

Quantum computing, The next big...wait, what is it really?

By [Sumit Kumar Sharma](#)

3 Apr 2019

Initially, computers were primarily used by academics and for research. Today, one cannot fathom life and work without some sort of computing power aiding in our daily activities. In addition, we have reached the point where a pocket-sized device is vastly more powerful than a computer the size of a city block was just a few decades ago.



Sumit Kumar Sharma, Enterprise Architect at In2IT

However, as small as we can make processor chips, there is a limit to this miniaturisation. Beyond these physical size limits, we enter a completely new realm – the world of quantum computing.

This technology is not simply a more powerful processor or platform, but an entirely different universe, where the rules of physics operate differently. As such, it is impossible to fully understand its potential. Two things we do know, however: quantum computing is coming, and it will change life as we know it.

So, what is quantum computing?

A complete and accurate explanation of quantum computing involves a fairly technical and highly scientific discussion around the laws of physics. It is also challenging to explain as quantum computers are not a mainstream commodity at present – it is a concept that is emerging and that is being developed, and the broader potential for it is currently unknown. However, simply put, quantum computing changes the rules of computing as we know it.



It's time to take note of quantum computing

17 Oct 2018



All electronic devices today are powered by computer chips. These chips are made up of tiny 'transistors'. In layman's terms, transistor can be perceived as a switch that controls the flow of electricity, i.e., "flow of electrons".

Over the years we have reduced the size of these transistors to pack more and more computing power into smaller packages. The smallest computer transistors are currently around 14 nanometres. The bad news is there is a physical limit to which we can reduce the size of transistors. Beyond this point, transistors no longer function correctly.

The flow of electrons, controlled in a computer by a transistor, can no longer be switched on or off. Electrons are no longer bound by the physical world we experience every day. In this sub-atomic world, electrons will be subject to the laws of quantum physics and the building block of today's computers, namely transistors, will become useless.

Quantum particles are not static and do not move in a straight line, but are constantly in motion in a wavelike pattern in any direction. In quantum computing, we try to measure such movements (like polarisation) of sub-atomic particles. The values, once limited to the bits 0 and 1, suddenly becomes fluid, called a Qbit, and one Qbit can represent multiple values.

This can be compared to a light switch (the traditional transistor), which can either be on or off, and a dimmer switch (a quantum particle), which can be on, off, or any value in between.

What does this mean?

Essentially it means that the entire manner in which a computer operates must change as we enter the world of quantum. However, this opens up practically limitless power and potential. With a traditional binary system, computers are able to work with two values at a time, which limits the speed at which they operate, no matter how powerful they are.

A quantum computer, however, would be able to work with hundreds simultaneously. This unlocks massive amounts of processing power, enabling computers to do complex calculations and massive database searches in a fraction of the time they can currently be completed.



Quantum, AI turns computing into a 'loaded gun'

1 Apr 2019



Top three use cases for quantum computing

It is impossible to fully understand the potential for quantum computing, however, there are three current focus areas: healthcare and medicine, security, and the 'new Internet'.

- **Healthcare and medicine**

In the healthcare space, quantum computing opens up a new world of potential. The proteins and molecules that make up the human body, and also medicines, viruses, bacteria and pathogens, do not operate in binary, they are bound by the laws of quantum physics.

This has limited the ability of traditional computers, as it has never been possible to accurately simulate the behaviour

of proteins and other molecules to predict progression of a disease, the effectiveness of medicine and so on. It makes sense to use quantum computers to build quantum simulation models that can far more accurately mimic the behaviours of these proteins and molecules.

This means that complex and powerful simulations can be run to predict disease outcomes, develop more effective medicines, simulate responses to new treatments and more. Healthcare could be completely revolutionised, and deaths from diseases like cancer and AIDS, that have been difficult to treat and cure, could become something of the past.

- **The security sector**

Encryption is the cornerstone of digital security, but encryptions are bound by the laws of binary, and as such are not infallible. If security keys are lost or stolen, then data is placed under threat. In the world of quantum, encryption can be made so complex that it is, for all intents and purposes, unbreakable.

Instead of using traditional encryption keys, quantum computers will use quantum encryption keys. Banks, in particular, are exploring the potential for quantum encryption, to secure electronic devices as well as information sharing and transactions.

- **The ‘new’ internet**

This use case for quantum computing reads like something from a science fiction novel. Effectively, since quantum identities or particles can exist at multiple points in space and time, they can be manipulated in one place and the same particle, existing in another location, will reflect the manipulation. It sounds confusing, right?

Let’s assume that these subatomic particles were a person. In a quantum world, if a person becomes angry or happy it can induce the same behaviour in another person sitting maybe 1000km away, and this can happen without any contact or exchange of information. As fantastic as it sounds, this is actually something that has been demonstrated in laboratories and it has amazing potential. Once quantum computers are ubiquitous and quantum networks abound, information could be shared without being transmitted. Collaboration takes on a whole new level and even the way in which we store information will change.

It’s coming...but when?

Quantum computing is undoubtedly the next big thing, nevertheless, organisations need to understand that it will still take some time to commoditise quantum computers. The financial services and healthcare sectors are leading the way and IBM has begun to master quantum computing, but mostly the concept is still firmly in the research and development phase.

One thing is for sure - quantum computing is coming, and possibly sooner than we think. The next decade is bound to be an exciting one as we discover the potential for this incredible new technology.

ABOUT THE AUTHOR

Surjit Kumar Sharma is Enterprise Architect at In2IT

For more, visit: <https://www.bizcommunity.com>