UPDATE NOTE OF THE SCIENTIFIC ADVISORY BOARD

QUANTUM COMPUTING

WHAT IS QUANTUM COMPUTING?

Quantum computing[1] operates on the principles of quantum mechanics, a 100-year-old theory of physics that describes the behaviour of very small (atomic and sub-atomic) particles. Instead of existing in certain places and times, quantum particles are better understood as existing in many possible states (see below). These properties defy our usual logic of cause and effect, but are already well-established and used in everyday technologies like lasers, magnetic resonance imaging, semiconductors, biological research, and smartphones.[2]

Traditional computers use bits that are either a 0 or a 1, but quantum computers work with "qubits" (quantum bits) that can be in several states at once. This means qubits can handle much more information, perform many calculations simultaneously, and solve problems much faster than traditional machines. Another remarkable property of qubits is entanglement, a phenomenon in which two qubits become interconnected so that the state of one instantly reveals information about the other, regardless of the distance between them.[3]

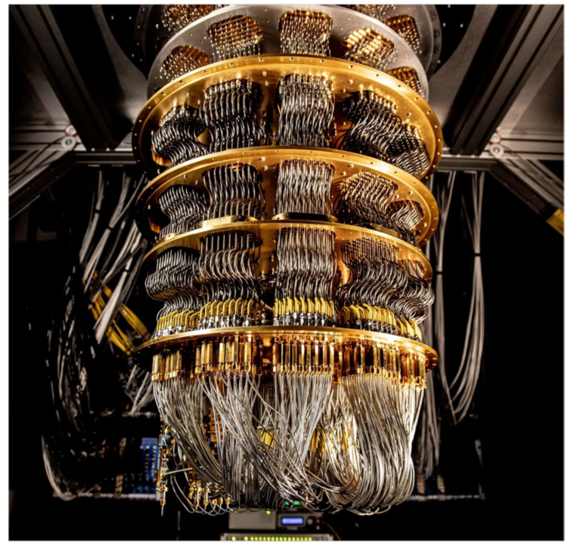


Figure 1 Google's quantum computing system

The physical and technological aspects of quantum computing present challenges. Qubits are delicate and highly susceptible to environmental disruptions, easily falling into what physicists call "decoherence" or other errors.[4] Addressing these physical challenges is both expensive and technologically difficult, because it requires protecting qubits from interference using techniques such as extreme cooling and magnetic shielding that are still largely under development.[5] The complexity of quantum programming and lack of universal standards also mean that software production is costly, restricted to a relatively small number of companies, and often applied only to a single device. As of today, most of the applications of quantum computing remain theoretical and none can be scaled for market rollout, though some significant breakthroughs in the past year suggest that quantum computing may arrive sooner than expected.

BREAKTHROUGHS AND LATEST DEVELOPMENTS

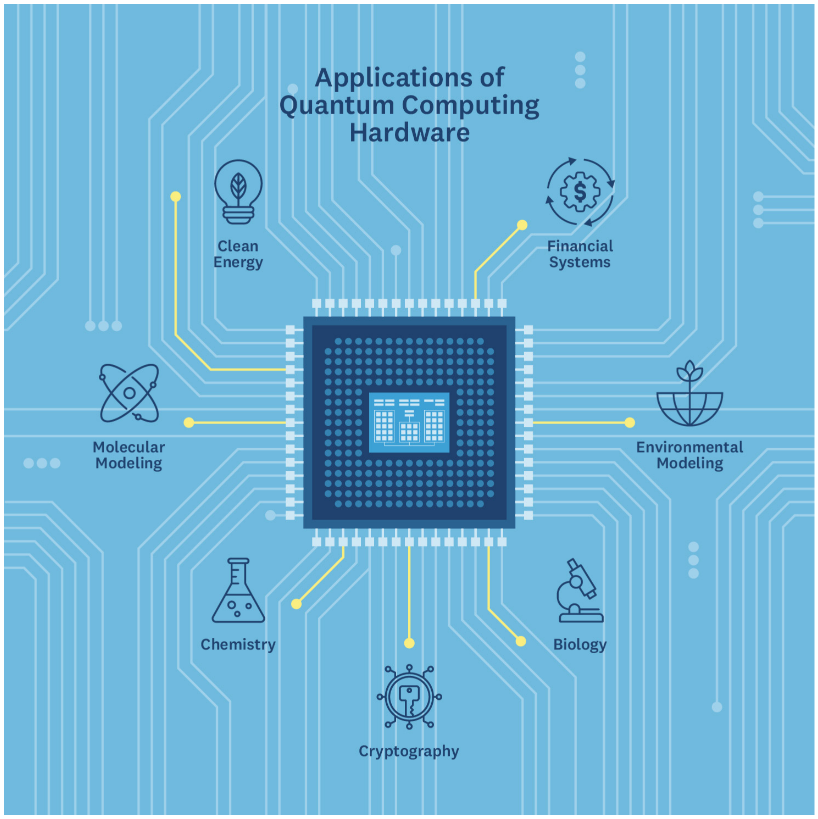
In 2019, a group at Google Quantum AI demonstrated that their quantum processor could perform a computational task in 200 seconds that would take a classical computer more than 10,000 years to complete.[6] Since then, important breakthroughs have helped to address challenges of interference and the ability to connect qubits into more powerful machines, including: (a) the December 2024 "Willow" quantum computer chip by Google, able to suppress noise and dramatically reduce error rates; (b) the February 2025 rollout of distributed quantum computing processors by Oxford University, which will enable far greater processing power; and (c) a 62-qubit superconducting quantum processor produced by the University of Science and Technology of China in 2021.[7]

Investment in quantum computing has skyrocketed in recent years as governments and major tech companies race to be the first to market practical applications.[8] The US, China, EU, Germany, UK, Japan, India, and many more countries have significantly increased their investments in national quantum strategies.[9] Today, more than $50 billion has been invested in quantum computing research and development.[10] Over the coming years, some of the most important practical applications in quantum computing may include the following:

Security and cryptography: Quantum computers may become capable of cracking classical computer security in seconds, requiring the development of secure "quantum communications." This has driven significant national investment and new security protocols to meet this potentially transformative security applications of quantum computing. [11]

Health and medicine: Drug design relies on simulating the behavior of molecules, often testing billions of different potential interactions and outcomes. Early research indicates that the convergence of quantum processing and AI tools could tackle some of the most complex simulations, including modeling protein folding.[12] Other health applications include disease diagnostics, simulations of the effects of gene editing, and global pandemic modeling.[13]

Climate and energy: Modeling future climate scenarios and scaling up renewable energy could benefit directly from the enormous potential of quantum computing. In some scenarios, quantum-driven approaches could enable a dramatic increase in clean energy production, highly optimized energy solutions, more accurate climate modeling, and the use of far less energy than classical computing.[14]



Finance and trade: Complex financial systems are difficult to predict via traditional computing methods, but quantum could provide far more accurate and reliable modeling in the relatively near future.[15] This could include modeling of financial markets as well as optimization of trade routes and structures around the world.

Conclusion: The potential for quantum computing to more accurately predict and model complex global trends and outcomes could enable more effective investments in sustainable development, with massive implications for our collective ability to transition to net zero and address the interrelated crises of climate change, pollution, and biodiversity loss. Other arenas, such as in transport, industrial production, biological research, and neurotechnology could rapidly become heavily reliant on quantum computing as soon as scalable, practical systems are developed.[16] The "Open Quantum Institute (OQI)," which was initiated at GESDA, launched in 2023 and now incubated at CERN for its pilot phase (2024-2026), has taken the precisely that mission to promote global, equitable and inclusive access to quantum computing, and through this explore applications that would benefit humanity.

CONSIDERATIONS FOR THE UN

The UN General Assembly has declared 2025 the International Year of Quantum Science and Technology, with UNESCO playing a coordinating role for the UN system.[17] This provides an important impetus for dedicated focus on the potential for quantum technologies to accelerate progress on sustainable development, and also a careful assessment of the risks associated with the rapid advancements coming our way. Some of the most important questions and risk areas to assess for the UN system include:

A quantum arms race: Governments are scrambling to prepare their national security systems for potential disruptions from quantum computing, even though major breakthroughs in cryptography appear at least ten years out.[18] Similar to the race for AI dominance, the quantum race could easily escalate if one government or company claimed a breakthrough that could allow it to crack the national security systems of others. Within the UN, the ITU is developing standards to support the secure and interoperable adoption of these technologies, which will be crucial as the quantum race intensifies. The UN could build on this work by promoting mechanisms for verifying quantum computing capabilities and developing broad principles and norms for their safe development and deployment.

Human rights: With the capability to easily break traditional encryption systems, quantum computing could potentially be used to invade privacy, manipulate communities, or limit freedom of expression. Last year, UNESCO hosted a series of discussions around some of the social, ethical, and rights-based implications of quantum computing.[19] Going forward it will be important to develop a clear understanding of the human rights implications and the potential role for the UN to adapt its approaches to emerging risks.

Social and economic concerns: Today, investments in quantum computing are driven by a small number of countries, with growing investment by the private sector. Similarly to AI, this could lead to scenarios where the benefits of quantum computing (e.g. in the realms of financial investments, health, and development) are unequally distributed globally, leading to a greater digital divide than we see today. UNESCO is coordinating within the framework of the International Year of Quantum Science and Technology (IYQ) to develop strategies aimed at addressing the quantum divide, with a focus on reducing disparities between global North and South. Building on this, UN's role in helping to set international norms, standards, and regulations could be especially important as quantum computing becomes more of a reality in the coming decade.

Today, no practical applications of quantum computing yet exist. But the enormous global investment in the technology is a clear indicator that many governments and other actors see the potential for quantum to revolutionize some of the most important sectors around the world. How to position the UN for this kind of emerging transformational moment is an excellent use-case for the Secretary-General's newly established UN Futures Lab, the horizon scanning functions of this Scientific Advisory Board, important science-based partners of the UN like the Geneva Science Diplomacy Anticipator, the Open Quantum Institute, and the coming UN Special Envoy for Future Generations. Building on the International Year of Quantum Science and Technology this year, the UN could draw attention to the many transformative applications quantum computing could offer.

REFERENCES

1 This brief represents the views of the independent scientists on the Scientific Advisory Board. It benefitted from a review from experts within ITU, UNESCO, UNU, and GESDA. It does not necessarily reflect the UN's position or those of network institutions. Mention of a commercial company or product in this document does not imply endorsement by the UN or the authors. The use of information from this document for publicity or advertising is not permitted. Trademark names and symbols are used in an editorial fashion with no intention on infringement of trademark or copyright laws. We regret any errors or omissions that may have been unwittingly made.

2 See, e.g., Taylor, Michael A., and Warwick P. Bowen. "Quantum metrology and its application in biology." Physics Reports 615 (2016): 1-59; Gill, Sukhpal Singh, et al. "Quantum Computing: Vision and Challenges." arXiv preprint arXiv:2403.02240 (2024); Gmachl, Claire, et al. "Recent progress in quantum cascade lasers and applications." Reports on progress in physics 64.11 (2001): 1533; Yukawa, Hiroshi, et al. "Quantum life science: biological nano quantum sensors,

quantum technology-based hyperpolarized MRI/NMR, quantum biology, and quantum biotechnology." Chemical Society Reviews (2025); McDermott, Robert, et al. "Microtesla MRI with a superconducting quantum interference device." Proceedings of the National Academy of Sciences 101.21 (2004): 7857-7861; Wang, Aijuan, et al. «HQNet: A hybrid quantum network for multi-class MRI brain classification via quantum computing.» Expert Systems with Applications 261 (2025): 125537.

3 For more on the potential applications of quantum computing, see, Azhari, Rama, and Agita Nisa Salsabila. "Analyzing the Impact of Quantum Computing on Current Encryption Techniques." IAIC Transactions on Sustainable Digital Innovation (ITSDI) 5.2 (2024): 148-157; Vadisetty, Rahul, and Anand Polamarasetti. «Quantum Computing For Cryptographic Security With Artificial Intelligence.» 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA). IEEE, 2024.

4 See, Bacon, Dave Morris. Decoherence, control, and symmetry in quantum computers. University of California, Berkeley, 2001; Martinez, Josu Etxezarreta. "Decoherence and quantum error correction for quantum computing and communications." arXiv preprint arXiv:2202.08600 (2022); Abad, Tahereh, et al. "Impact of decoherence on the fidelity of quantum gates leaving the computational subspace." arXiv preprint arXiv:2302.13885 (2023); Park, Kimin, et al. "Slowing quantum decoherence of oscillators by hybrid processing." npj Quantum Information 8.1 (2022): 67; Gill, Sukhpal Singh, et al. "Quantum Computing: Vision and Challenges." arXiv preprint arXiv:2403.02240 (2024).

5 Gill, Sukhpal Singh, et al. "Quantum computing: A taxonomy, systematic review and future directions." Software: Practice and Experience 52.1 (2022): 66-114.

6 Arute, Frank, et al. "Quantum supremacy using a programmable superconducting processor." Nature 574.7779 (2019): 505-510.

7 See, Jerbi, S., Gyurik, C., Marshall, S.C. et al. Shadows of quantum machine learning. Nat Commun 15, 5676 (2024). https://doi.org/10.1038/s41467-024-49877-8; Wang, Yunfei, and Junyu Liu. "A comprehensive review of Quantum Machine Learning: from NISQ to Fault Tolerance." Reports on Progress in Physics (2024); Melnikov, Alexey, et al. "Quantum machine learning: from physics to software engineering." Advances in Physics: X 8.1 (2023): 2165452.

8 For a list of private sector companies involved in quantum, see https://technologymagazine.com/top10/top-10-quantum-computing-companies.

9 For a helpful mapping of investments, see https://www.qureca.com/quantum-initiatives-worldwide/.

10 See, https://radar.gesda.global/opportunities/open-quantum-institute-incubation-phase; https://www.forbes.com/sites/sylvainduranton/2024/06/26/quantum-now/

11 S. Mitra, B. Jana, S. Bhattacharya, P. Pal and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India, 2017, pp. 1-7, doi: 10.1109/OPTRONIX.2017.8350006; Portmann, Christopher, and Renato Renner. "Security in quantum cryptography." Reviews of Modern Physics 94.2 (2022): 025008; Sonko, Sedat, et al. «Quantum cryptography and US digital security: a comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security.» Computer Science & IT Research Journal 5.2 (2024): 390-414.

12 Blunt, Nick S., et al. "Perspective on the Current State-of-the-Art of Quantum Computing for Drug Discovery Applications." Journal of Chemical Theory and Computation, vol. 18, no. 12, 2022, pp. 7001-7023; Robert, Anton, et al. "Resource-efficient quantum algorithm for protein folding." npj Quantum Information 7.1 (2021): 38; Casares, Pablo Antonio Moreno, Roberto Campos, and Miguel Angel Martin-Delgado. "QFold: quantum walks and deep learning to solve protein folding." Quantum Science and Technology 7.2 (2022): 025013; Casares, Pablo Antonio Moreno, Roberto Campos, and Miguel Angel Martin-Delgado. "QFold: quantum walks and deep learning to solve protein folding." Quantum Science and Technology 7.2 (2022): 025013.

13 See, Ur Rasool, Raihan, et al. "Quantum computing for healthcare: A review." Future Internet 15.3 (2023): 94; Kumar, Avinash, et al. «Quantum computing for health care: a review on implementation trends and recent advances.» Multimedia Technologies in the Internet of Things Environment, Volume 3 (2022): 23-40; Flöther, Frederik F. "The state of quantum computing applications in health and medicine." Research Directions: Quantum Technologies 1 (2023): e10; Jayanthi, Prisilla, Bharatendra K. Rai, and Iyyanki Muralikrishna. «The potential of quantum computing in healthcare.» Technology Road Mapping for Quantum Computing and Engineering. IGI Global, 2022. 81-101; Aggarwal, Lakshita, Shelly Sachdeva, and Puneet Goswami. "Quantum healthcare computing using precision based granular approach." Applied Soft Computing 144 (2023): 110458.

14 See, Berger, Casey, et al. "Quantum technologies for climate change: Preliminary assessment." arXiv preprint arXiv:2107.05362 (2021); Ajagekar, Akshay, and Fengqi You. «Quantum computing and quantum artificial intelligence for

renewable and sustainable energy: A emerging prospect towards climate neutrality.» Renewable and Sustainable Energy Reviews 165 (2022): 112493; Ho, Kin Tung Michael, et al. «Quantum computing for climate resilience and sustainability challenges.» 2024 IEEE International Conference on Quantum Computing and Engineering (QCE). Vol. 2. IEEE, 2024; Ashwani, Siddhant, et al. "Quantum Computing for Climate Change: A Comprehensive Review of Current Applications, Challenges, and Future Directions." 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2024.

15 Orús, Román, Samuel Mugel, and Enrique Lizaso. "Quantum computing for finance: Overview and prospects." Reviews in Physics 4 (2019): 100028.

16 For more literature on these topics, see, Herman, Dylan, et al. "Quantum computing for finance." Nature Reviews Physics 5.8 (2023): 450-465; De Leon, Nathalie P., et al. "Materials challenges and opportunities for quantum computing hardware." Science 372.6539 (2021): eabb2823; Ollitrault, Pauline J., Alexander Miessen, and Ivano Tavernelli. "Molecular quantum dynamics: A quantum computing perspective." Accounts of Chemical Research 54.23 (2021): 4229-4238; Preskill, John. "Quantum computing 40 years later." Feynman Lectures on Computation. CRC Press, 2023. 193-244; Caleffi, Marcello, et al. "Distributed quantum computing: a survey." Computer Networks 254 (2024): 110672; Kim, Youngseok, et al. "Evidence for the utility of quantum computing before fault tolerance." Nature 618.7965 (2023): 500-505; Gill, Sukhpal Singh, et al. "Quantum computing: A taxonomy, systematic review and future directions." Software: Practice and Experience 52.1 (2022): 66-114; LaPierre, Ray. Introduction to quantum computing. Springer Nature, 2021; Ur Rasool, Raihan, et al. "Quantum computing for healthcare: A review." Future Internet 15.3 (2023): 94; Nimbe, Peter, Benjamin Asubam Weyori, and Adebayo Felix Adekoya. "Models in quantum computing: a systematic review." Quantum Information Processing 20.2 (2021): 80; Peral-García, David, Juan Cruz-Benito, and Francisco José García-Peñalvo. "Systematic literature review: Quantum machine learning and its applications." Computer Science Review 51 (2024): 100619; Arute, Frank, et al. "Quantum supremacy using a programmable superconducting processor." Nature 574.7779 (2019): 505-510.

17 United Nations General Assembly. International Year of Quantum Science and Technology, 2025. Resolution adopted by the General Assembly A/RES/78/287 (United Nations, 2024).

18 E.g., in 2021 the US put in place a strategy that would require all federal agencies to have PQC by 2030. The European Commission, Singapore, Australia, and others have put in place quantum capacity monitoring schemes, recommendations, and roadmaps to upgrade cryptography and communications.

19 https://unesdoc.unesco.org/ark:/48223/pf0000388955.