How does it work?

The secret to a quantum computer's power lies in its ability to generate and manipulate quantum bits, or qubits. Both superposition and entanglement are critical for the computational "speedup" associated with quantum computing.

Superposition: A qubit can store not only 0 or 1 but also a betwixt state called a superposition—which can assume lots of different values. Without superposition, qubits would behave like classical bits, and would not be in the multiple states that allow quantum programmers to run the equivalent of many calculations at once.

Entanglement: Entanglement is an extremely strong correlation that exists between quantum particles — so strong, in fact, that two or more quantum particles can be inextricably linked in perfect unison, even if separated by great distances. The particles are so intrinsically connected, they can be said to "dance" in perfect unison, even when placed at opposite ends of the universe.

Without entanglement, qubits would sit in superposition without generating additional insight by interacting. No calculation would take place because the state of each qubit would remain independent of others.

Superposition analogy

If information were color, then a classical bit could be either black or white. A qubit when it's in superposition could be any color on the spectrum and could also vary in brightness.

Entanglement analogy

If you flip two coins, the result of one coin toss has no influence on the result of the other. They're independent. In entanglement, two particles are linked together, even if they're physically separate. If one comes up heads, the other one will also be heads.

Note

A large-scale, fault-tolerant quantum computer capable of carrying out tasks of practical interest has not yet been achieved in the open science enterprise.

Qubits need to be almost perfectly isolated from heat, vibration, and stray atoms—hence the "chandelier" refrigerators in Google's quantum lab. Even then, they can function for at most a few hundred microseconds before they "decohere" and lose their superposition.

They aren't always faster than classical computers. They're just different, faster at some things and slower at others, and require different kinds of software.