

What Is Quantum Computing?

ITIF Technology Explainer Series • www.itif.org

Quantum computing leverages principles from quantum mechanics (a branch of physics), notably the unique behaviors of subatomic particles such as electrons and photons, to enable new, extremely powerful computing architectures. Instead of processing information using binary bits of ones and zeros, quantum computers use qubits, which leverage the quantum properties of “superposition” and “entanglement” to operate in multiple states at once. Qubits can effectively be a one and a zero simultaneously—and one qubit’s state can be programmed to vary according to another’s state. This allows quantum computers to store vastly more information than binary systems—in fact, their data storage capacity doubles with each additional qubit. And it allows quantum computers to operate far faster than conventional computers, because they can perform certain types of calculations in many fewer steps. Take the example of searching for a number in a phonebook. If the phonebook has 10 million entries, then a classical search algorithm would have to try 5 million times, on average, to find the right one. But a quantum search algorithm could do it in just 1,000 operations—which is to say, 5,000 times faster.

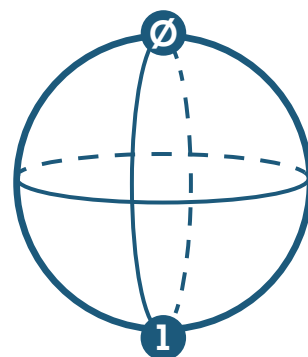
Why Now?

A major obstacle to quantum computing has been that qubits are extremely fragile and must be operated at temperatures near absolute zero. Their fragility has made them susceptible to systemic failure, as when a Christmas light blows and causes a whole strand of others to go dark. But researchers have made great strides in recent years figuring out how to stabilize qubits, so they are starting to build rudimentary quantum computers. Now applications of “quantum information science”—including quantum computing, quantum communications, and quantum sensing and imaging—are beginning to move from laboratory prototypes to practical applications and even commercial products. For instance, in 2016, IBM launched quantum computing as a cloud-based service (its “Q Experience”), allowing researchers to upload computational queries to be resolved by a 5-qubit quantum computer. IBM later introduced a 20-qubit quantum computer for cloud-based commercial use and announced that its researchers had successfully built a 50-qubit prototype computer (although it can only hold this state for 90 microseconds). In March 2018, Google introduced “Bristlecone,” a 72-qubit quantum computer. Others, such as D-Wave Technology in Vancouver, Canada, are marketing highly specialized quantum computers that deliver thousands of qubits—a level of complexity that can begin to deliver on the full promise of quantum computing—but these are specially designed to solve certain types of algorithms. Meanwhile, Intel has announced it has identified a method to fabricate quantum chips from silicon, which in theory would enable it to maintain the viability of its existing semiconductor fabrication infrastructure, while incorporating quantum capabilities.

BIT



QUBIT



In quantum computing, the basic unit of information is a qubit, which can effectively be a one and a zero simultaneously.

Prospects for Advancement

While it’s hard to say how long it will be before there are general-purpose quantum computers capable of a wide variety of useful work at an affordable price, quantum computers are already producing commercial value. For example, companies have purchased specialized machines like D-Wave’s 10-foot-tall, 2,000-qubit quantum computer, which retails for \$15 million and is purpose-built to run algorithms that solve specific types of optimization problems, such as identifying optimal transportation routes, trading strategies, and supply-chain management solutions. Commercially, quantum computing today is probably akin to digital computing the early 1960s, when state of the art lay between the first integrated circuits and the first useful microprocessors. But analysts anticipate that the evolution of quantum computing will generally mirror that of the “classical” computing paradigm, in that it will be characterized by a continual series of performance improvements and declining costs reminiscent of Moore’s Law.

Applications and Impact

Extrapolating from the phonebook example, it’s easy to see why quantum computers are expected to make some existing forms of encryption obsolete. Certain calculations, such as factoring large numbers, that are the foundation for many encryption algorithms are computationally difficult for supercomputers today, but have been proven to be relatively simple to solve using quantum computers. This example hints at how quantum computing isn’t only about solving complex problems faster than conventional supercomputers can; it’s also about delving into problems that are too complex for

conventional supercomputers to solve at all—problems that require stretching beyond the realm of binary calculations into the realm of quantum physics, where the variable relationships between elements are mindboggling. It's too soon to say where this might eventually lead, but near-term applications will likely include assignments such as ascertaining optimal trading strategies in financial markets; conducting chemistry simulations to improve batteries for electric vehicles or to develop new pharmaceuticals; synthesizing the nitrogen reaction that makes fertilizer; or making robotics more effective.

Policy Implications

Quantum computing will become increasingly essential for both national economic competitiveness and national security, which explains why at least a dozen countries fund quantum computing research. China has identified quantum computing as a field in which it seeks global leadership. The United Kingdom and the European Commission have gone so far as to launch formal, “national” quantum computing strategies. In the United States, federally funded basic and applied research in quantum information science in recent years has averaged about \$200 million per year, with several federal agencies operating quantum computing research programs, including DARPA, the Department of Defense, the Department of Energy, and the National Science Foundation's Physics Division, which runs a program on Quantum Information Systems and Revolutionary Computing. But the United States has lacked a concerted national quantum computing strategy and, given that America's economy is six times larger than Britain's, would need to be investing closer to \$2 billion annually to match the United Kingdom's investments on a per-GDP basis.

To help address this, in September 2018 the U.S. House passed a National Quantum Computing Initiative Act that would direct federal agencies to invest more in quantum computing R&D and increase funding for quantum computing education and training. (The U.S. Senate is considering similar legislation.) The House version of the legislation would allocate \$1.275 billion to quantum information science R&D over the next five years—with \$125 million annually to support up to five competitively awarded “National Quantum

Information Science Research Centers”—plus funding to create a National Quantum Coordination Office that would be responsible for developing a national quantum computing strategy. Congress and the administration should support this legislation and the actions it envisions. The administration and Congress also should support efforts underway at the National Institute of Standards and Technology to evaluate new encryption systems that could withstand quantum-powered attacks. It's high time the United States develops a serious quantum computing leadership strategy that reflects the technology's enormous commercial, scientific, and national security implications.

Recommended Reading

Tom Simonite, “The Wired Guide to Quantum Computing,” *Wired*, August 22, 2018, <https://www.wired.com/story/wired-guide-to-quantum-computing>.

Jason Palmer, “Technology Quarterly: Here, There, and Everywhere,” *The Economist*, March 11, 2017, <https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own>.

Executive Office of the President, Interagency Working Group on Quantum Information Science of the Subcommittee on Physical Sciences, “Advancing Quantum Information Science: National Challenges and Opportunities” (Committee on Science and Committee on Homeland and National Security of the National Science and Technology Council, July 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/Quantum_Info_Sci_Report_2016_07_22%20final.pdf.

National Photonics Initiative, “Call for a National Quantum Initiative” (National Photonics Initiative, June 22, 2017), <https://www.lightourfuture.org/getattachment/7ad9e04f-4d21-4d98-bd28-e1239977e262/NPI-Recommendations-to-HSC-for-National-Quantum-Initiative-062217.pdf>.