**Quantum computer, device that employs properties described by**[**quantum mechanics**](https://www.britannica.com/science/quantum-mechanics-physics)**to**[**enhance**](https://www.merriam-webster.com/dictionary/enhance)**computations.**

As early as 1959 the American physicist and Nobel laureate [Richard Feynman](https://www.britannica.com/biography/Richard-Feynman) noted that, as electronic components begin to reach microscopic scales, effects predicted by [quantum](https://www.merriam-webster.com/dictionary/quantum) mechanics occur—which, he suggested, might be exploited in the design of more powerful computers. In particular, quantum researchers hope to harness a phenomenon known as [superposition](https://www.britannica.com/science/principle-of-superposition-wave-motion). In the quantum mechanical world, objects do not necessarily have clearly defined states, as demonstrated by the famous experiment in which a single photon of light passing through a screen with two small slits will produce a wavelike [interference](https://www.britannica.com/science/interference-physics) pattern, or superposition of all available paths. However, when one slit is closed—or a detector is used to determine which slit the photon passed through—the interference pattern disappears. In consequence, a quantum system “exists” in all possible states before a measurement “collapses” the system into one state. Harnessing this phenomenon in a computer promises to expand computational power greatly. A traditional [digital computer](https://www.britannica.com/technology/digital-computer) employs binary digits, or bits, that can be in one of two states, represented as 0 and 1; thus, for example, a 4-bit computer register can hold any one of 16 (24) possible numbers. In contrast, a [quantum bit](https://www.britannica.com/technology/qubit) (qubit) exists in a wavelike superposition of values from 0 to 1; thus, for example, a 4-qubit computer register can hold 16 different numbers simultaneously. In theory, a quantum computer can therefore operate on a great many values in parallel, so that a 30-qubit quantum computer would be comparable to a digital computer capable of performing 10 trillion floating-point operations per second (TFLOPS)—comparable to the speed of the fastest [supercomputer](https://www.britannica.com/technology/supercomputer)s.

During the 1980s and ’90s the theory of quantum computers advanced considerably beyond Feynman’s early speculations. In 1985 David Deutsch of the [University of Oxford](https://www.britannica.com/topic/University-of-Oxford) described the construction of quantum logic gates for a universal quantum computer, and in 1994 Peter Shor of AT&T devised an [algorithm](https://www.britannica.com/science/algorithm) to factor numbers with a quantum computer that would require as few as six qubits (although many more qubits would be necessary for factoring large numbers in a reasonable time). When a practical quantum computer is built, it will break current encryption schemes based on multiplying two large primes; in compensation, quantum mechanical effects offer a new method of secure communication known as quantum encryption. However, actually building a useful quantum computer has proved difficult. Although the potential of quantum computers is enormous, the requirements are equally stringent. A quantum computer must maintain [coherence](https://www.merriam-webster.com/dictionary/coherence) between its qubits long enough to perform an algorithm; because of nearly inevitable interactions with the [environment](https://www.merriam-webster.com/dictionary/environment) (decoherence), practical methods of detecting and correcting errors need to be devised; and, finally, since measuring a quantum system disturbs its state, reliable methods of extracting information must be developed.

Plans for building quantum computers have been proposed; although several demonstrate the fundamental principles, none is beyond the experimental stage. Three of the most promising approaches are presented below: [nuclear magnetic resonance](https://www.britannica.com/science/nuclear-magnetic-resonance) (NMR), ion traps, and quantum dots.

In 1998 Isaac Chuang of the [Los Alamos National Laboratory](https://www.britannica.com/topic/Los-Alamos-National-Laboratory), Neil Gershenfeld of the [Massachusetts Institute of Technology](https://www.britannica.com/topic/Massachusetts-Institute-of-Technology) (MIT), and Mark Kubinec of the University of California at Berkeley created the first quantum computer (2-qubit) that could be loaded with data and output a solution. Although their system was [coherent](https://www.merriam-webster.com/dictionary/coherent) for only a few nanoseconds and trivial from the perspective of solving meaningful problems, it demonstrated the principles of quantum computation. Rather than trying to isolate a few subatomic particles, they dissolved a large number of chloroform molecules (CHCL3) in water at room temperature and applied a [magnetic field](https://www.britannica.com/science/magnetic-field) to orient the spins of the carbon and hydrogen nuclei in the chloroform. A spin parallel to the external magnetic field could then be interpreted as a 1 and an antiparallel spin as 0, and the hydrogen nuclei and carbon-13 nuclei could be treated collectively as a 2-qubit system. In addition to the external magnetic field, radio frequency pulses were applied to cause spin states to “flip,” thereby creating superimposed parallel and antiparallel states. Further pulses were applied to execute a simple [algorithm](https://www.merriam-webster.com/dictionary/algorithm) and to examine the system’s final state. This type of quantum computer can be extended by using molecules with more individually addressable nuclei. In fact, in March 2000 Emanuel Knill, Raymond Laflamme, and Rudy Martinez of Los Alamos and Ching-Hua Tseng of MIT announced that they had created a 7-qubit quantum computer using trans-crotonic acid. However, many researchers are skeptical about extending magnetic techniques much beyond 10 to 15 qubits because of diminishing coherence among the nuclei.

Just one week before the announcement of a 7-qubit quantum computer, physicist [David Wineland](https://www.britannica.com/biography/David-Wineland) and colleagues at the U.S. National Institute for Standards and Technology (NIST) announced that they had created a 4-qubit quantum computer by entangling four ionized beryllium atoms using an electromagnetic “trap.” After confining the ions in a linear arrangement, a [laser](https://www.britannica.com/technology/laser) cooled the particles almost to [absolute zero](https://www.britannica.com/science/absolute-zero) and synchronized their spin states. Finally, a laser was used to entangle the particles, creating a superposition of both spin-up and spin-down states simultaneously for all four ions. Again, this approach demonstrated basic principles of quantum computing, but scaling up the technique to practical dimensions remains problematic.

Quantum computers based on semiconductor [technology](https://www.britannica.com/technology/technology) are yet another possibility. In a common approach a discrete number of free electrons ([qubits](https://www.britannica.com/technology/qubit)) reside within extremely small regions, known as [quantum dots](https://www.britannica.com/science/quantum-dot), and in one of two spin states, interpreted as 0 and 1. Although prone to decoherence, such quantum computers build on well-established, solid-state techniques and offer the prospect of readily applying [integrated circuit](https://www.britannica.com/technology/integrated-circuit) “scaling” technology. In addition, large ensembles of identical quantum dots could potentially be manufactured on a single [silicon](https://www.britannica.com/science/silicon) [chip](https://www.britannica.com/technology/computer-chip). The chip operates in an external magnetic field that controls electron spin states, while neighboring electrons are weakly coupled (entangled) through quantum mechanical effects. An array of superimposed wire electrodes allows individual quantum dots to be addressed, [algorithms](https://www.merriam-webster.com/dictionary/algorithms) executed, and results deduced. Such a system necessarily must be operated at temperatures near absolute zero to minimize environmental decoherence, but it has the potential to incorporate very large numbers of qubits.

https://www.britannica.com/technology/quantum-computer