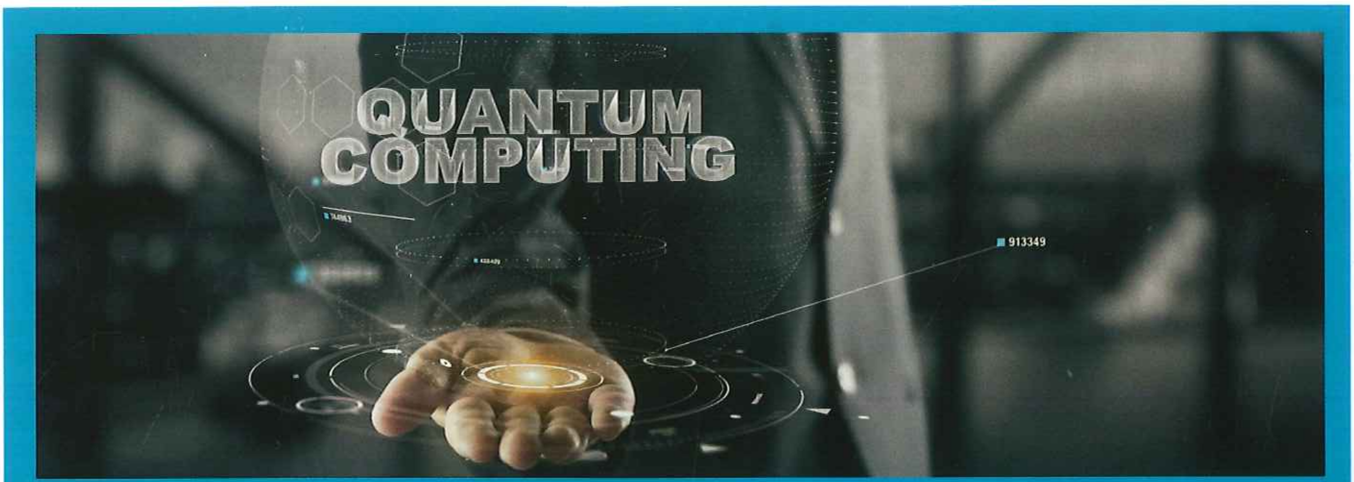
Quantum computing

By Vanessa Clark



Quantum computing – this is what's going to ruin the blockchain and crypto-everything for all of us, right?

Well, certainly in its current form, cryptography will become wafer-thin protection when quantum computing becomes a reality, but no one is committing to when that is yet. A recent milestone in the race to quantum supremacy, or a theoretical tipping point where quantum computing overtakes traditional computing, was Google's release of Bristlecone, a 72-quantum bit (qubit) computing chip. But it's unlikely you're going to be picking up a quantum computer from Incredible Connection anytime soon. IBM's 50-qubit quantum computer is only stable for 90 microseconds at a time, and D-Wave's quantum computers run at -273°C, in a vacuum 10 billion times lower than atmospheric pressure. So, not available as a laptop just yet.

So what exactly is quantum computing? It sounds a bit science fiction-y.

It is brain-breaking stuff. For an explanation, we need to go back to high school physics, where we were taught that light acts like both a wave and a particle. Or, if you want to get philosophical, until we open the box, Schrödinger's hypothetical cat is both alive and dead. Basically, quantum taps into the phenomenon that atomic and sub-atomic particles act differently to bigger objects. They literally don't obey the laws of (traditional) physics.

Okay, but what has this got to do with computing?

You know how traditional computing systems are built on bits that are either ones or zeroes? With quantum computing, it's no longer a binary situation. Thanks to weird science called superposition and entanglement, qubits – quantum's version of bits – can exist in more than one version of a state simultaneously, and they can impact each other even though they are not connected. In fact, every pair of qubits can exist in four states, a trio can exist in eight states and so on. This means that quantum computing is potentially faster than traditional computing, can do things that were previously impossible, can store more information and will use way less power.

Ah, so this is where it becomes crypto's kryptonite?

Yep, the blockchain and other cryptography applications rely on the fact that traditional computing doesn't have the processing power to break codes quickly enough to be a threat to security. For quantum computing, and its ability to do things like find very large prime numbers very quickly, however, this is potentially not a problem.

Oops, what then?

A: Well, the jury is out, but presumably, as is typical with most big technology step changes, cryptography will advance in parallel. (Get your thinking caps on, crypto-wizards!)

What else will quantum computing be good for?

At the moment, commentators are getting most excited about its ability to model complicated chemical reactions, and what this means for the creation of new materials and medicines. Also, quantum computing can deal with vast volumes of unstructured data, which makes it a key to unlocking artificial intelligence.

It is worth bearing in mind that, despite the anticipation, quantum computing is not always going to be more useful or faster than its non-quantum counterpart, and that it is likely we will see a hybrid situation of quantum and traditional computing working together.

Another interesting quirk is that in the same way qubits aren't binary, the results of a quantum computer aren't definitive, but, instead, based on the most likely probability. When submitting a request, you can specify how many alternative solutions you want the system to return.

How do I get in on the action today?

Google, IBM and D-Wave offer access to their quantum processors via the cloud for programmers to tinker with quantum algorithms, with a range of qubit processors to choose from. It's worth pointing out that despite the drama of the race to quantum supremacy, lower qubit machines can actually be more helpful in some cases. More qubits mean increased complexity, which means more quantum weirdness and higher error rates. b