OPINION

Quantum computing has a hype problem

Quantum computing startups are all the rage, but it's unclear if they'll be able to produce anything of use in the near future.

By Sankar Das Sarma

March 28, 2022

MS TECH | GETTY

10:42 / 10:42

Listen to this article

Listen later, on the Noa app.

As a buzzword, quantum computing probably ranks only below AI in terms of hype. Large tech companies such as Alphabet, Amazon, and Microsoft now have substantial research and development efforts in quantum computing. A host of startups have sprung up as well, some boasting staggering valuations. IonQ, for example, was valued at $2 billion when it

MIT Technology Review Subscribe

I am as pro-quantum-computing as one can be: I've published more than 100 technical papers on the subject, and many of my PhD students and postdoctoral fellows are now well-

known quantum computing practitioners all over the world. But I'm disturbed by some of the quantum computing hype I see these days, particularly when it comes to claims about how it will be commercialized.

Established applications for quantum computers do exist. The best known is Peter Shor's 1994 theoretical demonstration that a quantum computer can solve the hard problem of finding the prime factors of large numbers exponentially faster than all classical schemes. Prime factorization is at the heart of breaking the universally used RSA-based cryptography, so Shor's factorization scheme immediately attracted the attention of national governments everywhere, leading to considerable quantum-computing research funding.

The only problem? Actually making a quantum computer that could do it. That depends on implementing an idea pioneered by Shor and others called quantum-error correction, a process to compensate for the fact that quantum states disappear quickly because of environmental noise (a phenomenon called "decoherence"). In 1994, scientists thought that such error correction would be easy because physics allows it. But in practice, it is extremely difficult.

The most advanced quantum computers today have dozens of decohering (or "noisy") physical qubits. Building a quantum computer that could crack RSA codes out of such components would require many millions if not billions of qubits. Only tens of thousands of these would be used for computation—so-called logical qubits; the rest would be needed for error correction, compensating for decoherence.

Related Story

This new startup has built a record-breaking 256-qubit quantum computer

approach to tackle impossibly hard computational tasks.

The qubit systems we have today are a tremendous scientific achievement, but they take us no closer to having a quantum computer that can solve a problem that anybody cares about. It is akin to trying to make today's best smartphones using vacuum tubes from the early

to work together in a coherent, seamless manner, you could achieve all kinds of miracles. What, however, is

missing is the breakthrough of integrated circuits and CPUs leading to smartphones—it took 60 years of very difficult engineering to go from the invention of transistors to the smartphone with no new physics involved in the process.

There are in fact ideas, and I played some role in developing the theories for these ideas, for bypassing quantum error correction by using far-more-stable qubits, in an approach called topological quantum computing. Microsoft is working on this approach. But it turns out that developing topological quantum-computing hardware is also a huge challenge. It is unclear whether extensive quantum error correction or topological quantum computing (or something else, like a hybrid between the two) will be the eventual winner.

Physicists are smart as we all know (disclosure: I am a physicist), and some physicists are also very good at coming up with substantive-sounding acronyms that stick. The great difficulty in getting rid of decoherence has led to the impressive acronym NISQ for "noisy intermediate scale quantum" computer—for the idea that small collections of noisy physical qubits could do something useful and better than a classical computer can. I am not sure what this object is: How noisy? How many qubits? Why is this a computer? What worthy problems can such a NISQ machine solve?

A recent laboratory experiment at Google has observed some predicted aspects of quantum dynamics (dubbed "time crystals") using 20 noisy superconducting qubits. The experiment was an impressive showcase of electronic control techniques, but it showed no computing advantage over conventional computers, which can readily simulate time crystals with a similar number of virtual qubits. It also did not reveal anything about the fundamental physics of time crystals. Other NISQ triumphs are recent experiments simulating random quantum circuits, again a highly specialized task of no commercial value whatsoever.

Using NISQ is surely an excellent new fundamental research idea—it could help physics research in fundamental areas such as quantum dynamics. But despite a constant drumbeat of NISQ hype coming from various quantum computing startups, the commercialization potential is far from clear. I have seen vague claims about how NISQ could be used for fast optimization or even for AI training. I am no expert in optimization or AI, but I have asked the experts, and they are equally mystified. I have asked researchers involved in various startups how NISQ would optimize any hard task involving real-world applications, and I interpret their convoluted answers as basically saying that since we do not quite understand how classical machine learning and AI really work, it is possible that NISQ could do this even faster. Maybe, but this is hoping for the best, not technology.

There are proposals to use small-scale quantum computers for drug design, as a way to quickly calculate molecular structure, which is a baffling application given that quantum chemistry is a minuscule part of the whole process. Equally perplexing are claims that near-

significant optimization in algorithmic trading or risk evaluation or arbitrage or hedging or

targeting and prediction or asset trading or risk profiling. This however has not prevented several investment banks from jumping on the quantum-computing bandwagon.

A real quantum computer will have applications unimaginable today, just as when the first transistor was made in 1947, nobody could foresee how it would ultimately lead to smartphones and laptops. I am all for hope and am a big believer in quantum computing as a potentially disruptive technology, but to claim that it would start producing millions of dollars of profit for real companies selling services or products in the near future is very perplexing to me. How?

Quantum computing is indeed one of the most important developments not only in physics, but in all of science. But "entanglement" and "superposition" are not magic wands that we can shake and expect to transform technology in the near future. Quantum mechanics is indeed weird and counterintuitive, but that by itself does not guarantee revenue and profit.

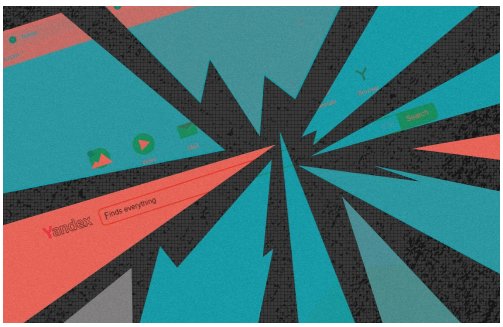
A decade and more ago, I was often asked when I thought a real quantum computer would be built. (It is interesting that I no longer face this question as quantum-computing hype has apparently convinced people that these systems already exist or are just around the corner). My unequivocal answer was always that I do not know. Predicting the future of technology is impossible—it happens when it happens. One might try to draw an analogy with the past. It took the aviation industry more than 60 years to go from the Wright brothers to jumbo jets carrying hundreds of passengers thousands of miles. The immediate question is where quantum computing development, as it stands today, should be placed on that timeline. Is it with the Wright brothers in 1903? The first jet planes around 1940? Or maybe we're still way back in the early 16th century, with Leonardo da Vinci's flying machine? I do not know. Neither does anybody else.

Sankar Das Sarma is the director of the Condensed Matter Theory Center at the University of Maryland, College Park.

by Sankar Das Sarma

DEEP DIVE

COMPUTING



Russia is risking the creation of a “splinternet”—and it could be irreversible

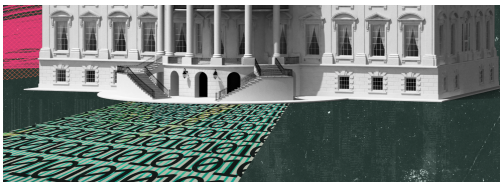
If Russia disconnects from—or is booted from— the internet’s governing bodies, the internet may never be the same again for any of us.

By James Ball

These hackers showed just how easy it is to target critical infrastructure

Two Dutch researchers have won a major hacking championship by hitting the software that runs the world’s power grids, gas pipelines, and more. It was their easiest challenge yet.

By Patrick Howell O'Neill



Inside the plan to fix America's never-ending cybersecurity failures

The specter of Russian hackers and an overreliance on voluntary cooperation from the private sector means officials are finally prepared to get tough.

By Patrick Howell O'Neill

The end of passwords

Companies are finally shifting away from notoriously insecure alphanumerics to other methods of authentication.

By Mat Honan

STAY CONNECTED

Illustration by Rose Wong

Cover Art by Michael Byers

Back to top ↑