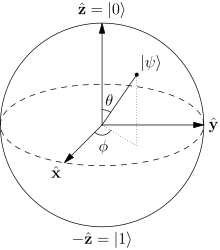
* **Quantum computing supremacy**

Quantum supremacy describes the ability of a quantum computer to outperform their classical counterparts.

In [quantum computing](https://www.sciencealert.com/quantum-computers), operations instead use the quantum state of an object to produce what's known as a [qubit](https://en.wikipedia.org/wiki/Qubit). These states are the undefined properties of an object before they've been detected, such as the spin of an electron or the polarisation of a photon. The complex mathematics behind these unsettled states of entangled 'spinning coins' can be plugged into special algorithms to make short work of problems that would take a classical computer a long time to work out... if they could ever calculate them at all.

Some companies, such as IBM and Google, [claim we might be close](https://www.scientificamerican.com/article/quantum-computers-compete-for-supremacy/), as they continue to cram more qubits together and build more accurate devices.

* Such algorithms would be useful in solving complex mathematical problems, producing hard-to-break security codes, or predicting multiple particle interactions in chemical reactions.
* **History Of Quantum Computing**

Quantum computing began in 1980 when physicist [Paul Benioff](https://en.wikipedia.org/wiki/Paul_Benioff) proposed a [quantum mechanical](https://en.wikipedia.org/wiki/Quantum_mechanics) model of the [Turing machine](https://en.wikipedia.org/wiki/Turing_machine).[[3]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-The_computer_as_a_physical_system-3) [Richard Feynman](https://en.wikipedia.org/wiki/Richard_Feynman) and [Yuri Manin](https://en.wikipedia.org/wiki/Yuri_Manin) later suggested that a quantum computer had the potential to simulate things a [classical computer](https://en.wikipedia.org/wiki/Computer) could not feasibly do.[[4]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-4)[[5]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-manin1980vychislimoe-5) In 1994, [Peter Shor](https://en.wikipedia.org/wiki/Peter_Shor) developed [a quantum algorithm](https://en.wikipedia.org/wiki/Shor%27s_algorithm) for [factoring integers](https://en.wikipedia.org/wiki/Integer_factorization) with the potential to decrypt [RSA](https://en.wikipedia.org/wiki/RSA_(cryptosystem))-encrypted communications.[[6]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-6) Despite ongoing experimental progress since the late 1990s, most researchers believe that "[fault-tolerant](https://en.wikipedia.org/wiki/Quantum_threshold_theorem) quantum computing [is] still a rather distant dream."[[7]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-preskill2018-7) In recent years, investment in quantum computing research has increased in the public and private sectors.[[8]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-8)[[9]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-9) On 23 October 2019, [Google AI](https://en.wikipedia.org/wiki/Google_AI), in partnership with the U.S. National Aeronautics and Space Administration ([NASA](https://en.wikipedia.org/wiki/NASA)), claimed to have performed a quantum computation that was [infeasible on any classical computer](https://en.wikipedia.org/wiki/Quantum_supremacy),[[10]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-10)[[11]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-11) but whether this claim was or is still valid is a topic of active research.[[12]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-12)[[13]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-13) 

There are several types of quantum computers (also known as quantum computing systems), including the [quantum circuit model](https://en.wikipedia.org/wiki/Quantum_circuit), [quantum Turing machine](https://en.wikipedia.org/wiki/Quantum_Turing_machine), [adiabatic quantum computer](https://en.wikipedia.org/wiki/Adiabatic_quantum_computation), [one-way quantum computer](https://en.wikipedia.org/wiki/One-way_quantum_computer), and various [quantum cellular automata](https://en.wikipedia.org/wiki/Quantum_cellular_automata). The most widely used model is the [quantum circuit](https://en.wikipedia.org/wiki/Quantum_circuit), 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.

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.[[1]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-2018Report-1): 2–13 These qubits may be designed differently, depending on the full quantum computer's computing model, 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). 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) and [state fidelity](https://en.wikipedia.org/wiki/Fidelity_of_quantum_states). Quantum computers therefore require [error correction](https://en.wikipedia.org/wiki/Quantum_error_correction).

## For some problems, supercomputers aren’t that super !!

Until now, we’ve relied on supercomputers to solve most problems. These are very large classical computers, often with thousands of classical CPU and GPU cores. However, supercomputers aren’t very good at solving certain types of problems, which seem easy at first glance. This is why we need quantum computers.

## Contents

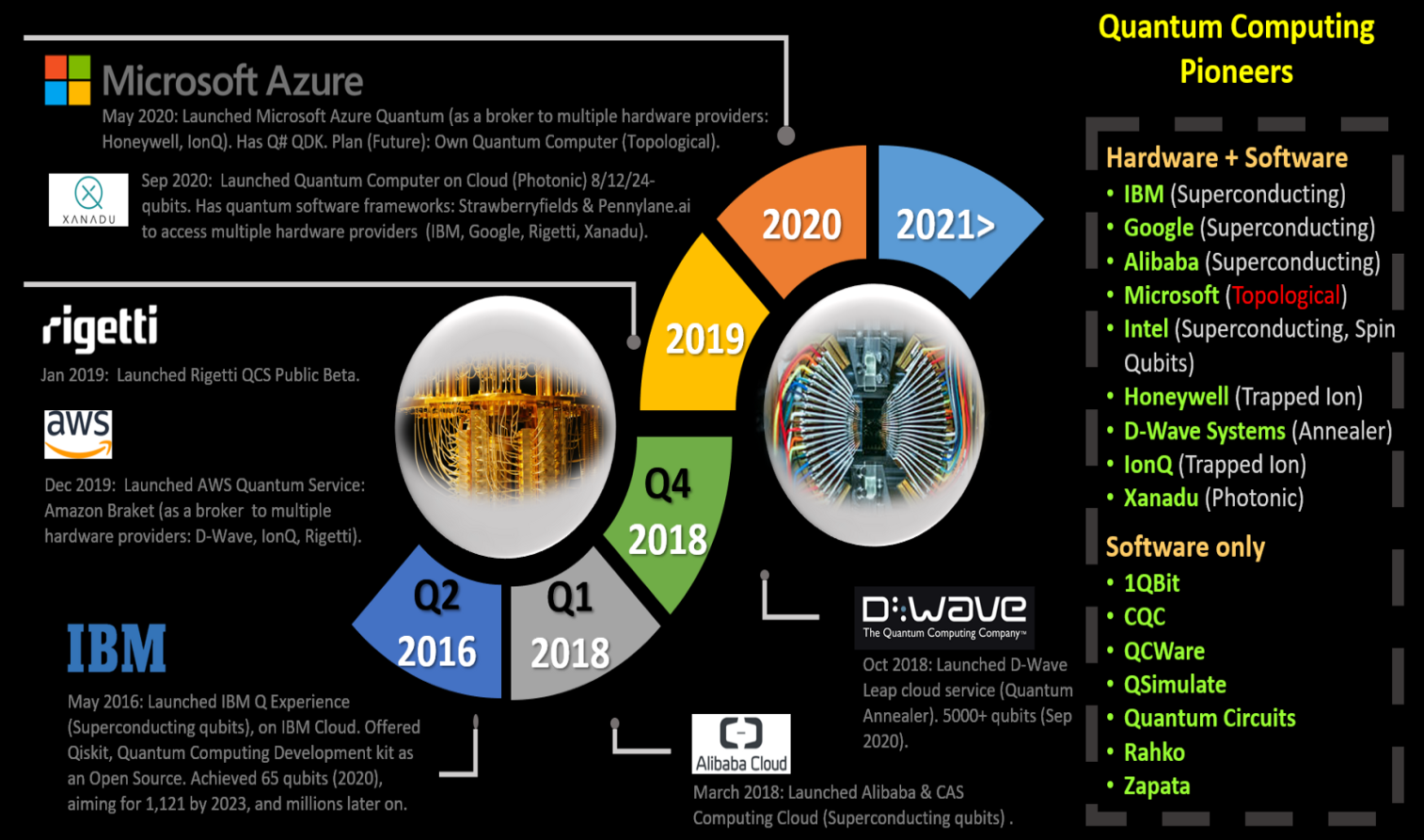
## 1.AI ‘s capcantancy

* + History of techno AI
  + Accessibility to the world
* 2.Potential applications of AI
* Astronomy
* Gaming
* Finance
* Data Security
* Social Media
* Travel and Transport
* Automotive Industry
* Robotics
* Entertainment
* Agricultre
* E-Commerce
* Education
* 3. Future of AI
* [1Quantum circuit](https://en.wikipedia.org/wiki/Quantum_computing#Quantum_circuit)
  + [1.1Definition](https://en.wikipedia.org/wiki/Quantum_computing#Definition)
  + 1.2 History of quantum computing.
* [2Potential applications](https://en.wikipedia.org/wiki/Quantum_computing#Potential_applications)
  + [2.1Cryptography](https://en.wikipedia.org/wiki/Quantum_computing#Cryptography)
  + [2.2Search problems](https://en.wikipedia.org/wiki/Quantum_computing#Search_problems)
  + [2.3Simulation of quantum systems](https://en.wikipedia.org/wiki/Quantum_computing#Simulation_of_quantum_systems)
  + [2.4Quantum annealing and adiabatic optimization](https://en.wikipedia.org/wiki/Quantum_computing#Quantum_annealing_and_adiabatic_optimization)
  + [2.5Machine learning](https://en.wikipedia.org/wiki/Quantum_computing#Machine_learning)
  + [2.6Computational biology](https://en.wikipedia.org/wiki/Quantum_computing#Computational_biology)
  + [2.7Computer-aided drug design and generative chemistry](https://en.wikipedia.org/wiki/Quantum_computing#Computer-aided_drug_design_and_generative_chemistry)
* [3Developing physical quantum computers](https://en.wikipedia.org/wiki/Quantum_computing#Developing_physical_quantum_computers)
  + [3.1Challenges](https://en.wikipedia.org/wiki/Quantum_computing#Challenges)
    - [3.1.1Quantum decoherence](https://en.wikipedia.org/wiki/Quantum_computing#Quantum_decoherence)
  + [3.2Quantum supremacy](https://en.wikipedia.org/wiki/Quantum_computing#Quantum_supremacy)
  + [3.3Skepticism](https://en.wikipedia.org/wiki/Quantum_computing#Skepticism)
  + [3.4Candidates for physical realizations](https://en.wikipedia.org/wiki/Quantum_computing#Candidates_for_physical_realizations)
* [4Relation to computability and complexity theory](https://en.wikipedia.org/wiki/Quantum_computing#Relation_to_computability_and_complexity_theory)
  + [4.1Computability theory](https://en.wikipedia.org/wiki/Quantum_computing#Computability_theory)
  + [4.2Quantum complexity theory](https://en.wikipedia.org/wiki/Quantum_computing#Quantum_complexity_theory)
* [5See also](https://en.wikipedia.org/wiki/Quantum_computing#See_also)
* [6References](https://en.wikipedia.org/wiki/Quantum_computing#References)
* [7Further reading](https://en.wikipedia.org/wiki/Quantum_computing#Further_reading)
  + [7.1Textbooks](https://en.wikipedia.org/wiki/Quantum_computing#Textbooks)
  + [7.2Academic papers](https://en.wikipedia.org/wiki/Quantum_computing#Academic_papers)
* [8External links](https://en.wikipedia.org/wiki/Quantum_computing#External_links)

# Quantum Turing machine

A **quantum Turing machine** (**QTM**) or **universal quantum computer** is an [abstract machine](https://en.wikipedia.org/wiki/Abstract_machine) used to model the effects of a [quantum computer](https://en.wikipedia.org/wiki/Quantum_computer). It provides a simple model that captures all of the power of quantum computation—that is, any [quantum algorithm](https://en.wikipedia.org/wiki/Quantum_algorithm) can be expressed formally as a particular quantum Turing machine. However, the computationally equivalent [quantum circuit](https://en.wikipedia.org/wiki/Quantum_circuit) is a more common model.[[1]](https://en.wikipedia.org/wiki/Quantum_Turing_machine#cite_note-equivalence-1)[[2]](https://en.wikipedia.org/wiki/Quantum_Turing_machine#cite_note-newequivalence-2): 2

Quantum Turing machines can be related to classical and probabilistic Turing machines in a framework based on [transition matrices](https://en.wikipedia.org/wiki/Stochastic_matrix). That is, a matrix can be specified whose product with the matrix representing a classical or probabilistic machine provides the quantum probability matrix representing the quantum machine. This was shown by [Lance Fortnow](https://en.wikipedia.org/wiki/Lance_Fortnow).[[3](https://en.wikipedia.org/wiki/Quantum_Turing_machine#cite_note-transition-3)



# Quantum cryptography

**Quantum cryptography** is the science of exploiting [quantum mechanical](https://en.wikipedia.org/wiki/Quantum_mechanics) properties to perform [cryptographic](https://en.wikipedia.org/wiki/Cryptographic) tasks. The best known example of quantum cryptography is [quantum key distribution](https://en.wikipedia.org/wiki/Quantum_key_distribution) which offers an [information-theoretically secure](https://en.wikipedia.org/wiki/Information-theoretic_security) solution to the [key exchange](https://en.wikipedia.org/wiki/Key_exchange) problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication. For example, it is [impossible to copy](https://en.wikipedia.org/wiki/No-cloning_theorem) data encoded in a [quantum state](https://en.wikipedia.org/wiki/Quantum_state). If one attempts to read the encoded data, the quantum state will be changed due to [wave function collapse](https://en.wikipedia.org/wiki/Wave_function_collapse) ([no-cloning theorem](https://en.wikipedia.org/wiki/No-cloning_theorem)). This could be used to detect eavesdropping in [quantum key distribution](https://en.wikipedia.org/wiki/Quantum_key_distribution).

Quantum computing began in 1980 when physicist [Paul Benioff](https://en.wikipedia.org/wiki/Paul_Benioff) proposed a [quantum mechanical](https://en.wikipedia.org/wiki/Quantum_mechanics) model of the [Turing machine](https://en.wikipedia.org/wiki/Turing_machine).[[3]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-The_computer_as_a_physical_system-3) [Richard Feynman](https://en.wikipedia.org/wiki/Richard_Feynman) and [Yuri Manin](https://en.wikipedia.org/wiki/Yuri_Manin) later suggested that a quantum computer had the potential to simulate things a [classical computer](https://en.wikipedia.org/wiki/Computer) could not feasibly do.[[4]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-4)[[5]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-manin1980vychislimoe-5) In 1994, [Peter Shor](https://en.wikipedia.org/wiki/Peter_Shor) developed [a quantum algorithm](https://en.wikipedia.org/wiki/Shor%27s_algorithm) for [factoring integers](https://en.wikipedia.org/wiki/Integer_factorization) with the potential to decrypt [RSA](https://en.wikipedia.org/wiki/RSA_(cryptosystem))-encrypted communications.[[6]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-6) Despite ongoing experimental progress since the late 1990s, most researchers believe that "[fault-tolerant](https://en.wikipedia.org/wiki/Quantum_threshold_theorem) quantum computing [is] still a rather distant dream."[[7]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-preskill2018-7) In recent years, investment in quantum computing research has increased in the public and private sectors.[[8]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-8)[[9]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-9) On 23 October 2019, [Google AI](https://en.wikipedia.org/wiki/Google_AI), in partnership with the U.S. National Aeronautics and Space Administration ([NASA](https://en.wikipedia.org/wiki/NASA)), claimed to have performed a quantum computation that was [infeasible on any classical computer](https://en.wikipedia.org/wiki/Quantum_supremacy),[[10]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-10)[[11]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-11) but whether this claim was or is still valid is a topic of active research.[[12]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-12)[[13]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-13)

There are several types of quantum computers (also known as quantum computing systems), including the [quantum circuit model](https://en.wikipedia.org/wiki/Quantum_circuit), [quantum Turing machine](https://en.wikipedia.org/wiki/Quantum_Turing_machine), [adiabatic quantum computer](https://en.wikipedia.org/wiki/Adiabatic_quantum_computation), [one-way quantum computer](https://en.wikipedia.org/wiki/One-way_quantum_computer), and various [quantum cellular automata](https://en.wikipedia.org/wiki/Quantum_cellular_automata). The most widely used model is the [quantum circuit](https://en.wikipedia.org/wiki/Quantum_circuit), 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.

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.[[1]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-2018Report-1): 2–13 These qubits may be designed differently, depending on the full quantum computer's computing model, 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). 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) and [state fidelity](https://en.wikipedia.org/wiki/Fidelity_of_quantum_states). Quantum computers therefore require [error correction](https://en.wikipedia.org/wiki/Quantum_error_correction).[[](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-14)