Quantum Computing: An Introduction

Barbara Widholm

April 2026

How do quantum computers work?

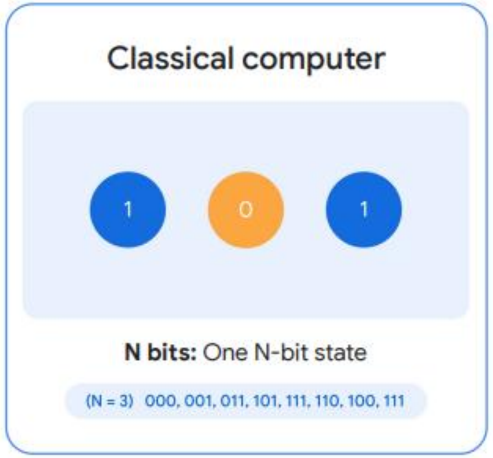
- Quantum computers use quantum bits, or qubits, as their fundamental units of computation.
- In classical computers, the basic building blocks are bits, which can be in one of two states: 0 or 1, much like a light bulb that is either on or off. Qubits, however, can exist in a state called superposition, where they are not just 0 or 1 but can exist in both simultaneously (like a light dimmer, or the light being on and off at the same time).
- We can imagine the state as a position on the surface of the Earth, with the north and south poles representing the states 0 and 1. Being in a superposition is like standing at the equator, where there’s a 50% chance of measuring the state as 0 and a 50% chance of measuring it as 1.
- Unlike classical bits, whose state remains the same unless altered, qubits in superposition provide a probabilistic outcome when measured.

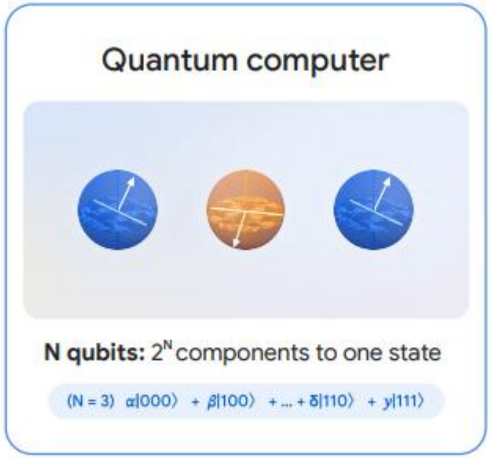
Quantum computers are fundamentally different from classical computers and are expected to complement them rather than replace them.

While classical computers handle everyday tasks like organizing information, quantum computers introduce a new computing paradigm suited for some complex problems that classical machines cannot solve

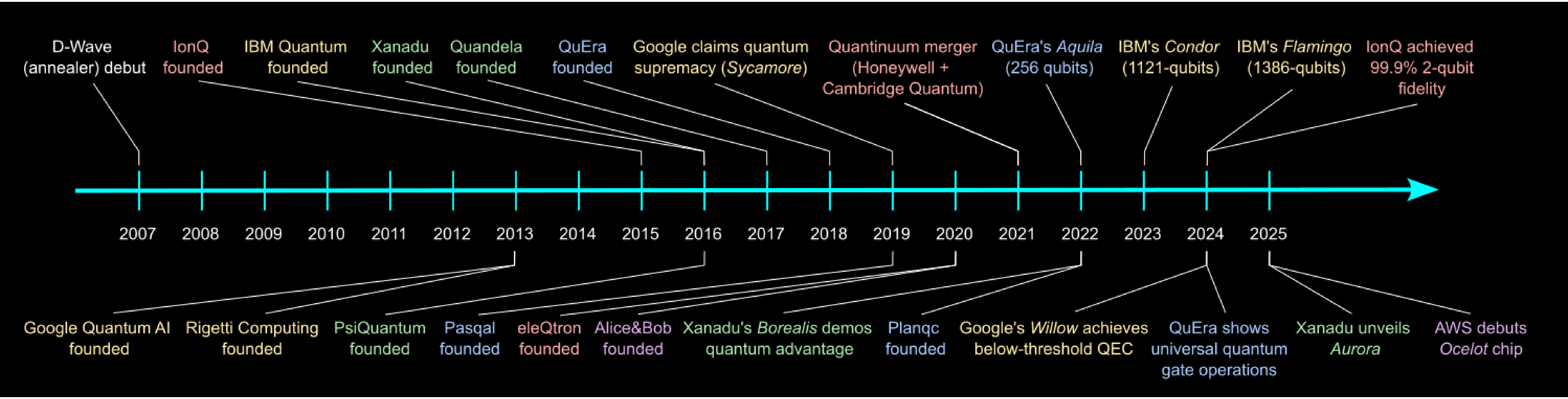
What quantum computing is not:

- It’s not a faster version of your laptop.
- It won’t run Excel or Python quicker.
- It is not broadly better at all computing tasks.





Quantum Computing Trailblazers roadmap



D-Wave (annealer) debut

IonQ founded

IBM Quantum founded

Xanadu founded

Quandela founded

QuEra founded

Google claims quantum supremacy (*Sycamore*)

Quantinuum merger (Honeywell + Cambridge Quantum)

QuEra's *Aquila* (256 qubits)

IBM's *Condor* (1121-qubits)

IBM's *Flamingo* (1386-qubits)

IonQ achieved 99.9% 2-qubit fidelity

Google Quantum AI founded

Rigetti Computing founded

PsiQuantum founded

Pasqal founded

eleQtron founded

Alice&Bob founded

Xanadu's *Borealis* demos quantum advantage

Planqc founded

Google's *Willow* achieves below-threshold QEC

QuEra shows universal quantum gate operations

Xanadu unveils *Aurora*

AWS debuts *Ocelot* chip

Types of Quantum Computers

Hardware options, trade-offs and selection implications

Type	How It Works	Companies/Status
Superconducting circuits	Qubits are microwave-driven Josephson junction circuits at millikelvin temperatures	IBM, Google, Rigetti: commercial cloud-accessible machines
Trapped ions	Individual ions held by electromagnetic fields; qubits encoded in ion energy levels	IonQ, Honeywell (Quantinuum): high fidelity, slower gate speeds
Photonic systems	Qubits or continuous variables encoded in photons; operate at or near room temperature	PsiQuantum, Xanadu: pros for integration and room-temperature operation
Quantum annealers	Analog optimization using controlled quantum tunneling to find low-energy states	D-Wave: specialized for optimization problems
Quantum dots / Topological	Solid-state qubits in semiconductors or protected anyon-based qubits for error resilience	Intel, academic teams, startups: research and early pilot efforts
Neutral atoms	Qubits formed by trapping neutral atoms in optical lattices using laser beams	ColdQuanta, Pasqal: emerging players

Key points to consider:

Scalability:

Assess qubit counts, error rates, and roadmap for growth.

Cryogenics and environment:

Need for millikelvin refrigeration versus room-temperature options.

Integration complexity:

Control electronics, photonics links, and cloud access impact pilots.

Operator trade-offs summary:

Choose by target algorithms, error mitigation, and deployment path.

Key Concepts and Terminologies

Qubit
The quantum version of a bit that can represent 0, 1, or both simultaneously through superposition. A qubit in superposition can encode multiple possibilities, enabling faster optimization.

Superposition
A principle where a qubit exists in multiple states at once, allowing parallel computation paths. Used in quantum search algorithms to explore many solutions simultaneously.

Entanglement
A phenomenon where qubits become correlated so that the state of one affects the other, even at a distance. Enables quantum teleportation and secure communication protocols.

Shor's Algorithm
A quantum algorithm that can factor large integers exponentially faster than classical algorithms, threatening RSA and ECC cryptography.

Decoherence
The loss of quantum state due to environmental interference, causing errors and instability. Quantum computers need error correction to counter decoherence during computations.

Interference
Quantum interference occurs when probability amplitudes of different quantum states combine, reinforcing or canceling each other. This is key to how quantum algorithms amplify correct answers like Grover's algorithm boosts searching solutions faster.

Gates
Operations that manipulate qubits by changing their amplitude and phase, forming the basis of quantum algorithms. The Hadamard gate creates superposition, essential for quantum parallelism.

Grover's Algorithm
Provides a quadratic speed-up for unstructured search problems compared to classical algorithms.

Where Quantum Computing stands

Qubit Counts Are Growing

We now have devices with:

· 50–100 high-quality qubits(superconducting, trapped ion)

· Specialized systems optimized for simulation or optimization

· Roadmaps toward 1,000+qubits with error correction in the next few years

Noise is still a limiting factor

Today's systems are called NISQ: Noisy Intermediate-Scale Quantum computers. They are powerful but fragile. Qubits lose coherence quickly, and results require careful error mitigation.

Hybrid Quantum-Classical Systems Are the Near-Term Reality

Many meaningful applications will come from hybrid workflows, where aquantum processor handles specific sub problems inside a classical pipeline.

Real Experiments Are Happening

Banks, pharmaceutical companies, energy firms, and government agencies are already:

· Running proof-of-concepts

· Adding quantum-suitable datasets

· Experimenting with algorithms for simulation and optimization

· Preparing for post-quantum cryptography

Why learn Quantum Computing?

Practical reasons, impacted fields, and next steps

Understand Potential Disruptions

Quantum advantage is approaching:

Early breakthroughs in quantum algorithms for optimization and cryptography signal potential disruption in finance, supply chains, and security.

Post-quantum security urgency:

Governments and enterprises are racing to adopt quantum-safe encryption standards before quantum computers break current cryptographic systems.

Competitive edge:

Organizations that anticipate quantum-driven changes can adapt business models faster than competitors.

Spot High-Impact Use Cases

Industry pilots are scaling:

Financial institutions, pharma, and logistics companies are already running quantum-inspired pilots for portfolio optimization and drug discovery.

AI acceleration:

Quantum machine learning research is gaining traction, promising breakthroughs in pattern recognition and large-scale data analysis.

Cybersecurity stakes:

Quantum computing threatens RSA and ECC encryption, making cybersecurity a top priority for future-proofing systems.

Evaluate Strategic Experiments

Hardware maturity:

Cloud providers like IBM, AWS, and Google offer access to real quantum machines, enabling practical experimentation without huge capital investment.

Benchmarking classical vs quantum:

Comparing performance on optimization and simulation tasks helps identify where quantum offers real advantage today.

Risk mitigation:

Running pilots now reduces uncertainty and prepares organizations for rapid adoption when quantum scales.

Learn Through Hands-On Access

Accessible platforms:

Quantum-as-a-service is available through major cloud providers, making hands-on learning affordable and practical.

Skill gap is widening:

Demand for quantum-literate professionals is growing; early adopters will lead in shaping standards and applications.

Immediate ROI in learning:

Experimenting with quantum circuits builds foundational knowledge for future integration into workflows.

Map Where Quantum Adds Value

Targeted advantage areas:

Quantum excels in optimization, simulation, and cryptography, fields critical to finance, logistics, and pharma today.

Strategic prioritization:

Identifying problems that benefit most from quantum ensures efficient resource allocation and avoids hype-driven investments.

Future-proofing decisions:

Mapping quantum opportunities now positions organizations to pivot quickly as technology matures.

What can we do today?

Quantum Simulation

This is the “killer app” in the near term. Quantum systems naturally model other quantum systems: molecules, materials, and chemical reactions.

Applications include:

- Drug discovery
- Battery chemistry
- Catalyst design
- Carbon capture materials
- Semiconductor modeling

Quantum Optimization

Quantum computers can explore vast solution spaces using:

- Quantum Approximate Optimization Algorithm (QAOA)
- Quantum annealing
- Amplitude amplification

Industries impacted:

- Logistics and transport
- Portfolio optimization and risk modeling
- Staffing and shift optimization
- Manufacturing and scheduling

Quantum ML

Quantum can help AI with:

- Feature transformation
- Kernel methods
- Optimization in training loops
- Sampling and generative modeling

Quantum Cryptography

Quantum computers pose a future threat to RSA and ECC encryption. Governments are already acting:

- Moving to post-quantum cryptography
- Preparing for “harvest-now, decrypt-later” risks

Key use cases across industries

HPC

- AI accelerators
- Cloud computing services
- Materials simulations
- Climate modelling
- Hybrid computing

RIKEN

JÜLICH
Forschungszentrum

CINECA

lrz

NVIDIA

Chemical/Pharma

- Quantum chemistry simulations
- Molecular modeling
- Drug & marker discovery
- Peptide engineering

AMGEN

janssen

bp

MERCK

JSR

abbvie

Automotive

- Computational fluid dynamics
- Workflow scheduling
- Performance optimization
- Multi-car paint shop problem
- Battery materials

Mercedes-Benz

GEELY

ROLLS
ROYCE

ANDRETTI
AUTOSPORT

Aerospace

- Advanced fluid dynamics
- Physics simulations
- Flight mechanics
- Advanced materials discovery

Raytheon
Technologies

BOEING

AIRBUS

LOCKHEED MARTIN

NASA

U.S. AIR FORCE

Financial

- Pricing optimization
- Collateral optimization
- Finance simulations
- Transactional fraud detection

SoftBank

WELLS
FARGO

mastercard

CRÉDIT AGRICOLE

Bank of America

Quantum Computing Programming Languages & SDKs

Software Development Kits (SDKs):

Quantum programming involves high-level SDKs (like Python-based Qiskit, Cirq, PennyLane) for familiar syntax, domain-specific languages (Q# for Microsoft, QCL) for quantum logic, and hardware-agnostic intermediate representations (OpenQASM, QIR) for compiling to different machines. These SDKs are often layered over classical languages like Python, C++, or Julia to build and run quantum algorithms.

Provider	Full-Stack Libraries	Quantum Algorithms	Quantum Circuits	Assembly Language	Hardware
IBM	Qiskit	Qiskit Aqua	Qiskit Terra	OpenQASM	Superconducting, Trapped Ions
Rigetti	Forest	Grove	Pyquil	Quil	Superconducting
D-Wave	—	Qsage, ToQ	qbsolv	QMASM	Superconducting
Xanadu	Strawberry Fields	—	—	Blackbird	Photonic
Google	Cirq	OpenFermion-Cirq	Cirq	—	Superconducting, Trapped Ions
Microsoft	Quantum Developer Kit	Q#	—	Other Quantum Machine Instruction Languages	Superconducting, Topological
Qilimanjaro	Qibo	—	—	—	Superconducting, Trapped Ions

Current Limitations and The Road Ahead

Hardware limits

Noisy, small systems (tens to hundreds of qubits)

Current quantum computers are limited in scale and suffer from high error rates due to noise and instability. Achieving fault-tolerant systems will require significant advances in error correction and qubit quality.

Ongoing actions

Pilot experiments and monitor hardware and software advances

Organizations need to track vendor roadmaps, test algorithms on available quantum hardware, and monitor progress in error correction and software frameworks to stay ahead.

Near-term use

Specialized hard problems, not general replacement

Quantum computing is not ready to replace classical systems broadly. Instead, it excels in niche areas like optimization, cryptography, and molecular simulation where classical methods struggle.

Progress areas

Qubit counts, error correction, tooling

Steady improvements in hardware, error mitigation, and developer tools are expanding capabilities. Growth in qubit counts and better algorithms will gradually unlock more practical applications.

Organizational posture

Hybrid architectures and incremental pilots

Enterprises should adopt hybrid approaches, integrating quantum as a co-processor alongside classical systems. Incremental pilots help build expertise while minimizing risk.

Classical vs. Quantum Computing

Key Differences and Why They Matter Now

Aspect	Classical Computer	Quantum Computer	Why is it Relevant
Data Representation	Uses bits: 0 or 1	Uses qubits: 0, 1, or both (superposition)	Superposition enables massive parallelism, critical for solving complex optimization problems.
Outcome Nature	Deterministic outcomes	Probabilistic outcomes; require repeated sampling	Algorithms must adapt to uncertainty; industries need probabilistic models for real-world data.
Logic Operations	Classical logic gates (AND, OR, NOT)	Quantum gates (X, H, CNOT) that change amplitudes and phase	Quantum gates allow interference and entanglement, enabling faster algorithms for hard problems.
Processing Model	Processes one state per operation	Explores many possibilities simultaneously via superposition	Parallelism accelerates tasks like portfolio optimization and molecular simulation.
Entanglement	No entanglement; state independence	Entanglement links qubits, enabling correlated states	Entanglement powers secure communication and advanced simulations in chemistry and physics.
Measurement & State Behavior	Can be measured completely without changing state; bits can be copied and erased	Measurement changes the state; qubits cannot be copied or erased (No-Cloning Theorem)	Impacts algorithm design and error correction; requires probabilistic sampling and careful state management

Key points to consider:

Algorithm Design Implication:

Must rethink control flow; quantum algorithms combine amplitude manipulation with classical post-processing.

Error Handling:

Quantum systems are noisy; error mitigation and redundancy strategies are essential.

Output Interpretation:

Requires repeated sampling and aggregation to estimate probabilities and confidence.

Practical Note:

Quantum changes both how and what we compute—impacting cryptography, optimization, and AI.

Types of Quantum Computers

Hardware options, trade-offs and selection implications

Type	How It Works	Companies/Status
Superconducting circuits	Qubits are microwave-driven Josephson junction circuits at millikelvin temperatures	IBM, Google, Rigetti: commercial cloud-accessible machines
Trapped ions	Individual ions held by electromagnetic fields; qubits encoded in ion energy levels	IonQ, Honeywell (Quantinuum): high fidelity, slower gate speeds
Photonic systems	Qubits or continuous variables encoded in photons; operate at or near room temperature	PsiQuantum, Xanadu: pros for integration and room-temperature operation
Quantum annealers	Analog optimization using controlled quantum tunneling to find low-energy states	D-Wave: specialized for optimization problems
Quantum dots / Topological	Solid-state qubits in semiconductors or protected anyon-based qubits for error resilience	Intel, academic teams, startups: research and early pilot efforts
Neutral atoms	Qubits formed by trapping neutral atoms in optical lattices using laser beams	ColdQuanta, Pasqal: emerging players

Key points to consider:

Scalability:

Assess qubit counts, error rates, and roadmap for growth.

Cryogenics and environment:

Need for millikelvin refrigeration versus room-temperature options.

Integration complexity:

Control electronics, photonics links, and cloud access impact pilots.

Operator trade-offs summary:

Choose by target algorithms, error mitigation, and deployment path.