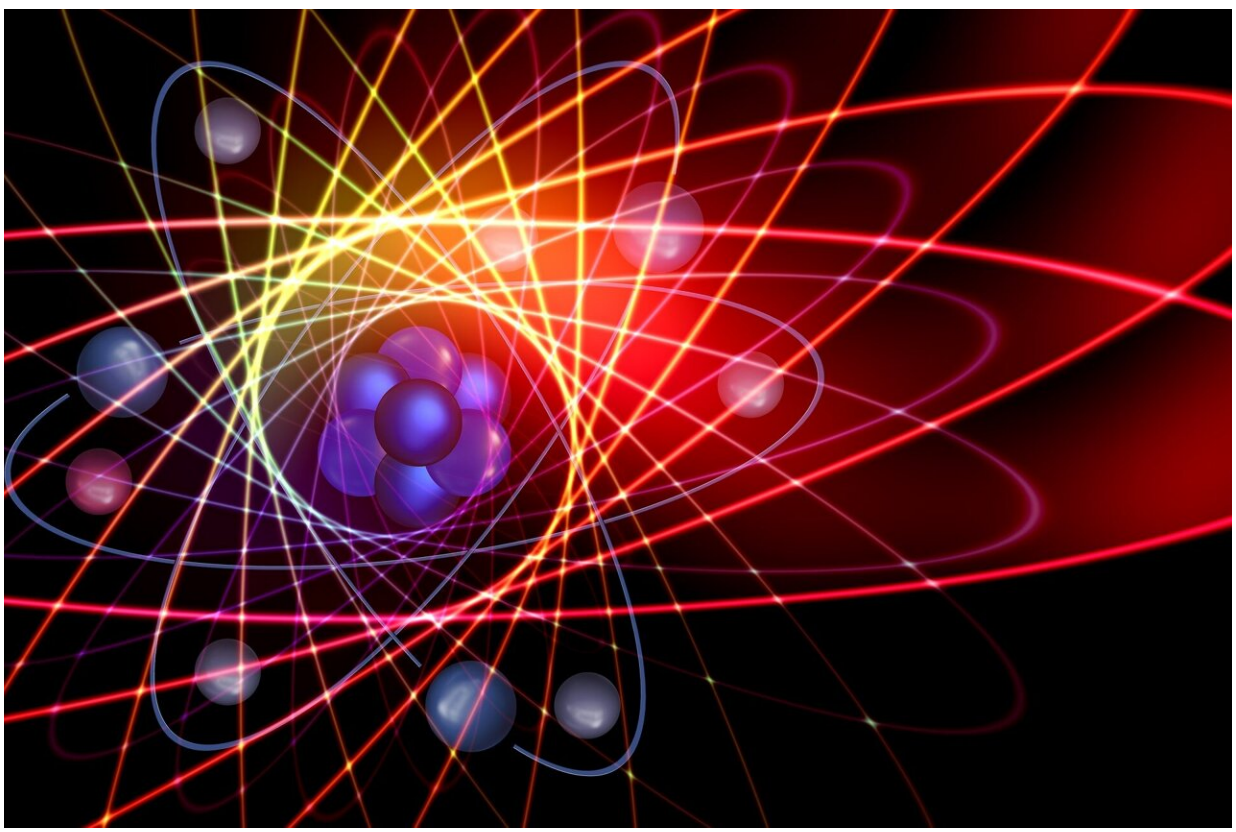
How long before quantum computers can benefit society? That's Google's US$5 million question

March 27 2024, by Adam Lowe



Credit: Pixabay/CC0 Public Domain

Google and the XPrize Foundation have launched a competition worth US$5 million (£4 million) to develop real-world applications for quantum computers that benefit society—by speeding up progress on one of the UN Sustainable Development Goals, for example. The principles of quantum physics suggest quantum computers could perform very fast calculations on particular problems, so this competition may expand the range of applications where they have an advantage over conventional computers.

In our everyday lives, the way nature works can generally be described by what we call classical physics. But nature behaves very differently at tiny quantum scales—below the size of an atom.

The race to harness quantum technology can be viewed as a new industrial revolution, progressing from devices that use the properties of classical physics to those utilizing the weird and wonderful properties of quantum mechanics. Scientists have spent decades trying to develop new technologies by harnessing these properties.

Given how often we are told that quantum technologies will revolutionize our everyday lives, you may be surprised that we still have to search for practical applications by offering a prize.

However, while there are numerous examples of success using quantum properties for enhanced precision in sensing and timing, there has been a surprising lack of progress in the development of quantum computers that outdo their classical predecessors.

The main bottleneck holding up this development is that the software—using quantum algorithms— needs to demonstrate an advantage over computers based on classical physics. This is commonly known as "quantum advantage".

A crucial way quantum computing differs from classical computing is in using a property known as "entanglement". Classical computing uses "bits" to represent information. These bits consist of ones and zeros, and everything a computer does comprises strings of these ones and zeros. But quantum computing allows these bits to be in a "superposition" of ones and zeros. In other words, it is as if these ones and zeros occur simultaneously in the quantum bit, or qubit.

It is this property which allows computational tasks to be performed all at once. Hence the belief that quantum computing can offer a significant advantage over classical computing, as it is able to perform many computing tasks at the same time.

Notable quantum algorithms

While performing many tasks simultaneously should lead to a performance increase over classical computers, putting this into practice has proven more difficult than theory would suggest. There are actually only a few notable quantum algorithms which can perform their tasks better than those using classical physics.

The most notable are the BB84 protocol, developed in 1984, and Shor's algorithm, developed in 1994, both of which use entanglement to outperform classical algorithms on particular tasks.

The BB84 protocol is a cryptographic protocol—a system for ensuring secure, private communication between two or more parties which is considered more secure than comparable classical algorithms.

Shor's algorithm uses entanglement to demonstrate how current classical encryption protocols can be broken, because they are based on the factorisation of very large numbers. There is also evidence that it can perform certain calculations faster than similar algorithms designed for conventional computers.

Despite the superiority of these two algorithms over conventional ones, few advantageous quantum algorithms have followed. However, researchers have not given up trying to develop them. Currently, there are a couple of main directions in research.

Potential quantum benefits

The first is to use quantum mechanics to assist in what are called large-scale optimization tasks. Optimization—finding the best or most effective way to solve a particular task—is vital in everyday life, from ensuring traffic flow runs effectively, to managing operational procedures in factory pipelines, to streaming services deciding what to recommend to each user. It seems clear that quantum computers could help with these problems.

If we could reduce the computational time required to perform the optimization, it could save energy, reducing the carbon footprint of the many computers currently performing these tasks around the world and the data centers supporting them.

Another development that could offer wide-reaching benefits is to use quantum computation to simulate systems, such as combinations of atoms, that behave according to quantum mechanics. Understanding and predicting how quantum systems work in practice could, for example, lead to better drug design and medical treatments.

Quantum systems could also lead to improved electronic devices. As computer chips get smaller, quantum effects take hold, potentially reducing the devices's performance. A better fundamental understanding of quantum mechanics could help avoid this.

While there has been significant investment in building quantum computers, there has been less focus on ensuring they will directly benefit the public. However, that now appears to be changing.

Whether we will all have quantum computers in our homes within the next 20 years remains doubtful. But, given the current financial commitment to making quantum computation a practical reality, it seems that society is finally in a better position to make use of them. What precise form will this take? There's US$5 million dollars on the line to find out.

Provided by The Conversation

Citation: How long before quantum computers can benefit society? That's Google's US$5 million question (2024, March 27) retrieved 27 April 2024 from https://techxplore.com/news/2024-03-quantum-benefit-society-google-us5.html