Hype and cash are muddying public understanding of quantum computing

August 23 2017, by Michael J. Biercuk

An ion trap used for quantum computing research in the Quantum Control Laboratory at the University of Sydney. Michael Biercuk, Author provided Special piping and wiring supports quantum research in the Sydney Nanoscience Hub. Credit: AINST, Author provided

It's no surprise that quantum computing has become a media obsession.

A functional and useful quantum computer would represent one of the century's most profound technical achievements.

For researchers like me, the excitement is welcome, but some claims appearing in popular outlets can be baffling.

A recent infusion of cash and attention from the tech giants has woken the interest of analysts, who are now eager to proclaim a breakthrough moment in the development of this extraordinary technology.

Quantum computing is described as "just around the corner", simply awaiting the engineering prowess and entrepreneurial spirit of the tech sector to realise its full potential.

What's the truth? Are we really just a few years away from having quantum computers that can break all online security systems? Now that the technology giants are engaged, do we sit back and wait for them to deliver? Is it now all "just engineering"?

Why do we care so much about quantum computing?

Quantum computers are machines that use the rules of quantum physics – in other words, the physics of very small things – to encode and process information in new ways.

They exploit the unusual physics we find on these tiny scales, physics that defies our daily experience, in order to solve problems that are exceptionally challenging for "classical" computers. Don't just think of quantum computers as faster versions of today's computers – think of them as computers that function in a totally new way. The two are as different as an abacus and a PC.

They can (in principle) solve hard, high-impact questions in fields such as codebreaking, search, chemistry and physics.

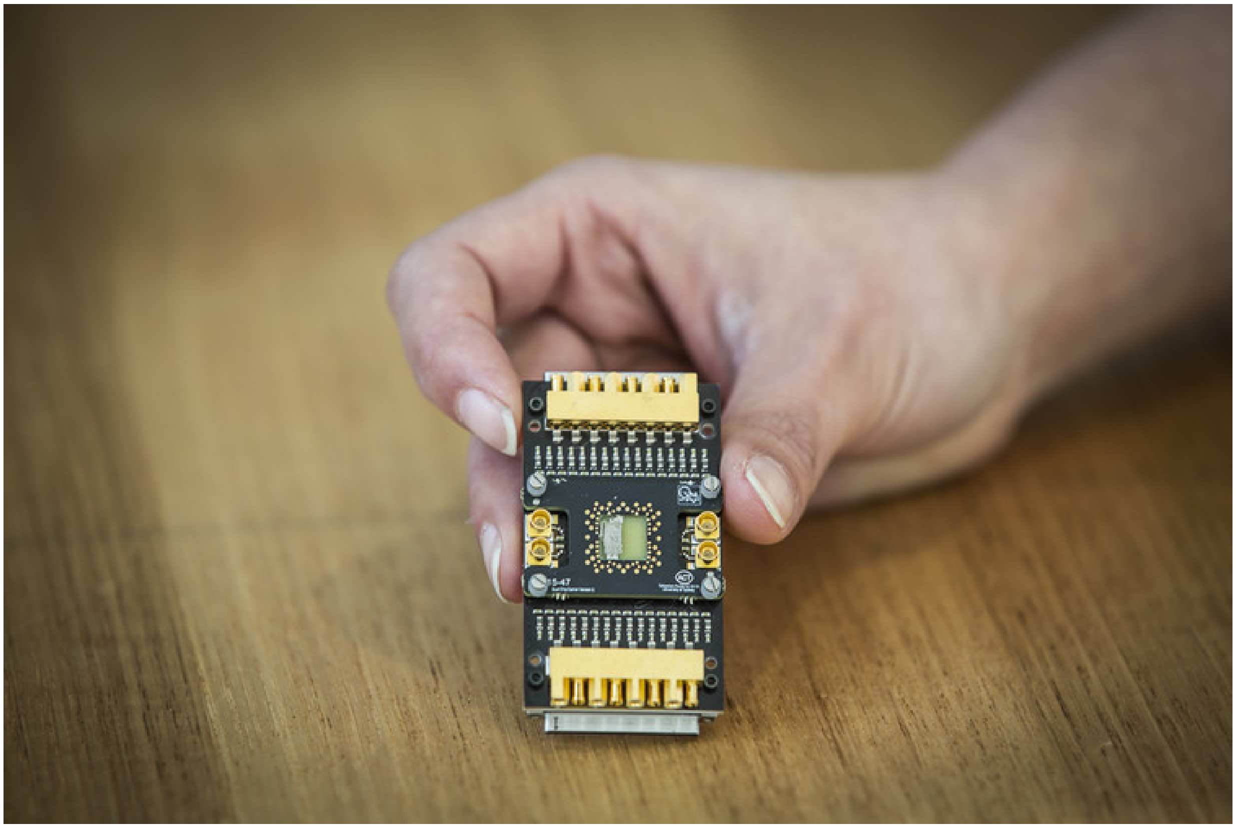
Chief among these is "factoring": finding the two prime numbers, divisible only by one and themselves, which when multiplied together reach a target number. For instance, the prime factors of 15 are 3 and 5.

As simple as it looks, when the number to be factored becomes large, say 1,000 digits long, the problem is effectively impossible for a classical computer. The fact that this problem is so hard for any conventional computer is how we secure most internet communications, such as through public-key encryption.

Some quantum computers are known to perform factoring exponentially faster than any classical supercomputer. But competing with a supercomputer will still require a pretty sizeable quantum computer.

Money changes everything

Quantum computing began as a unique discipline in the late 1990s when the US government, aware of the newly discovered potential of these machines for codebreaking, began investing in university research



A semiconductor qubit device mounted on a custom cryogenic printed circuit board. Credit: Jayne Ion/University of Sydney, Author provided

The field drew together teams from all over the world, including Australia, where we now have two Centres of Excellence in quantum technology (the author is part of of the Centre of Excellence for Engineered Quantum Systems).

But the academic focus is now shifting, in part, to industry.

IBM has long had a basic research program in the field. It was recently joined by Google, who invested in a University of California team, and Microsoft, which has partnered with academics globally, including the University of Sydney.

Seemingly smelling blood in the water, Silicon Valley venture capitalists also recently began investing in new startups working to build quantum computers.

The media has mistakenly seen the entry of commercial players as the genesis of recent technological acceleration, rather than a *response* to these advances.

So now we find a variety of competing claims about the state of the art in the field, where the field is going, and who will get to the end goal – a large-scale quantum computer – first.

The state of the art in the strangest of technologies

Conventional computer microprocessors can have more than one billion fundamental logic elements, known as transistors. In quantum systems, the fundamental quantum logic units are known as qubits, and for now, they mostly number in the range of a dozen.

Such devices are exceptionally exciting to researchers and represent huge progress, but they are little more than toys from a practical perspective. They are not near what's required for factoring or any other application – they're too small and suffer too many errors, despite what the frantic headlines may promise.

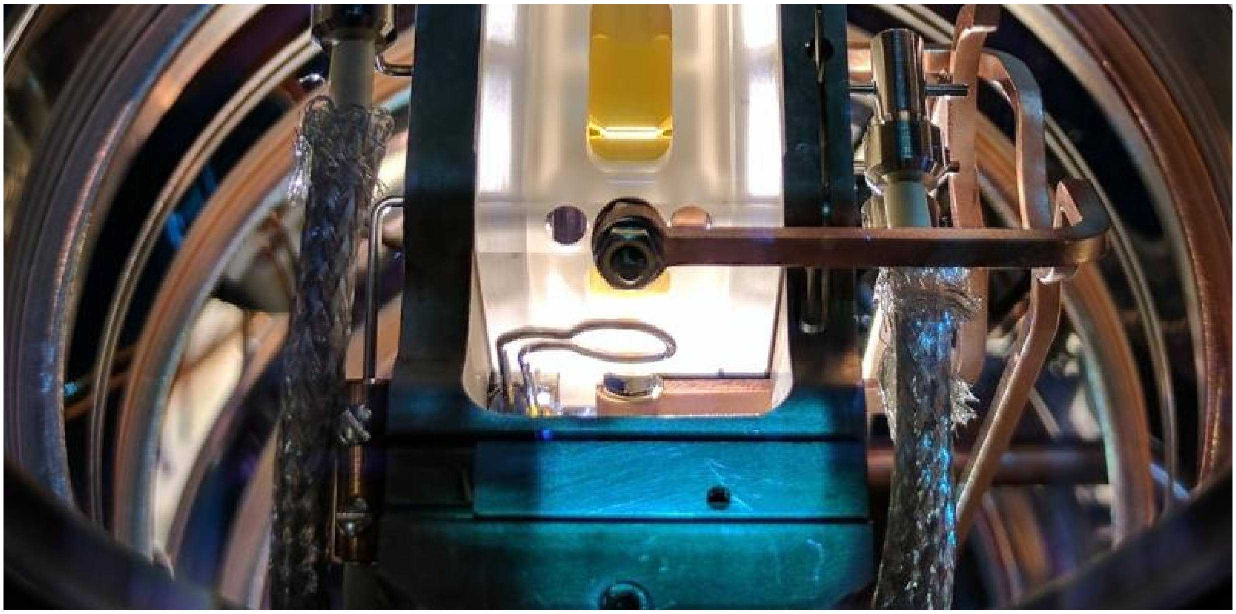
For instance, it's not even easy to answer the question of which system has the best qubits right now.

Consider the two dominant technologies. Teams using trapped ions have qubits that are resistant to errors, but relatively slow. Teams using superconducting qubits (including IBM and Google) have relatively error-prone qubits that are much faster, and may be easier to replicate in the near term.

Which is better? There's no straightforward answer. A quantum computer with many qubits that suffer from lots of errors is not necessarily more useful than a very small machine with very stable qubits.

Because quantum computers can also take different forms (general purpose versus tailored to one application), we can't even reach agreement on which system currently has the greatest set of capabilities.

Similarly, there's now seemingly endless competition over simplified metrics such as the number of qubits. Five, 16, soon 49! The question of whether a quantum computer is useful is defined by much more than this.



An ion trap used for quantum computing research in the Quantum Control Laboratory at the University of Sydney. Credit: Michael Biercuk, Author provided

Where to from here?

There's been a media focus lately on achieving "quantum supremacy". This is the point where a quantum computer outperforms its best classical counterpart, and reaching this would absolutely mark an important conceptual advance in quantum computing.

But don't confuse "quantum supremacy" with "utility".

Some quantum computer researchers are seeking to devise slightly arcane problems that might allow quantum supremacy to be reached with, say, 50-100 qubits – numbers reachable within the next several years.

Achieving quantum supremacy does not mean either that those machines will be useful, or that the path to large-scale machines will become clear.

Moreover, we still need to figure out how to deal with errors. Classical computers rarely suffer hardware faults – the "blue screen of death" generally comes from software bugs, rather than hardware failures. The likelihood of hardware failure is usually less than something like one in a billion-quadrillion, or 10^{-24} in scientific notation.

The best quantum computer hardware, on the other hand, typically achieves only about one in 10,000, or $10^{-4.}$ That's 20 *orders of magnitude* worse.

Is it all just engineering?

We're seeing a slow creep up in the number of qubits in the most advanced systems, and clever scientists are thinking about problems that might be usefully addressed with small quantum computers containing just a few hundred qubits.

But we still face many fundamental questions about how to build, operate or even validate the performance of the large-scale systems we sometimes hear are just around the corner.

As an example, if we built a fully "error-corrected" quantum computer at the scale of the millions of qubits required for useful factoring, as far as we can tell, it would represent a totally new state of matter. That's pretty fundamental.

At this stage, there's no clear path to the millions of error-corrected qubits we believe are required to build a useful factoring machine. Current global efforts (in which this author is a participant) are seeking to build just one error-corrected qubit to be delivered about five years from now.

At the end of the day, none of the teams mentioned above are likely to build a useful quantum computer in 2017 … or 2018. But that shouldn't cause concern when there are so many exciting questions to answer along the way.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Hype and cash are muddying public understanding of quantum computing (2017, August 23) retrieved 20 March 2024 from https://phys.org/news/2017-08-hype-cash-muddying-quantum.html