Quantum Computing
An Introduction

Author
Brian O'Donnell
Executive-in-Residence, Global Risk Institute

Computing capacity continues to expand and transform the world we live in. Sixty years on Moore's law continues unabated, with computing capacity doubling every two years, as engineers cram ever more transistors onto microprocessors. And what is the result? Today's smart phones have the computing capacity of a mainframe computer 50 years ago, such that basically everyone has this awesome computing power at their fingertips with applications there to help manage every aspect of their life. But a crossroads is emerging in the near future that will both amplify and imperil our new app based lifestyle.

Quantum computing will lead to a leap forward in computing power, significantly altering the landscape. In the brave new world of quantum computing the basic binding constraints that computer engineers have been working around for sixty years will be overcome. Today's computers are beautiful in their simplicity. For all their capacity they are constrained in a few basic ways:

- *They convert all input into binary digits – 1's and 0's – such that every number, letter, picture and video we stream are represented and processed digitally by our computers and smartphones;*

- *They utilize simple binary gates to perform arithmetic and logic operations - e.g. addition, subtraction, greater than and equal to;*

- *They use electrical impulses and circuits (crammed by the millions onto semiconducting silicon chips) in order to receive input, process logic, and display output (usually in a fraction of a second.)*

And, as an increasing part of our personal and financial life is digitized onto our smartphones, they are protected with increasingly sophisticated security encryption algorithms to protect us from hackers.

Quantum computing relies on the great advances in particle physics to unleash computing capacity that is millions of times more powerful than even the most powerful computers that exist today. Over the past hundred years or so great physicists have concentrated on the physical nature of sub atomic particles, the building blocks of matter and life, which adhere to rules that are profoundly different then the world (described by classical physics) we observe in our daily life. While the details of quantum physics are beyond the scope of this article, the following basics will be helpful:

- *Whereas in traditional computing units there are binary digits (i.e. 1's and 0's) called Bits, quantum computing units are called Qubits and are not constrained by binary outcomes – they rely on the quantum principle of Superposition (i.e. superimposed upon each other), which means they can 1 and 0 at the same time (i.e. in a binary world a cat is alive or dead; in a quantum world the cat can be alive and dead at the same time);*

- *Whereas the outcome of a traditional computer is said to be deterministic (the computer circuit says the cat is dead), Qubits display the quantum phenomenon of Entanglement, which means the atoms being manipulated become entangled such that the state of one atom becomes directly correlated with the state of another atom (if Qubit 1 concludes that that cat is dead, and if Qubit 2 becomes entangled with Qubit 1, then Qubit 2 will automatically say the*

inverse, that the cat is alive; in quantum physics, entanglement can occur across great distances, with the state of atom on one side of the universe impacting the state of an atom on the other side of the universe);

- *If the above leaves you dazed and confused you are in good company. Albert Einstein skeptically said of quantum mechanics "God does not play dice with the universe"; and another leader in the field, Niels Bohr added "If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet."*

Still, here we are 100 years since the pioneering work on quantum mechanics and on the brink (give or take a decade) of the quantum computing age. Universities and private company researchers are making great strides in developing a quantum computer, which will operate at speeds millions of times faster than today's computers. How will they achieve this? Instead of sending electric impulses through millions of circuits etched on to a silicon computer chip, a quantum computer manipulates the "the spinning" of sub atomic particles. Despite the strides that have been made there are still challenges to overcome. For example, one challenge in the superconducting approach to quantum computing is that one needs to achieve a purified environment for the sub atomic particles, which includes a temperature of (approximately) absolute zero, the coldest temperature known (-273.15 degrees Celsius; required to avoid heat energy from disrupting the movements of the qubits). While that is a surmountable challenge(to date the coldest known natural location in the universe is the Boomerang Nebula at 272.15 degrees), one must be careful not to directly observe the results of the quantum calculation, as mere observation can "bump" the particles and alter the results.

One impressive Canadian contribution to the development of quantum computing is through the Institute for Quantum Computing (IQC) at the University of Waterloo. The institute was launched 14 years ago through an incredibly generous personal investment made by Mike Lazaridis (Blackberry creator; has personally contributed over $100 million to the institute). The IQC funds ongoing research and laboratory experimentation in quantum information science, and they are well on their way to a goal of 30 faculty members, 50 post-doctoral fellows and 125 students.

So what are the benefits of quantum computing? As noted above, computer technology has continued its impressive run of doubling capacity every 2 years over the past half century. However, following that trend, in about 10-20 years each transistor on a microchip will approach the size of an atom which will likely then signal the natural conclusion to Moore's law. The next step forward therefore is likely quantum computing, which computes via the manipulation of sub atomic particles. The quantum computer will utilize sub atomic principles, such as superposition, to massively increase computing speed and capacity. Quantum computers will be able to perform tasks, such as factoring very large numbers (think in terms of factoring a 500 digit number, which is impossible for today's circuit based computers). But, herein lies one of the emerging risks from quantum technology, as its ability to solve such complex calculations and algorithms means that they can "decode" today's encryption codes, which keep computers and smartphone applications safe from hackers. Therefore one of the first developments had better be encryption capabilities that are secure against quantum technologies.

About the Author

Brian O'Donnell is an Executive in Residence at the Global Risk Institute, after retiring from CIBC in 2015. Most recently Brian was CIBC's Executive Vice President and Chief Data Officer, where he developed their data strategy and governance framework. Prior to the CDO position Brian lead the Bank's Enterprise Risk Management group, including balance sheet and capital management.

Read Brian's full Bio on GRI Website >