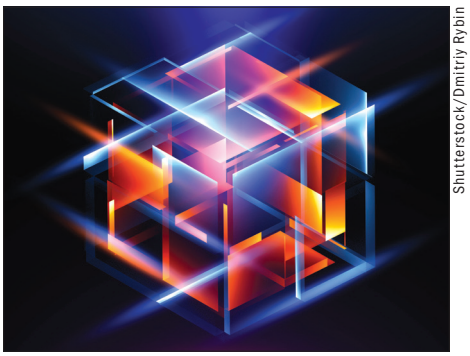
Delivering on a quantum promise

With the European Commission investing €1bn over 10 years in quantum technologies, **Karl Svozil** warns against overselling many of the initiative's longer-term goals



Shutterstock/Dmitriy Rybin

Quantum questions Are the applications of quantum physics as viable as we are led to believe?

Unlike modern-day politicians, scientists have great authority regarding the pursuit of truth. As a consequence, many members of the public – as well as political bodies and institutions – tend to uncritically take science as a matter of fact. Yet there are some occasions where the benefits and risks of science need to be communicated carefully. A striking example is nuclear energy and the bold claims made by some that nuclear-fission technology is "safe beyond doubt". One only has to look at the nuclear power plants at Three Mile Island, Chernobyl and Fukushima to know that such claims can prove spurious.

In a similar fashion, I believe that the alleged applications of quantum physics are, in some cases, being oversold to the public. The "quantum mechanics is magic" tour – expressed through European physicists' "quantum manifesto" – has resulted in the European Commission launching a €1bn quantum-technologies flagship initiative in quantum technology. The campaign promises to deliver nothing less than a "second quantum revolution" (see June 2016 p8).

Feasibility of goals

To me, the initiative, along with other framework and flagship programmes, resembles Soviet-style five-year plans – a bureaucrat's delight. I have no doubt that €1bn spent on quantum physics is being wisely invested and that something worthy will come out of it. What worries me is the deceptive and potentially harmful way that this and similar quantum-related initiatives are promoted. While many of the quantum manifesto's short- and medium-term goals appear feasible, some of the long-term goals might not be achievable even in principle. And when it comes to quantum random-number generators and quantum cryptography, certain goals are impossible, as I outlined recently in *Ethics in Science and Environmental Politics* (**16** 25).

Take, for example, the manifesto's call to "build a universal quantum computer able to demonstrate the resolution of a problem that, with current techniques on a supercomputer, would take longer than the age of the universe". I am at a loss to imagine what that could be, given the rather sober situation regarding the capacity of quantum computers. Although the Quantum Algorithmic Zoo – a catalogue of quantum algorithms compiled by the US National Institute of Standards and Technology – showcases a growing number of potential speed-ups by utilizing quantum computers, no substantial "killer apps" have been suggested in the last few years. Indeed, there is not even a consensus about what exactly could make quantum computation better than classical computation.

> Should "fairy tales" be marketed to the public and politicians?

Most physicists seem to agree that one advantage might be "quantum parallelism". This is based on coherently superposing classically distinct and mutually exclusive computational states and pushing all of them through a quantum computer simultaneously. It seems, however, that this strategy is applicable only in particular instances. It is also unclear if quantum computation is scalable so that an increase in quantum bits would need no excessive – possibly exponential – overhead in resources to create and maintain the additional bits. Another genuine quantum application is the use of quantum entanglement for communication. While exponential speed-ups have been proposed, there is again no common understanding of the issues involved.

Regarding quantum random-number generators, the situation is confused, to say the least. Indeed, it is not even clear where exactly quantum randomness resides. It cannot originate from elements such as lossless beam splitters because these are merely "permuting" the quantum state. If measurements were the source of randomness, then any such randomness would be tied to the notorious quantum-measurement problem – how or whether wave-function collapse occurs. Moreover, because of "incompleteness theorems", any statements regarding the indeterminism, let alone randomness, of empirical bit sequences are unprovable. Thus regardless of what we may be inclined to believe, and whatever authoritative certificates are issued, such claims remain metaphysical and conjectural.

Security considerations

Finally, contrary to publicized claims, quantum cryptography is insecure and can be successfully cryptanalysed through man-in-the-middle attacks. As a consequence, to be safe, such quantum-cryptographic protocols require both an uncompromised classical as well as quantum communication channel. With these provisos, one may ask: what exactly is the advantage and what is the "added security"? Is quantum cryptography presenting itself as the solution to a problem while at the same time requiring the absence of the threat it purports to resolve? If you push the experts with such questions, they respond that, rather than generating a key out of the blue, within certain error bounds, they could "enlarge" an existing key. This is the type of confidence that is implied by "unconditional security" in many of these papers.

As the quantum fairy is about to deliver €1bn, the question is whether we should allow such "fairy tales" to be marketed to the public and politicians. Should those conveying the most sentimental and overstated promises prevail? Maybe this is unavoidable, but it is not without consequences. One might also ask why we are not funding other initiatives to provide solutions to the upcoming energy crisis, as well as alleviate our dependencies on crude oil. One option is thermonuclear fusion – a yet-utopian "solar" energy source – that might be sustainable at moderate operating costs and perils. This will require much higher "whatever it takes" investment, but while much has been done already, much more is needed.

Karl Svozil is at the Institute for Theoretical Physics at Vienna University of Technology, e-mail svozil@tuwien.ac.at