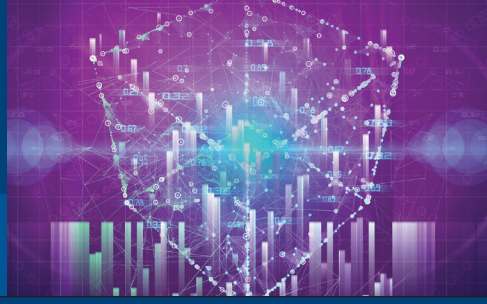
Association for Computing Machinery

acm Technology Policy Council

TechBriefs



QUANTUM COMPUTING AND SIMULATION

Simson L. Garfinkel and Chris J. Hoofnagle, Lead Authors

PROBLEM

Quantum simulation, an imminent offshoot of quantum computing that has received relatively little attention, poses profound societal and individual risks as well as benefits.

POLICY IMPLICATIONS

- Focus on the code-breaking implications of future quantum computers has obscured the impending viability, and potential consequences, of quantum simulation technology.
- Quantum simulation has the potential to profoundly affect science, industry, and warfare.
- Privacy and other civil liberties could be adversely affected by technological developments accelerated by quantum simulation.

QUANTUM SIMULATION: BY THE NUMBERS

20,000,000	Estimated number of information units ("qubits") necessary for a quantum computer to defeat the strongest widely used public key encryption.[1]
127	Maximum number of such qubits achieved to date.[2]
10	Minimum estimated number of years for quantum computing to become viable.[3]
40	Maximum estimated number of years for quantum computing to become viable.[3]
2	Maximum estimated number of years for quantum simulation to become widely used.[4]
263,000	Google search returns for news stories on "quantum computing."[5]
20,400	Google search returns for news stories on "quantum computing" and "encryption."[5]
8,050	Google search returns for news stories on "quantum simulation."[5]
4.86	In trillions of US dollars, combined market value of five leading quantum research companies.[6]

Overview

Quantum computers have garnered enormous interest and media attention because of their predicted ability to one day crack encryption algorithms that are widely used today. While such machines would have profound impacts within both the public and private sectors, they are not predicted to become a reality for at least a decade or, by some estimates, as many as forty years—if ever. By contrast, powerful quantum *simulators* are nearly a reality. Their practical applications could be just two years away.

Powerful quantum simulators are nearly a reality.

In its 2019 report on quantum computing, the U.S. National Academy of Sciences identified quantum simulators as a potentially practical, near-term commercial application of today's computers.[3] That same year, a National Science Foundation workshop found that, while reliable universal digital quantum computers are "likely decades away," special-purpose machines built to solve specific problems beyond the range of today's conventional computers "offer extraordinary opportunities for applications realizable on a 2-5 year time scale."[4] Indeed, even if a "quantum winter" of decreased investment due to inadequate progress in large-scale general-purpose quantum computing occurs, quantum simulators might nonetheless rapidly move from the laboratory to practice.[7]

What is a quantum computer?

Quantum computers take a different approach to computing from traditional digital machines, one based on calculating probabilities instead of discrete values. Rather than processing bits that can represent only a 0 or 1, they compute with qubits (quantum bits), which can initially represent many values. Quantum computers then manipulate the qubits with mechanisms called quantum gates, causing the qubits to change over time. Finally, each qubit is measured by a conventional computer and converted to a 0 or 1 that the ordinary digital computer can record. This process may need to be repeated many times for a single quantum computation. These inherent differences in structure and methodology between standard digital and quantum computers make each best suited to very different kinds of calculations.[8]

What is a quantum simulator?

Computer simulations produce insights into the behavior of real-world phenomena by using algorithms and data to create dynamic models of relevant processes. The term *quantum simulator* as used here refers to specialized quantum computers tailored to performing such simulations (rather than conventional computers simulating quantum phenomena). When Nobel laureate Richard Feynman proposed the idea of quantum computing back in 1981, he envisioned a new kind of computer that could directly simulate the quantum mechanical behaviors of atoms and subatomic particles using those same mechanisms. Feynman didn't know how such a computer could be built or how it would work, but he knew it would be the only way to simulate the physics of increasingly complex systems in a computer without requiring exponentially longer processing times.[9]

Quantum simulators may hasten development of a practical, general-purpose quantum computer.

Ordinary computers always generate the same output from the same input. Quantum computers, however, perform their computations using an ensemble of quantum particles that don't produce definite answers. Instead, they identify how probable particular answers are from multiple possibilities. As a result, the architecture of these computers simulates what physicists believe happens in a real mechanical system. That allows quantum computers to directly and efficiently model the quantum interactions of other such systems, thus enabling the simulation of extremely complex phenomena.

Quantum simulation poses promise and peril

Like any disruptive technology, quantum simulation has both enormous positive and negative potential for science, industry, and society:

- ***Computing.*** Just as early success in traditional digital computers was leveraged to design

more powerful computers, quantum simulators may hold the key to hastening the development of a practical, general-purpose quantum computer. As simulators scale up in size, they may enable breakthrough discoveries in materials science that would make general-purpose quantum computers more feasible. Advances in traditional digital computers were produced and shared by many. Given their likely extraordinary monetary value, however, proprietary leaps in quantum computing technology might be held close by their early developer(s). If then used to produce yet more-robust quantum computers, a definable risk exists that such technology could be "captured" by a single actor that would enjoy asymmetrical market advantages with potentially profound economic and social effects.[10]

Quantum simulators could permit clandestine weapons development without threat of detection.

- ***Critical Industry.*** Less publicly familiar applications of quantum simulation technology may be equally profound and valuable.[11] Nitrogen fixation, for example, is a key process in food and pharmaceutical production, as well as in many other industries. Currently, it occurs naturally with just air, water, sunlight, and microbes. Quantum simulation is ideally suited to advancing our understanding of the complex natural interactions that produce nitrogen fixation so that we can create more-efficient industrial fixation processes. Similarly, quantum simulation may yield a more precise understanding of photosynthesis that, in turn, could help feed more people worldwide.

Quantum simulators have the potential to substantially undermine rights to personal privacy worldwide.

- ***Weapons Design.*** Quantum simulators could permit clandestine weapons development without threat of detection, notwithstanding international agreements banning such practices. These weapons might include massive conventional bombs as well as novel chemical or biological agents.[12] To allow innovation while guarding against misuse, governments may need to manage access to quantum simulation through export controls or other measures. In doing so, however, care must be taken not to inhibit foundational research.[13]

- ***Civil Liberties.*** Quantum simulators also have the potential to substantially undermine rights to personal privacy worldwide if applied to develop surveillance technologies that far exceed any currently available. These might take the form of fundamentally new antenna designs, exquisitely sensitive sensors, or new means of creating and detecting chemical or physical markers (taggants).[14] New governance mechanisms, including methods of risk analysis, will need to be developed and, in some cases, built on existing protection regimes.

KEY CONCLUSIONS

- Quantum simulation, a less recognized element of the quantum technology revolution, must be planned for thoroughly to realize its tremendous promise.
- Because quantum simulators are likely to be developed far sooner than general-purpose quantum computers, such planning is needed immediately.
- Strategic investment, and government oversight and controls, will be critical to securing the benefits of quantum simulation while mitigating both its foreseeable and unforeseen risks.

NOTES AND SOURCES

1. See, e.g., Gidney, C. and Ekera, M., "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum* 5: 433, 2021, https://quantum-journal.org/papers/q-2021-04-15-433/.
2. Researchers are currently working with multiple quantum computer designs. This estimate is based on one of the most popular, known as a noisy intermediate-scale quantum (NISQ) computer. See, "IBM Unveils Breakthrough 127-Qubit Quantum Processor," press release, Nov. 16, 2021, https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor.
3. Grumbling, E. and Horowitz, M. *Quantum Computing: Progress and Prospects*. Washington, DC: National Academies Press.
4. Altman, E. et al. "Quantum Simulators: Architectures and Opportunities." *PRX Quantum*, 2(1): 017003. See also "CCNY-based team scripts breakthrough quantum algorithm," press release, July 25, 2022, https://www.ccny.cuny.edu/news/ccny-based-team-scripts-breakthrough-quantum-algorithm
5. All searches conducted with the quoted terms indicated on July 21, 2022.
6. Data current as of July 16, 2022. See, "U.S. Commerce – Stock Market Capitalization of the 50 Largest American Companies," http://www.iweblists.com/us/commerce/MarketCapitalization.html. The companies referenced are: Alphabet, Amazon, IBM, Intel, and Microsoft.
7. See Hoofnagle, C.J. and Garfinkel, S. "What if Quantum Computing Is a Bust?" *Slate*, posted Jan. 26, 2022, https://slate.com/technology/2022/01/quantum-computing-winter-scenario.html.
8. Ordinary digital computers are well suited to familiar tasks like word processing, creating accounting systems, tabulating large quantities of data, and "traffic-controlling" the World Wide Web, while quantum computers (if the theories animating their development are correct) are likely to be best employed to factor large numbers (a requirement of cracking messages encrypted with public key cryptography, for example) and optimizing complex systems (e.g., by setting the "weights" of computational nodes in neural networks).
9. Feynman, R. "Simulating physics with computers." *International Journal of Theoretical Physics*, 21(6): 467–488.
10. Such a "winner take all" scenario could, for example, exacerbate existing national and regional economic disparities, as well as spur potential conflict. Policies and budgets targeted specifically at developing workable quantum simulator technology and making it broadly available and affordable could help prevent this possibility. Such a course, however, could conflict with efforts to prevent access for nefarious purposes.
11. See, e.g., Daley, A.J., Bloch, I., Kokail, C. et al. "Practical quantum advantage in quantum simulation." *Nature* 607, 667–676 (2022). https://doi.org/10.1038/s41586-022-04940-6.
12. It is easy to imagine, for example, how quantum simulators could be used to develop devices even more powerful than the largest conventional bombs, or to optimize the creation and delivery of myriad chemical or biological weapons. Historically, the development of the latter technologies required specialized facilities.
13. See, e.g., the ACM US Technology Policy Committee's Joint Comments to Department of Commerce Bureau of Industry Security on Foundational Technology Export Controls, Oct. 29, 2020.
14. By potentially speeding and enhancing the design of quantum computing itself, quantum simulation also has the potential, for both good and ill, of supercharging current cryptanalysis capabilities.

ADDITIONAL INFORMATION

With 100,000 members in 190 countries, the nonprofit **Association for Computing Machinery** is the world's largest and longest-established organization of professionals involved in all aspects of computing. The association's global policy agenda concerning computing and information technology is guided by the ACM Technology Policy Council. Under the council's auspices, technology policy committees in the United States and Europe provide cutting-edge, apolitical, non-lobbying information about computing and its social impacts to policy makers at all levels of government in many forms. These include public presentations, private briefings, public testimony, formal consultation, and rulemaking comments, as well as detailed reports and analyses.

To tap the deep expertise of ACM's global membership, please contact ACM's Global Policy Office at acmpo@acm.org or +1 202.580.6555.

AUTHORSHIP & ACKNOWLEDGEMENTS

Simson L. Garfinkel chairs the ACM U.S. Technology Policy Committee's Subcommittee on Digital Governance. He was previously Senior Data Scientist in the Office of the Chief Information Officer at the U.S. Department of Homeland Security and a part-time faculty member at George Washington University in Washington, DC. He is a guest researcher at the U.S. National Institute of Standards and Technology. Chris J. Hoofnagle is Professor of Law in Residence at Berkeley Law in Berkeley, CA, as well as Professor of Practice in the UC Berkeley School of Information and an affiliated faculty member of the Simons Institute for the Theory of Computing. They coauthored *Law and Policy for the Quantum Age*, Cambridge University Press, 2022. This brief was produced for the ACM Technology Policy Council and may be cited as "*ACM TechBrief: Quantum Computing and Simulation*, ACM Technology Policy Council (Issue 4, July 2022)."