A Guided Tour of Quantum Computing
and
the French Quantum Landscape

Mariane Mangin-Brinet – IRN Terascale – 24 novembre 2025

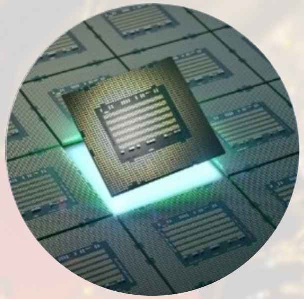
Outline of the presentation:

1. **Introduction: qubits, gates, circuits, and all that….**
2. **Quantum computing in HEP : three examples of applications**
3. **French initiatives in quantum computing**
4. **Conclusion**

What I won’t be talking about:

Quantum communications

Quantum Cryptography



Quantum sensing

Quantum Computing

Quantum Simulation

What I won't be talking about:

Quantum communications

Quantum Cryptography

Quantum sensing

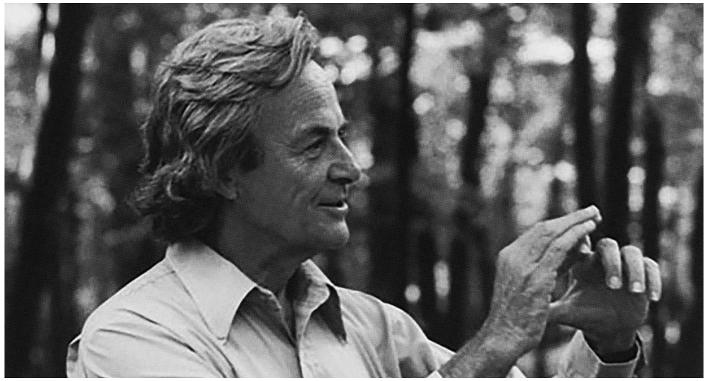
Quantum Computing

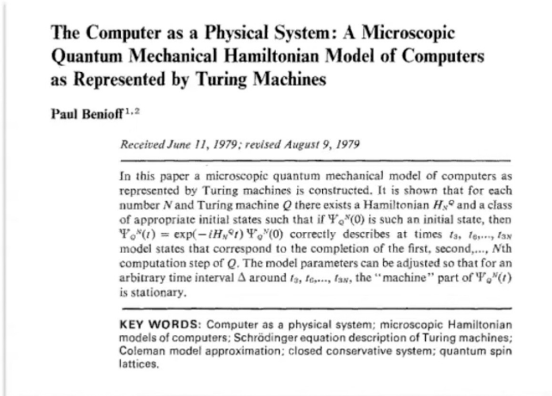
Quantum Simulation

What is quantum computing?

Quantum computing is a computational approach that leverages the principles of quantum mechanics — such as superposition, entanglement, and interference — to perform calculations.

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical."(*)





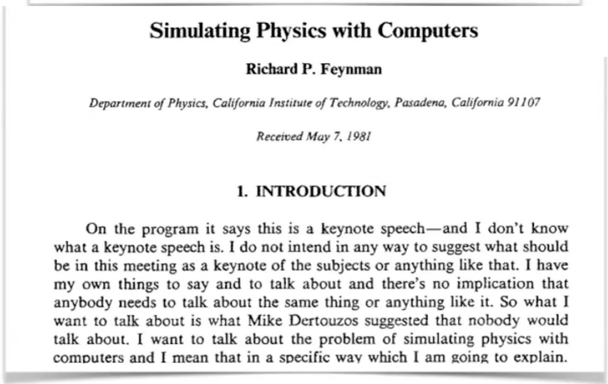
The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines

Paul Benioff[1,2]

Received June 11, 1979; revised August 9, 1979

In this paper a microscopic quantum mechanical model of computers as represented by Turing machines is constructed. It is shown that for each number N and Turing machine Q there exists a Hamiltonian H_N^Q and a class of appropriate initial states such that if $\Psi_Q^N(0)$ is such an initial state, then $\Psi_Q^N(t) = \exp(-iH_N^Q t)\Psi_Q^N(0)$ correctly describes at times $t_3, t_6, \ldots, t_{3N}$ model states that correspond to the completion of the first, second,..., Nth computation step of Q. The model parameters can be adjusted so that for an arbitrary time interval Δ around $t_3, t_6, \ldots, t_{3N}$, the "machine" part of $\Psi_Q^N(t)$ is stationary.

KEY WORDS: Computer as a physical system; microscopic Hamiltonian models of computers; Schrödinger equation description of Turing machines; Coleman model approximation; closed conservative system; quantum spin lattices.



Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain.

[1](*) R. P. Feynman. Simulating Physics with Computers. Int. J. Theor. Phys., 21:467, 1982.
[2] P. Benioff, The Computer as a Physical System, Journal of Stat. Phys., 22: 563–591, 1980
[3] Yu. Manin, Computable and Uncomputable (in Russian), Sovetskoye Radio, Moscow, 1980

What is quantum computing?

Every computation has three main ingredients: data, operations and results

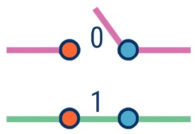
- In quantum circuits:
  - Data = **qubits**
  - Operations = **quantum gates**
  - Results = **measurements**

Qubits

Every computation has three main ingredients: data, operations and results

- In quantum circuits:
  - Data = **qubits**
  - Operations = **quantum gates**
  - Results = **measurements**

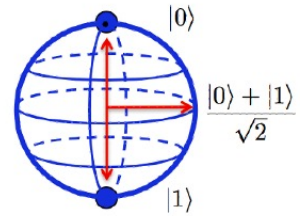
- A classical bit can take two values: 0 or 1.
- It is discrete : a bit is either in state 0, OR in state 1.



Classical bit

- A qubit has two states: |0> or |1>.
- It is continuous: it can be in any superposition state:

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



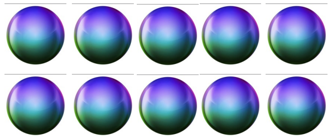
Qubit

Quantum computers rely on encoding information in a fundamentally different way than classical computers

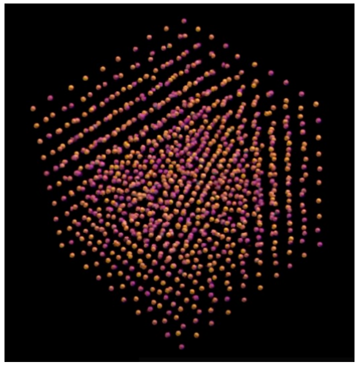
The Exponential Power of Qubits: From 10 to the Universe….

n qubits form a sort of a single object. Qubits are « entangled », that is qubits are correlated.

Hilbert space is a big place.
– Carlton Caves



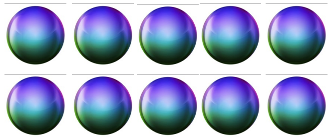
10 qubits can store 2^{10} values simultaneously



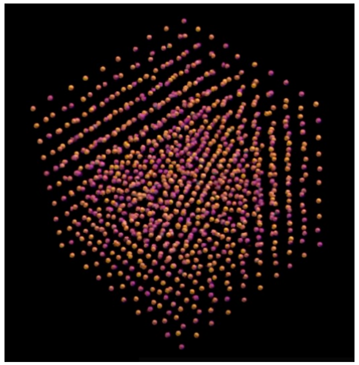
300 qubits can store 2^{300} values in parallel

The Exponential Power of Qubits: From 10 to the Universe….

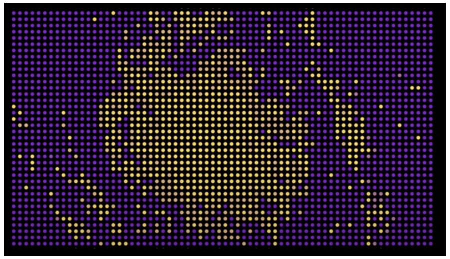
n qubits form a sort of a single object. Qubits are « entangled », that is qubits are correlated.



10 qubits can store 2^{10} values simultaneously



300 qubits can store 2^{300} values in parallel

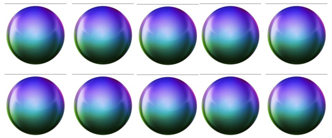


$2^{10} \times 2 \times 10 = 20\,480$ bits

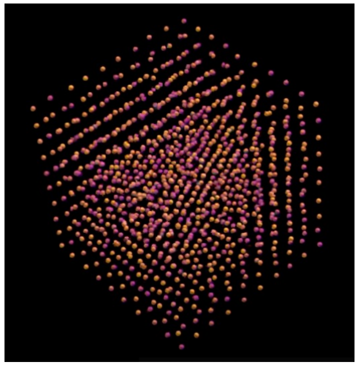
Hilbert space is a big place.
– Carlton Caves

The Exponential Power of Qubits: From 10 to the Universe….

n qubits form a sort of a single object. Qubits are « entangled », that is qubits are correlated.

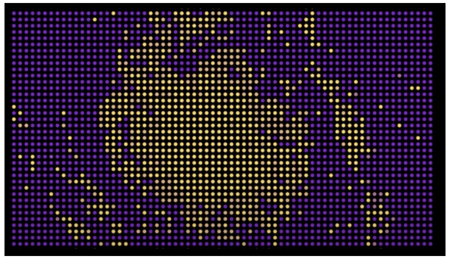


10 qubits can store 2^{10} values simultaneously



300 qubits can store 2^{300} values in parallel

Hilbert space is a big place.
– Carlton Caves



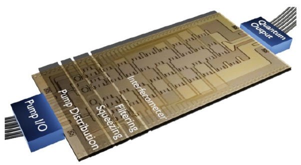
2^{10} x 2 x 10 = 20 480 bits

# of bits bigger than the estimated number of baryons in the visible Universe….

…and more concretely ?

A qubit (or, more precisely, the embodiment of a qubit) is simply a quantum two-level system like the two spin states of a spin 1/2 particle, the ground and excited states of an atom, or the vertical and horizontal polarization of a single photon.

IBM superconducting computer



https://strawberryfields.ai/photonics/hardware/details.html
https://youtu.be/v7iAqcFCTQQ

XANADU

Types of Qubit

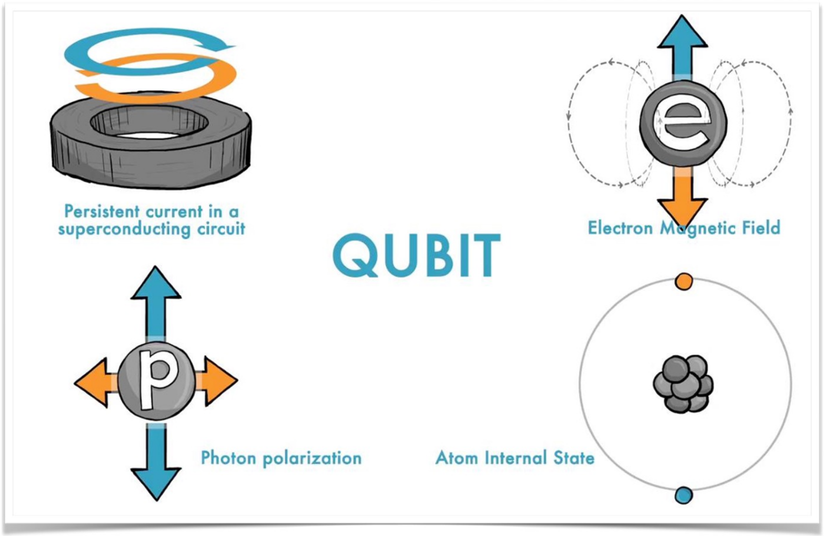
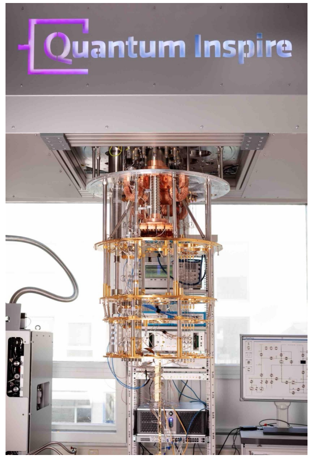
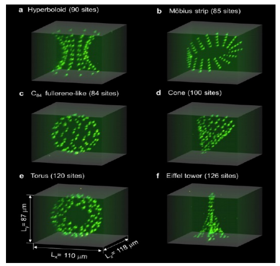


Image Credit: John Preskill



PASQAL



Quantum gates

Every computation has three main ingredients: data, operations and results

- In quantum circuits:
  - Data = **qubits**
  - Operations = **quantum gates**
  - Results = **measurements**

Quantum gates

Theoretical version

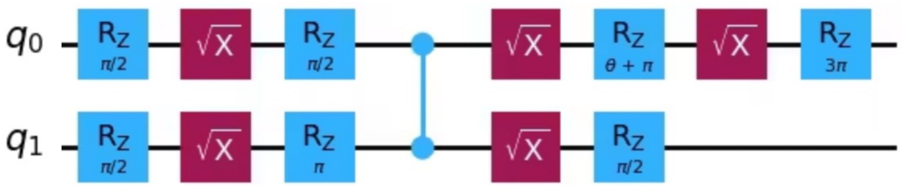
- Quantum systems evolve according to:

$$|\Psi(t)\rangle = \underbrace{e^{iH(t-t_0)}}_{U}|\Psi(t_0)\rangle$$

- For one qubit, the **unitary** 2x2 matrix *U* is identified as a « one-qubit quantum gate ».

- Every such matrix is a possible quantum gate.

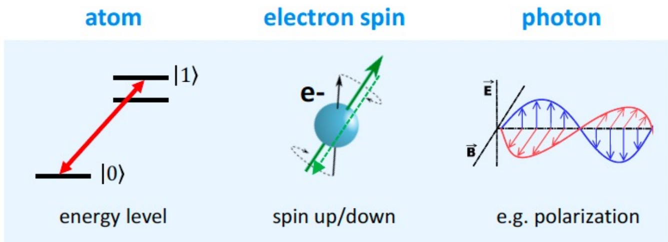
- Qubits + quantum gates = quantum circuit:



logic flows from left to right

Experimental version

Quantum systems are manipulated using techniques depending on the qubit type



laser pulses
microwaves

microwaves
DC current

beam splitters
polarizers

Running a quantum algorithm means applying a succession of pulses/microwave radiations/… to 2-level quantum systems.

Quantum gates

- All gates have the same number of inputs and outputs
- We cannot directly implement some classical gates such as OR, AND, NAND,….
- But we can simulate any classical computation with small overhead
- All operations have an inverse : **reversible computing**
- Theoretically, we could compute without wasting energy (Landauer’s principle, 1961)

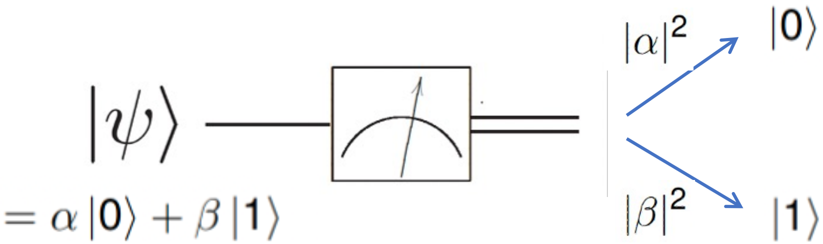
The problem of measurement

Every computation has three main ingredients: data, operations and results

- In quantum circuits:
  - Data = **qubits**
  - Operations = **quantum gates**
  - Results = **measurements**

The problem of measurement

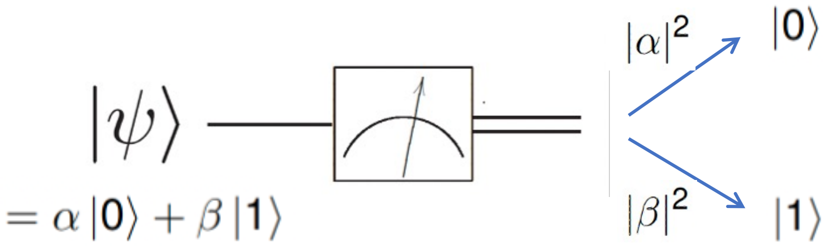
When a quantum system is measured, it collapses into a classical state.



- To get information from a qubit we need to measure it
- After measurement, the qubit **collapses** in one of its possible states.
- When we measure, we obtain **only one** (classical) bit of information
- Measurement result is **probabilistic**, not deterministic
- To reconstruct the probability distribution, we need to perform many measurements

The problem of measurement

When a quantum system is measured, it collapses into a classical state.



- To get information from a qubit we need to measure it
- After measurement, the qubit **collapses** in one of its possible states.
- When we measure, we obtain **only one** (classical) bit of information
- Measurement result is **probabilistic**, not deterministic
- To reconstruct the probability distribution, we need to perform many measurements

⇒ We cannot perform several independent measurements of $|\psi\rangle$ because we cannot copy the state (**no-cloning theorem**)

⇒ Qubit measurement is done only at the end of computing

⇒ We cannot measure a qubit state in the middle of an algorithm to perform some conditional branching

→ totally new paradigm of computation

Quantum computing challenges

- In classical computing, results are deterministic. In quantum computing, they are not. You have to run the experiment **many times** to get probabilistic results.

- Measurements intrinsically modify the system
  → **system needs to be totally isolated**

- We need to interact with the qubits to control them (entanglement, input and output data,…)
  → **system must not be totally isolated!**

- Several sources of noise:
  - Quantum decoherence: spontaneous decay from the excited state $|1\rangle$ to the ground state $|0\rangle$
    → progressively disturbing superposition and entanglement
  - Errors occur during the application of quantum gates:
    - a gate to one qubit affects nearby qubits unintentionally.
    - qubits can go to higher energy states.

- Limit on the number of gates that can be applied to quantum systems (« depth of circuits »)

→ NISQ era and quantum error correction techniques

Quantum algorithm's main goal is to amplify the computational basis state amplitude that is the sought result, while reducing all the other amplitudes to near zero.

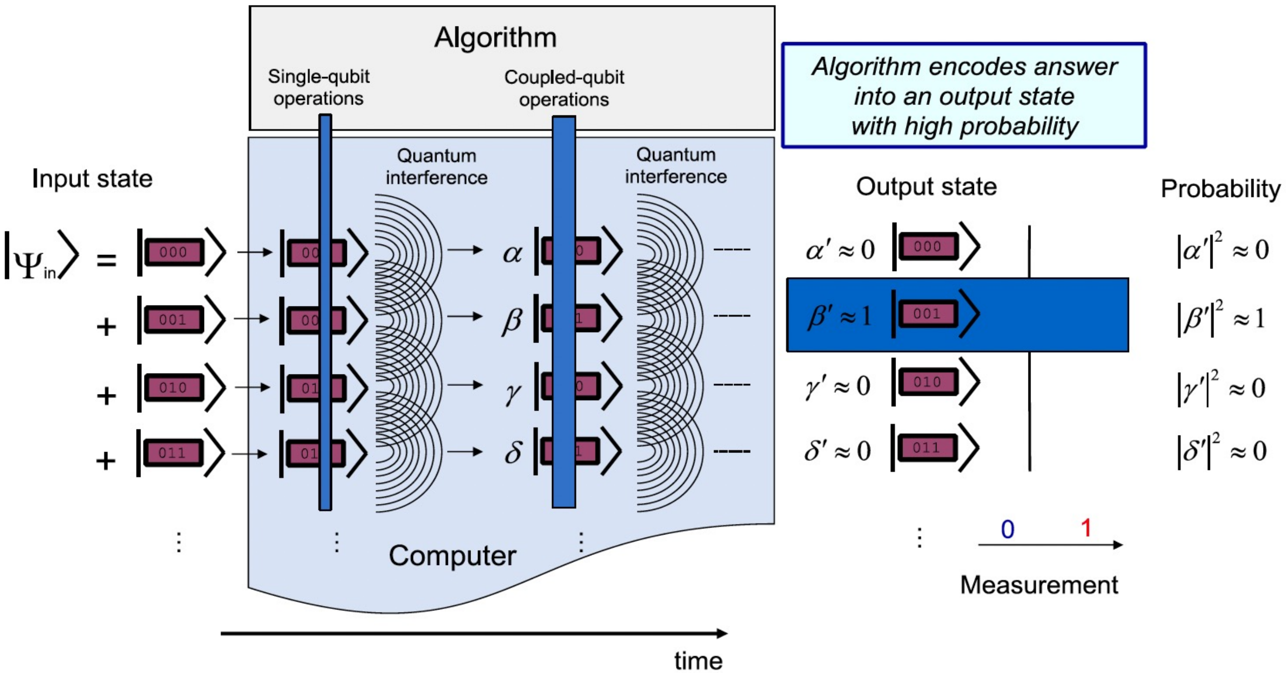
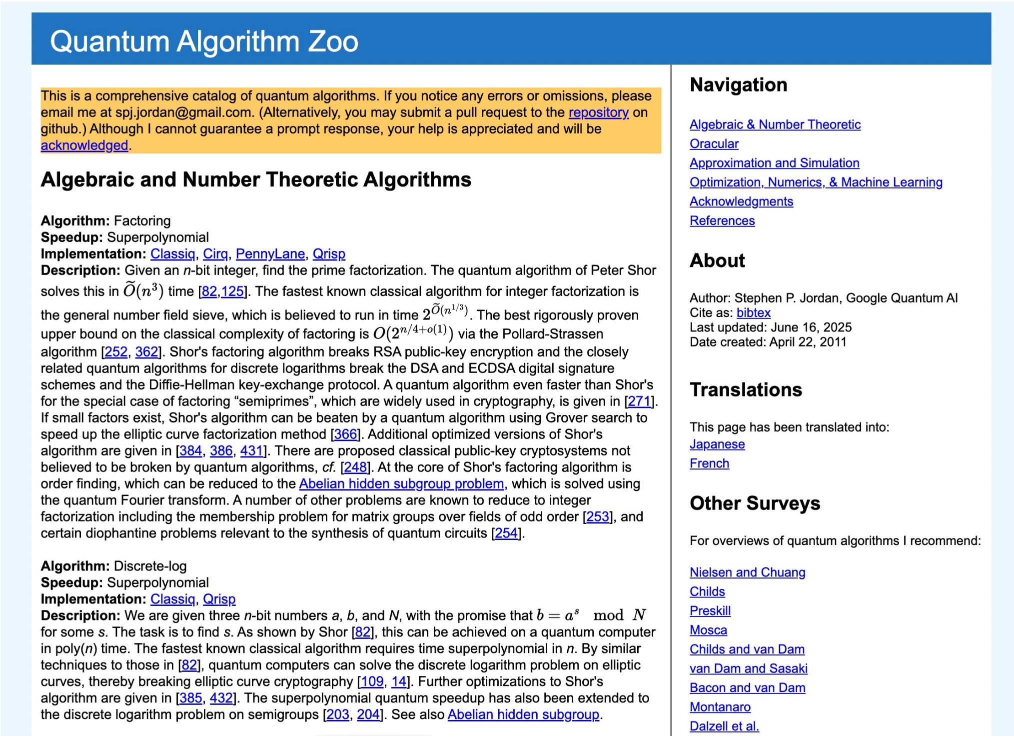


Figure 186: representing qubits manipulations with interferences.
Source: Introduction to Quantum Computing by William Oliver from MIT, December 2019 (21 slides).

Quantum algorithms



Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at spj.jordan@gmail.com. (Alternatively, you may submit a pull request to the repository on github.) Although I cannot guarantee a prompt response, your help is appreciated and will be acknowledged.

Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Implementation: Classiq, Cirq, PennyLane, Qrisp
Description: Given an *n*-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\widetilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time $2^{\widetilde{O}(n^{1/3})}$. The best rigorously proven upper bound on the classical complexity of factoring is $O(2^{n/4+o(1)})$ via the Pollard-Strassen algorithm [252, 362]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. A quantum algorithm even faster than Shor's for the special case of factoring "semiprimes", which are widely used in cryptography, is given in [271]. If small factors exist, Shor's algorithm can be beaten by a quantum algorithm using Grover search to speed up the elliptic curve factorization method [366]. Additional optimized versions of Shor's algorithm are given in [384, 386, 431]. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, *cf.* [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem, which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

Algorithm: Discrete-log
Speedup: Superpolynomial
Implementation: Classiq, Qrisp
Description: We are given three *n*-bit numbers *a*, *b*, and *N*, with the promise that $b = a^s \mod N$ for some *s*. The task is to find *s*. As shown by Shor [82], this can be achieved on a quantum computer in poly(*n*) time. The fastest known classical algorithm requires time superpolynomial in *n*. By similar techniques to those in [82], quantum computers can solve the discrete logarithm problem on elliptic curves, thereby breaking elliptic curve cryptography [109, 14]. Further optimizations to Shor's algorithm are given in [385, 432]. The superpolynomial quantum speedup has also been extended to the discrete logarithm problem on semigroups [203, 204]. See also Abelian hidden subgroup.

Navigation

Algebraic & Number Theoretic
Oracular
Approximation and Simulation
Optimization, Numerics, & Machine Learning
Acknowledgments
References

About

Author: Stephen P. Jordan, Google Quantum AI
Cite as: bibtex
Last updated: June 16, 2025
Date created: April 22, 2011

Translations

This page has been translated into:
Japanese
French

Other Surveys

For overviews of quantum algorithms I recommend:

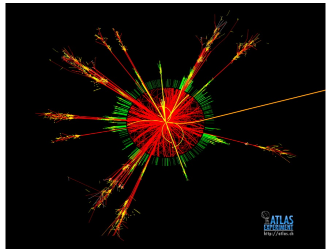
Nielsen and Chuang
Childs
Preskill
Mosca
Childs and van Dam
van Dam and Sasaki
Bacon and van Dam
Montanaro
Dalzell et al.

- Factorisation algorithms
- Search algorithms
- Optimisation algorithms
- Simulation algorithms
- Hybrid algorithms
- Useless algorithms

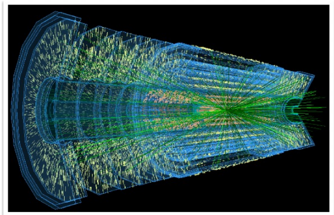
Quantum computing in High Energy Physics

How can quantum computing be useful in HEP?

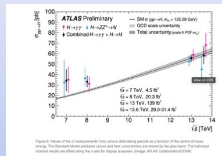
- Simulation
    - Lattice field theories



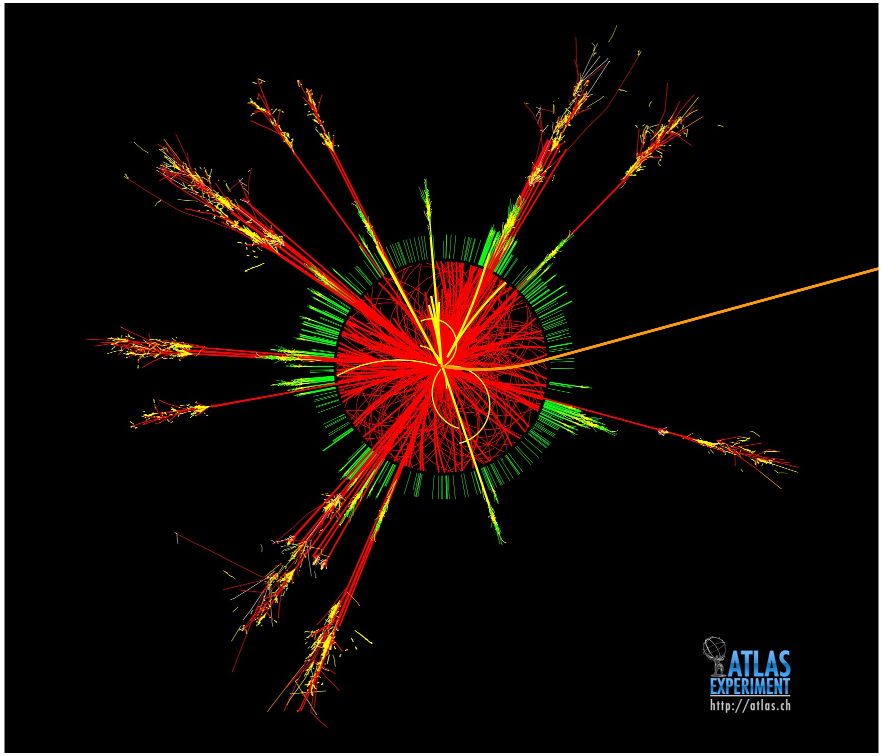
- Reconstruction
    - Particle tracking



- Analysis
    - A machine-learning inspired example



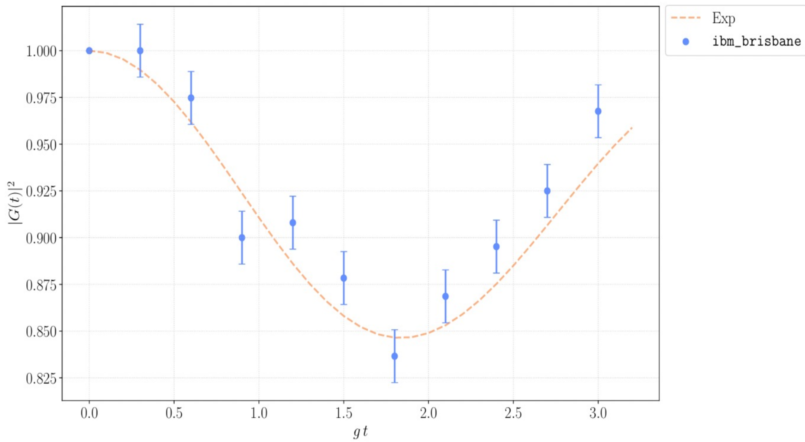
Simulation



Quantum computing in High Energy Physics

- Lattice field theory aim: solving field theory from first principles and without approximation (non-perturbative regime)
- Active developments in
  - Hamiltonian construction for non-abelian gauge theory
  - Hybrid classical/quantum algorithms
  - Simulation of low-dimensional toy models (1+1D Schwinger model, SU(2) gauge theories,…):

$$G(t) = \langle \mathrm{vac} \left| e^{-iHt} \right| \mathrm{vac} \rangle$$

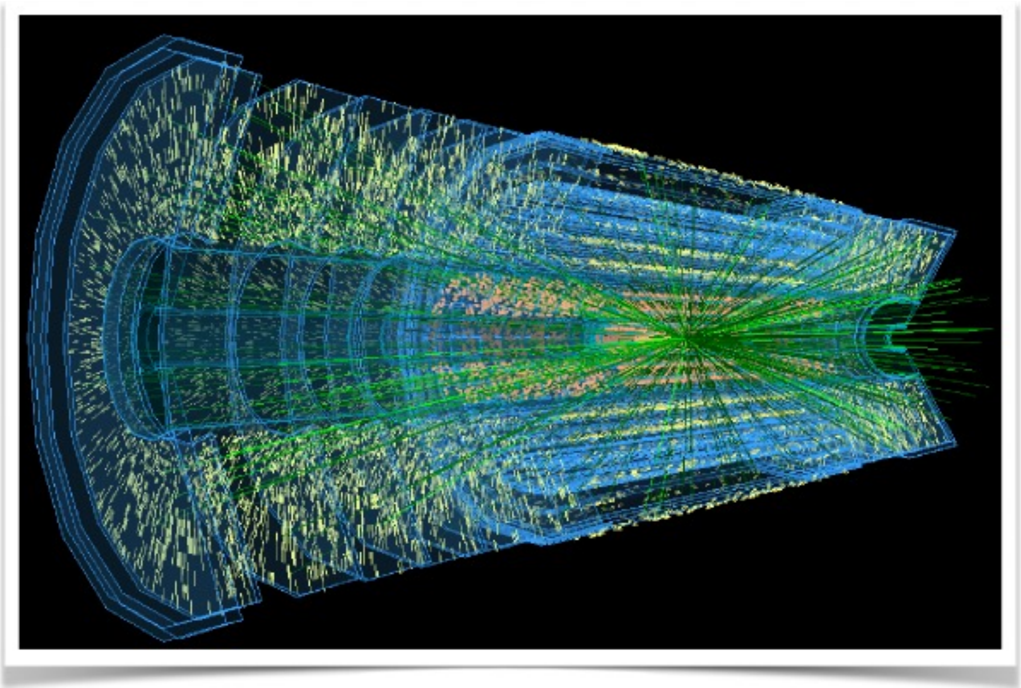


(*) Time-evolution of the Schwinger model via HT run on the ibm brisbane 127-qubit quantum computer.

- Many challenges to overcome
  - Maintaining Gauss's law constraints on quantum circuits is nontrivial
  - Long-time simulations are highly sensitive to gate fidelity and noise

(*)J. Ingoldby et al., *Enhancing quantum field theory simulations on NISQ devices with Hamiltonian truncation,* Phys. Rev. D **110**, 096016

Reconstruction

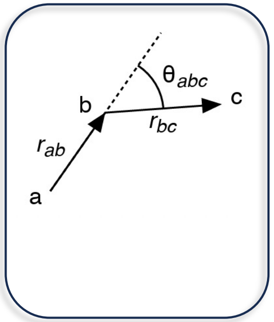


The tracking challenge

Quantum annealing algorithm (in a very small nutshell….): technique to solve combinatorial optimization problems by encoding the solution as the ground state of some Hamiltonian.

Two steps:

- Reformulate the track reconstruction as an energy minimisation problem:



(simplified) representation of three hits *a*, *b*, and *c*

$$|\Psi(t)\rangle = e^{iH(t-t_0)}|\Psi(t_0)\rangle$$

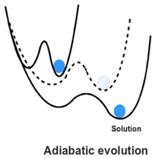
qubits state → $|\Psi(t)\rangle$

Hamiltonian (energy) encoding information on track classification → H

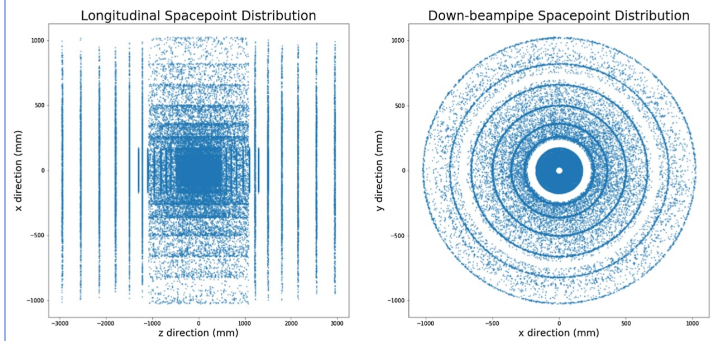
$$H \approx -\sum_{a,b,c}\left(\frac{\cos\theta_{abc}}{r_{ab}+r_{bc}}s_{ab}s_{bc}\right) - \alpha W_{reward} + \beta W_{penalty}$$

If s_{ab}= 1 then *a* and *b* are assumed to have been created by the same particle (0 otherwise)

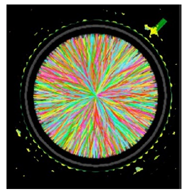
- Initialize the quantum system in the ground state of another known, and easy to control, Hamiltonian and then let the system evolve by slowly changing the Hamiltonian to the target one.



Based on A. Zlokapa, et al., *Charged particle tracking with quantum annealing-inspired optimization*, Quantum Mach. Intell. 3, 27 (2021)



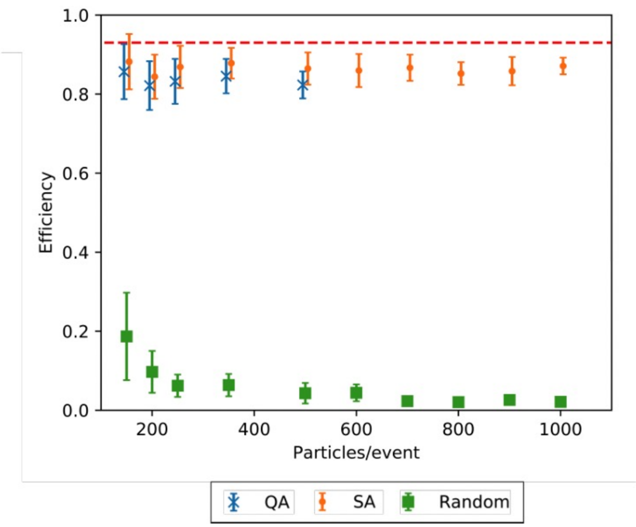
Spatial distribution of the spacepoints of a typical event (TrackML dataset).

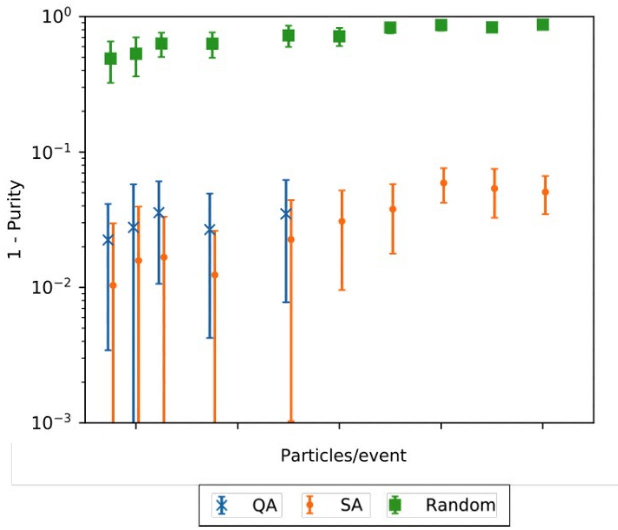


- ~ 5000 charged particles per event
- Need to reconstruct all these particles
  - efficiently (>99%),
  - with low fake rate (<<1%)
  - and quickly…

The tracking challenge

Interesting because global way of solving the problem
→ potential to have a solution which does not scale exponentially with the number of tracks





- Run on D-Wave 2X (1098 superconducting qubits)
- Proved to work on a real quantum computer, even if with a limited number of tracks (500)
- Quantum speedup not directly identified in this work, but very promising (quantum annealing is one of the only quantum hardware approaches that can accommodate very large tracking problems).

Based on A. Zlokapa, et al., *Charged particle tracking with quantum annealing-inspired optimization*, Quantum Mach. Intell. 3, 27 (2021)

Quantum computing in High Energy Physics

Analysis

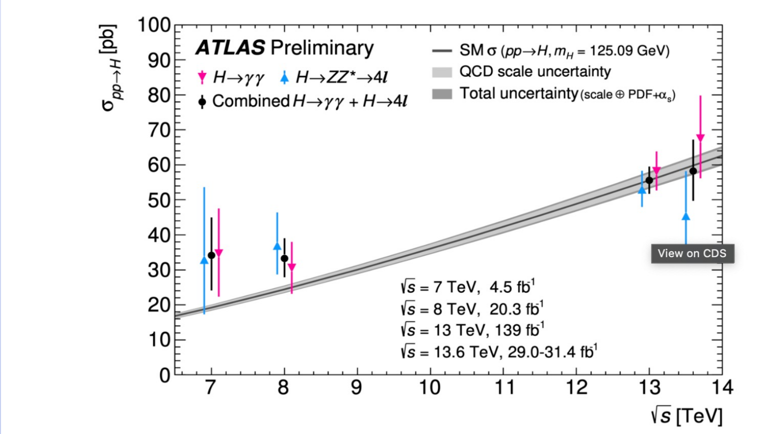


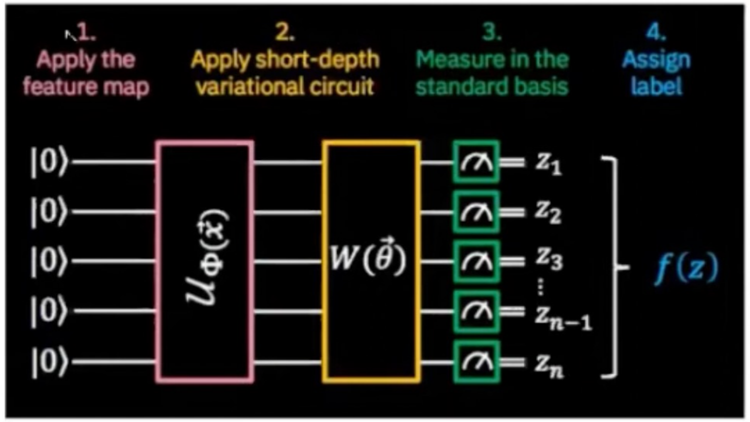
Figure 6: Values of the σ measurements from various data-taking periods as a function of the centre-of-mass energy. The Standard-Model predicted values and their uncertainties are shown by the grey band. The individual channel results are offset along the x-axis for display purposes. (Image: ATLAS Collaboration/CERN)

Quantum computing in High Energy Physics

Quantum Machine Learning (QML) at the intersection between machine learning and quantum computing
No fully quantum machine learning: most promising methods are hybrid classical/quantum.

- Proof of principe : Variational Quantum Classifier (100 events, 10 variables) for $t\bar{t}H$ and $H \rightarrow \mu\,\mu$

  1. Encode input data $\vec{x}$ in quantum state $|\Psi(t)\rangle$
  2. Apply a variational circuit *W(θ)* which is parametrized by gate angles θ
  3. Measure the qubits
  4. Assign the label « signal » or « background » to the event

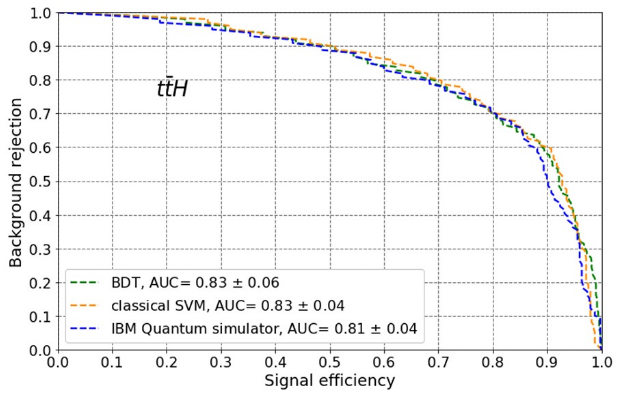


- During the training phase, a set of events are used to train the circuit *W(θ)* to reproduce correct classification
- Using *W(θ)* optimized, an independent set of events are used for evaluation and testing

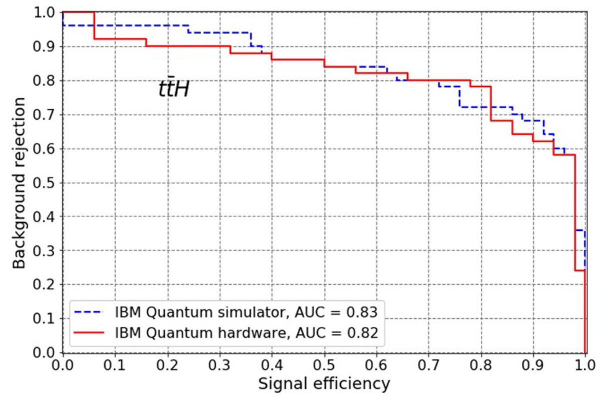
S. L. Wu et al, *Application of Quantum Machine Learning using the Quantum Variational Classifier Method to High Energy Physics Analysis at the LHC on IBM Quantum Computer Simulator and Hardware with 10 qubits, arXiv:2012.11560v2,* J. Phys. G: Nucl. Part. Phys. 48 125003
https://quanthep.eu/event/quanthep-seminar-sau-lan-wu/

Quantum computing in High Energy Physics

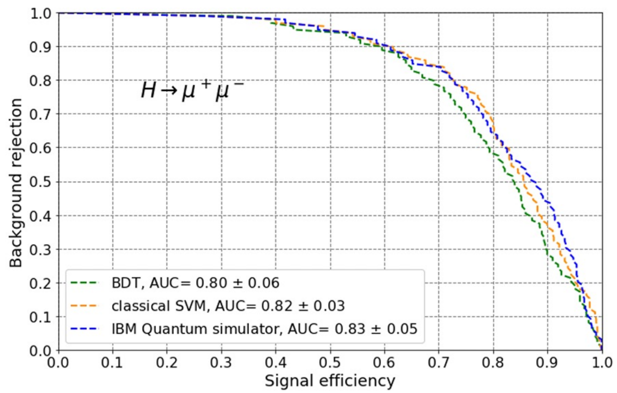
Quantum Machine Learning (QML) at the intersection between machine learning and quantum computing
No fully quantum machine learning: most promising methods are hybrid classical/quantum.



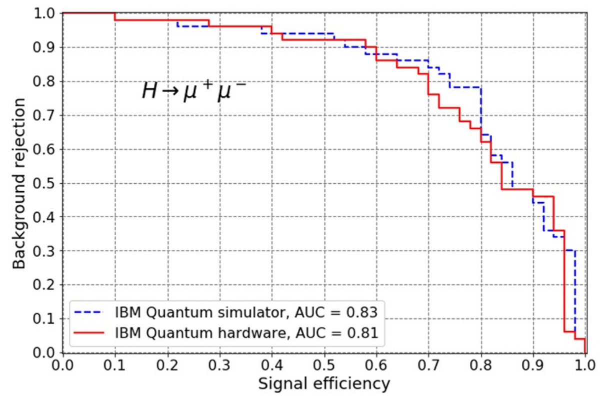
(a)



(a)



(b)



(b)

French quantum computing landscape

French National Quantum Strategy (2021):

- Launched in **2021**, 5-year strategy
- Budget: **€1.8 billion**
- Coordinated across several ministries
- Contributions from **CNRS**, **CEA**, **INRIA**, **Conférence des Présidents d'Université (CPU)**
- Strong support for industry, training, and innovation

Three pillars:

- Academic landscape:
    - World-class expertise in quantum physics, mathematics, computing science,…
    - Strong national projects:
        - **PEPR Quantique**, ANR grants
        - QuanTEdu-France: national training program to develop skills in quantum technologies.
    - Active hubs: Paris-Saclay, Paris-Centre, Grenoble, Occitanie,…

French quantum computing landscape

French National Quantum Strategy (2021):

- Launched in **2021**, 5-year strategy
- Budget: **€1.8 billion**
- Coordinated across several ministries
- Contributions from **CNRS**, **CEA**, **INRIA**, **Conférence des Présidents d'Université (CPU)**
- Strong support for industry, training, and innovation

Three pillars:

- Industry Ecosystem:
  - **Pasqal**, a global leader in neutral-atom analog quantum processors.
  - **Quandela**, specializing in photonic qubits and already shipping machines to customers.
  - **Alice & Bob**, focused on cat qubits and hardware-efficient error correction.
  - **C12,** exploring carbon-nanotube-based qubits.
  - …

French quantum computing landscape

French National Quantum Strategy (2021):

- Launched in **2021**, 5-year strategy
- Budget: **€1.8 billion**
- Coordinated across several ministries
- Contributions from **CNRS**, **CEA**, **INRIA**, **Conférence des Présidents d'Université (CPU)**
- Strong support for industry, training, and innovation

Three pillars:

- Infrastructure & Access:

  Providing access to quantum machines and HPC–quantum hybrid architectures

  - **HQI** (Hybrid Quantum Infrastructure): program combining classical supercomputing with quantum systems (GENCI, TGCC): aims to build a hybrid platform and software stack for quantum-classical computation, open to academic and industrial users.
  - Neutral-atom (Pasqal) and photonic (Quandela) platforms are available for academic users (https://www.edari.fr/).

French quantum computing landscape

French National Quantum Strategy (2021):

- Launched in **2021**, 5-year strategy
- Budget: **€1.8 billion**
- Coordinated across several ministries
- Contributions from **CNRS**, **CEA**, **INRIA**, **Conférence des Présidents d'Université (CPU)**
- Strong support for industry, training, and innovation

Three pillars:

- Infrastructure & Access:

  Providing access to quantum machines and HPC–quantum hybrid architectures

  - **HQI** (Hybrid Quantum Infrastructure): program combining classical supercomputing with quantum systems (GENCI, TGCC), aims to build a hybrid platform and software stack for quantum-classical computation, open to academic and industrial users.

  - Neutral-atom (Pasqal) and photonic (Quandela) platforms are available for academic users (https://www.edari.fr/).

Reality check:

- Strong scientific foundations but **scaling remains challenging**
- Competing with US and Chinese investments several orders of magnitude larger

French quantum computing landscape

IN2P3 initiatives

- QC2I project: quantum simulation, QML & N-body problems
- Simulation of nuclear and particle-physics systems (IJCLab, LPSC)
- Strategic quantum-tech watch

INP intiatives

- Photon-photon interaction research (LPENS, LPTHE) → toward photonic qubits
- “Plaquette Quantique”: cross-disciplinary R&D & partnerships (Pasqal, Alice-&-Bob, C12)
- Quantum education & community building: QUANTSIM school, Quantum Frontiers

CERN Quantum Technology Initiative & QC4HEP:

- Launched in 2020 to explore quantum computing, sensing and communication for HEP
- Coordinate together CERN departments, European universities, and industry partners
- Structures R&D themes, training, and technology road-mapping.
- QC4HEP: Working groups identifying HEP problems suited for quantum algorithms
- Organizes workshops, tutorials and QT4HEP events

CERN | IQ QUANTUM TECHNOLOGY INITIATIVE

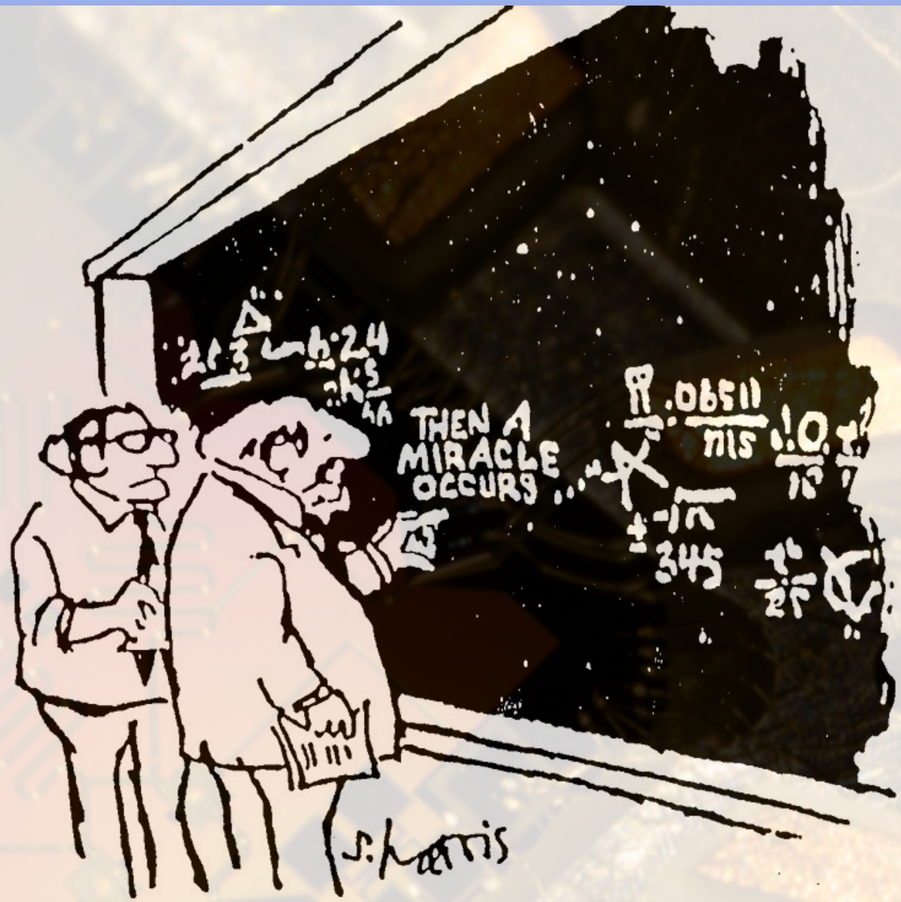
Conclusion

- Quantum computing is a fascinating field of research.
- It is evolving rapidly, both on the theoretical and technological point of view: although theorized more than 40 years ago, technology has only become available in the past decades (first online accessible quantum computing : 2016). Still many difficulties to overcome…
- A wide range of technologies are being actively explored : trapped ions, superconducting, photonic, silicon…
- Quantum computers are not general purpose computers: they may be able to perform tasks that classical computers cannot and to solve **certain** problems far more quickly than classical ones.
- There is a constant and fruitful quantum–classical interplay: quantum research is improving classical computing.
- Long-haul research program, and short-term expectations must stay modest….
- …but research field evolving rapidly and it is the right time to start diving into it !

Some references used for this talk

- R. P. Feynman. *Simulating Physics with Computers.* Int. J. Theor. Phys., 21:467, 1982.
- P. Benioff*, The Computer as a Physical System,* Journal of Stat. Phys., 22: 563–591, 1980
- Yu. Manin*, Computable and Uncomputable* (in Russian), Sovetskoye Radio, Moscow, 1980
- H. Gray, *Introduction to Quantum Computing – Lectures 1, 2 and 3 – CERN Lectures*
- *E. Combarro A practical introduction to quantum computing - CERN Lectures*
- Ju, X., Murnane, D., Calafiura, P. *et al. Performance of a geometric deep learning pipeline for HL-LHC particle tracking*. *Eur. Phys. J. C* **81**, 876 (2021).
- A. Zlokapa, et al., *Charged particle tracking with quantum annealing-inspired optimization*, Quantum Mach. Intell. 3, 27 (2021)
- *C. Bauer,*
- *O. Ezraty, "Understanding Quantum Technologies", https://www.oezratty.net/wordpress/2024/understanding-quantum-technologies-2024/*
- S. L. Wu et al*, Application of Quantum Machine Learning using the Quantum Variational Classifier Method to High Energy Physics Analysis at the LHC on IBM Quantum Computer Simulator and Hardware with 10 qubits, arXiv:2012.11560v2,* J. Phys. G: Nucl. Part. Phys. 48 125003, *https://quanthep.eu/event/quanthep-seminar-sau-lan-wu/*
- *Atlas experiment, public results, https://twiki.cern.ch/twiki/bin/view/AtlasPublic*
- *Google Quantum AI website*
- *https://quantique.france2030.gouv.fr/talents/programme-de-formation/*
- …
-

THANK YOU !



"I think you should be more explicit here in step two"