Quantum Computing: ‘Physicist’s Dream’ or ‘Engineer’s Nightmare’?

The technology has the potential to create a tectonic shift in computing.

Kevin McCaney
Fri, 03/23/2018 - 16:00

Illustration: Rost-9D/iStock

Word is going around that quantum computing is on the doorstep. In fact, it’s already ringing the bell, by some assessments.

IBM, which two years ago made a 5-qubit quantum machine available online and has since built a 50-qubit prototype chip, confidently proclaims quantum computing will be mainstream in five years. Google also says five years is the magic number for its first viable quantum computer. Ditto Microsoft, which claims it already has the best, most-stable qubits. Intel, which unveiled a 49-qubit quantum chip at CES in January, also is in the game, as are other companies and a number of startups,
like Rigetti Computing.

Government IT officials, along with the general public, might wonder what all this means for their own computing systems, how it could affect their plans, how does quantum computing work, and what the heck is a qubit.

The short answer: Quantum computing has the potential to create a tectonic shift in computing and has made impressive strides in the last couple of years, but it’s not quite ready for everyday use.

For one thing, when IBM says quantum will go “mainstream” in five years, it doesn’t mean people will have quantum smartphones or be applying qubits — which, by the way, is short for quantum bits — to their dating apps. It means quantum computing will escape hardcore research labs and get into the classroom, where a new generation will begin to work with quantum principles and lay the groundwork for future applications.

Universities around the world (and even a few high schools) will all have quantum programs, which will be a requirement for science and engineering programs, according to IBM’s forecast.

“No student will graduate without having been exposed to quantum-related education,” the company says. This will give rise to a new developer community and, in that 5-year time frame, “help initiate the dawn of the commercial quantum era - a formative period when quantum computing technology and its early use cases develop rapidly.”

**Corralling the Qubits**

Before getting from here to there, quantum computing still has a hurdle or two to clear.

At the heart of quantum computing is the qubit, which differs significantly from traditional computer bits. The computing method the world has always known consists of strings of 1s and 0s, with each bit being one or the other.

A qubit, however, exists in a twin state of yes and no, a quantum mechanical property called superposition in which something can exist in multiple states at one time. When qubits are linked, in a process called entanglement, the computing
power of a processor increases exponentially. This raises the possibility that, some day, a relatively tiny quantum processor could outperform several supercomputers, and use a lot less power in the process.

But qubits can be touchy. They’re sensitive to outside forces and can easily “decohere” from a quantum state back to a traditional computing state of being just a one or a zero. As qubits are added to a system, keeping them in coherence becomes more difficult. The solution so far has been to operate quantum machines at extremely cold temperatures near absolute zero. But even then, qubits can decohere quickly, producing errors that need to be compensated for. Quantum computing could produce results beyond the reach of traditional computing, there are also countless ways it can go wrong.

Nevertheless, the potential of quantum computing is well worth the trouble, researchers say.

“The thing driving the hype is the realization that quantum computing is actually real,” MIT professor Isaac Chuang told Technology Review. “It is no longer a physicist’s dream—it is an engineer’s nightmare.”

**Potential into Practice**

The 50-qubit threshold for a quantum chip is seen as a starting point for serious calculations in chemistry and other fields, though researchers say larger arrangements of hundreds or more will be necessary for truly groundbreaking work.

"You have to think what it will take to do useful quantum computing," Dr. Tom Watson of Delft University of Technology in the Netherlands, told BBC News. “The numbers are not very well defined, but it's probably going to take thousands, maybe millions, of qubits, so you need to build your qubits in a way that can scale up to these numbers."

Watson was a co-author of a recent paper published in Nature that proposes silicon as an option for building stable, scalable quantum processors.

For now, many of the ideas for the early uses for quantum computing involve research along the lines of modeling complex processes inside atoms. Another important application is cryptography, for both good and ill. While quantum computing could create a theoretically unbreakable encryption, researchers at the National Institute of Science and Technology
and elsewhere are concerned about quantum hacks of current encryption standards, which they say would be “catastrophic.”

Meanwhile, a new generation of quantum-trained students can get to work on quantum’s killer app for more widespread use. The next five years are going to be interesting.