

calcul quantique
usages, état de l'art et défis

#QEI
the quantum energy initiative

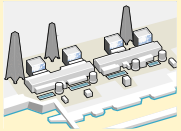
Olivier Ezratty
⟨ ... | quantum engineer | QEI cofounder | ... ⟩
olivier@oezratty.net **www.oezratty.net** **@olivez**

JCAD, Nantes, 6 octobre 2026

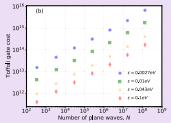
ambitions du calcul quantique



- **résoudre plus vite certains problèmes complexes.**
- **rendre accessibles des calculs impossibles classiquement.**



- **réduire potentiellement la consommation d'énergie** (question ouverte)**.**

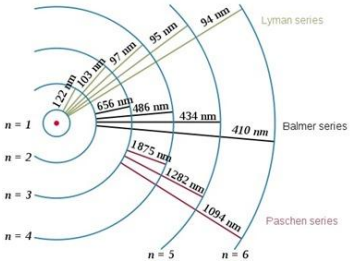


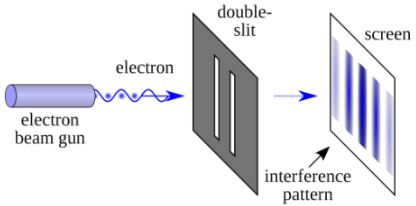
- **améliorer la qualité des résultats** (heuristique, précision chimique).

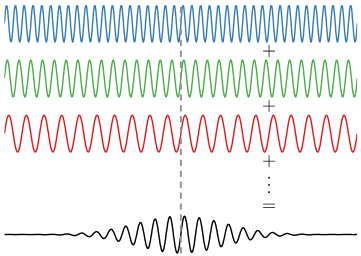


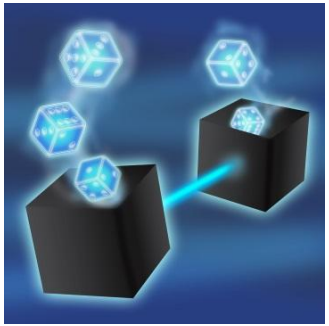
- **utilité** qui dépend de l'utilisateur (recherche scientifique, industriels, gouvernements).

qu’est-ce être « quantique »?









quantification

propriétés physiques discrètes: niveaux d’énergie, projection du spin, …

objets quantiques à deux niveaux (qubits)

dualité onde-particule

électrons, photons, atomes, neutrons

interférences utilisées dans les algorithmes quantiques

superposition d’état

liée à la dualité et à la linéarité de l’équation de Schrödinger

espace mémoire interne de 2^N nombres complexes + mesure probabiliste

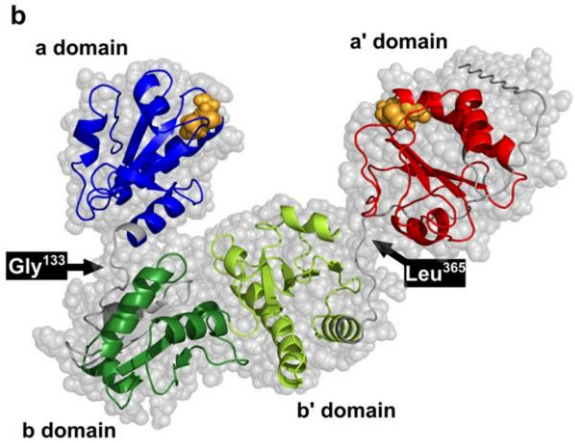
intrication

corrélation d’états distants lors d’une mesure aléatoire

interactions entre qubits, contribuent à l’accélération quantique

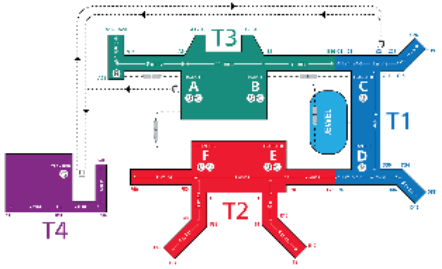
+ contrôle individuel d’objets quantiques (atomes, électrons, photons

problèmes cibles typiques

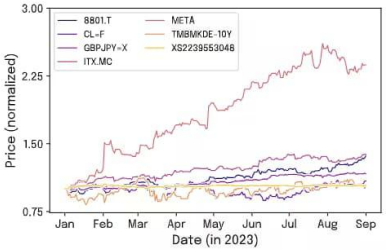


$$i\hbar \frac{\partial \Psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m} \frac{\partial^2 \Psi(x,t)}{\partial x^2} + V(x)\Psi(x,t)$$

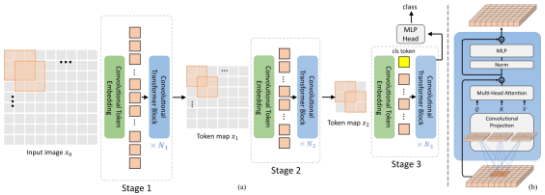
simuler la matière quantique



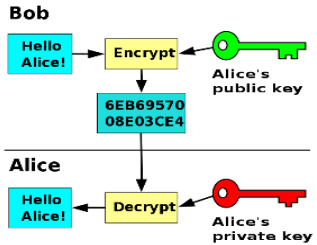
optimisations combinatoires et problèmes de décision



résolution d'équations aux dérivées partielles



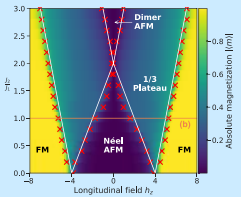
machine learning et deep learning



cryptanalyse

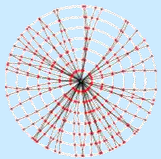
usages, de la recherche aux opérations

recherche fondamentale

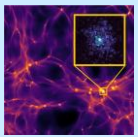


matière condensée

matière corrélée

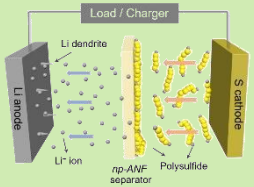


particules à hautes énergies

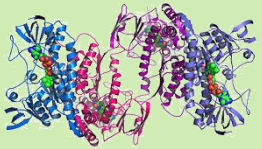


astrophysique

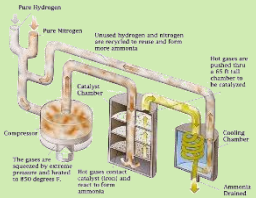
recherche appliquée



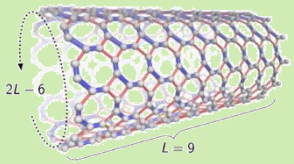
batteries



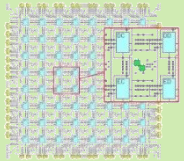
biotech



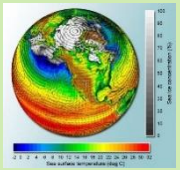
production d'engrais



matériaux



semiconducteurs

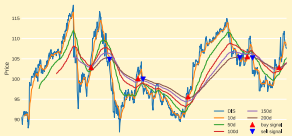


modélisation

opérations



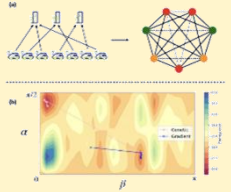
transports



services financiers



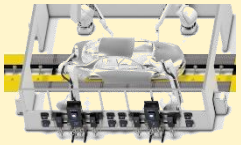
logistique et commerce



énergie



télécommunications



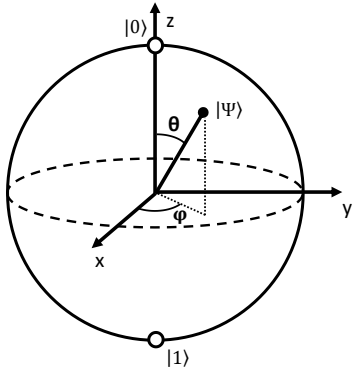
industrie

le « quantum bit » du calcul quantique

mathematiquement

unité de gestion de l'information

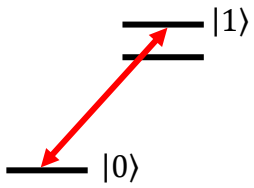
équivaut à deux nombres réels



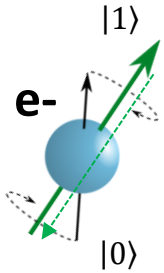
souvent représenté sous la forme d'une amplitude et d'une phase d'une onde, dans la sphère de Bloch

physiquement

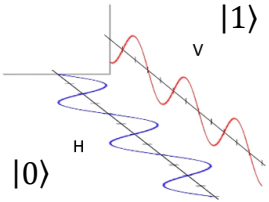
objet quantique
à deux états contrôlables



deux niveaux d'énergie d'un atome



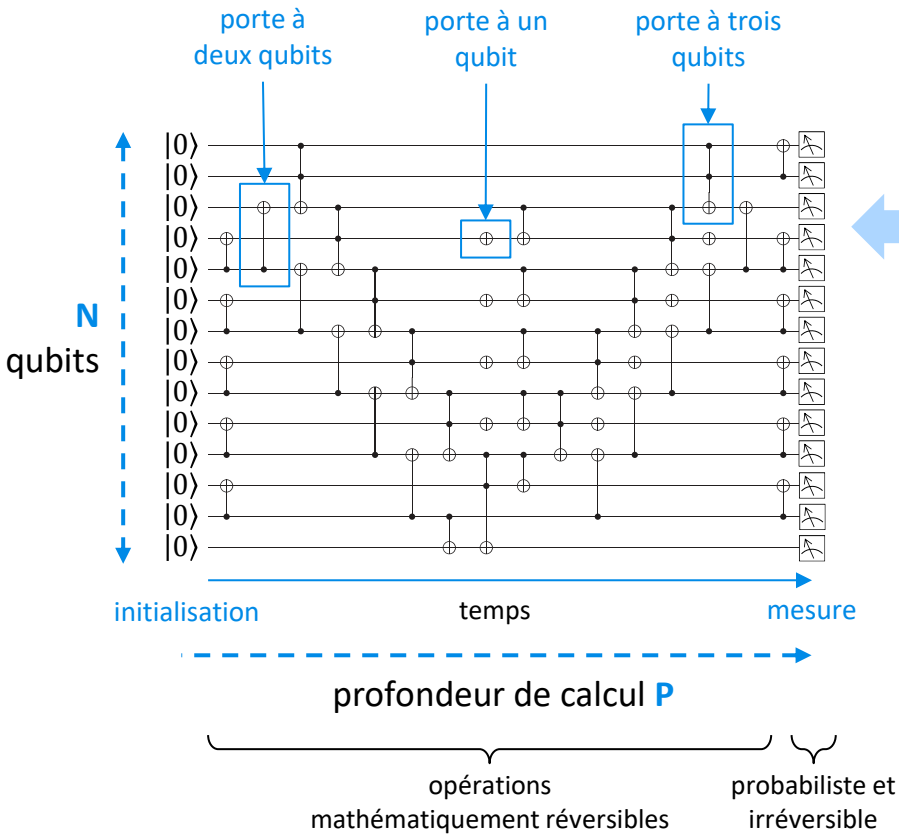
spin d'un électron



polarisation d'un photon

(cc) Olivier Ezratty, 2023-2024

qu’est-ce qu’un algorithme quantique?



algorithme quantique : décompose un problème mathématique en circuit quantique.

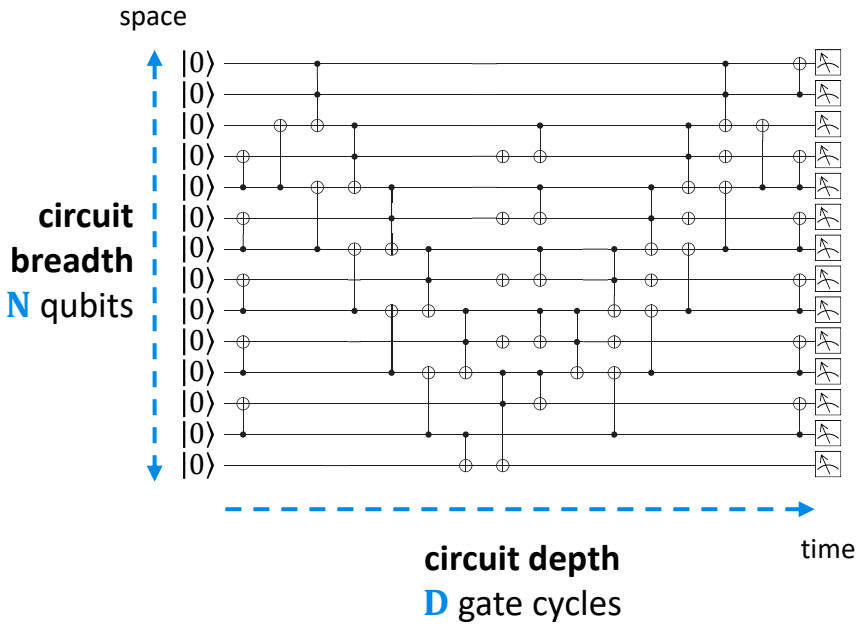
circuit quantique : suite d’opérations agissant sur une mémoire quantique de qubits, individuellement (superposition) ou les reliant entre eux (intrication), et se terminant par une mesure (probabiliste).

modèle mathématique : calcul matriciel-vectoriel opérant sur un espace mémoire de 2^{N+1} nombres réels. algèbre linéaire!

mécanisme : exploite diverses techniques comme la génération d’interférences pour faire ressortir une valeur d’intérêt sous forme de bits classiques lus en sortie.

calcul classique : utilisé pour préparer le circuit, y encoder les données, et extraire les résultats.

besoins en fidélité d'opérations



$$\epsilon_{operations} < \frac{1}{\mathbf{N} \times \mathbf{D}}$$

corresponds to all qubit operations:

- single qubit gates errors
- two-qubit gates errors
- idle state errors
- readout errors

paradigmes du calcul quantique

ordinateurs **classiques**

ordinateurs **quantiques analogiques**

ordinateurs **quantiques digitaux**

quantum inspired
algorithmes classiques inspirés par la physique quantique

améliorer les algorithmes classiques

QbitSoft Quantum as a Service

QUANTUM SIGNALS

quantum emulators
pour tester du code quantique sur des ordinateurs classiques

apprendre, tester, déboguer

Bull

IBM

QPerfect

Google

Pasqal

C12

QUANDELA

ALICE & BOB

quantum annealing computers

problèmes d'optimisation et de simulations physiques

D-Wave The Quantum Computing Company™

analog quantum simulators

problèmes d'optimisation et de simulations physiques

Pasqal

QuEra Putting Quantum to Work

AQT

gate-based

NISQ (Noisy Intermediate Scale Quantum)
qubits bruités, pas de correction d'erreurs

FTQC (Fault-Tolerant Quantum Computers)
correction d'erreurs et tolérance aux fautes

calcul quantique généraliste

IBM

rigetti

PsiQuantum

QUANTINUUM

IQM

XANADU

ALICE & BOB

IONQ

OQC

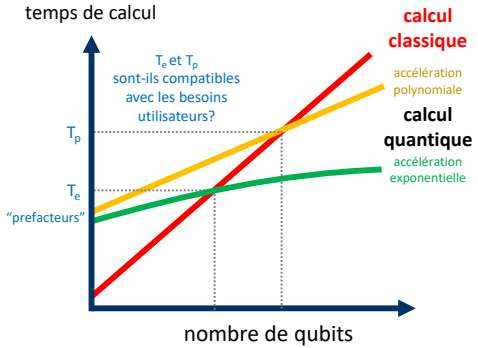
Microsoft

QUANDELA

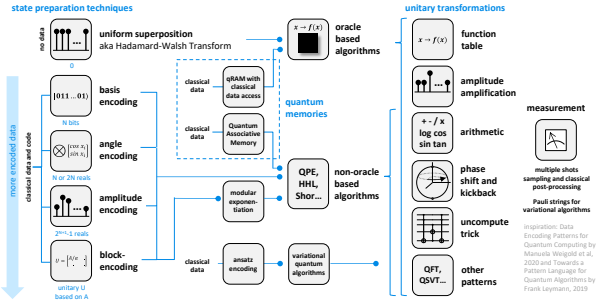
AQT

(cc) Olivier Ezratty, 2024-2026

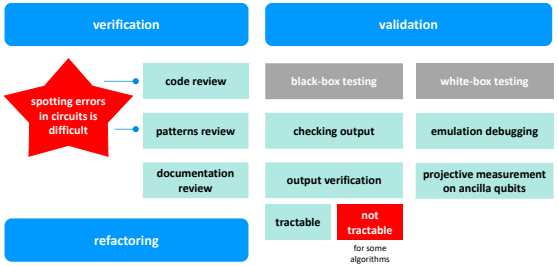
défis logiciels



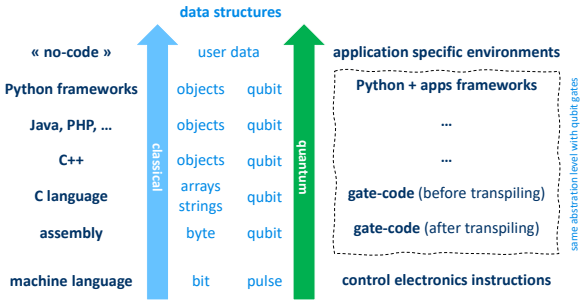
algorithmes



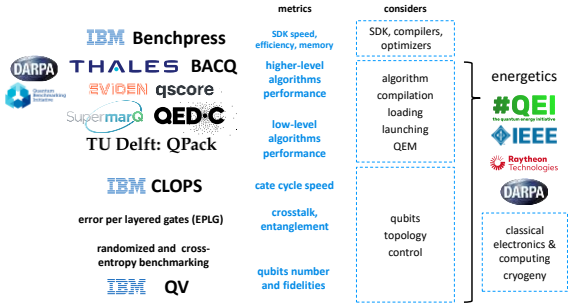
chargement des données



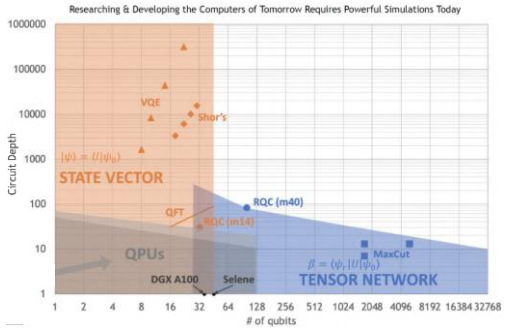
génie logiciel



niveaux d'abstraction



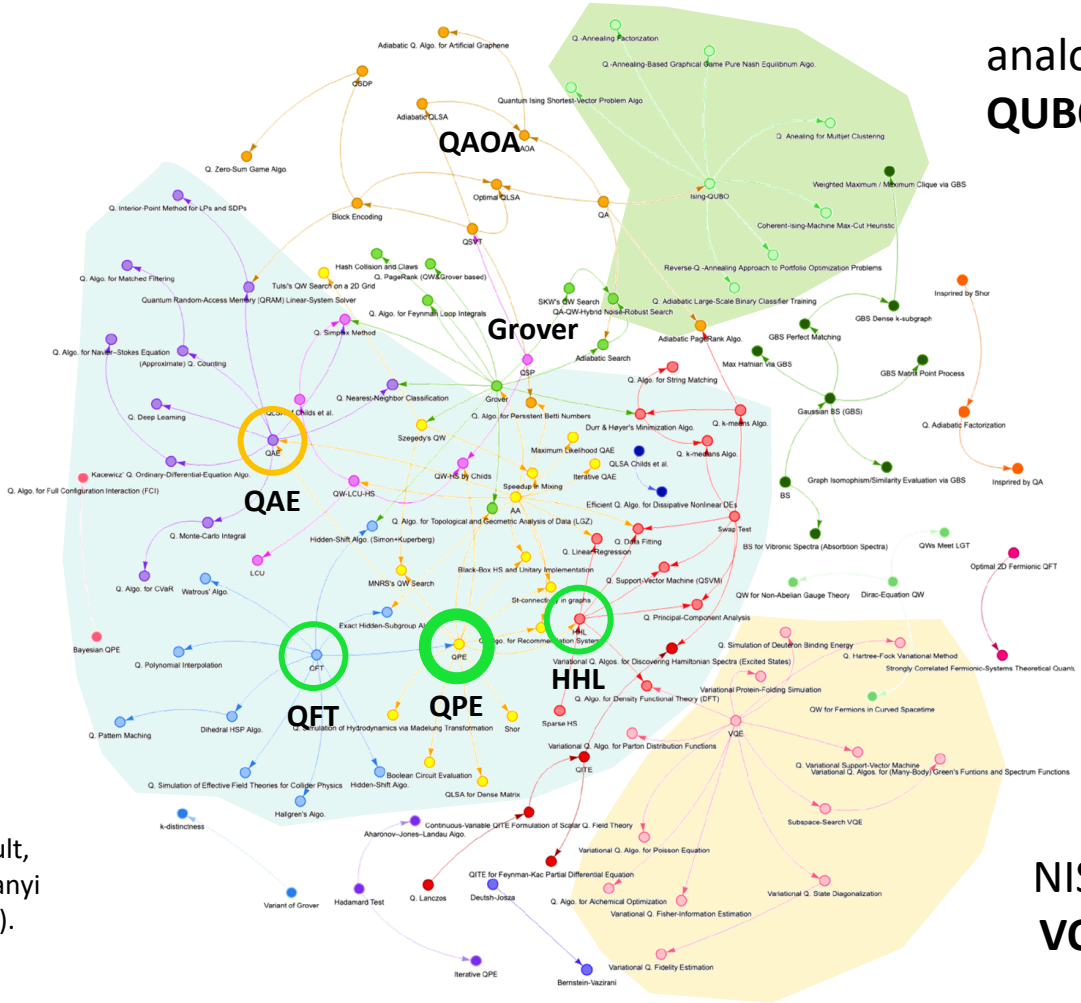
benchmarking



IA, réseaux de tenseurs

clusters des algorithmes quantiques

FTQC
QPE & QFT based

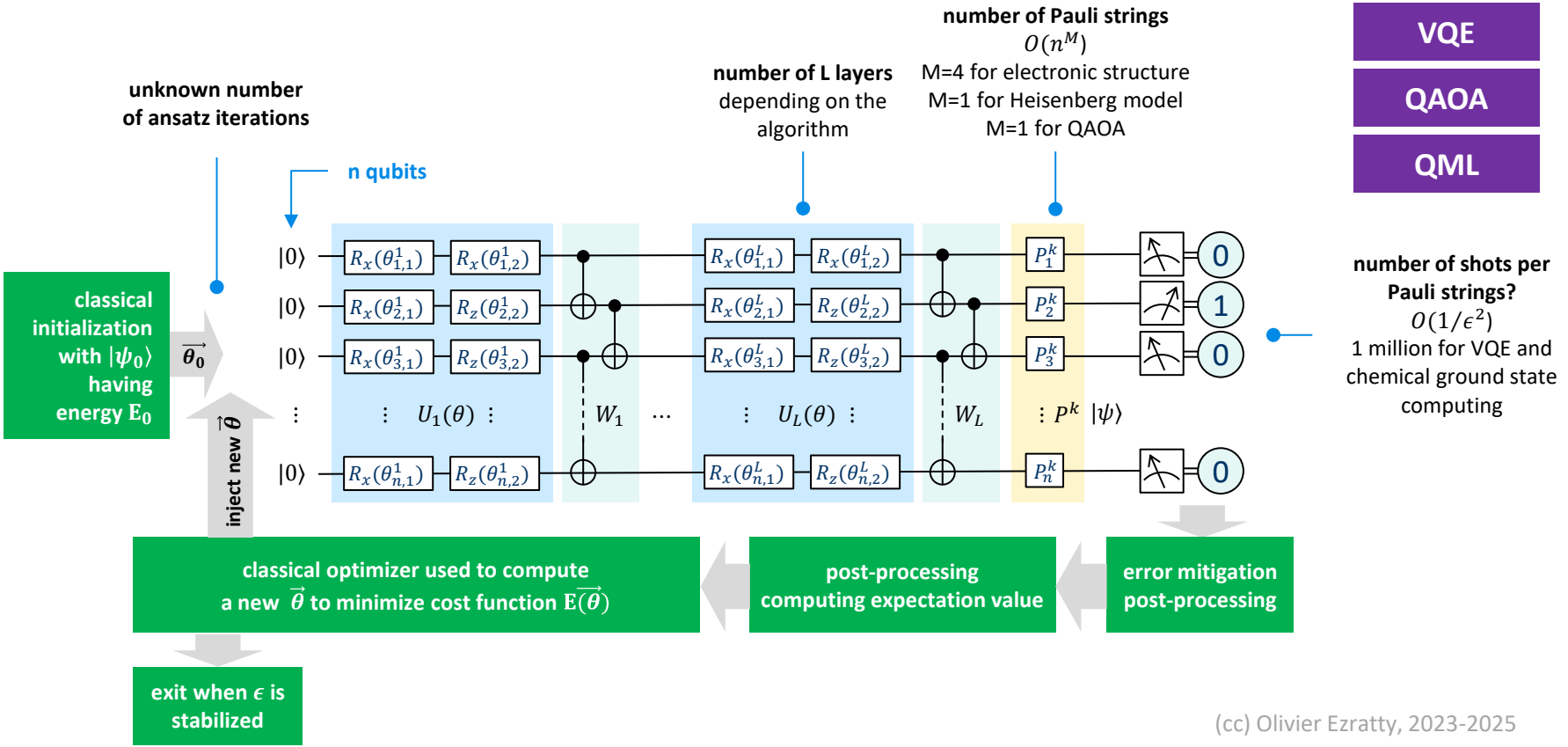


analog
QUBO

NISQ
VQE

[A typology of quantum algorithms](#) by Pablo Arnault, Pablo Arrighi, Steven Herbert, Evi Kasnetsi, and Tianyi Li, Inria, Quantinuum, arXiv, July 2024 (60 pages).

exemple d'algorithme quantique NISQ



(cc) Olivier Ezratty, 2023-2025

exemple d'algorithme quantique FTQC

problem metrics

H = problem Hamiltonian.

M = number of spin-orbitals, conditioning m.

ϵ = desired chemical accuracy ≈ 1.6 10^{-3} Ha

δ = acceptable failure probability.

p_0 = initial state overlap, decreasing exponentially with molecule size.

classical pre-processing (HF, FCI, DFT, …) for *N* orbitals

state vector encoding circuit

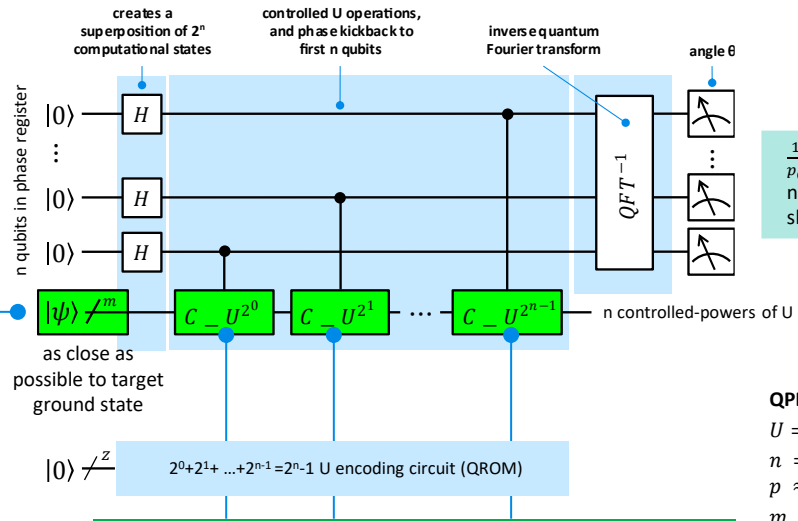
classical computing time scale $O(M^3)$ to $O(2^M)$

classical computing time scale $O(M^3)$ to $O(M^5)$

$$||U - e^{-iHt}|| < \epsilon$$

H= system Hamiltonian

U= unitary encoding it



$\frac{1}{p_0}\ln(\frac{1}{\delta})$ QPE number of circuit shots

results post-processing

problem Hamiltonian encoding

find *U* using

- Block-encoding.
- Trotter-Suzuki decomposition.
- QSVT.
- Chebyshev approximation.
- Linear Combination of Unitaries (LCU).

QPE quantum circuit metrics

U = unitary encoding the Hamiltonian H.

n = phase register qubits, $\lceil \log_2(1/\epsilon) \rceil + p \approx 13$ *to* 15 for $\epsilon \approx 1.6\ 10^{-3}$ Ha

m = system register qubits encoding the initial state $|\psi\rangle$ and on which controlled powers of unitary U are applied.

z = additional ancilla logical qubits required to encode U which depends on its parallelization.

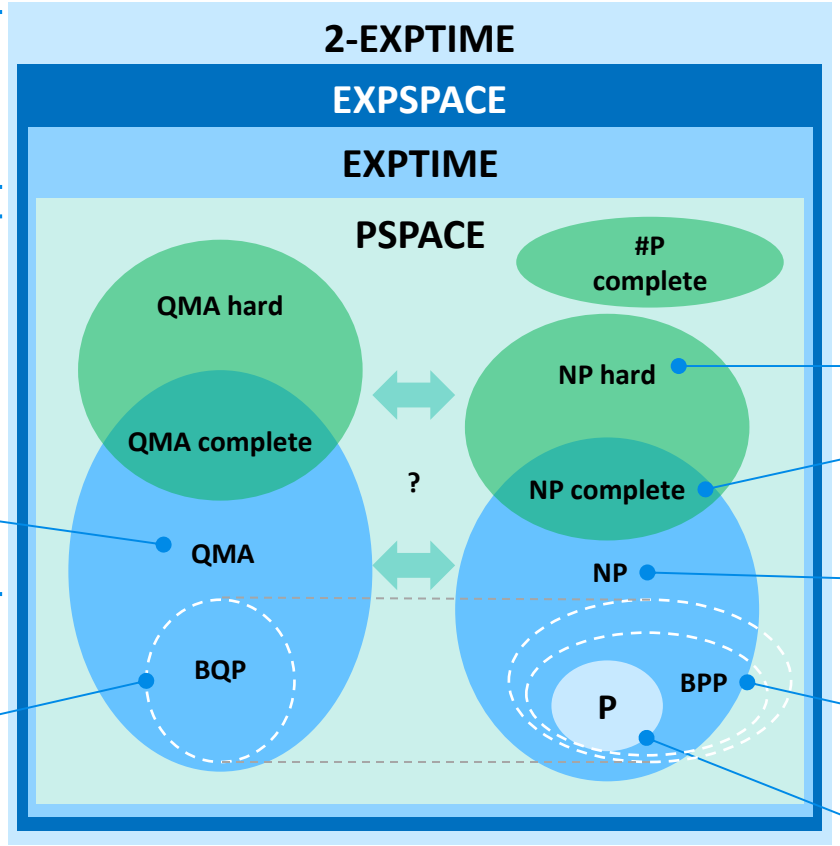
quantum phase estimation algorithm, inspired by Quantum chemistry, classical heuristics, and quantum advantage by Garnet Kin-Lic Chan, arXiv, July 2024 & On the feasibility of performing quantum chemistry calculations on quantum computers by Thibaud Louvet, Thomas Ayral, and Xavier Waintal, arXiv, June 2023-October 2024.

et les problèmes non linéaires ?

$$\frac{\partial \boldsymbol{u}}{\partial t} + \boldsymbol{u} \cdot \nabla \boldsymbol{u} + \frac{1}{\rho} \nabla p = \boldsymbol{g} + v \nabla \cdot \nabla \boldsymbol{u}$$

1. **répartition des rôles**
   https://arxiv.org/abs/1907.09032
2. **calcul à variables continues**
   https://arxiv.org/abs/2011.06571
3. **mid-circuit measurement and feed-forward**
   https://arxiv.org/abs/2410.03838
   https://arxiv.org/abs/2607.12269

classes de complexité... pour des problèmes de décision



forget it with any computer!

hard to solve for quantum computers

QMA: a solution can be verified in polynomial time with a quantum computer

BQP: polynomial problems for quantum computers, integer factoring

et des problèmes reformulés en problèmes de décision (factorisation, ground state)

NP-hard: problems at least as difficult to solve as NP problems,
finding optimal path in a graph, map coloring, theorems demonstrations.

NP-Complete : all NP problems can be polynomially reduced to a NP problem,
finding a sub-set of an ensemble of integers with a zero sum, proteins folding, MaxCut problem, SAT problem.

NP : "Nondeterministic Polynomial", complex decision problems solved in polynomial time on a non-deterministic Turing machine and/or verifiable in polynomial time on a deterministic Turing machine,
has one subset of 3 numbers with a sum = 0, integer primality test, linear equations.

BPP: "Bounded-Error Probabilistic Polynomial time", decision problems that can be solved by a probabilistic Turing machine in polynomial time.
primality testing, randomized algorithms for problems in graph theory.

P: "Polynomial", problem solvable in polynomial time on a deterministic Turing machine,
has a matrix a proper value of 1.2? matrix addition, multiplication, inversion, lists sorting, finding a path in a labyrinth.

(cc) Olivier Ezratty, 2021-2026

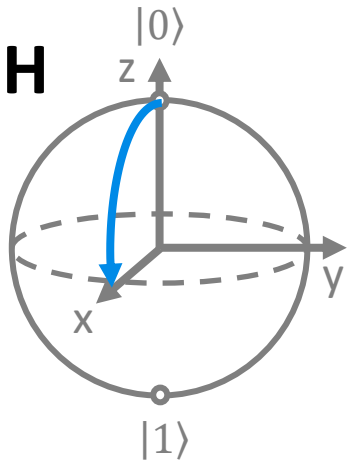
sources d'avantage quantique

« computational basis state vector »

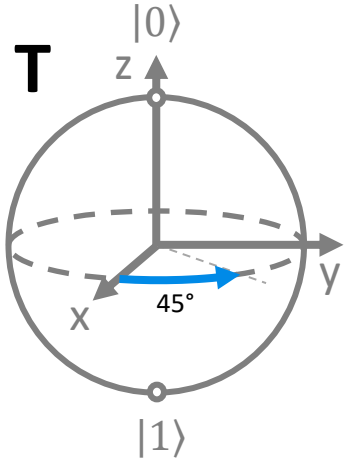
complex amplitudes | of all combinations of 0 and 1

$$\begin{bmatrix} \alpha_1 \\ \dots \\ \dots \\ \dots \\ \dots \\ \alpha_{2^N} \end{bmatrix} \quad \begin{matrix} |00\dots00\rangle \\ \vdots \\ |01\dots11\rangle \\ \vdots \\ |11\dots11\rangle \end{matrix}$$

N qubits register
2^N superposed states
complex amplitudes

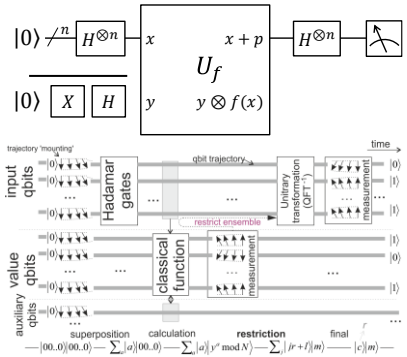


Clifford qubits gates
H, S, X, Y, Z, CNOT, SWAP
single qubit gates with half/quarter turns in Bloch sphere, discrete # of gates



non-Clifford qubits gates
T, Toffoli and R_{phase} enabling arbitrary angles rotations and an infinite # of gates

algorithms compilers

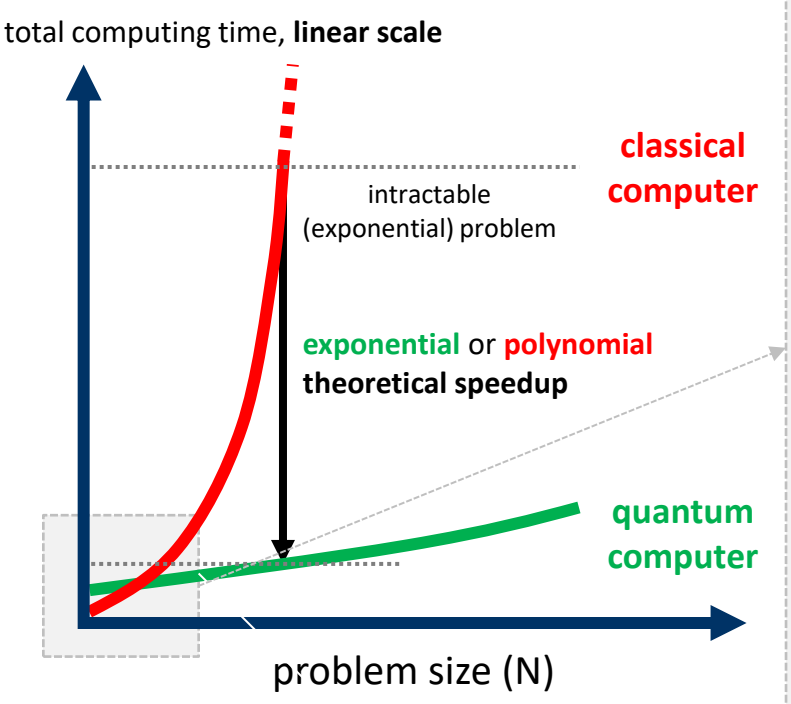


maximally entangled states
a large number of qubits are entangled

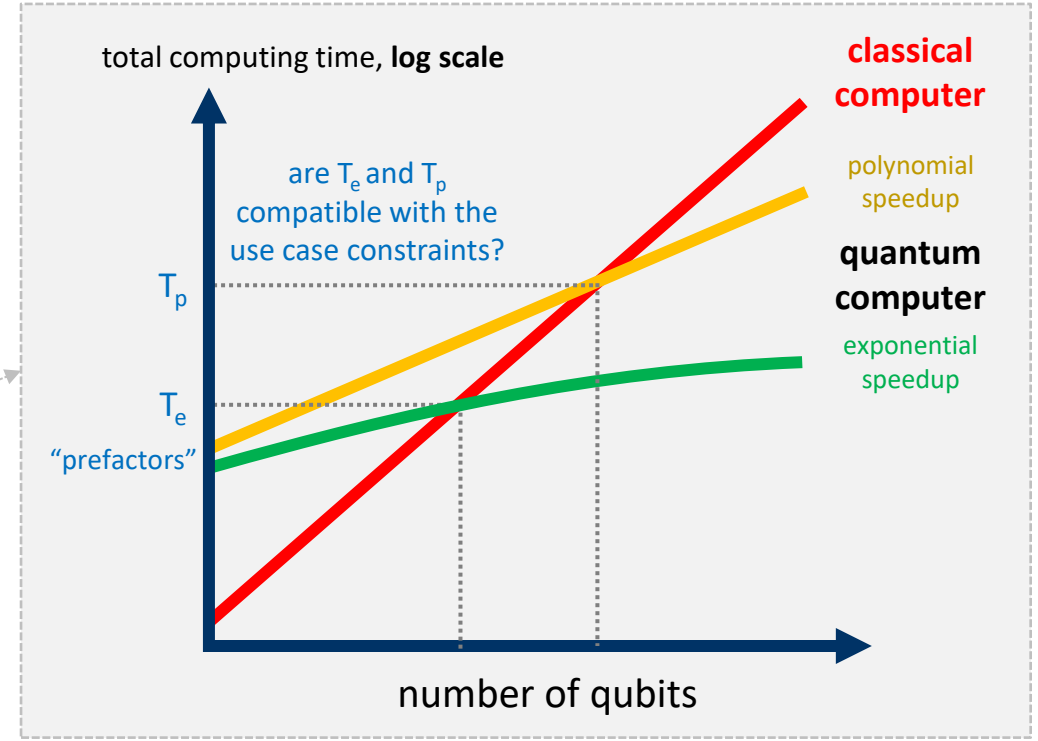
space advantage	polynomial speedup	superpolynomial speedup	
internal memory space advantage, **but not for input/output**	**can be efficiently simulated per the Gottesman-Knill theorem**	necessary (**but not sufficient**) condition for obtaining a superpolynomial speedup, but not sufficient	entangled states must be larger than what can be simulated classically

(cc) Olivier Ezratty, 2022-2026

accélération asymptotique vs pratique

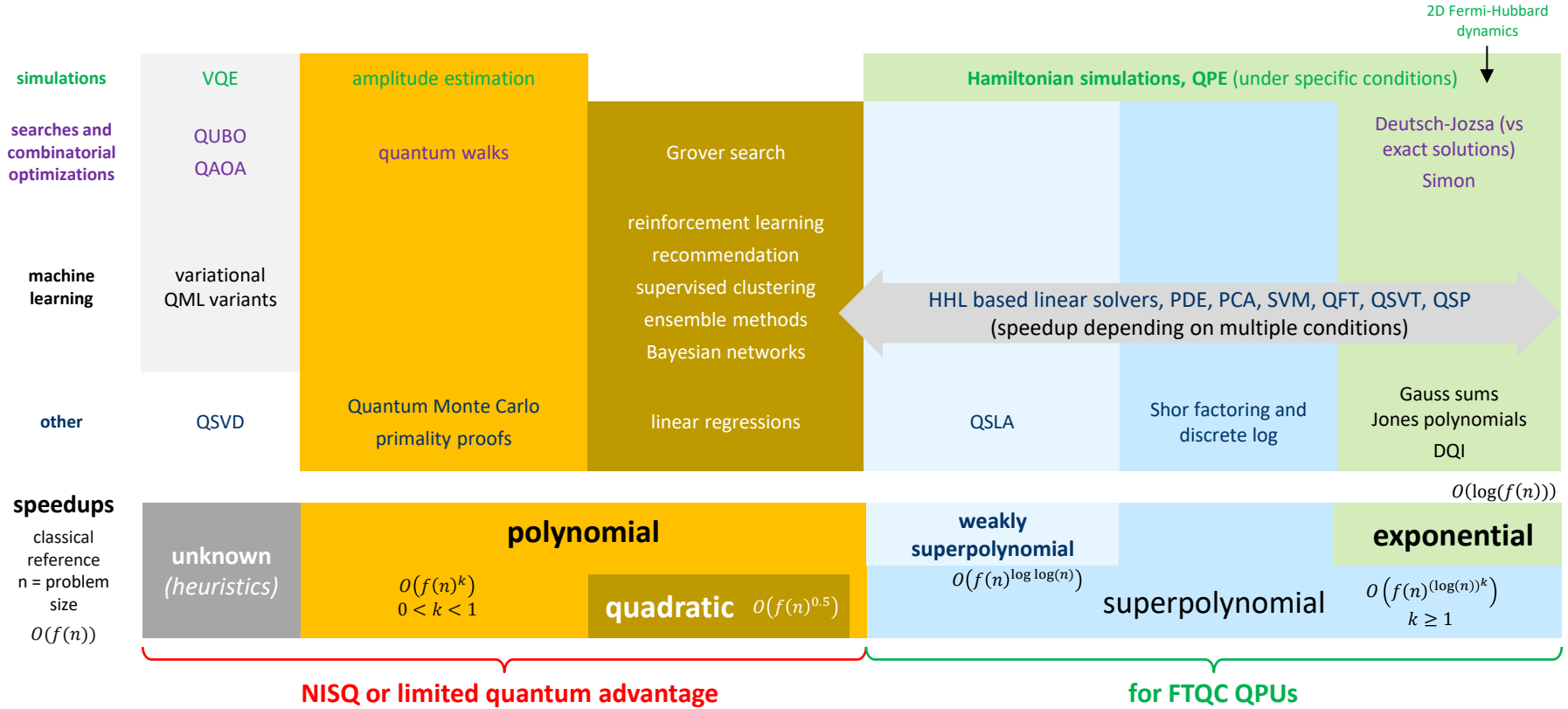


the typical way to illustrate quantum computing theoretical speedups.



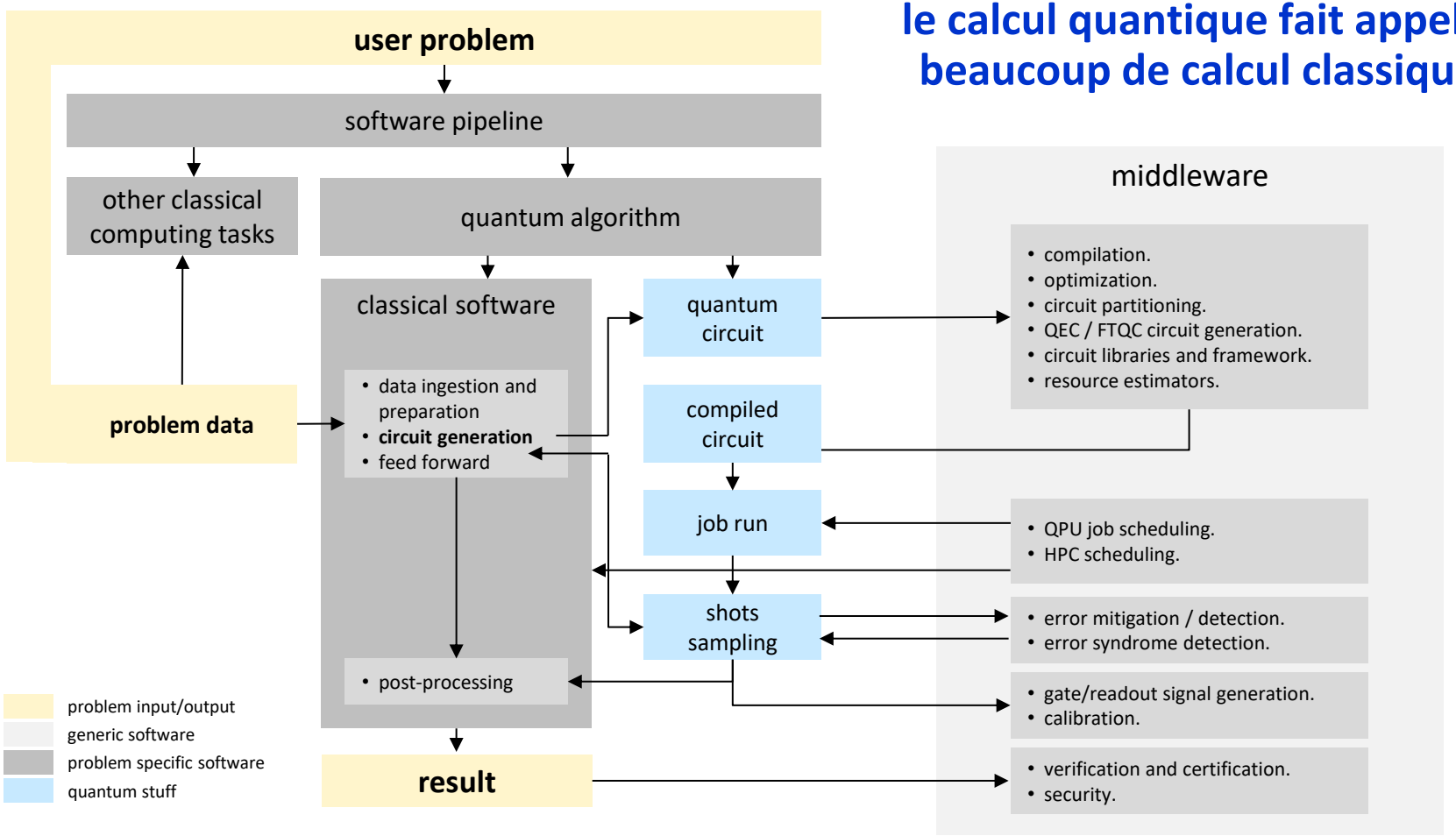
Opening the Black Box inside Grover's Algorithm, E. Miles Stoudenmire and Xavier Waintal, PRX, November 2024.

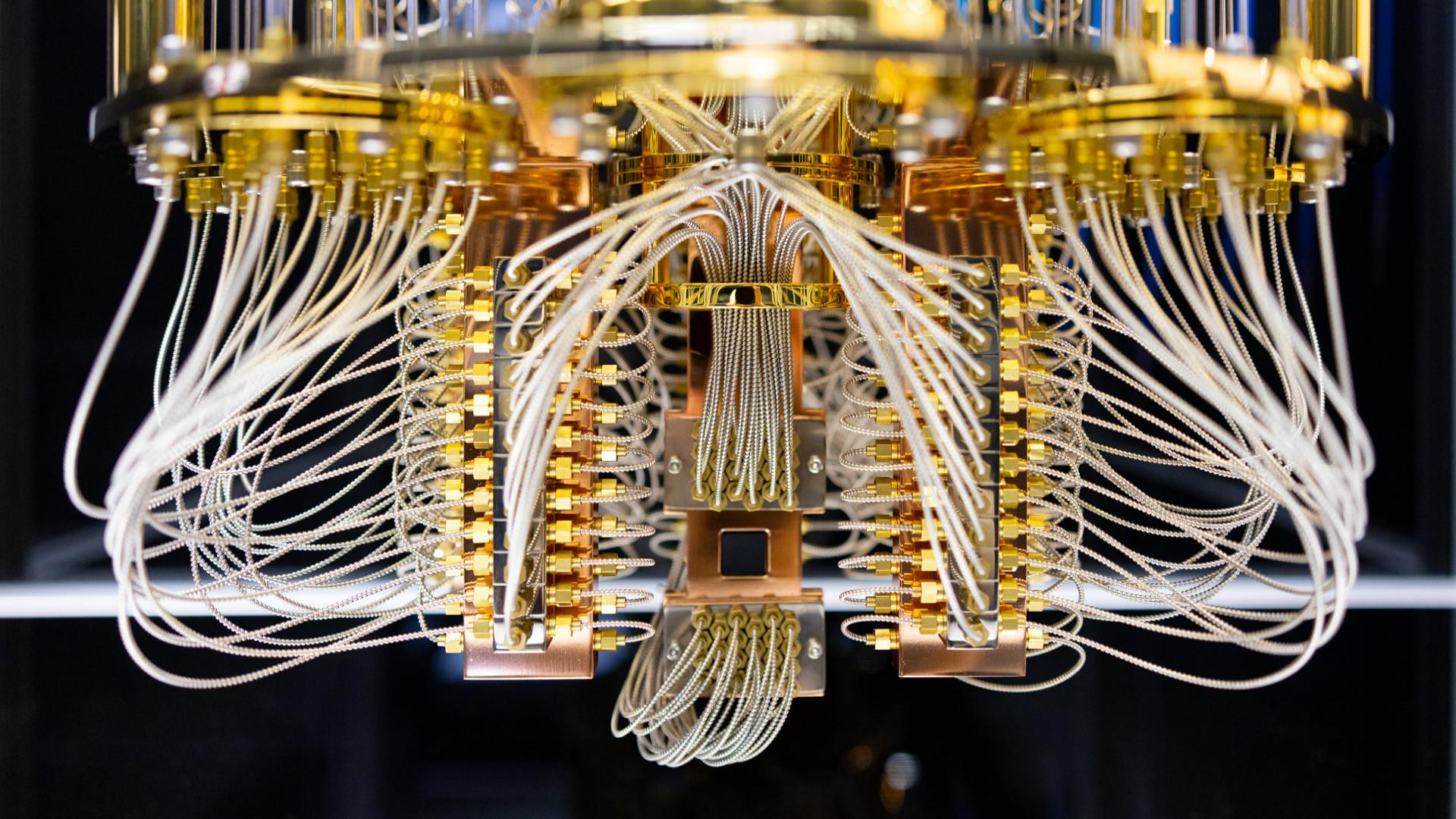
types d'accélération quantique

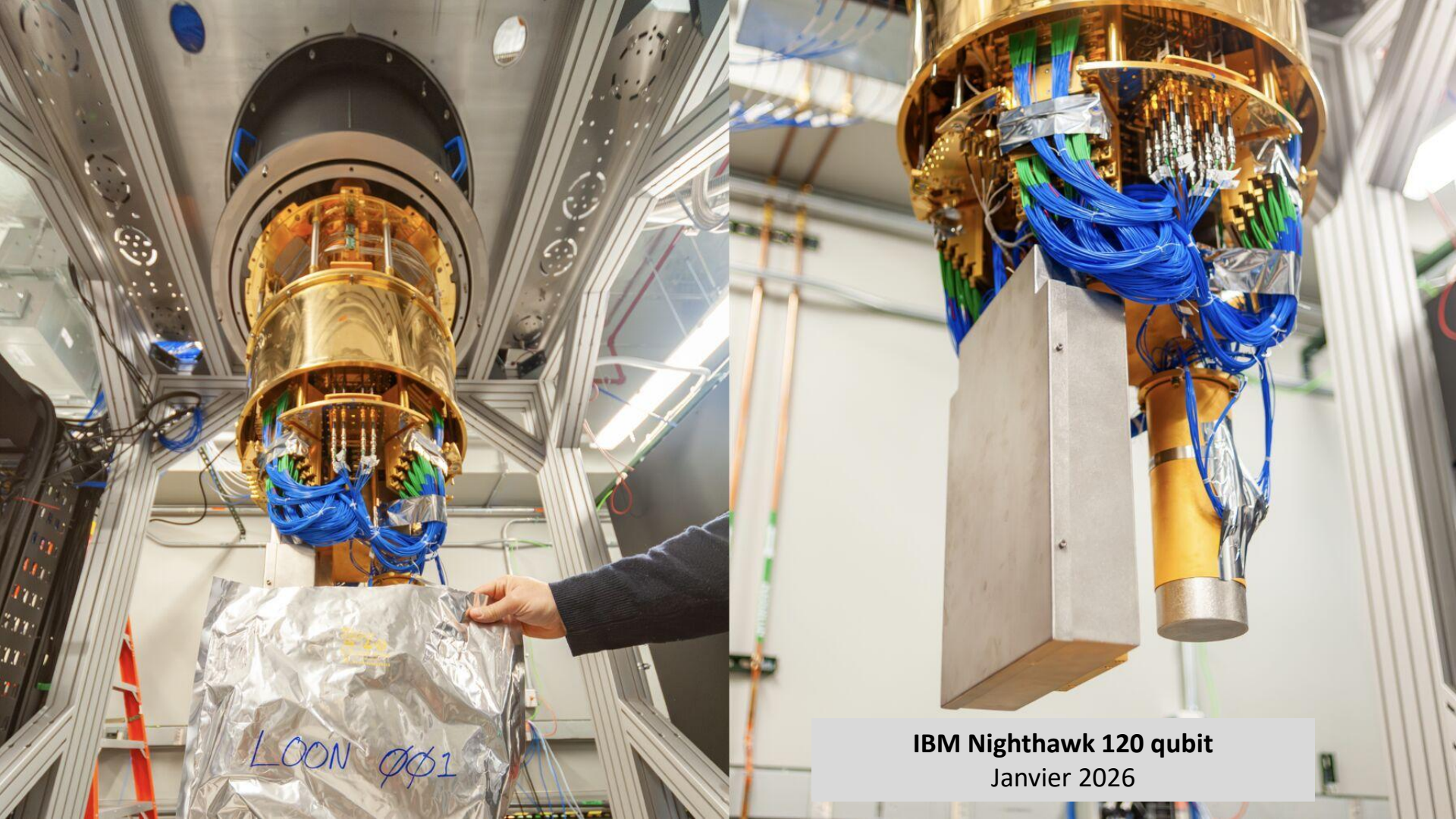


Understanding Quantum Technologies by Olivier Ezratty, as of Septemnber 2026.

le calcul quantique fait appel à beaucoup de calcul classique

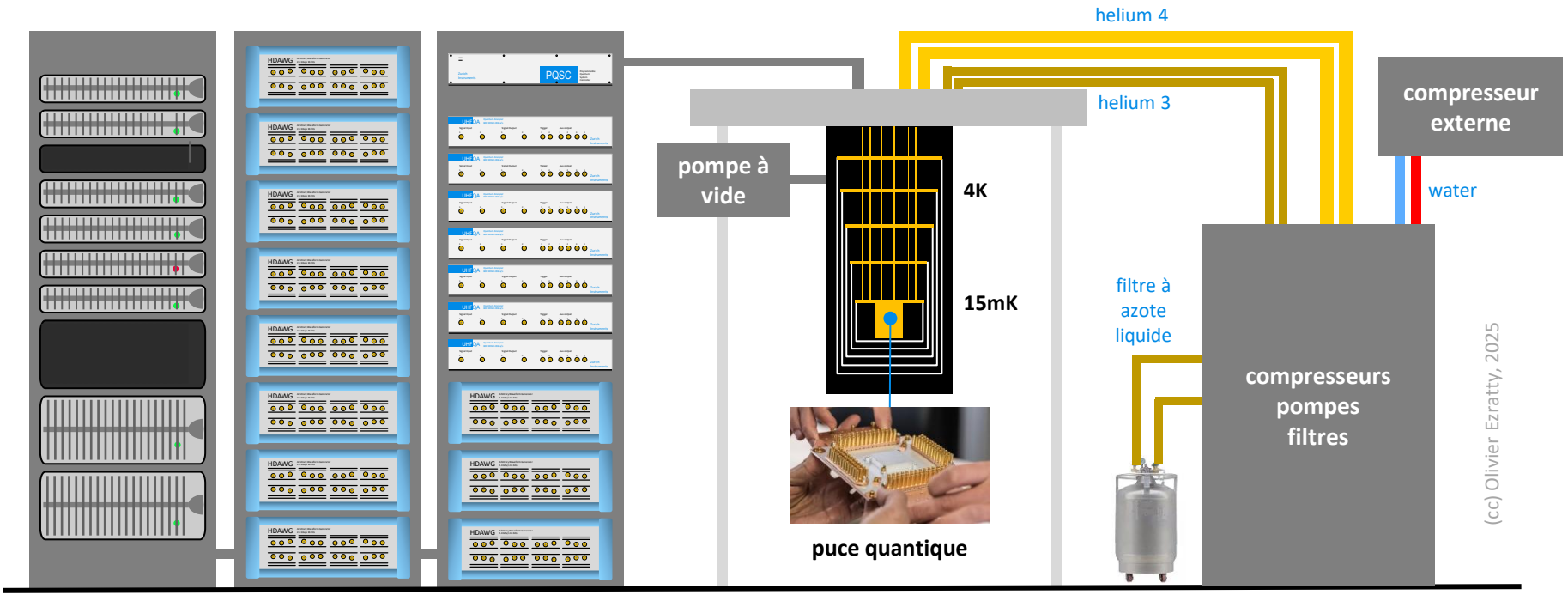






IBM Nighthawk 120 qubit
Janvier 2026

composantes d’un ordinateur quantique



pour des qubits supraconducteurs ou spins dans le silicium

où on est …

ordinateurs quantiques « analogiques »

Pasqal

D-Wave The Quantum Computing Company™

ordinateurs quantiques bruités « NISQ »
(noisy intermediate scale quantum)

IBM IONQ QUANTINUUM QUANDELA

et où on veut aller

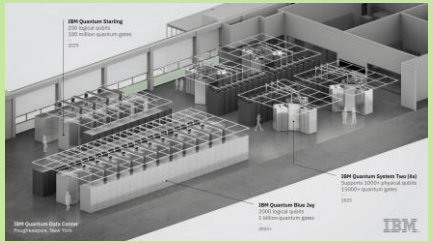
ordinateurs quantiques tolérants aux fautes
« FTQC » (fault tolerant quantum computers)

objectifs

- plus grande capacité de calcul.
- « avantage quantique » vs le calcul classique.

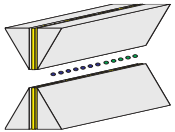
moyens

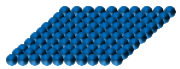
- mécanismes de correction d'erreurs.
- plus grand nombre de qubits physiques.

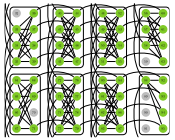


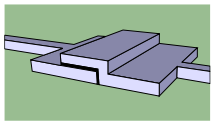
>90 constructeurs dans le calcul quantique

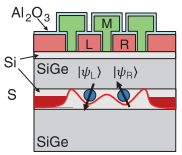
atoms | **electrons** *controlled spin and microwave cavities* | **photons**


trapped ions

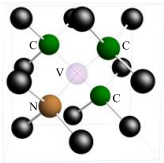

cold atoms

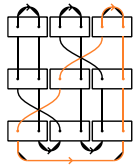

annealing

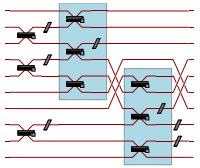

superconducting



silicon


vacancies


topological

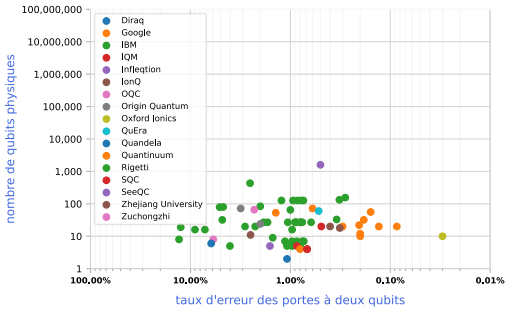

photons

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16

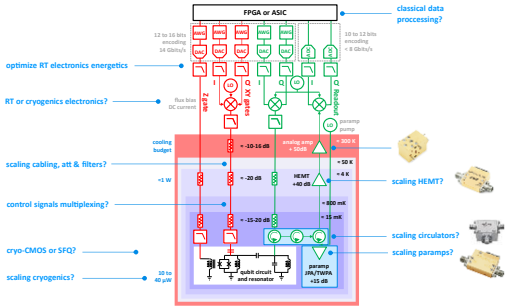
(cc) Olivier Ezratty, September 2026

défis matériels

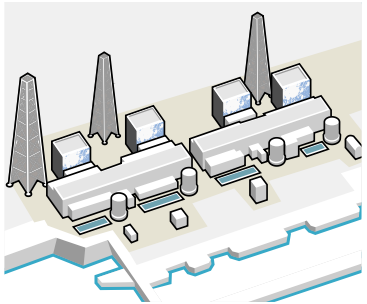
#QEI
the quantum energy initiative



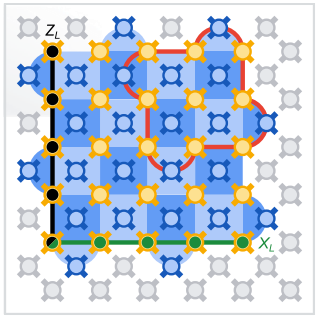
lutte contre le bruit



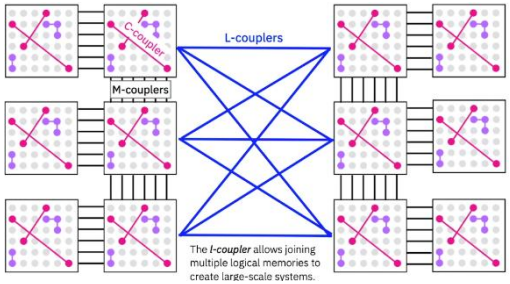
électronique, câblage, cryogénie



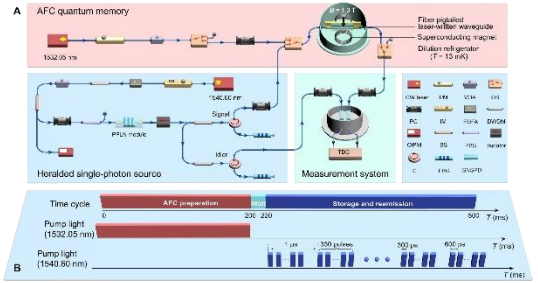
coût et énergie



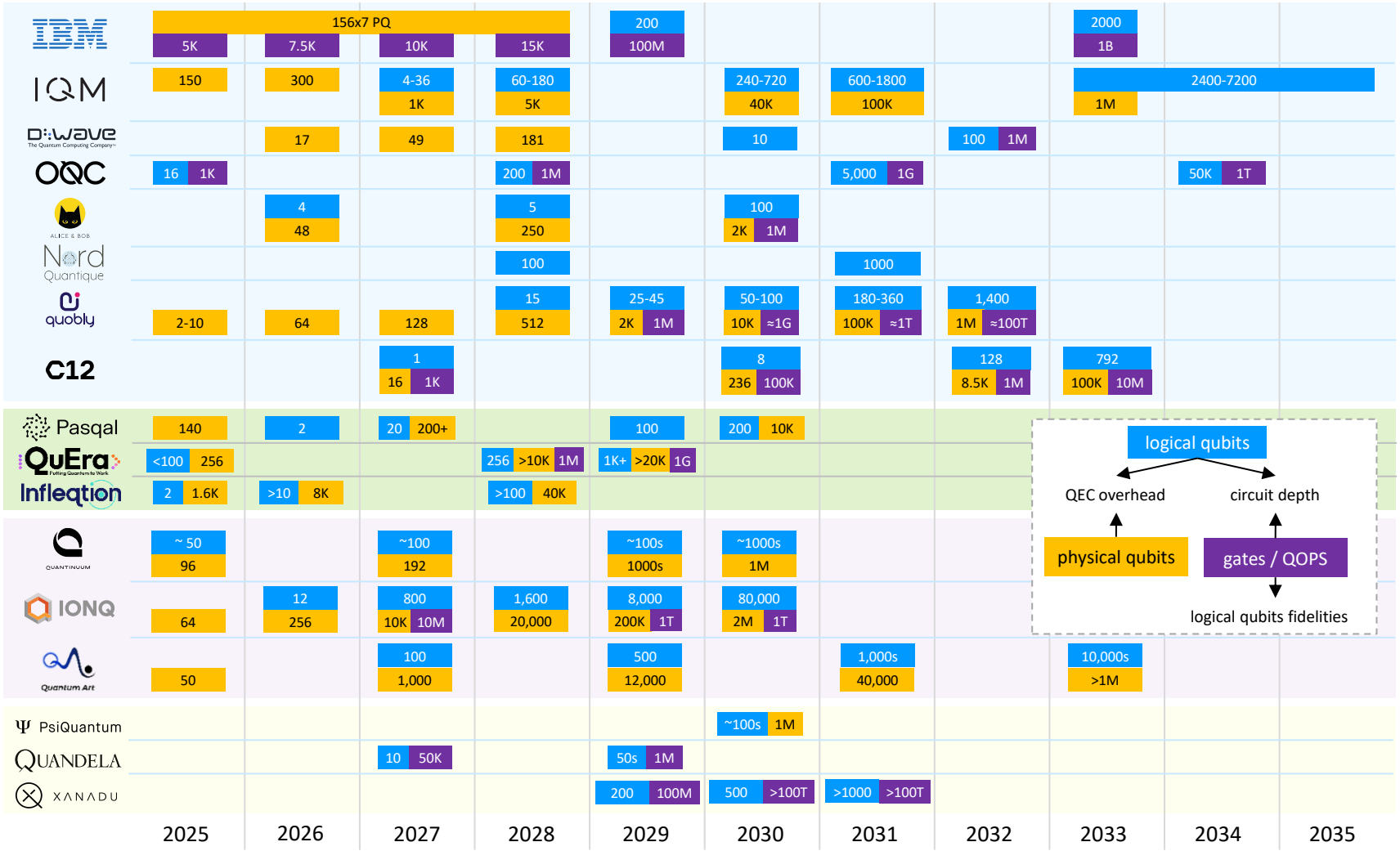
correction d'erreurs



interconnexion quantique



mémoires quantiques



(cc) Olivier Ezratty, September 2026.

la fin du monde (Internet) approche-t-elle?

Iceberg Quantum

The Pinnacle Architecture: Reducing the cost of breaking RSA-2048 to 100 000 physical qubits using quantum LDPC codes

Paul Webster,* Lucas Berent, Omprakash Chandra, Evan T. Hockings, Nouédyn Baspin, Felix Thomsen, Samuel C. Smith, and Lawrence Z. Cohen†
Iceberg Quantum, Sydney

https://arxiv.org/abs/2602.11457

Q-CTRL

Heterogeneous architectures enable a 138x reduction in physical qubit requirements for fault-tolerant quantum computing under detailed accounting

Pranav S. Mundada,* Aleksei Khindanov,† Yulun Wang,† Claire L. Edmunds, Paul Coote, Michael J. Biercuk, Yuval Baum, and Michael Hush
Q-CTRL, Los Angeles, CA USA and Sydney, NSW Australia
(Dated: April 15, 2026)

https://arxiv.org/abs/2604.06319

Oratomic

Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

Madelyn Cain[1,*,†], Qian Xu[1,2,*,‡], Robbie King[1], Lewis R. B. Picard[1], Harry Levine[1,3], Manuel Endres[1,2], John Preskill[1,2], Hsin-Yuan Huang[1,2], Dolev Bluvstein[1,2,§]
[1] *Oratomic, Pasadena, California 91125, USA*
[2] *California Institute of Technology, Pasadena, California 91125, USA*
[3] *Department of Physics, University of California, Berkeley, California 94720, USA*
[†] *mcain@oratomic.com,* [‡] *qxu@oratomic.com,* [§] *dbluvstein@oratomic.com*
[*] *These authors contributed equally*
(Dated: March 31, 2026)

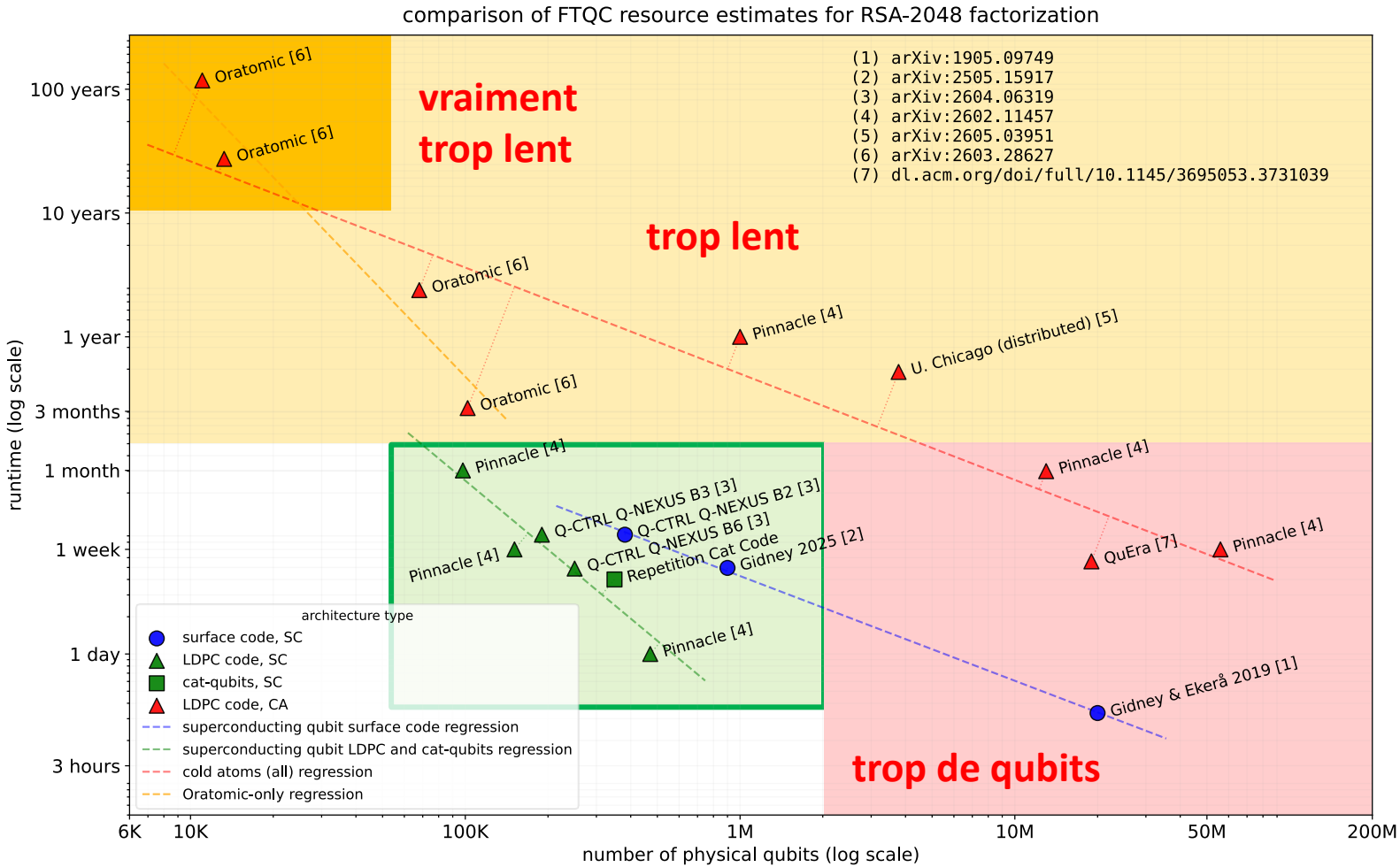
https://arxiv.org/abs/2603.28627v1

Google

Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations

Ryan Babbush,[1,*] Adam Zalcman,[1,†] Craig Gidney,[1,‡] Michael Broughton,[1] Tanuj Khattar,[1] Hartmut Neven,[1] Thiago Bergamaschi,[1,2] Justin Drake,[3] and Dan Boneh[4]
[1] *Google Quantum AI, Santa Barbara, CA 93111, United States*
[2] *Department of Computer Science, University of California Berkeley, Berkeley, CA 94720, United States*
[3] *Ethereum Foundation, Zeughausgasse 7a, 6300 Zug, Switzerland*
[4] *Department of Computer Science, Stanford University, Stanford, CA 94305, United States*
(Dated: April 17, 2026)

https://arxiv.org/abs/2603.28846

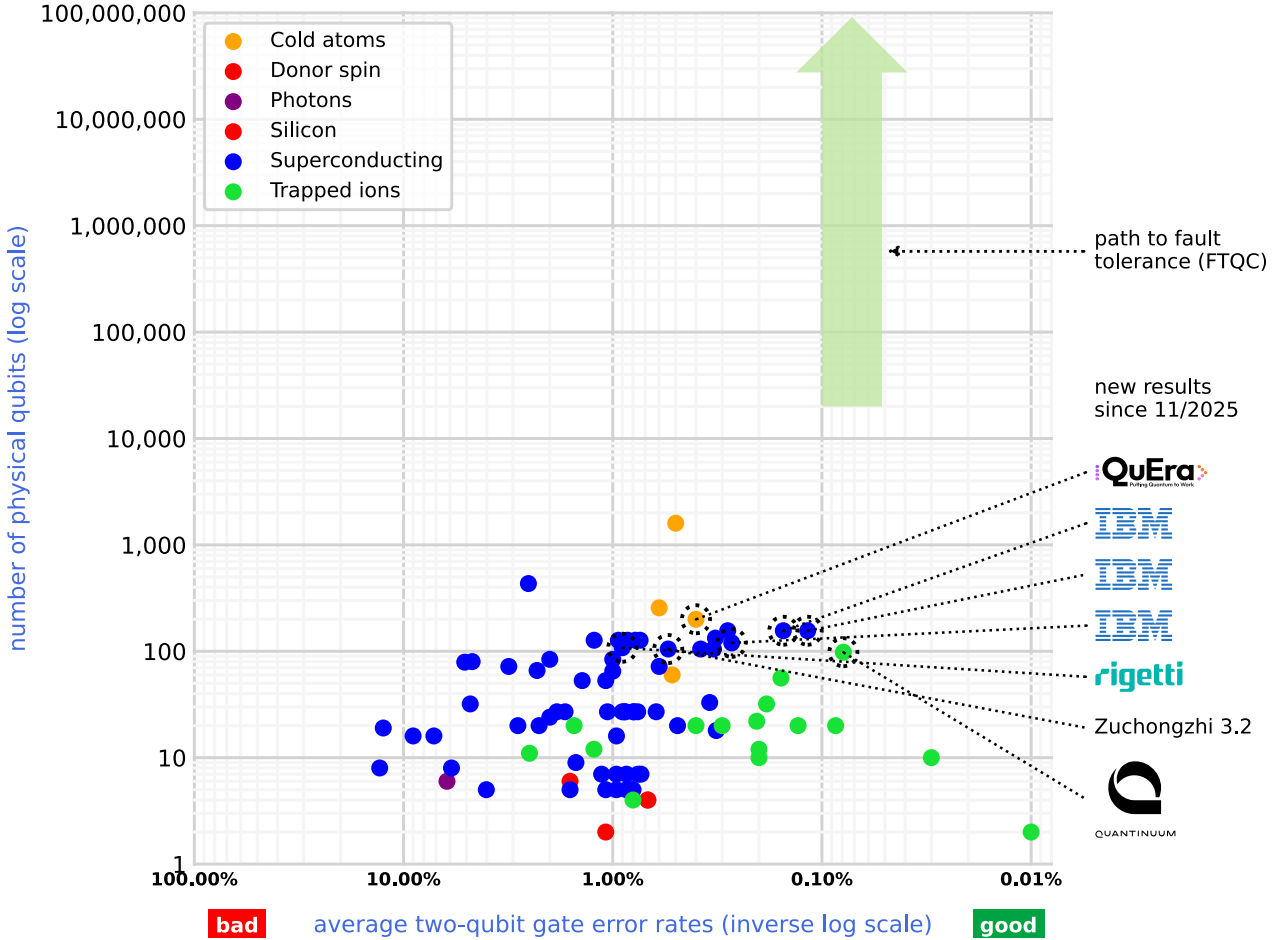

comparison of FTQC resource estimates for RSA-2048 factorization
(1) arXiv:1905.09749
(2) arXiv:2505.15917
(3) arXiv:2604.06319
(4) arXiv:2602.11457
(5) arXiv:2605.03951
(6) arXiv:2603.28627
(7) dl.acm.org/doi/full/10.1145/3695053.3731039
vraiment trop lent
trop lent
trop de qubits
Oratomic [6]
Oratomic [6]
Oratomic [6]
Oratomic [6]
Pinnacle [4]
U. Chicago (distributed) [5]
Pinnacle [4]
Pinnacle [4]
Q-CTRL Q-NEXUS B3 [3]
Q-CTRL Q-NEXUS B2 [3]
Q-CTRL Q-NEXUS B6 [3]
Repetition Cat Code
Gidney 2025 [2]
Pinnacle [4]
Pinnacle [4]
QuEra [7]
Pinnacle [4]
Gidney & Ekerå 2019 [1]
architecture type
surface code, SC
LDPC code, SC
cat-qubits, SC
LDPC code, CA
superconducting qubit surface code regression
superconducting qubit LDPC and cat-qubits regression
cold atoms (all) regression
Oratomic-only regression
100 years
10 years
1 year
3 months
1 month
1 week
1 day
3 hours
runtime (log scale)
6K
10K
100K
1M
10M
50M
200M
number of physical qubits (log scale)

physical error rate assumptions by quantum error correction resource estimates

- 99.9% single qubit gate fidelity
- 99.9% two qubit gate fidelity
- 99.9% idle state fidelity
- 99.9% reset fidelity
- 99.9% readout fidelity

=>

- quantum physics.
- materials.
- high-quality manufacturing.
- high-quality qubit control.
- unknown noise sources.



calcul quantique dans le cloud

	scientific computing centers	OVHcloud	Scaleway	IBM	aws	Microsoft	Google
emulation	40 qubits Bull	 Qiskit QUANDELA		Qiskit on your own hardware	34-50 qubits	30 qubits	40 qubits
quantum computing	TGCC JÜLICH LUMI lrz CINECA PCSS EuroHPC	Pasqal 100 qubits (analog) QUANDELA 12 qubits	Pasqal 100 qubits (analog) QUANDELA 12 qubits IQM 54 qubits	IBM 120, 127, 133 & 156 qubits	IQuEra 256 qubits (analog) IONQ 36 qubits rigetti 84 qubits IQM 20 qubits	Pasqal 100 qubits (analog) IONQ 25-32 qubits rigetti 84 qubits IQM 20 qubits QUANTINUUM 56 qubits	IONQ 11 qubits

(cc) Olivier Ezratty, 2026

un défi énergétique ?

New Scientist

Technology

Some quantum computers might need more power than supercomputers

A preliminary analysis suggests that industrially useful quantum computers designs come with a broad spectrum of energy footprints, including some larger than the most powerful existing supercomputers

By Karmela Padavic-Callaghan

8 January 2026

https://www.newscientist.com/article/2509492-some-quantum-computers-might-need-more-power-than-supercomputers/

PT PHYSICS TODAY

NEWS / ARTICLE

How much electricity does a quantum computer need?

JUN 15, 2026

The question is attracting attention amid rising energy use by classical computing data centers.

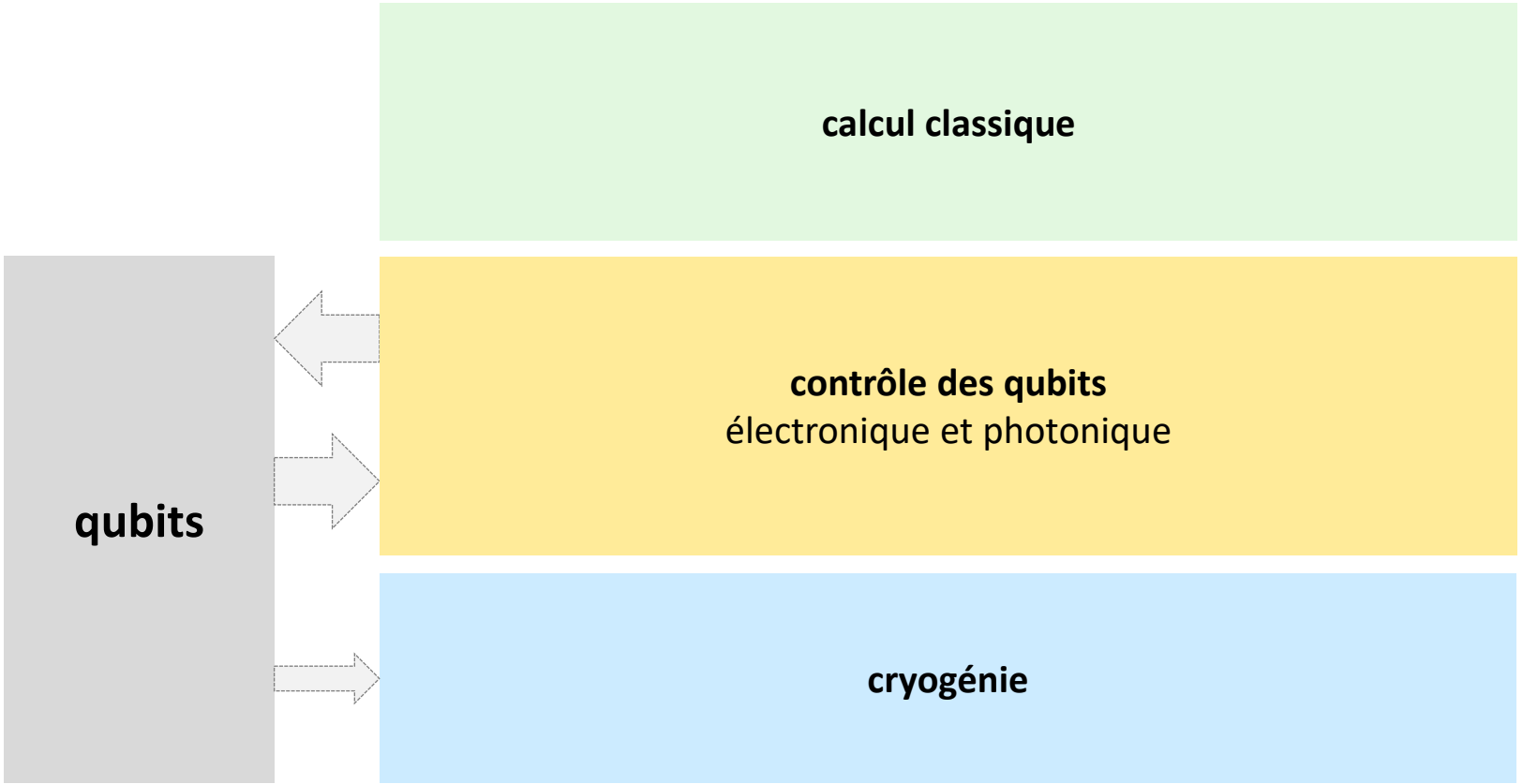
DOI: 10.1063/pt.41fbb5d95c



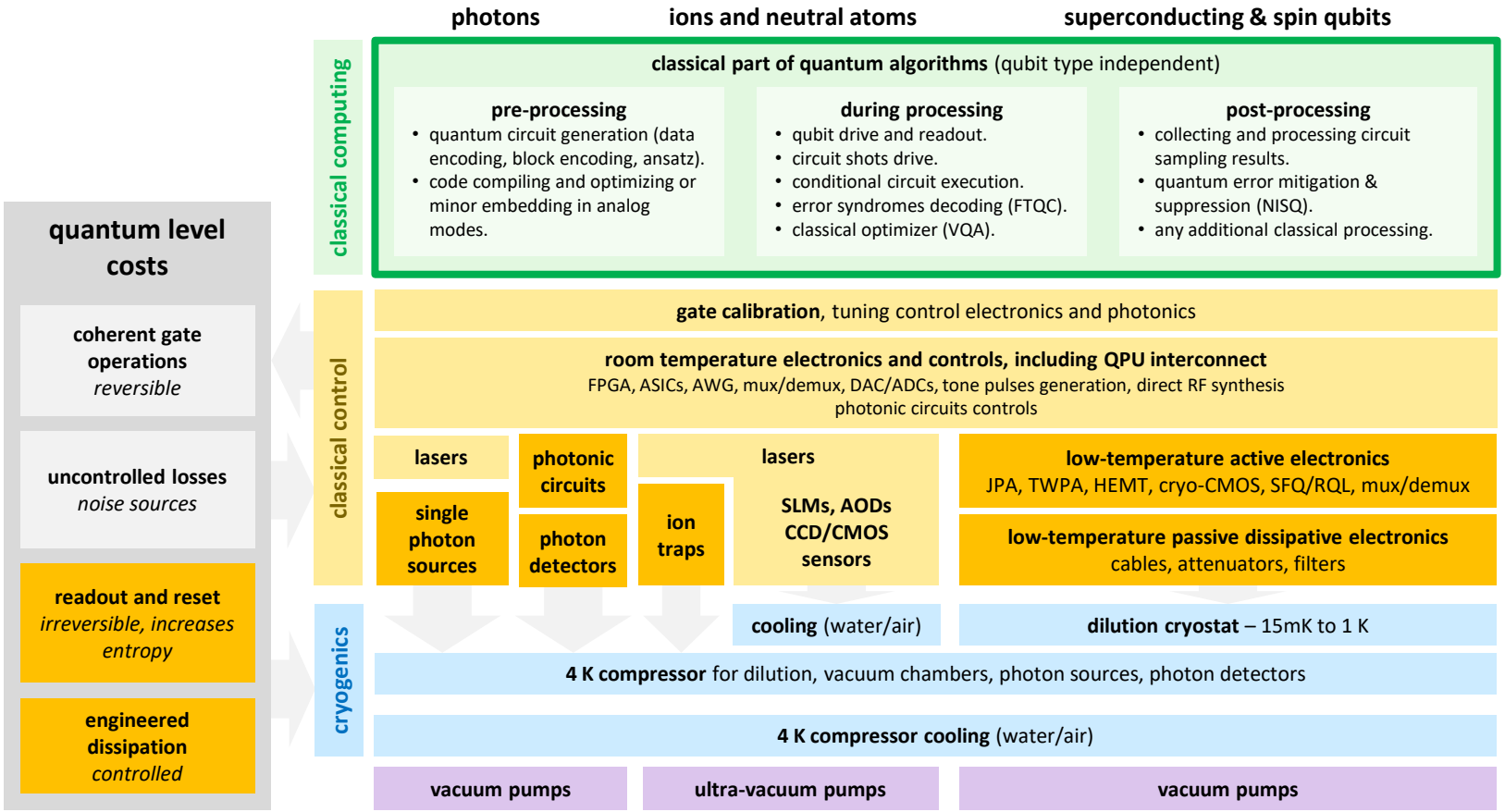
Jenessa Duncombe

https://physicstoday.aip.org/news/how-much-electricity-does-a-quantum-computer-need

sources de consommation d’énergie

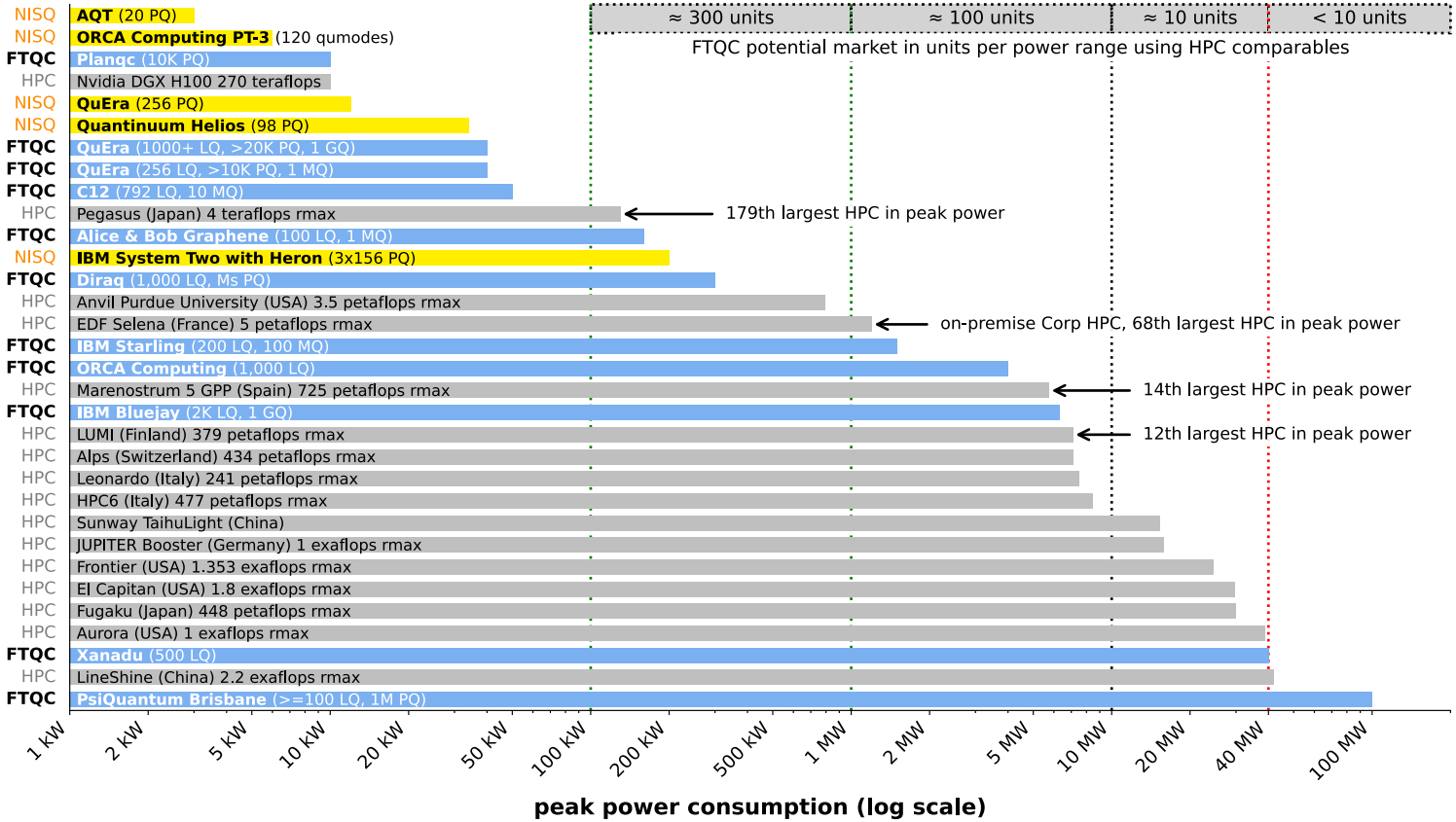


sources de consommation d'énergie



Understanding Quantum Technologies by Olivier Ezratty, as of Septemnber 2026.

estimations de puissances consommées



estimate base power for various FTQCs and actual for existing largest HPCs WW and NISQ QCs. HPC source: TOP 500 and Nvidia. FTQC sources: vendor data or data reconciliation.
PQ: physical qubits
LQ: logical qubits.
MQ: megaquop (logical operations).
TQ: teraquop.

source: Understanding Quantum Technologies 2026, Olivier Ezratty, September 2026

#QEI

the quantum energy initiative

quantum-energy-initiative.org/





QEI 2025 (Grenoble) and 2026 (Barcelona)

why

- ICT energy consumption is growing fast.
- most quantum technologies will add an incremental energetic cost to existing ICT.
- it is time to work on this as quantum technologies and applications are designed.
- responsible innovation imperative.

what

- build a **new** science and engineering field.
- create full-stack methodologies and standards to **evaluate**, **optimize**, and **benchmark** quantum technologies energy consumption.
- favor integrative **full-stack approaches**.

how

- QEI scientific board (10).
- QEI community (545 participants from 67 countries) *.
- QEI workshops (2023 in Singapore, 2025 in Grenoble, 2026 in Barcelona, 2027 in Lisbon).
- QEI IEEE standards Workgroup.
- ≈30 industry partners including IBM, Quandela, etc.

* : as of September 28th, 2026

un nouveau champ scientifique

l'appel initial

Perspective

PRX QUANTUM **3,** 020101 (2022)

Quantum Technologies Need a Quantum Energy Initiative

Alexia Auffèves*
Université Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, Grenoble 38000, France

(Received 18 November 2021; revised 11 April 2022; published 1 June 2022)

prxquantum 3.020101

première méthodologie

PRX QUANTUM **4,** 040319 (2023)

Optimizing Resource Efficiencies for Scalable Full-Stack Quantum Computers

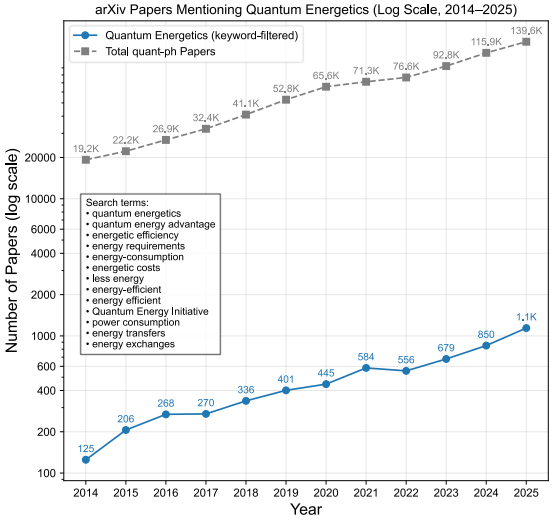
Marco Fellous-Asiani,[1,2,*] Jing Hao Chai,[2,3,4] Yvain Thonnart,[5] Hui Khoon Ng,[6,3,7,†] Robert S. Whitney,[8,‡] and Alexia Auffèves[2,3,7,§]

[1] *Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, Warsaw 02-097, Poland*
[2] *Université Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, Grenoble 38000, France*
[3] *Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore*
[4] *Entropica Labs, 186b Telok Ayer Street, 068632 Singapore*
[5] *Université Grenoble Alpes, French Alternative Energies and Atomic Energy Commission (CEA)–Laboratory for Integration of Systems and Technology (LIST), Grenoble F-38000, France*
[6] *Yale–National University of Singapore (NUS) College, Singapore*
[7] *MajuLab, CNRS-UCA-SU-NUS-NTU International Joint Research Laboratory, Singapore*
[8] *Université Grenoble Alpes, CNRS, Laboratoire de Physique et Modélisation des Milieux Condensés (LPMMC), Grenoble 38000, France*

(Received 29 November 2022; accepted 31 July 2023; published 30 October 2023)

prxquantum 2.040335 arxiv 2112.04022

publications

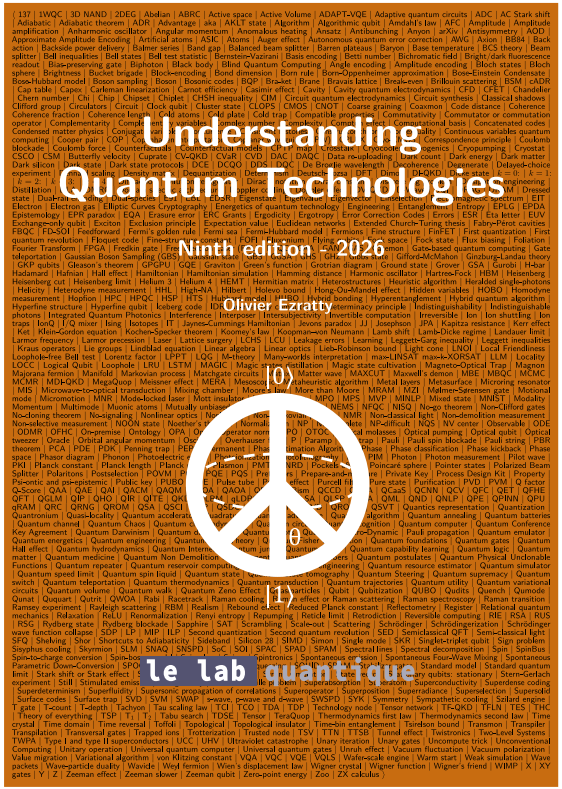


standardisation

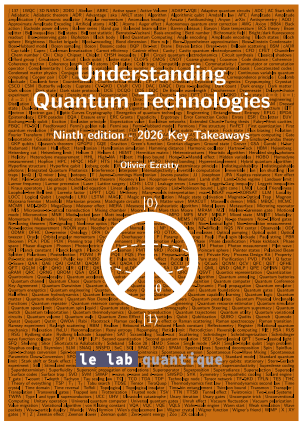


https://sagroups.ieee.org/qei/

téléchargement libre
sans fournir d'information



nouvelle édition
1822 pages
publiée 28 septembre 2026



version courte
38 pages

discussion



support de présentation