DOI: 10.24425/academiaPAS.2024.150226

The Quest for Qubits

Prof. Artur Ekert is a Polish-British theoretical physicist, a graduate of the Jagiellonian University and Oxford University. He is a Professor of quantum physics at the Mathematical Institute of Oxford University, and the Lee Kong Chian Centennial Professor at the National University of Singapore. His research interests focus on information processing in quantum-mechanical systems, especially in the areas of cryptography and quantum computing. He is a Fellow of the Royal Society and he has received numerous distinctions and awards, including the IOP Maxwell Medal, the Royal Society Huygens Medal, the EU Descartes Prize, and the Milner Award.

artur.ekert@maths.ox.ac.uk

Quantum computers excel at tasks where classical computers falter – explains **Prof. Artur Ekert** from the Mathematical Institute at Oxford University and the National University of Singapore.

Just a few years ago, the race among top research centers was still focused on creating the fastest conventional supercomputer. Nowadays, a lot of the talk is about quantum computers. Is this emphasis on quantum physics really warranted, or is it predominantly just a PR strategy?

ARTUR EKERT: Classical supercomputers and quantum computers are fundamentally different things. The classical theory of computation does not usually refer to physics. Pioneers, such as Alan Turing, managed to capture the correct classical theory by intuition alone and, as a result, it is often falsely assumed that its foundations are self-evident and purely abstract. They are not! The concepts of information and computation can be properly formulated only in the context of a physical theory — information is stored, transmitted and processed always by physical means. There is no computation that isn't a physical process.

Has our better understanding of the laws of nature that govern the micro-world of quantum mechanics now changed anything?

The discovery of new phenomena in physics naturally opens up new possibilities for processing information. Until the early twenty century, classical physics underpinned the computational machines that were developed. Charles Babbage's computer and subsequent electromechanical computing machines were based on classical physics. But with the advent of quantum mechanics, new inherently quantum phenomena were discovered. These newly mastered phenomena can now be utilized to process information in new, unconventional ways.

So, has a bit ceased to be a bit?

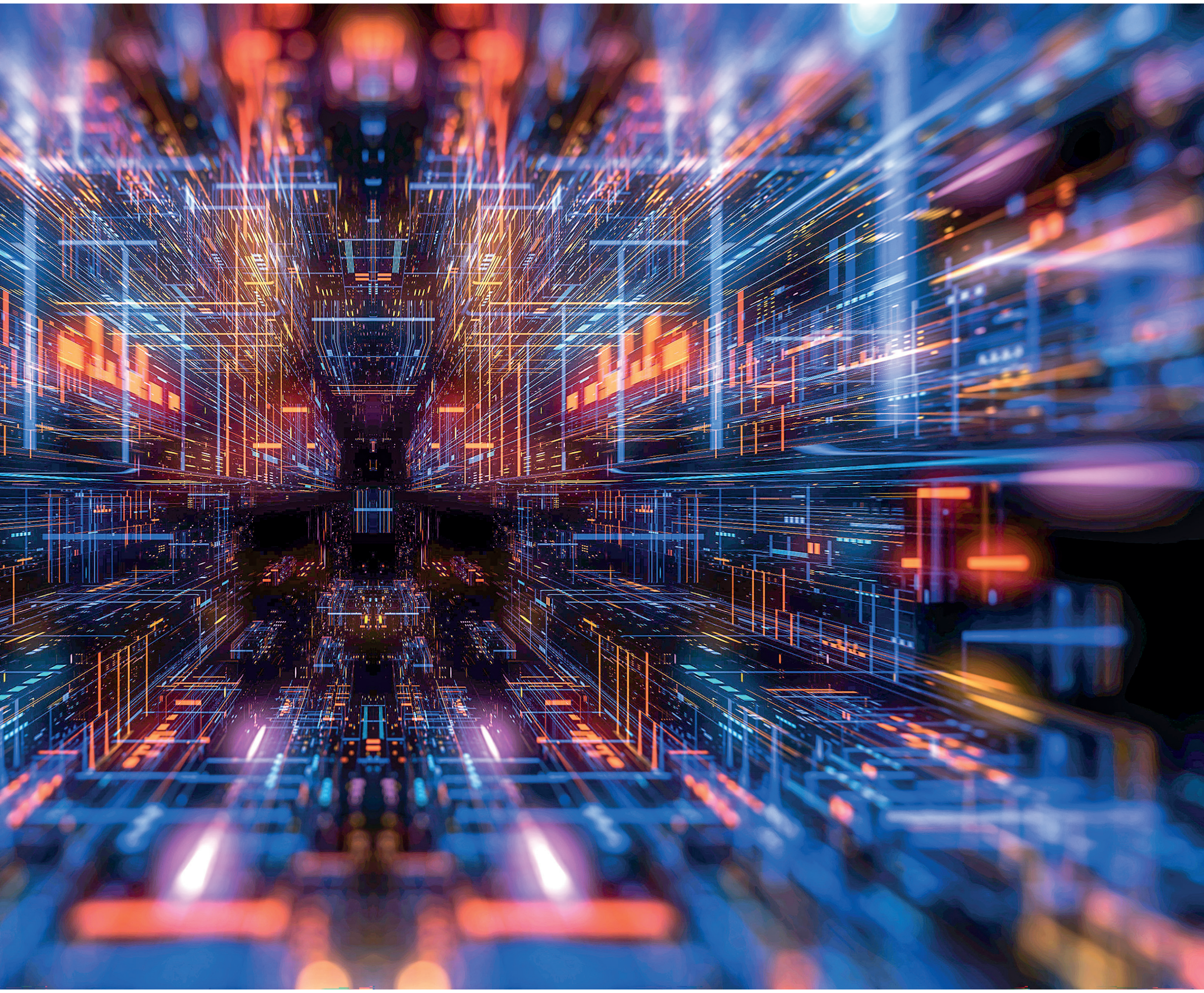
From a physicist's perspective, traditionally, a bit is any physical system that can be placed in one of two states, conventionally labeled "zero" or "one." Regardless of the technology used, it always involves a physical process that allows the bit's value to be toggled

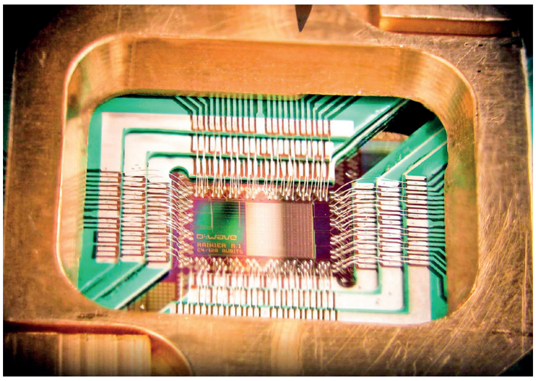
QUARDIA/SHUTTERSTOCK.COM

from "zero" to "one" or vice versa. Linking several bits together allows us to create logic gates. For instance, a simple operation that changes a bit from "zero" to "one" or from "one" to "zero" is known as a Bit-Flip, which performs the logical NOT operation. Other basic operations involve logic gates like AND and OR. Quantum physics represents the next transformative stage in computational processes. A quantum physical system can exist not only in the states "zero" and "one" but also in intermediate states. It remains a two--state system in the sense that any measurement of this object will always result in either "zero" or "one", and nothing more. However, experiments suggest that many more states are possible. Thus, a quantum bit, or "qubit," differs from a classical bit in that, while the latter exists solely in the states of "zero" or "one," a quantum bit can exist in many other states, which can then be utilized in computational processes.

In other words, physics is everywhere, even permeating computer science. Do we have a concept for the hardware for quantum computing – has it been successfully built, is it operational?

Not yet, but that certainly is a pertinent question. Quantum computing has an intriguing history of development, as it has been largely driven by theoretical research. It became apparent that leveraging quantum mechanics for calculations would offer numerous advantages. The theory of computational complexity





System constructed by D-Wave Systems, containing 128 qubits implemented using superconductors

D-WAVE SYSTEMS, INC., CC BY 3.0, VIA WIKIMEDIA COMMONS

has proved particularly useful in this context. Physicists often explore whether a phenomenon can occur based on established rules that declare certain phenomena impossible, for instance, because they would violate the principles of the conservation of energy or momentum. Hence, certain physical processes are deemed impossible because they would contradict known principles, while others are not. Therefore, the essential question posed by physicists is: "Is something possible or not?" Computer scientists ask similar questions: whether something is computable or not, and whether the algorithms for computing it are efficient and effective.

What does it mean for an algorithm to be efficient?
Certain algorithms give us a way to do something, to solve some problem, but when we try to apply it to bigger versions of the same problem, we find that the amount of steps required increases very quickly. Factoring a number into its prime components is a good example. The larger the number, the more time and memory a computer needs to factor it. Mathematicians have pondered how this scales with the size of the number – for instance, does factoring a number twice as large take twice as long? If the time and memory usage is a polynomial function of the number of bits in the number being factored, the algorithm is considered "efficient." However, if it is an exponential function, then the algorithm is inefficient.

It has been observed that the algorithm for multiplying two numbers is indeed efficient – the time it takes for a computer to perform the multiplication increases gradually with the number of bits of the factors, that is, with the size of both numbers. The larger the two numbers to be multiplied, the longer the computation takes, but the rate of increase is not drastic. On the other hand, it turns out that the algorithm by which a regular computer carries out the *reverse* process is not efficient. We know from mathematics that every composite number can be broken down into prime factors, for example, 15 into 3 times 5, which is referred to as the factoring problem. The time it takes to factor a number into primes grows exponentially with the size of the number being factored. Factoring a very large number into primes therefore demands an extensive amount of computer time. And this represents a significant mathematical challenge.

Of course, we might build a new, faster computer that is, say, a million times faster than the previous one. Factoring each number would take a million times less time, but the overall problem will still remain: an algorithm that is inefficient on a slow computer will remain just as inefficient on a fast one. Exponential growth in computation time remains exponential.

Will quantum computers usher in a breakthrough?
Technological progress alone will not allow us to change how an algorithm is classified. To do that, we would need to create a new law or develop a new algorithm. But it turns out that for solving certain problems, while we do not yet have an efficient classical algorithm, we do actually know of efficient quantum algorithms. If we had a functioning quantum computer, therefore, those algorithms would be runnable on it. The power of quantum computers lies in the fact that quantum physics offers a broader and more extensive set of instructions that can be utilized for programming. Furthermore, certain instructions, which mirror physical processes, are only applicable to quantum computers. By leveraging these additional instructions, we can develop new, even more efficient algorithms.

Classical computers are often used to perform calculations in physics or chemistry. Couldn't they be programmed to simulate quantum effects as well?
Classical computers can simulate quantum effects, but this simulation is usually not efficient. But once we have quantum computers, we will be able to simulate quantum phenomena efficiently.

So, it turns out we do have some concept for the quantum-computing software, but not yet for the hardware?
As I see it, we are currently in the early stages. We have managed to assemble a few logic gates and qubits using various technologies, be they ion traps or superconductors. They have been successfully interconnected and a few instructions have been executed. It has been demonstrated that quantum computing is possible, but we are a long way away from being able to fully realize its extraordinary capabilities, such as achieving an exponential improvement in performance. However, we are undoubtedly making progress with each passing day.

INTERVIEW BY **WITOLD ZAWADZKI**

Further reading:

Kaku M., *The Quantum Supremacy: How the Quantum Computer Revolution Will Change Everything*, 2023.

Fernández-Vidal S., Miralles F., *Desayuno con partículas: La ciencia como nunca antes se ha contado*, 2013.

Johnson G., *A Shortcut Through Time: The Path to the Quantum Computer*, 2003.