Moshe Y. Vardi

DOI:10.1145/3322092

Quantum Hype and Quantum Skepticism

THE FIRST THIRD of the 20th century saw the collapse of many absolutes. Albert Einstein's 1905 special relativity theory eliminated the notion of absolute time, while Kurt Gödel's 1931 incompleteness theorem questioned the notion of absolute mathematical truth. Most profoundly, however, quantum mechanics raised doubts on the notion of absolute objective reality. Is Schrödinger's cat dead or alive? Nearly 100 years after quantum mechanics was introduced, scientists still are not in full agreement on what it means.

The problem with objective reality stems from the *superposition principle*. In a nutshell, quantum systems can exist in a superposition of their possible observable states before measurement. While a classical bit has a unique value, 0 or 1, a quantum bit, or *qubit*, exists as a superposition of two classical bits. The physicist Richard Feynman hinted at the possibility of using quantum effects for computation in his 1959 lecture, "There's Plenty of Room at the Bottom." But this possibility seemed somewhat remote, until Peter Shor's seminal 1994 paper, where he showed it is theoretically possible to use quantum computation to factor numbers in polynomial time, which would break current public-key cryptographic schemes. This made the realization of quantum computing one of the holy grails of computing in the 21st century. In fact, quantum computing is an important part of one of the U.S. National Science Foundation's "Ten Big Ideas."

The popular media regularly reports breathlessly on quantum computing: "Quantum computing will break your encryption in a few years"; "Why quantum's computing time is now"; and "The computer that could rule the world." Yet the physical realization of quantum comput-

ing has been a hard slog. A Canadian company, D-Wave Systems, has claimed to be the world's first company to sell computers that exploit quantum effects in their operation. But the D-Wave machine is far from being a general quantum computer, and several researchers disagree with D-Wave's claims.

In fact, several quantum-computing researchers have expressed skepticism regarding the physical realizability of the quantum-computing dream.^a Quantum skeptics agree that quantum computation does offer an exponential advantage of classical computation in theory, but they argue it is not physically possible to build scalable quantum computers. Gil Kalai is one of the most prominent quantum skeptics. All physical systems are noisy, he argues,^b and qubits kept in highly sensitive superpositions will inevitably be corrupted by any interaction with the outside world. In contrast, quantum-skepticism skeptics, such as Scott Aaronson, view the realizability of quantum computing as an outstanding question in physics,^c and regard the skeptical view as representing an implausible revolution in physics.

A recent U.S. National Academies report^d reviewed current progress and prospects of quantum computing, taking a sober view of the field. Given the current state of quantum computing and the significant challenges that still must be overcome, the report argues it is highly unlikely a quantum computer that can compromise public-key cryptography—a basis for the security of most of today's computers and networks—will be built within the next decade. Yet, because re-

placing an established Internet protocol generally takes over a decade, work to develop and deploy algorithms that are resilient against an attack by a quantum computer is critical now, the report advised.

The report identified major challenges that lie ahead for quantum computing. Agreeing somewhat with Kalai, the report stated the need to correct the errors in a quantum system, without which it is unlikely that a highly complex quantum program would ever run correctly on the system. Error-correcting algorithms incur significant costs, so in the near term quantum computers are likely to be error-prone, the report concluded.

An important part of the report is an analysis of why and how computing technology scaled exponentially in performance for over half a century. This scaling was mostly the result of a virtuous cycle, where products using the new technology allowed the industry to make more money, which it then used to create newer technology. For quantum computing to be similarly successful, it must create a virtuous cycle to fund the development of increasingly useful quantum computers. But the beauty of classical computing is that developing algorithms is incredibly easy. Every teenager writing a program is developing an algorithm. In contrast, in more than 25 years of intense research on quantum computing, only a few dozen algorithms have been developed.^e It is conceivable that governments will pour major investments into a small number of critical quantum-computing applications, but this will not give rise to the thriving marketplace that is needed to sustain the virtuous cycle. Count me a quantum skeptic! **C**

^e <https://bit.ly/2uq1r0f>

See p. 15 for more on the quantum argument.

Moshe Y. Vardi (vardi@cs.rice.edu) is the Karen Ostrum George Distinguished Service Professor in Computational Engineering and Director of the Ken Kennedy Institute for Information Technology at Rice University, Houston, TX, USA. He is the former Editor-in-Chief of *Communications*.

Copyright held by author.

^a <https://bit.ly/2Bie8i3>

^b <https://bit.ly/2nQ44Vy>

^c <https://bit.ly/2U4Qz6x>

^d <https://bit.ly/2QkA45i>