THEME 02

The quantum computing paradigm

QUANTUM COMPUTING | TECHNOLOGY | AI

Everything in the natural world can be described by quantum mechanics, and doing so has led to the development of everyday technologies from MRI scans and nanotechnology to the transistor. Progress in quantum mechanics has also led to a new computing paradigm that will disrupt many industries and businesses. As such, quantum computing will be a key technology of our future technological stack.

Our observations

- China is currently building a $10 billion National Laboratory for Quantum Information Sciences, which is due to open in 2020. The U.S. is lagging behind in quantum computing investments, as a 10-year federal $1.3 billion National Quantum Initiative is currently being discussed in Congress. The European Union invested $1 billion to make quantum computing practical in 2016, and unveiled a roadmap for quantum computing in the next decades. A report by the U.S. China Economic and Security Review Commission said that China has "closed the technological gap" with respect to quantum computing sciences, an area previously dominated by the U.S. for decades.
- Commercial interest is also nascent in quantum computing, led by big tech companies. Google researchers are betting that within a few years there will be a demonstration of quantum supremacy. And in China, Alibaba has teamed up with the prestigious Chinese Academy of Science to explore quantum computing services via the cloud. IBM announced that it's actually launching the world's first commercial quantum-computing service, which will allow people to make use of (currently slow) quantum hardware via the internet, and Microsoft just launched its first quantum development kits and "quantum programming language". Global spending on quantum computing will grow by 35% each year between 2018 and 2024.
- Rigetti, a U.S. startup, recently designed a microchip for quantum computers that would have more than six times as many qubits as Rigetti's current machines, making it more powerful than IBM's 50-qubit computer and more powerful than Google's record-holding 72-qubit machine. Rigetti is hoping to build a functioning computer with 128 qubits in the next 12 months. If successful, this could be the world's most powerful quantum computer and outpace traditional supercomputers. Furthermore, the company recently revealed its new Quantum Cloud Service (QCS) that will run 20 to 50 times faster than regular cloud setups.
- We have written before about the increased complexity of our economic and geopolitical reality. As a result, models are emerging that are based on quantum principles for example for explaining stock market prices, development economics or the rise of Trump.

>> see next page

Connecting the dots

There have been two quantum revolutions. The first one was in (quantum) physics: understanding how things work on the sub-atomic level, and was initiated in the early 20th century by the work of Schrödinger, Bohr, Heisenberg and Einstein, among others. During the 1920s, quantum physicists did the math that underpins these conclusions, but they were made manifest in laboratory experiments only later on in the 20th century with the second quantum revolution in the 1980s: applying the physics and mathematics to model computers that could perform "quantum computations". In 2011, Canadian company D-Wave Systems launched the first commercially available quantum computer, which is now currently used by NASA for robotics missions, Google for search, image labeling and voice recognition and by Volkswagen to predict traffic patterns in Beijing. However, these quantum computers have a very narrow scope, leveraging quantum algorithms and applications for very specialized tasks. Just as AI researchers are trying to develop strong or general AI instead of narrow AI, quantum scientists are trying to develop universal and supreme quantum computers: quantum computers that can compute and solve all kinds of problems and questions, and better than current traditional computers.

Quantum computing's main idea is to program atoms to represent all possible input combinations simultaneously and run an algorithm that tests all the possible combinations at once, instead of serially cycling every possibility by varying input to arrive at a solution, like "traditional computers". Three concepts – which defy our intuition – are at the basis of quantum computing. The first is superposition. Traditional computing depends on bits that can only take on two binary values: 0 or 1. Qubits, their quantum analogues, can be arranged in "states": something like a mixture of 0, 1 or both 0 and 1 (tertiary value). For example, instead of switching between hot and cold, qubits take on an infinite number of temperature degrees. The second concept, "entanglement", unleashes the power of qubits. Binary bits are isolated from one another, but inside a quantum computer, all qubits are interrelated, or "entangled" with each other. And a quantum computer can run its computations on all "entangled superpositions" simultaneously. That means that to operate on one qubit is to operate on all entangled qubits: changing the temperature of one thing means changing all temperatures. This makes the computational power of a quantum computer an exponential function of its qubits. For example, to describe all the states of a (binary) 50-bit traditional computer requires 50 bits of digital memory; a description of a(n) (entangled) 50-qubit quantum computer would require 2.5 quadrillion.

The last concept concerns the fact that algorithms using quantum math use "probability amplitude", meaning that a quantum computer can take shortcuts to the right answer. It does so by reducing the probability of wrong answers and increasing the probability of the right answers from its own operations.

These three properties make quantum computing radically different from traditional computing, because quantum computing reverses the order and concept of a computation. Consider, for example, the scenario that we would want to know all possible computations of the number 1,000, using only prime numbers. Because traditional computing is binary, with isolated events and fixed probabilities, a traditional computer will start factoring all possible operations by trial and error. The problem for the system is the question itself: what we want to know. But quantum computing works the other way around: its system uses programmed atoms that already contain every possible answer, and the problem is how to ask it. In other words, the quantum system already knows or contains how many prime number operations yield the number 1,000, while we only need to formulate the right problem statement or question. So the quantum system no longer considers the operation as an "either...or problem" (binary) but as "and...and" (entangled superpositions).

This makes quantum computers significant for data- and computation-intensive activities, such as searching huge datasets (e.g. in finance), cryptography, material design in pharmaceutical and chemical R&D, simulations, and machine learning. Given these radical improvements over traditional computing, companies and countries are rushing to build functional quantum computers with a broad range of applications. Currently, the technology is in the phase that quantum computers can be built, but that quantum information errors and engineering problems (e.g. quantum computers require very stable and cold environments) require solutions. The next phase is reaching "quantum supremacy": performing certain calculations traditional computers cannot do, such as some physical processes (e.g. wave-particle duality) that cannot be emulated by non-quantum models.

Implications

- Companies that have developed functional and broad-scoped quantum computers will probably offer the first quantum application via cloud services. Although these services will not immediately render quantum supremacy, these companies will be able to reinforce their centralized power by becoming an important gatekeeper to this scarce and costly computational resource. A possible scenario is that most quantum computing will happen within the cloud, while a few large quantum computers are kept at special facilities around the world. This will require enormous investments in digital infrastructure (in the digital bandwidth to transform quantum computations, for example).
- The two primary prerequisites are currently processors with enough qubits to perform quantum computations (which cannot be done by traditional computers) and developing quantum algorithms to solve the mathematical problems underlying these applications. Different business models will emerge with respect to the quantum computing stack, such as integrated hardware-as-a service models accessed by APIs, or specialized, hardware-agnostic software (e.g. for pharmaceutical and chemical companies, cybersecurity agencies).
- Quantum computers will be, along with 5G and AI, ingredient technologies of the next technological paradigm. As a result, it may be considered a "strategic technology", which will become heavily scrutinized for foreign investments and foreign takeovers of quantum computing companies, as is currently happening with 5G and telecom companies.

>> see next page