**Quantum computing** is a type of [computation](https://en.wikipedia.org/wiki/Computation) whose operations can harness the phenomena of [quantum mechanics](https://en.wikipedia.org/wiki/Quantum_mechanics), such as [superposition](https://en.wikipedia.org/wiki/Quantum_superposition), [interference](https://en.wikipedia.org/wiki/Wave_interference#Quantum_interference), and [entanglement](https://en.wikipedia.org/wiki/Quantum_entanglement). Devices that perform quantum computations are known as **quantum computers**.[[1]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-Hidary-1)[[2]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-FOOTNOTENielsenChuang20101-2) Though current quantum computers are too small to outperform usual (classical) computers for practical applications, larger realizations are believed to be capable of solving certain [computational problems](https://en.wikipedia.org/wiki/Computational_problem), such as [integer factorization](https://en.wikipedia.org/wiki/Integer_factorization) (which underlies [RSA encryption](https://en.wikipedia.org/wiki/RSA_encryption)), substantially faster than classical computers. The study of quantum computing is a subfield of [quantum information science](https://en.wikipedia.org/wiki/Quantum_information_science).

There are several models of quantum computation with the most widely used being [quantum circuits](https://en.wikipedia.org/wiki/Quantum_circuit). Other models include the [quantum Turing machine](https://en.wikipedia.org/wiki/Quantum_Turing_machine), [quantum annealing](https://en.wikipedia.org/wiki/Quantum_annealing), and [adiabatic quantum computation](https://en.wikipedia.org/wiki/Adiabatic_quantum_computation). Most models are based on the quantum bit, or "[qubit](https://en.wikipedia.org/wiki/Qubit" \o "Qubit)", which is somewhat analogous to the [bit](https://en.wikipedia.org/wiki/Bit) in classical computation. A qubit can be in a 1 or 0 [quantum state](https://en.wikipedia.org/wiki/Quantum_state), or in a superposition of the 1 and 0 states. When it is measured, however, it is always 0 or 1; the [probability](https://en.wikipedia.org/wiki/Probability) of either outcome depends on the qubit's quantum state immediately prior to measurement. One model that does not use qubits is [continuous variable quantum computation](https://en.wikipedia.org/wiki/Continuous-variable_quantum_information).

Efforts towards building a physical quantum computer focus on technologies such as [transmons](https://en.wikipedia.org/wiki/Transmon" \o "Transmon), [ion traps](https://en.wikipedia.org/wiki/Trapped_ion_quantum_computer) and [topological quantum computers](https://en.wikipedia.org/wiki/Topological_quantum_computer), which aim to create high-quality qubits.[[3]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-2018Report-3): 2–13 These qubits may be designed differently, depending on the full quantum computer's computing model, as to whether [quantum logic gates](https://en.wikipedia.org/wiki/Quantum_logic_gate), [quantum annealing](https://en.wikipedia.org/wiki/Quantum_annealing), or [adiabatic quantum computation](https://en.wikipedia.org/wiki/Adiabatic_quantum_computation) are employed. There are currently a number of significant obstacles to constructing useful quantum computers. It is particularly difficult to maintain qubits' quantum states, as they suffer from [quantum decoherence](https://en.wikipedia.org/wiki/Quantum_decoherence). Quantum computers therefore require [error correction](https://en.wikipedia.org/wiki/Quantum_error_correction).[[4]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-4)[[5]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-5)

Any computational problem that can be solved by a classical computer can also be solved by a quantum computer.[[6]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-FOOTNOTENielsenChuang201029-6) Conversely, any problem that can be solved by a quantum computer can also be solved by a classical computer, at least in principle given enough time. In other words, quantum computers obey the [Church–Turing thesis](https://en.wikipedia.org/wiki/Church%E2%80%93Turing_thesis). This means that while quantum computers provide no additional advantages over classical computers in terms of [computability](https://en.wikipedia.org/wiki/Computability), [quantum algorithms](https://en.wikipedia.org/wiki/Quantum_algorithm) for certain problems have significantly lower [time complexities](https://en.wikipedia.org/wiki/Time_complexity) than corresponding known classical algorithms. Notably, quantum computers are believed to be able to quickly solve certain problems that no classical computer could solve in any *feasible* amount of time—a feat known as "[quantum supremacy](https://en.wikipedia.org/wiki/Quantum_supremacy)." The study of the [computational complexity](https://en.wikipedia.org/wiki/Computational_complexity) of problems with respect to quantum computers is known as [quantum complexity theory](https://en.wikipedia.org/wiki/Quantum_complexity_theory).