

Opinions Libres
le blog d'Olivier Ezratty

Actualités quantiques de novembre 2026

Dans ce 86ième épisode de Quantum, nous revenons sur l'actualité du mois de novembre 2026. Il s'est encore passé par mal de choses tant du point de vue scientifique que technologique et économique. Et tout ce bruit sur les prouesses de l'IA qui pourraient notamment remettre en cause la cryptographie classique, y compris la PQC, sans compter le calcul quantique lui-même. Ça chahute dans le Landerneau quantique !

Evénements

Nobel Symposium en Afrique du Sud fin octobre

Fin octobre avait lieu un **séminaire** en Afrique du Sud à l'université Stellenbosch rassemblant des pointures en physique et technologies du calcul quantique, dont deux prix Nobel, Alain Aspect et John Martinis. Il y avait notamment Peter Zoller, Rainer Blatt, John Preskill, Lieven Vandersypen sur les spins. Jian-Wei Pan pour la Chine, et côté français Antoine Browaeys et Alexia Auffèves. Les discussions portaient sur les défis aussi bien algorithmiques que physiques et technologiques dans le calcul quantique. Les présentations étaient à huit-clôt. On peut cependant récupérer la **présentation** de John Preskill sur la correction d'erreurs.

World Quantum Cannes Festival les 17 et 18 novembre

1200 personnes et près de 200 intervenants s'y retrouvaient pour la **première édition** de cet événement. Avec notamment Peter Zoller (Innsbruck), William Oliver (MIT) et de nombreux intervenants de startups connues (Quandela, Quobly, Pasqal, Welinq) et moins connues (Zuriq, Qarakal, Eleqtron, SaxonQ). Fanny y intervenait pour OVHcloud et moi sur **l'énergétique** et à animer un après-midi et un panel sur le FTQC avec Maud Vinet (Quobly), Pavel Hrmo (Zuriq) et Simon Groblacher (Qphox). Il y avait aussi, côté politique, une intervention de David Lisnard, l'un des candidats à l'élection présidentielle en France. On dit qu'il a un livre sur le quantique sur sa table de chevet mais on ne sait pas lequel.



SuperComputing Chicago du 15 au 20 novembre

Le grand événement du supercomputing. Avec plein de startups du quantique représentées dont Alice & Bob et Pasqal. Ainsi qu'IQM et plein d'autres acteurs du secteur, ce qui est tout à fait normal. La communauté du HPC est la première cible "commerciale" pour l'ordinateur quantique.

OVHcloud AI summit 19 novembre

Il rassemblait 2500 personnes au Carrousel du Louvre avec plusieurs conférences sur le quantique avec Serco et l'intégration de la plateforme quantique d'OVHcloud. L'intégration technologies a été faite avec l'ESA pour utiliser les données du jumeau numérique de la terre avec un émulateur quantique et de l'IA classique. Il y avait aussi une table ronde sur la cryptographie post-quantique et enfin, une masterclass de Quandela sur l'émulateur Merlin. Et le lancement d'Olala, le LLM d'OVHcloud.

Colloque Annales des Mines le 10 novembre à Bercy

Avec des interventions en keynote ou en panel des auteurs des **articles** des deux volumes de ce gros dossier préparé par Frédéric Barbaresco (Thales) et François Gérin (SEE) paru en mai et août 2026. J'y suis intervenu dans un panel pour parler, au hasard, d'énergétique du calcul quantique, sous la houlette d'Emmanuelle Vergnaud.

Intervention pour QuantMA à Marseille le 26 novembre

J'intervenais à l'Université Aix-Marseille à Marseille dans le cadre de la nouvelle série de séminaires sur le quantique lancée par QuantMA qui est l'écosystème quantique local, voisin dans sa forme de l'écosystème QuantAlps à Grenoble. Y participaient chercheurs doctorants, post-docs et enseignants. Voici mes **slides** ainsi qu'un **transcript édité de mon intervention** avec les slides réalisés en combinant Whisper pour le speech-to-text et ChatGPT pour la remise en forme et l'intégration des slides.

TQCI Benchmark les 26 et 27 novembre

Avec beaucoup d'interventions sur le benchmarking. J'y intervenais le second jour avec Marco Fellous-Asiani (Inria) et Ariane Soret (Quandela) sur les estimations de ressources du calcul FTQC, dont évidemment l'énergie (**slides**).

A noter l'intervention de Jeanette Lorenz de Fraunhofer qui évoquait un papier publié le jour-même sur la difficulté d'obtenir un avantage quantique avec de la QML à base de HHL pour un réseau de neurones de type ResNet à 32 couches. **A Realistic End-to-End Runtime Crossover Estimation for Quantum-Enhanced Training of Large-Scale Machine Learning Models** by Maximilian Alexander Wolf, Alona Sakhnenko, Florian Geissler, Andrea Matic, and Jeanette Miriam Lorenz, arXiv, November 2026 (15 pages). L'évaluation intègre l'encodage des données (level III), ce qui mène à un temps de calcul supérieur de plusieurs ordres de grandeur à l'âge de l'Univers. Mais c'est basé sur l'emploi d'une tomographie pour récupérer les poids du réseau de neurone entrainé et les utiliser pour réaliser des inférences classiques. Si on utilisait le circuit pour réaliser directement des inférences, le temps de calcul serait cependant aussi énorme. Avec un LLM de 405 milliards de paramètres type Llama, le temps pour une simple inférence serait de plus de 10^19 années. C'est un peu long pour obtenir un simple token !

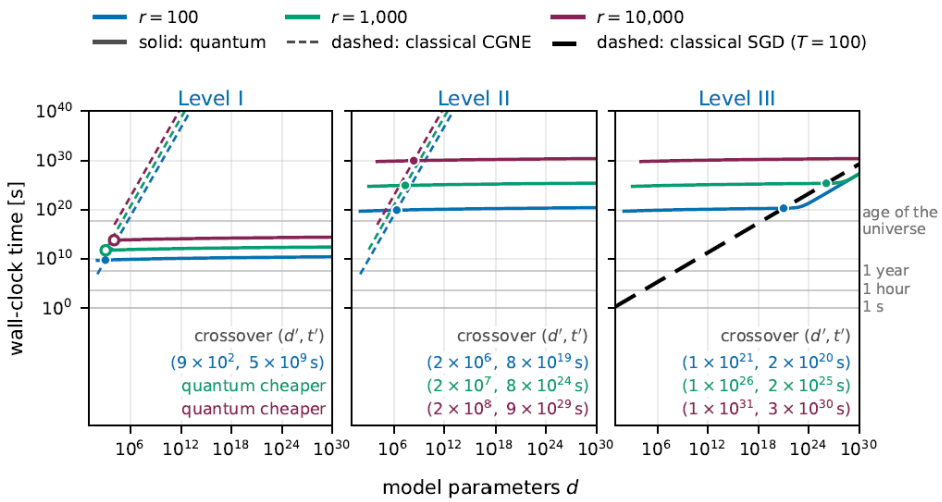


Figure 2: `Level I – III` for the constant sparsities $r = 100$ (blue), $r = 1{,}000$ (green) and $r = 10{,}000$ (purple) at $K = 3$, $T = 100$, $r_F = 10^9$ FLOP/s, $\tau_T = 10$ ns. Solid curves are the quantum estimation, dashed curves the classical one, the colour gives r, and a lower curve means a faster runtime. `Level I` (core solver): HHL vs CGNE solve of the lifted history system N_h. The core grows only as $\log d$, CGNE as d^3, and both scale with s_M, so the crossover point $d' \approx 10^3$ for $r = 100$, while for $r = 1{,}000$ and $r = 10{,}000$ the quantum core is already cheaper at the smallest admissible size $d = r$. `Level II` (full solver): HHL with state preparation and tomography vs CGNE solve. Every copy repeats the run and n_{copies} grows as r^3, so d' moves with r. `Level III` (full pipeline): HHL with state preparation and tomography plus classical preprocessing vs $T = 100$ steps of SGD (black). The quantum curves stay nearly flat until the one classical gradient calculation per window dominates.

A venir :

- **EQTC du 30 novembre au 3 décembre à Dublin.** Quatre jours à la croisée des chemins entre policy makers pour parler du Quantum Act annoncé le 25 novembre, scientifiques et entrepreneurs. Fanny et moi y intervenons à divers endroits, dans des panels et jury.

- **AdoptAI au Grand Palais** à Paris les 3 et 4 décembre avec le hackathon Défense-Quantique organisé par l'AID du ministère des Armées. Avec Quobly, Quandela et Alice & Bob et OVHcloud qui est partenaire et 12 équipes qui vont plancher pendant 3 jours et même dormir au Grand Palais.

- **Q2B Chicago** du 8 au 10 décembre (**agenda**). C'est la première fois que la conférence a lieu dans cette ville, après avoir été à Santa Clara depuis 2017.

- **Minalogic Innovation Talks quantique** le 17 décembre à Grenoble (**agenda**). J'y interviens en keynote sur l'énergétique du calcul quantique, accompagné de Christophe Domain d'EDF pour évoquer le projet OECQ qui associe EDF, Quandela, Alice & Bob, le CNRS ainsi que la QEI.

Understanding Quantum Technologies 2026 disponible sur Amazon

Les 5 parties y **sont disponibles**. C'est un beau cadeau de Noël pour ceux qui aiment le papier! Fin de la publicité.

Prix Jean Ricard de la SFP décerné à Alexia Auffèves

C'est une **belle reconnaissance** de la Société Française de Physique qui valorise un parcours original de scientifique à la croisée de nombreux chemins, dont celui de la Quantum Energy Initiative. Elle est directrice de recherche CNRS et directrice du laboratoire international Majulab du CNRS à Singapour. Parmi les lauréats précédents, citons Pascale Senellart, Jacqueline Bloch et Philippe Grangier.

Prix Yves Rocard de la SFP pour Cailabs

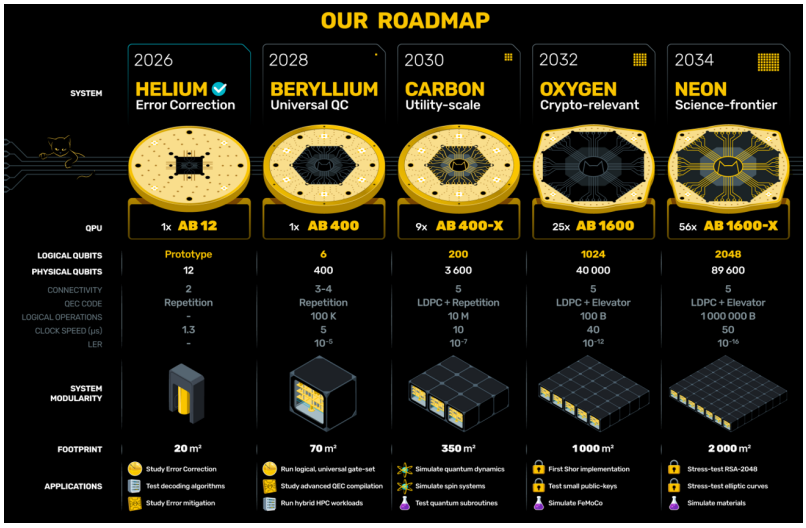
Il est **décerné** à la startup créée par Jean-François Morizur et Nicolas Treps. Le prix porte sur le transfert

technologique. La startup développe des outils de communication lasers servant notamment aux stations au sol de communications satellite. Le transfert technologique est ici assez direct avec un TRL bien plus élevé que nombre de startups dans les technologies quantiques.

France

Alice & Bob publie une roadmap et des estimations de ressources

La startup publiait une **nouvelle roadmap** qui s'aligne sur les nouveaux objectifs de Proqcima avec 200 qubits logiques (au lieu de 100) en 2030 (Graphene devient Carbon) et 2048 en 2034. Le tout avec des tailles de circuit bien précisées. C'est toujours ambitieux. A partir de Carbon, il leur faudra interconnecter plusieurs puces d'environ 400 qubits physiques.



Ils publiaient juste avant un préprint d'estimation de ressources pour casser une clé RSA-2048 bits en 3,14 jours avec 22 500 qubits physiques et un autre sur l'évaluation de l'état fondamental du fameux complexe chimique FeMoCo. Le tout s'appuie sur des hypothèses très optimistes en flip et phase rates pour les qubits physiques. Ils pensent pouvoir y arriver d'ici quelques années. Avec une erreur de flip plus raisonnable, le décompte passe à 45 000 qubits physiques. Cela correspond à la génération Neon dans leur roamdap, donc pour 2034. Donc, cela donne un Q-Day dans 8 ans si tout v a bien. Ou bien avant, si les LLMs font ce que l'on dit qu'ils vont faire bientôt.

Shor's algorithm compiled on cat qubits: 22 593 qubits for RSA-2048 in 3.14 days by Axel Pappalardo, Dahmun Goudarzi, Victor Hertz, Hugo Jacinto, Larissa Kroell, André Schrottenloher, Peter Shanahan, Élie Gouzien, Rémi de la Vieuville, and Vivien Londe, arXiv, October 2026 (128 pages).

Ground-state energy estimation compiled on cat qubits: 7 164 qubits for FeMoco-54 in 23.5 hours by Larissa Kroell, Hugo Jacinto, Victor Hertz, Axel Pappalardo, Adel Ben Moussa, Manuel Rispler, Peter Shanahan, Élie Gouzien, Christophe Vuillot, and Vivien Londe, arXiv, October 2026 (81 pages).

Quandela

Ils **annonçaient** un partenariat dans la fab avec la société taiwanaise Hermes-Epitek pour fabriquer des détecteurs de photons supraconducteurs, dans le cadre d'une intervention à Quantum Taiwan de Pascale Senellart. Et une très belle levée de fonds qui va être annoncée dans les jours qui viennent.

Pasqal

Ils **annonçaient** participer à un projet sur la correction d'erreurs avec ParityQC financé par le fonds de défense

européen. C'était présenté lors d'un événement à Innsbruck impliquant aussi Thales.

Qluster

La startup créée il y a un an par David Fainsin, Valentina Parigi et Clarisse Thibault **annonçait** une levée de fonds de 4.7M€.

Projet QC2030

Un **projet collaboratif** lancé par isentronic, Viqthor, Radiall, Silent Waves entre autres, pour faire scaler le contrôle d'un grand nombre de qubits. Le projet i-Démo est financé en grande partie par Bpifrance.

International

La révolution de l'IA générative continue dans les maths et la physique quantiques

Avec des conséquences potentielles sur la cryptographie classique et même à terme sur la PQC.

Il existe des rumeurs encore non vérifiées selon lesquelles :

- Factorisation classique d'entiers à cout polynomial : cata pour la crypto classique.
- Cassage de clés de PQC en classique en temps polynomial : cata pour la PQC.
- P = BQP => cata pour le calcul quantique.
- P = NP => idem.

Et en vrai :

- Algorithme classique de cassage de clés à base de courbes elliptiques basées sur le dlog. **https://eprint.iacr.org/2026/3020**. En fait avec des coefficients tels que cela n'a pas encore d'impact pratique.

Palmarès de découvertes mathématiques générées avec l'aide de LLMs en 4 jours de fin novembre:

#	Problem	Reported breakthrough	Date
1	Riemann hypothesis	RH and generalized RH proved	Nov 20
2	VP vs VNP	VP ≠ VNP	Nov 23–24
3	Matrix multiplication	Exact optimal exponent $\omega = 2.25$	Nov 24
4	Linear programming	Strongly polynomial algorithm	Nov 24
5	Minimum spanning tree	Deterministic $O(m)$ algorithm	Nov 23
6	Integer multiplication	Below $O(n \log n)$	Nov 24
7	Polynomial Hirsch conjecture	Disproved	Nov 24
8	NL vs UL	NL = UL	Nov 20
9	Valiant's complexity hierarchy	Strict separation of four classes	Nov 24
10	Sunflower conjecture	Exponential bound	Nov 24
11	Finite Fourier transforms	Optimal logarithmic exponent	Nov 24
12	Cluster editing	Subexponential parameterized algorithm	Nov 23
13	Resolution automatability	Progress on Tseitin contradictions	Nov 22

https://x.com/imjustnewatai/status/2126097539090796960/photo/1

Il est aussi intéressant de se pencher sur les nombreux papiers récemment publiés sur la génération de circuits quantiques optimisés grâce aux LLMs :

- **Discovering state-of-the-art quantum circuits with large language models** by Andi Gu, Alek H. Kemeny, Susanne F. Yelin, and Mikhail D. Lukin, arXiv, October 2026 (46 pages). QuEra avec Claude.
- **Discovering formally verified quantum programs with AI** by Sergey Shirobokov, Sergio Boixo, Ryan Babbush, Swarat Chaudhuri, Pushmeet Kohli et al, arXiv, November 2026 (45 pages), expliqué dans **Finding faster quantum algorithms with agents and formal verification** by Sergey Shirobokov, Ben Jaderberg and Ryan Babbush, Google DeepMind, November 2026.
- **Programming Quantum Circuit Parameters with Large Language Models** by Tiago de Souza Farias, Celso Jorge Villas-Boas, arXiv, November 2026 (31 pages).
- **Agentic AI for Discovering Fault-Tolerant Quantum Circuits** by Aritra Lahiri, and Florian Marquardt, arXiv, November 2026 (20 pages).
- **Agentic Pipelines for Mapping Topological Codes to Quantum Hardware** by Arpit Arora, Adam Holmes, Krysta M. Svore, and Taylor L. Patti, arXiv, November 2026 (23 pages).
- **Reimagining computational quantum research with AI scientists** by Yuxuan Du, Hanqing Zhao, Xinbiao Wang, Yiming Lu, Kaining Zhang, and Dacheng Tao, arXiv, November 2026 (57 pages).
- Le fait qu'un avantage quantique nécessite de la structure, mais pas trop : **https://psi.inc/research/aaronson-ambainis/**

Les LLMs servent aussi au niveau expérimental :

- **QuOptLab: Advancing Quantum Optics Experiments with an AI Agent** by Yuqing Li, Zeguan Wu, Yu Gan, Min Chen, and Junyu Liu, arXiv, November 2026 (12 pages).
- **AI Scientist Discovered Robust Quantum Control** by Jiahao Yan, Xuanying Lai, Xiaoshui Lin, Yizhou Wang, Changyu Yao, Guanghui He, Thomas Lewer, Chong Zu, and Chuanwei Zhang, arXiv, November 2026 (6 pages).

Annonce du Quantum Act européen

Le projet de loi a été **publié** le 25 novembre avec plein d'ambitions pour l'Europe, et l'annonce de challenges et appels d'offres d'achats pour des ordinateurs quantiques FTQC. L'Act couvre aussi les capteurs, les communications quantiques et les technologies habilitantes. L'énergétique y est citée comme faisant partie des figures de mérite clé des technologies quantiques dans l'Assessment Report Part 2. Le Quantum Act sera un gros sujet de discussion à Dublin pendant la conférence EQTC.

Architecture originale

Elle est proposée par John Preskill et son équipe de Caltech pour réduire le nombre de cables pilotant des qubits supraconducteurs. Il s'agit essentiellement d'un multiplexage temporel des instructions, couplé à une augmentation raisonnable du nombre de qubits physiques et du temps de calcul. Le principe repose sur le

déplacement des qubits au sens mathématique sur des sortes de tapis virtuels grâce à des portes SWAP. Ainsi, les portes sont exécutées à un nombre d'endroits limités, ce qui limite le nombre de qubits physiques à piloter. Les portes SWAPs sont exécutée de manière générique, indépendamment du circuit, et en parallèle. Le pilotage se ferait avec de l'électronique supraconductrice SFQ sur des qubits supraconducteurs, et avec de l'electron shuttling pour les qubits silicium. Cela fait penser à une sorte de machine de Turing quantique. Cela reste une proposition théorique !

Fault-tolerant quantum processor with minimal external control by Christopher A. Pattison, Jeongwan Haah, and John Preskill, arXiv, November 2026 (72 pages).

Google et les erreurs corrélées

Un papier sur un sujet très critique qui couvre la correction d'erreurs corrélées dans le temps : **Resolving and Suppressing Temporally Correlated Noise in Quantum Error Correction** by Alec Eickbusch, Nick Noll et al, arXiv, November 2026 (34 pages).

Et un autre sur une architecture multi-puces, enfin, qui montre deux choses, l'une que Google va peut-être se démarquer de son idée initiale de créer des puces avec 10 000 qubits supraconducteurs, et l'autre, qui montre que cette architecture modulaire permet d'améliorer l'efficacité de la correction d'erreurs : **Low-Overhead Quantum Error Correction with Boundary-Connected Planar Modules** by Oscar Higgott, Craig Gidney, Hartmut Neven et al., arXiv, October 2026 (112 pages).

IBM Nighthawk r3

IBM **annonçait** une troisième version (r3) de la puce Nighthawk qui contient 520 qubits contre 120 pour les versions r1 et r2. Et bientôt le double en les assemblant par deux sur un interposeur commun. Les fidélités ne sont pas encore annoncées mais pourraient être les mêmes que celles de r2. Il faudra attendre que le premier système comprenant cette puce soit en ligne d'ici début 2027. Cette puce a été fabriquée sur wafer 300 mm dans l'usine d'Albany d'IBM. C'est le seul constructeur à utiliser des process 300 mm pour des puces commerciales.

Xanadu

Xanadu annonce un **switch optique** avec de faibles pertes. Lien avec l'approche équivalent de PsiQuantum annoncée en octobre ? Pas vraiment. Plutôt avec leur switch pour le calcul FTQC.

FeMoCo réalisé classiquement en Chine

Une **performance** réalisée sur le Lineshine, le plus gros HPC au monde. Le calcul du ground state porte sur une configuration à 76 orbitales et a été réalisé en 105 minutes, vs les 8,6 heures évaluées sur plateformes FTQC par Google en 2025 demandant 4,5 millions de qubits physiques et les 23 heures du récent papier de Google. LineShine consomme 42 MW à pleine puissance. Une telle machine Google à base de qubits supraconducteurs pourrait en consommer autant mais les estimations de ressources fluctuent plus que le cours de la bourse des startups quantique, donc on ne peut pas trop extrapoler. La référence d'estimation de ressource quantique utilisée par les scientifiques chinois est **Fast quantum simulation of electronic structure by spectrum amplification** by Guang Hao Low, Ryan Babbush, Nicholas C. Rubin et al., arXiv, February 2025 (43 pages). Presque deux ans ! Elle est peut-être déjà dépassée.

Levée de fonds de Q-CTRL

Les grandes manœuvres dans le logiciel continuent avec celle **belle levée** de $260M qui fait remonter l'Australie dans le ranking des levées de fonds par pays.

Entropica Labs

Acquisition d'Entropica Labs par Horizon Quantum. Ils sont situés tous les deux dans le même pays, Singapour. **Horizon Quantum Integrates OQC's 32-Qubit Processor with Triple Alpha** by Mohib Ur Rehman, The Quantum Insider, November 2026.

SEALSQ acquiert QuintessenceLabs.

C'est une **startup australienne** dans la cybersécurité. Ce qui fait sens pour SEALSQ. Plus que leur investissement dans EeroQ et Quobly.

Chine

J'ai découvert de nouvelles startups chinoises dans les atomes froids que j'ai ajoutées dans mon livre. Il y en a maintenant plus d'une dizaine, soit plus de d'acteurs aux USA et en Europe, en cumulé ! Les chercheurs chinois se lancent donc dans la création de startups. Peut-être parce qu'ils considèrent maintenant que la technologie est plus mature.

Bêtisier

Un test de machine learning quantique qui décompose un LLM en petits bouts de calcul exploitant chacun 8 qubits, tournant sur un processeur IBM. A la fin, cela n'apporte aucun avantage quantique et cela coute plus cher qu'un calcul classique. Cela ne sert pas à grand-chose et cela ne scale pas bien du tout. **Researchers Fit Quantum Circuits Into a 30 Billion-Parameter AI Model** by Matt Swayne, The Quantum Insider, November 2026.

Une prouesse équivalente en Chine: **Non unitary and nonlinear quantum generative large model design and fast large-scale training without back propagation** by Tianze Zhu, Jian Yang et al., arXiv, November 2026 (55 pages). Cf **https://chatgpt.com/share/6b06b855-c0a4-83ed-a41e-8a6f095ba8c7** qui explique la chose.

Un titre tape à l'œil sur une expérience au Canada ayant réalisé une soi-disante puce de qubits silicium-germanium avec un million de qubits. En pratique, ils ont testé deux qubits en laboratoire. A comparer au record de 18 qubits de Delft et HRL Labs de cette année. **Canadian Researchers Piece Together a Million-Qubit Quantum Chip** by Matt Swayne, The Quantum Insider, November 2026. L'article de TQI reprend l'information du **gouvernement canadien**. Et côté scientifique, le **papier associé** de juin 2026 ne donne pas dans la surenchère. Et **un autre** sur le couplage longue distance.

C'est terminé pour novembre 2026 ! Dans le prochain podcast, nous ferons le bilan de l'année 2026 et étrennerons 2027.

*PS: Fanny Bouton et moi-même produisons ce podcast depuis l'automne 2019 comme les podcasts Decode Quantum depuis 2020. Ils permettent d'animer l'écosystème quantique en France (Quantum) et dans le monde (Decode Quantum, maintenant, avec une majorité des épisodes enregistrés en anglais). Nous faisons cela pro-bono, sans modèle économique. Ce n'est pas notre activité principale. Fanny Bouton et moi-même sommes actifs dans l'écosystème à plusieurs titres : elle est de son côté "quantum lead" chez OVHcloud et cofondatrice de l'événement France Quantum, et du mien, je suis enseignant (EPITA, CentraleSupelec, ENS Paris Saclay, etc.), **auteur** et **chercheur indépendant**, formateur, expert technique auprès de différents organismes publics (Bpifrance, l'ANR, l'Académie des Technologies, Union Européenne, etc.) et aussi cofondateur de la **Quantum Energy Initiative**.*

Cet article a été publié le 29 novembre 2026 et édité en PDF le 29 novembre 2026.
(cc) Olivier Ezratty – “Opinions Libres” – **https://www.oezratty.net**