

Two iconic algorithms illustrate the risks and opportunities brought by quantum computing.

❑ **Shor's algorithm(«risk») :**
Makes possible (with a fully functional quantum computer) the factorisation of large numbers in exponentially less time than with classical computers.

→ Will make possible breaking various public key encryption protocols such as RSA, Diffie-Hellman, elliptic curves, etc.

CERN (March 2021)



❑ **Grover's algorithm(«opportunity») :**
Makes possible (with a fully functional quantum computer) the search for an element in an unordered list in quadratically less time than with classical computers.

→ Will improve the speed of multiple industrial applications based on searching for an optimal element/configuration in a large set.

dotquantum.io (unknown date)

(the previous circuit implements Grover's algorithm for a list of $2^3 = 8$ éléments 😀)

Applications

There are numerous areas of application for quantum computing, at various stages of development (academic research, proof of concept, or already deployed) :

- ❑ Cryptography and cybersecurity
- ❑ Optimisation and operational research
- ❑ Simulation of physical and chemical systems
- ❑ AI and Machine Learning
- ❑ Data science and information retrieval
- ❑ Quantum communication
- ❑ Quantum metrology and sensors
- ❑ Finance and economics

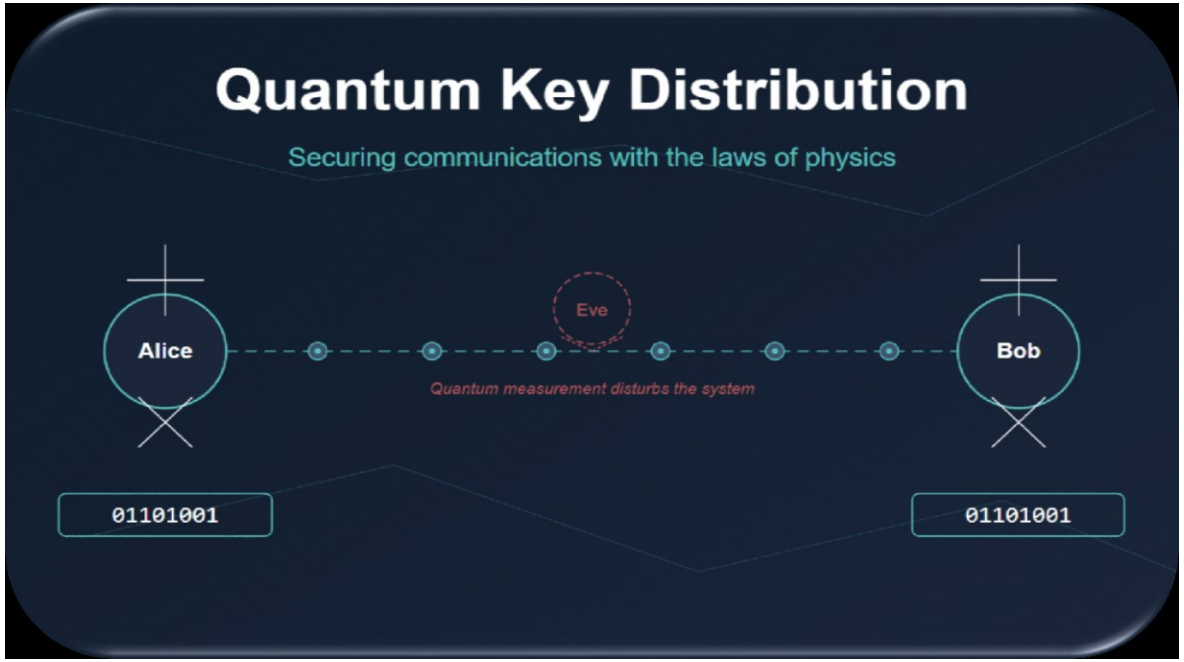


illustration Pranav Sanghadia (April 2025)

(tested by Geneva State for electronic vote between 2007 and 2014)

Current limitations and challenges

Quantum computing is still in its NISQ (Noisy Intermediate-Scale Quantum) phase. The main challenges are :

- ❑ Improved stability (coherence time), reliability, and number of qubits
- ❑ More affordable error correction methods (cost and infrastructure)
- ❑ Discovery of more useful quantum algorithms

Progress is rapid, but it will take years (or decades) to develop fault-tolerant quantum computers capable of solving problems beyond the reach of classical computers.

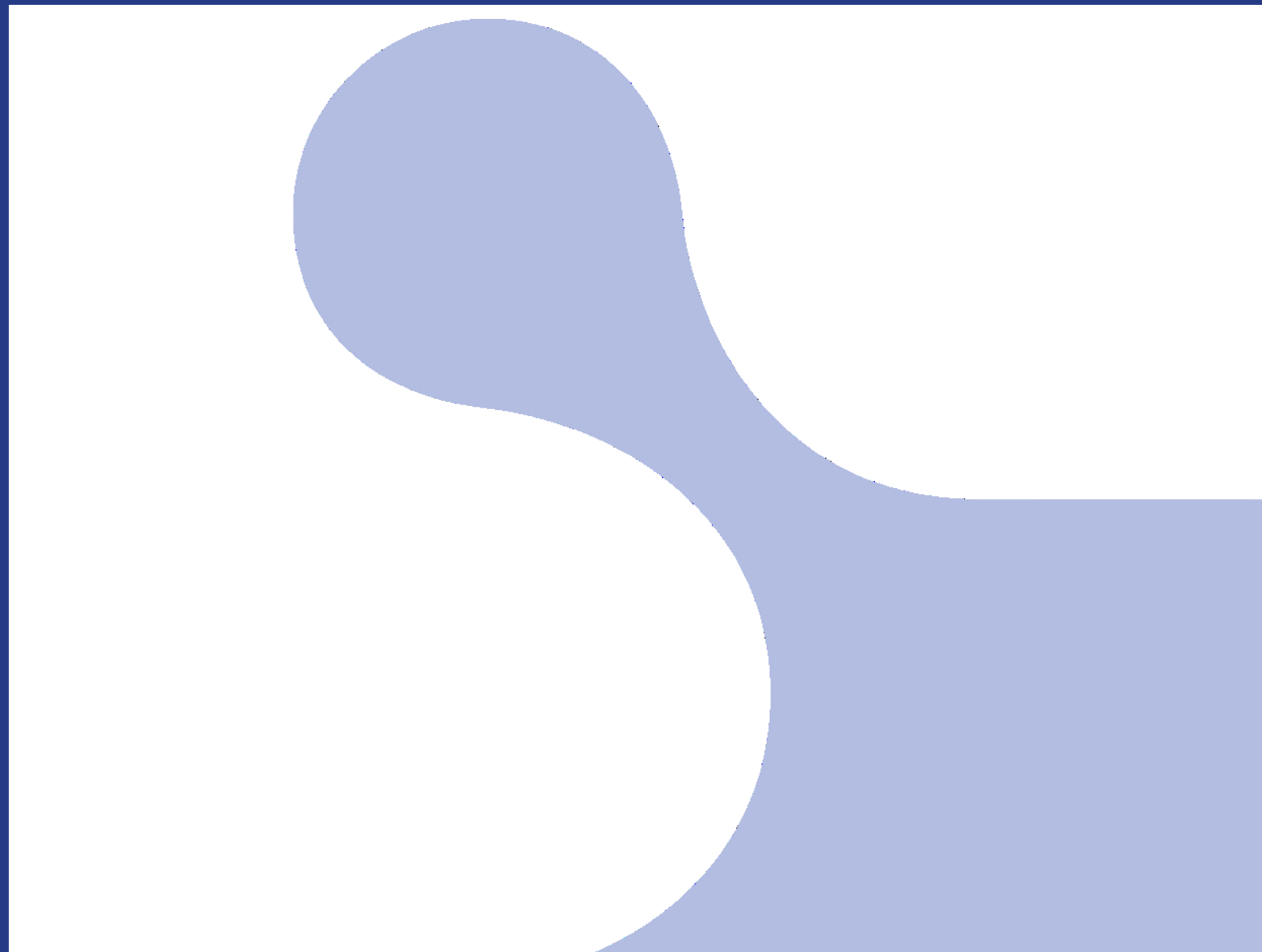
Some actions already taken (not public)

Quelques actions déjà menées par l'équipe IA-OCSIN :

- Présentation (brève) du sujet au Secrétariat Général du DIN
- Premiers tests sur les ordinateurs quantiques de IBM Quantum
- Participation à une table ronde Quantum EPFL
- Compilation de ressources et cours en informatique quantique
- Discussions avec :
  - Délégué au numérique du canton
  - Chef de service sécurité de l'information OCSIN
  - Directeur adjoint du support et des opérations de votre de la Chancellerie d'Etat
  - Consultant stratégie open source OCSIN (ex IO Quantique SA)
  - Open Quantum Institute du CERN
  - Geneva Science and Diplomacy Anticipator (GESDA)
  - Quantum Center (ETH Zurich)
  - D-Wave Quantum Inc. (entreprise US de quantum annealing)
  - Directeur DTN de (HUG)
  - Groupe Quantum (UNIGE)

En cours :

- Trouver une solution pérenne pour un accès à des ordinateurs quantiques
- Recherche de use-cases possibles et utiles pour l'Etat de Genève



Rafael Tiedra

References

Quantum Computing :

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

https://quantum.cloud.ibm.com/learning/en/courses/basics-of-quantum-information

https://quantum.cloud.ibm.com/learning/en/courses/fundamentals-of-quantum-algorithms

https://quantum.cloud.ibm.com/learning/en/courses/quantum-machine-learning/introduction

https://en.wikipedia.org/wiki/Introduction_to_Quantum_Mechanics_(book) (for enthusiasts)

Post-Quantum Cryptography :

https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

https://quantum.cloud.ibm.com/learning/en/courses/quantum-safe-cryptography

https://www.coursera.org/learn/advanced-data-structures-rsa-and-quantum-algorithms

Python Libraries :

https://pennylane.ai/

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