* **Quantum computing supremacy**

**Dr. Anasuya N J1,** **Nidhi Sinha 2, Sri Lakshmi M S3**

***DonBosco Institute of Technology,* Bangalore, Karnataka, India1,2,3Anasuya77.nj@gmail.com1** ,sinhaniya2071@gmail.com2,lakshdora@gmail.com3

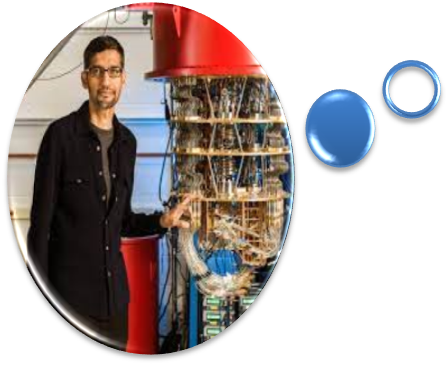
* ***Abstract*-** Quantum supremacy describes the ability of a quantum computer to outperform their classical counterparts. **Quantum computing** is a type of [computation](https://en.wikipedia.org/wiki/Computation) that harnesses the collective properties of [quantum](https://en.wikipedia.org/wiki/Quantum_physics) states, such as [superposition](https://en.wikipedia.org/wiki/Quantum_superposition), interference, and [entanglement](https://en.wikipedia.org/wiki/Quantum_entanglement), to perform calculations. The devices that perform quantum computations are known as **quantum computers**.[[1]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-2018Report-1): I-5[[2]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-2) The study of quantum computing is a subfield of [quantum information science](https://en.wikipedia.org/wiki/Quantum_information_science).

 Though current quantum computers are too small to outperform usual (classical) computers for practical applications, they 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.[[2]](https://en.wikipedia.org/wiki/Quantum_computing#cite_note-2) Quantum Computation is the future of future world and will be proven overdeal pillar in history of human civilization to technocrats.

Keywords—quantum information science,RSA,Qubits.

# **INTRODUCTION**

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 and would even open doors to new advanced parallel world.

# **LITRATURE SURVEY**

It is essential to perceive the past research done concerning this ﬁeld to have the option to effectively progress the correct way.

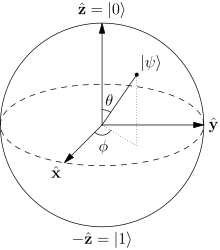
Fig.1.1

* **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.

 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). 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): 2–13There 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).



* **Working Principle**

Quantum computers are elegant machines, smaller and requiring less energy than supercomputers. An IBM Quantum processor is a wafer not much bigger than the one found in a laptop. And a quantum hardware system is about the size of a car, made up mostly of cooling systems to keep the superconducting processor at its ultra-cold operational temperature.

A classical processor uses bits to perform its operations. A quantum computer uses qubits (CUE-bits) to run multidimensional quantum algorithms. It can easily reduce higher order multiorder indefinite equations even.

## **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.

# **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)

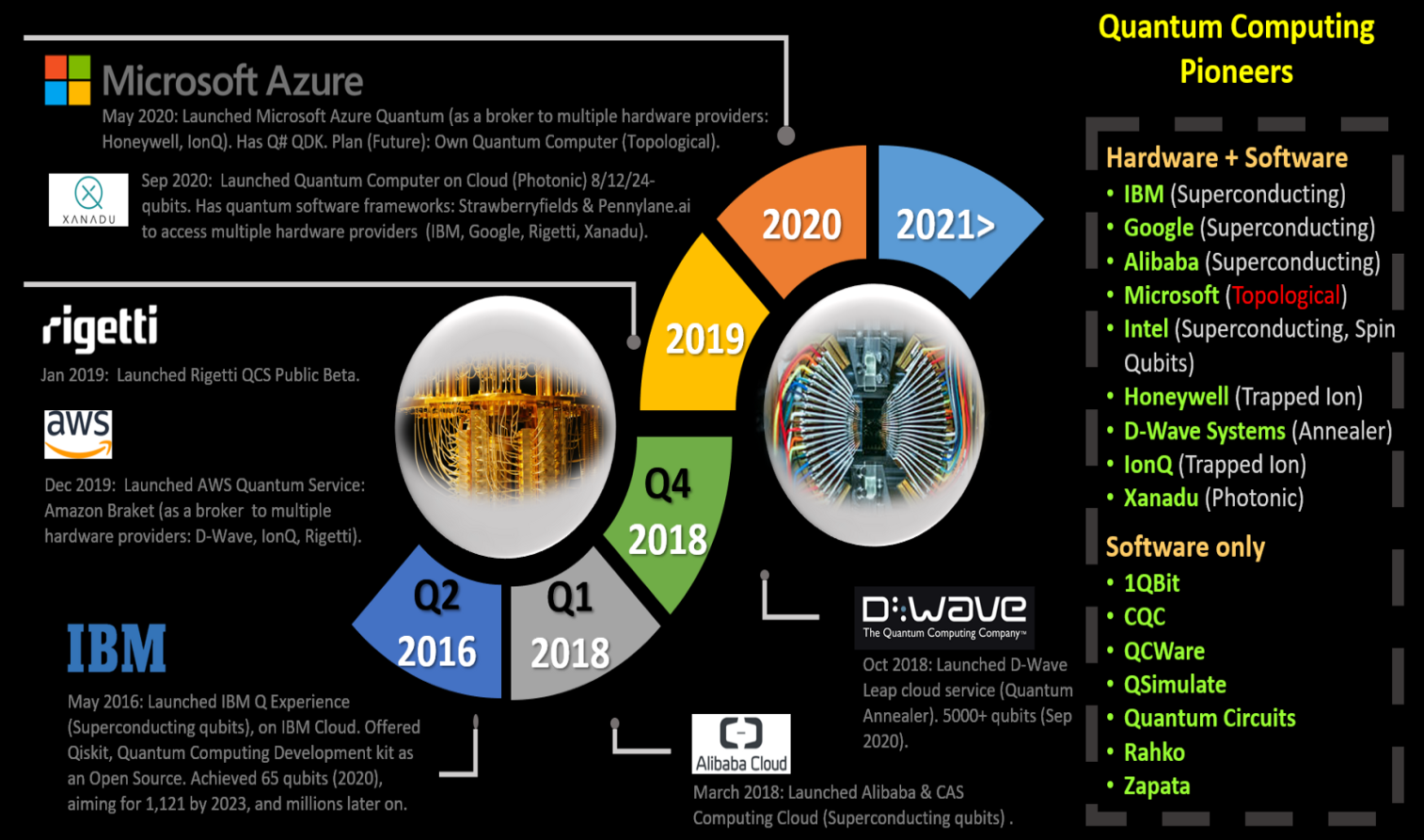


Fig 3.1

# 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)

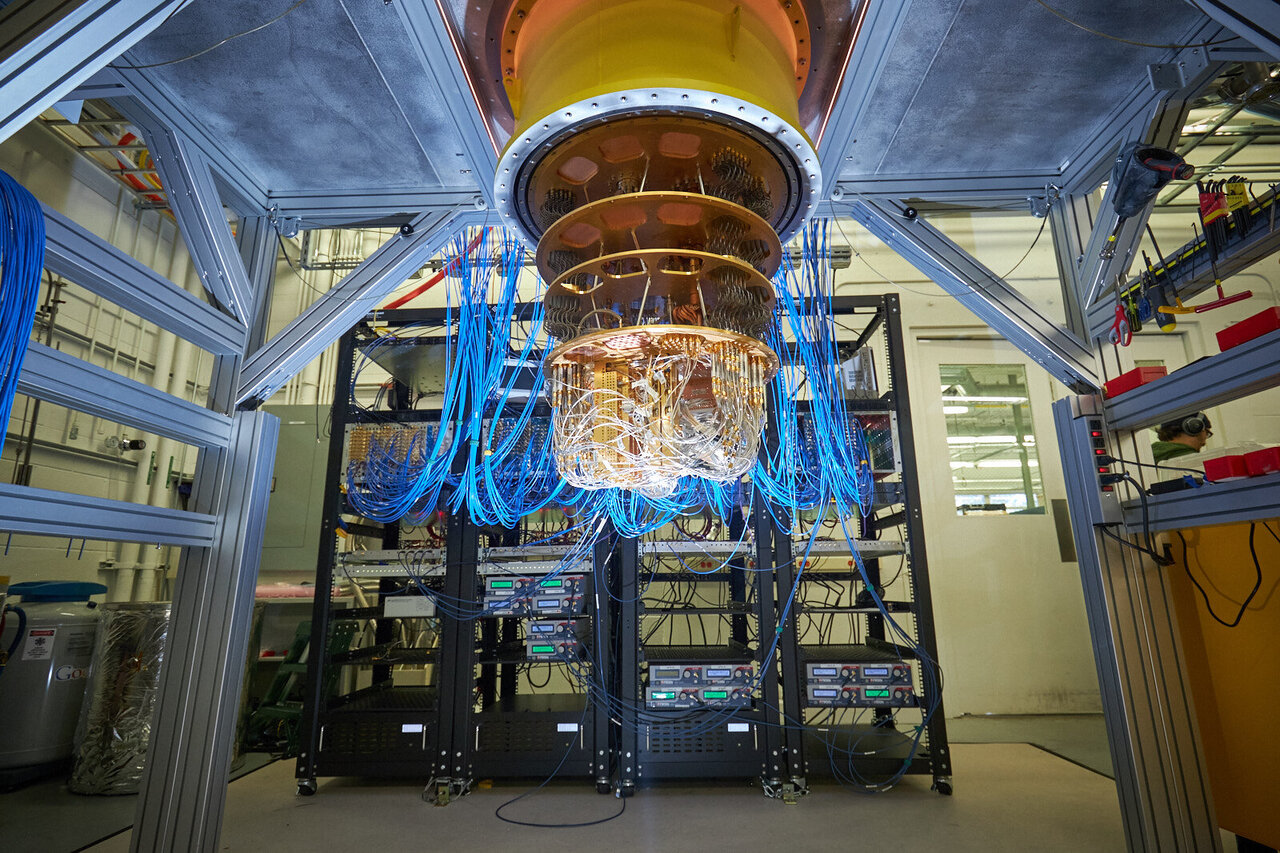


Fig.4.1

**External links**

**[1.Quantum computing – Wikipedia](1.Quantum computing – Wikipediahttps://en.wikipedia.org › wiki › Quantum_computing)**

### [https://en.wikipedia.org › wiki › Quantum\_computing](1.Quantum computing – Wikipediahttps://en.wikipedia.org › wiki › Quantum_computing)

[2.https://www.quantamagazine.org](https://www.quantamagazine.org )

##### **References**

[1]  The National Academies of Sciences, Engineering, and Medicine (2019). Grumbling, Emily; Horowitz, Mark (eds.). Quantum Computing : Progress and Prospects (2018). Washington, DC: National Academies Press. p. I-5. [*doi*](https://en.wikipedia.org/wiki/Doi_(identifier)):[*10.17226/25196*](https://doi.org/10.17226%2F25196). [*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier)) [*978-0-309-47969-1*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-309-47969-1). [*OCLC*](https://en.wikipedia.org/wiki/OCLC_(identifier)) [*1081001288*](https://www.worldcat.org/oclc/1081001288). [*S2CID*](https://en.wikipedia.org/wiki/S2CID_(identifier)) [*125635007*](https://api.semanticscholar.org/CorpusID:125635007).

[2.]**[^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-2" \o "Jump up)** Aaronson, Scott (8 June 2021). [*"What Makes Quantum Computing So Hard to Explain?"*](https://www.quantamagazine.org/why-is-quantum-computing-so-hard-to-explain-20210608/). Quanta Magazine*. Retrieved 9 November 2021*.

[3.] Feynman, Richard (June 1982). [*"Simulating Physics with Computers"*](https://web.archive.org/web/20190108115138/https:/people.eecs.berkeley.edu/~christos/classics/Feynman.pdf) *(PDF)*. International Journal of Theoretical Physics. **21** (6/7): 467–488. [*Bibcode*](https://en.wikipedia.org/wiki/Bibcode_(identifier)):*[1982IJTP...21..467F](https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F)*. [*doi*](https://en.wikipedia.org/wiki/Doi_(identifier)):[*10.1007/BF02650179*](https://doi.org/10.1007%2FBF02650179). [*S2CID*](https://en.wikipedia.org/wiki/S2CID_(identifier)) [*124545445*](https://api.semanticscholar.org/CorpusID:124545445). Archived from [*the original*](https://people.eecs.berkeley.edu/~christos/classics/Feynman.pdf) *(PDF)* on 8 January 2019*. Retrieved 28 February 2019*.

**[4.][^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-manin1980vychislimoe_5-0" \o "Jump up)** Manin, Yu. I. (1980). *[Vychislimoe i nevychislimoe](https://web.archive.org/web/20130510173823/http:/publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip)* [Computable and Noncomputable] (in Russian). Sov.Radio. pp. 13–15. Archived from [*the original*](http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5bdjv-fax%5d.zip) on 10 May 2013*. Retrieved 4 March 2013*.

**[5][^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-6" \o "Jump up)** Mermin, David (28 March 2006). [*"Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm"*](https://web.archive.org/web/20121115112940/http:/people.ccmr.cornell.edu/~mermin/qcomp/chap3.pdf) *(PDF)*. Physics 481-681 Lecture Notes. Cornell University. Archived from [*the original*](http://people.ccmr.cornell.edu/~mermin/qcomp/chap3.pdf) *(PDF)* on 15 November 2012.

**[6][^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-preskill2018_7-0" \o "Jump up)** Preskill, John (2018). "Quantum Computing in the NISQ era and beyond". Quantum. **2**: 79. [*arXiv*](https://en.wikipedia.org/wiki/ArXiv_(identifier)):[*1801.00862*](https://arxiv.org/abs/1801.00862). [*doi*](https://en.wikipedia.org/wiki/Doi_(identifier)):[*10.22331/q-2018-08-06-79*](https://doi.org/10.22331%2Fq-2018-08-06-79). [*S2CID*](https://en.wikipedia.org/wiki/S2CID_(identifier)) [*44098998*](https://api.semanticscholar.org/CorpusID:44098998).

[7] Gibney, Elizabeth (2 October 2019). [*"Quantum gold rush: the private funding pouring into quantum start-ups"*](https://doi.org/10.1038%2Fd41586-019-02935-4). Nature. **574** (7776): 22–24. [*Bibcode*](https://en.wikipedia.org/wiki/Bibcode_(identifier)):*[2019Natur.574...22G](https://ui.adsabs.harvard.edu/abs/2019Natur.574...22G)*. [*doi*](https://en.wikipedia.org/wiki/Doi_(identifier)):[*10.1038/d41586-019-02935-4*](https://doi.org/10.1038%2Fd41586-019-02935-4). [*PMID*](https://en.wikipedia.org/wiki/PMID_(identifier)) [*31578480*](https://pubmed.ncbi.nlm.nih.gov/31578480).

**[8][^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-9" \o "Jump up)** Rodrigo, Chris Mills (12 February 2020). [*"Trump budget proposal boosts funding for artificial intelligence, quantum computing"*](https://thehill.com/policy/technology/482402-trump-budget-proposal-boosts-funding-for-artificial-intelligence-quantum). The Hill.

**[9][^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-10" \o "Jump up)** Gibney, Elizabeth (23 October 2019). [*"Hello quantum world! Google publishes landmark quantum supremacy claim"*](https://doi.org/10.1038%2Fd41586-019-03213-z). Nature. **574** (7779): 461–462. [*Bibcode*](https://en.wikipedia.org/wiki/Bibcode_(identifier)):*[2019Natur.574..461G](https://ui.adsabs.harvard.edu/abs/2019Natur.574..461G)*. [*doi*](https://en.wikipedia.org/wiki/Doi_(identifier)):[*10.1038/d41586-019-03213-z*](https://doi.org/10.1038%2Fd41586-019-03213-z). [*PMID*](https://en.wikipedia.org/wiki/PMID_(identifier)) [*31645740*](https://pubmed.ncbi.nlm.nih.gov/31645740).

**[10][^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-11" \o "Jump up)** Aaronson, Scott (30 October 2019). [*"Opinion | Why Google's Quantum Supremacy Milestone Matters"*](https://www.nytimes.com/2019/10/30/opinion/google-quantum-computer-sycamore.html). The New York Times. [*ISSN*](https://en.wikipedia.org/wiki/ISSN_(identifier)) [*0362-4331*](https://www.worldcat.org/issn/0362-4331)*. Retrieved 25 September 2021*.

**[11][^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-12" \o "Jump up)** [*"On 'Quantum Supremacy'"*](https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/). IBM Research Blog. 22 October 2019*. Retrieved 9 February 2021*.

**[12][^](https://en.wikipedia.org/wiki/Quantum_computing" \l "cite_ref-13" \o "Jump up)** Pan, Feng; Zhang, Pan (4 March 2021). "Simulating the Sycamore quantum supremacy circuits". [*arXiv*](https://en.wikipedia.org/wiki/ArXiv_(identifier)):[*2103.03074*](https://arxiv.org/abs/2103.03074) [[*quant-ph*](https://arxiv.org/archive/quant-ph)].

## **Contents**

* [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.
* 2. literature survey
* 3. Working aspect
* 4.Clampdown to supercomputers
* [5.Potential applications](https://en.wikipedia.org/wiki/Quantum_computing#Potential_applications)
  + [5.1Cryptography](https://en.wikipedia.org/wiki/Quantum_computing#Cryptography)
  + 5.2 Quantum Turing Machine
* [6.References](https://en.wikipedia.org/wiki/Quantum_computing#References)
* [7.Further 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)
* [8.External links](https://en.wikipedia.org/wiki/Quantum_computing#External_links)

Fig 2.1