Quantum computing explained: harnessing particle physics to work faster

Nicola Davis, March 6, 2014
http://www.theguardian.com/science/2014/mar/06/quantum-computing-explained-particle-mechanics

The D-Wave, the world's only commercially available quantum computer.

Around the world teams of scientists are working on the next technological revolution: quantum computing. But what makes it so special? And why do we need it? We ask physicist Dr Ruth Oulton of the Bristol University to explain.

In a normal computer, information is stored as bits. How is it different in a quantum computer?

A normal computer has bits and each bit [is either] zero or one. A quantum computer has quantum bits. These are made out of quantum particles that can be zero, one, or some kind of state in between – [in other words they can have both values] at the same time.

So a quantum bit is made from a physical particle?

It pretty much could be any fundamental particle, so it could be a photon or an electron or it could be a nucleus, for example. It's a particle that can have two different properties [at once]. [For example], the particle can be in both one place and the other place at the same time.

How does this help with computing?

In a normal computer, a particular calculation might go through all the different possibilities of zeros and ones for a particular calculation. Because a quantum computer can be in all the states at the same time, you just do one calculation [testing a vast number of possibilities simultaneously]. So it can be much quicker.

What's the biggest challenge?

You need a very good control over individual particles. You can't just shove [all the particles] together because they would interact with each other [in an unpredictable way]. You need to be able to trap and direct them, but when the particles interact [with the trap itself] it makes them lose their information, so you need to make sure that you design the trap well.

What are the applications?

The biggest and most important one is the ability to factorise a very large number into two prime numbers. That's really important because that's what almost all encryption for internet computing is based on. A quantum computer should be able to do that relatively quickly to get back the prime numbers and that will mean that basically anything that has been with [that] encryption can be de-encrypted. If you were to do it with the classical computers we have now, it would take longer than the age of the universe to go back.

Are there other scientific uses?

Calculating the positions of individual atoms in very large molecules like polymers and in viruses. The way that the particles interact with each other – there's so many different possibilities that normally they say that you can't calculate anything properly [with] more than about 10 atoms inside the molecule. So if you have a quantum computer you could use it to develop drugs and understand how molecules work a bit better.

Are there commercial quantum computers?

There is a commercial computer out there but it's very expensive ($10m), it has very limited computing power and it hasn't yet been verified by anybody externally [as to] what it's actually doing.

Will quantum computers look like our desktops and laptops do now?

We are completely re-designing the computer. The very first quantum computers will probably fill a room. It's going to take us a while to get to desktops. Really, actually what is going to happen [is] you are going to have a hybrid laptop with a quantum chip and a classical chip.