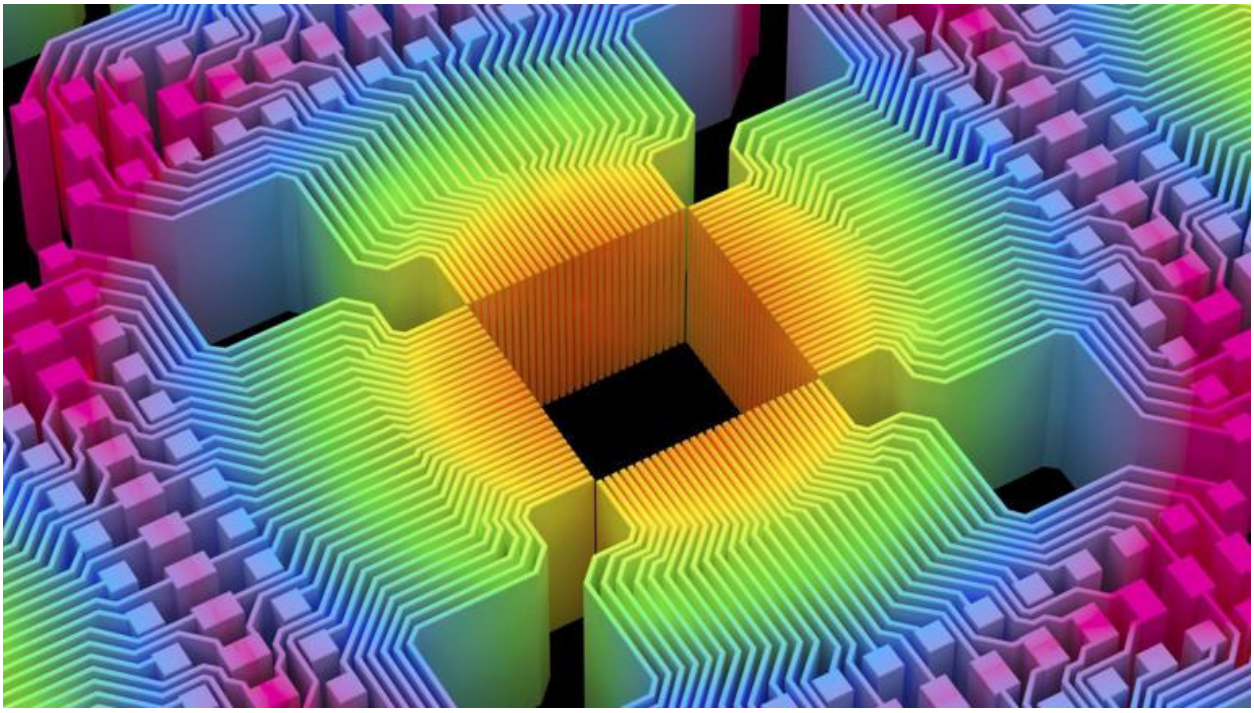

Quantum bit (qubit), defined

A quantum bit, otherwise known as a qubit, is the basic unit of data in quantum computing. Like a binary bit in classical computers, it can store information, but behaves very differently thanks to quantum mechanics.

Quantum computers normally use subatomic particles, such as photons (packets of light) or electrons, as qubits. In qubits, properties such as charge, photonic polarization, or spin represent the 1s and 0s in binary computing. However, qubits are also subject to phenomena known as superposition and entanglement, due to their quantum nature, which is where things start to get weird.

Bits vs qubits: What's the difference?

As well as being either 0 or 1, like a bit, qubits can occupy both states at the same time — or a superposition of 1 and 0. The qubit will remain in superposition until it is directly observed or disrupted by external environmental factors, such as heat. Because this quantum state is so delicate, qubits have to be kept free from interference, which requires very cold temperatures.

Superposition allows the qubits of a quantum computer to be in multiple states (0, 1, or both), and the number of possible states available grows exponentially as the more qubits increases. If you have two classical bits, for example, at any given time they could take the values of either 0,0; 0,1; 1,0; or 1,1.

With two qubits, you can encode data in all four states at once. As such, quantum computers potentially have far greater processing power than conventional computers using binary bits. The more qubits you have, the more calculations you can process in parallel — and this rises exponentially if you add more to the system. However, to see exponential growth in processing power, you must also entangle the qubits.

How does entanglement work?

In quantum entanglement, the states of subatomic particles are linked, regardless of how far apart they may be. Gaining information about a qubit will automatically provide information about its entangled particle.

Entangled particles are always in a correlated state. Consequently, if a property (such as spin) of one particle is measured, thus bringing it out of superposition, the same thing will also instantaneously happen to the entangled particle. Since the states of the two entangled particles are always correlated, knowing the state of one entangled particle means the state of the other can be inferred.

Rather than directly measuring the qubit and thereby causing it to lose its superposition state, scientists are investigating whether there might be a way of indirectly inferring information about a qubit from its interaction with the surrounding environment.

Quantum entanglement of qubits also allows them to interact with each other simultaneously, regardless of their distance from each other. When combined with superposition, quantum entanglement theoretically enables qubits to greatly enhance the computing power of quantum computers, allowing them to perform complex calculations that powerful binary computers would struggle to resolve.

This is currently possible at a small scale, but the challenge is to scale it up. For instance, some calculations, such as breaking encryption algorithms, would take classical computers millions of years to perform. However, if we could build a

quantum computer with millions of qubits, those same algorithms could be cracked within seconds.

Why are qubits so fragile and prone to decoherence?

So why haven't we simply stacked up more and more qubits to build such a machine? Unfortunately, qubits are short-lived, and the superposition can collapse with the very faintest of external environmental influences, like heat or movement. For that reason, they are deemed "noisy" and error-prone.

For that reason, many qubits need to be chilled to near absolute zero and maintained using specialized equipment. They also have incredibly short "coherence times," which is the measure of how long they retain the desired state needed to process quantum calculations. Coherence times usually only last fractions of a second. (The world record is 10 minutes for a single qubit — but experts think it's unlikely to be translated to a real quantum computer.) This factor also makes qubits unsuitable for long-term data storage.

Although many quantum computers exist today, we still need to apply "error correction" techniques to qubits to trust their results. One major error correction method under investigation today is building a "logical qubit." A logical qubit is actually a group of entangled, error-prone qubits that store the same information in different places. This spreads out the possible points of failure while a calculation is underway, thereby correcting the errors. Should qubits be stabilized sufficiently, with the superposition and quantum entanglement of qubits in place, quantum computers can one day perform calculations in a fraction of the time that a binary computer would need, as well as solve complex equations that are impossible for even today's most powerful supercomputers.