

Timeline of Quantum Computing

(For complete timeline visit https://en.wikipedia.org/wiki/Timeline_of_quantum_computing)

1980s

- 1980
 - Paul Benioff describes quantum mechanical Hamiltonian models of computers.
 - Yuri Manin briefly motivates the idea of quantum computing.
- 1981
 - Richard Feynman observes in his talk at the *First Conference on the Physics of Computation*, held at MIT in May, that it appeared to be impossible in general to simulate an evolution of a quantum system on a classical computer in an efficient way. He proposes a basic model for a quantum computer that would be capable of such simulations.
 - Paul Benioff gives talk at the same conference with the title “Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: application to Turing machines”.
 - Tommaso Toffoli introduces the reversible Toffoli gate, which, together with the NOT and XOR gates provides a universal set for reversible classical computation.
- 1982
 - Paul Benioff proposes the first recognisable theoretical framework for a quantum computer
 - William Wootters and Wojciech Zurek, and independently Dennis Dieks prove the no-cloning theorem.
- 1984
 - Charles Bennett and Gilles Brassard employ Wiesner’s conjugate coding for distribution of cryptographic keys.
- 1985
 - David Deutsch, at the University of Oxford, describes the first universal quantum computer. Just as a Universal Turing machine can simulate any other Turing machine efficiently (Church-Turing thesis), so the universal quantum computer is able to simulate any other quantum computer with at most a polynomial slowdown.
- 1989
 - Bikas K. Chakrabarti & collaborators from Saha Institute of Nuclear Physics, Kolkata, proposes the idea that quantum fluctuations could help explore rough energy landscapes by escaping from local minima of glassy stems having tall but thin barriers by tunneling (instead of climbing over using thermal excitations), suggesting the effectiveness of quantum annealing over classical simulated annealing.^[*citation needed*]

1990s

- 1991
 - Artur Ekert at the University of Oxford, invents entanglement-based secure communication.
- 1992
 - David Deutsch and Richard Jozsa propose a computational problem that can be solved efficiently with the determinist Deutsch–Jozsa algorithm on a quantum computer, but for which no deterministic classical algorithm is possible. This was perhaps the earliest result in the computational complexity of quantum computers, proving that they were capable of performing *some* well-defined computational task more efficiently than any classical computer.
- 1993
 - Dan Simon, at Université de Montréal, invents an oracle problem for which a quantum computer would be exponentially faster than a conventional computer. This algorithm introduces the main ideas which were then developed in Peter Shor’s factorization algorithm.
- 1994
 - Peter Shor, at AT&T’s Bell Labs in New Jersey, discovers an important algorithm. It allows a quantum computer to factor large integers quickly. It solves both the factoring problem and the discrete log problem. Shor’s algorithm can theoretically break many of the cryptosystems in use today. Its invention sparked a tremendous interest in quantum computers.
 - First United States Government workshop on quantum computing is organized by NIST in Gaithersburg, Maryland, in autumn.
 - In December, Ignacio Cirac, at University of Castilla-La Mancha at Ciudad Real, and Peter Zoller at the University of Innsbruck propose an experimental realization of the controlled-NOT gate with cold trapped ions.
- 1995
 - The first United States Department of Defense workshop on quantum computing and quantum cryptography is organized by United States Army physicists Charles M. Bowden, Jonathan P. Dowling, and Henry O. Everitt; it takes place in February at the University of Arizona in Tucson.
 - Peter Shor and Andrew Steane simultaneously propose the first schemes for quantum error correction.