What is quantum computing?

KS3 KS4 Ages 11-16 ⏰ 4 min read

A regular computer processes information as bits — each one is either 0 or 1. Everything your computer does — every calculation, every pixel on screen, every word processed — is ultimately a long sequence of 0s and 1s being manipulated by billions of tiny transistors switching on and off.

A quantum computer uses **qubits** instead of bits. Thanks to quantum mechanics, a qubit doesn't have to be just 0 or just 1 — it can be in a "superposition" of both states simultaneously. This sounds like a minor technical detail, but the implications are extraordinary.

Imagine searching a maze. A regular computer tries paths one at a time — left, dead end, back, right, dead end, back — until it finds the exit. A quantum computer is (very loosely) like exploring all possible paths simultaneously and finding the solution in one go. For certain types of problems — particularly those involving searching through enormous numbers of possibilities — this parallel exploration offers a colossal speedup over even the fastest classical computers.

What is entanglement?

Quantum entanglement is another property qubits can exploit. Two qubits can be entangled so that the state of one instantly affects the other, regardless of the distance between them. This allows quantum computers to process certain calculations in a fundamentally different — and for some problems, far more efficient — way than classical computers.

What could quantum computers do?

Drug discovery: Simulating molecular interactions at the quantum level — something classical computers can only approximate — could dramatically accelerate the discovery of new medicines. **Cryptography:** A sufficiently powerful quantum computer could factor the large prime numbers that underlie most current encryption (including the public-key encryption protecting online banking). This is a significant security concern and is driving research into "quantum-resistant" cryptography. **Optimisation:** Route planning, financial modelling, logistics — problems with astronomical numbers of possible solutions where quantum algorithms could find near-optimal answers far faster.

Are they ready now?

Not for most of these applications. Current quantum computers are small (dozens to hundreds of qubits), noisy (errors are frequent), and require cooling to near absolute zero. They've demonstrated "quantum advantage" on specific narrow tasks, but a general-purpose, fault-tolerant quantum computer powerful enough to break current encryption or simulate large molecules is likely still years to decades away. The field is moving rapidly, but practical quantum computing at scale is still a work in progress.