Quantum Computing – are your ready?

According to theoretical physicist, Jonathan Dowling, “if you have business and trade secrets that you would want to keep secret for ten to 50 years, then you need to start worrying [about quantum computing] now”.

The invention of computer chips and lasers have much to do with quantum technology. As we progress further into quantum computing, there are few issues we need to understand about the mysterious and wonderful quantum world, focusing on nature at the atomic scale. For a start, do we realise the following quantum phenomena:

1. it is possible for a type of liquid to flow upwards
2. an atom can be at various locations simultaneously
3. a cup of hot tea is heavier than the same cup of cold tea
4. you become older at the top of a mountain than at the bottom
5. Light is both a particle and a wave; light is actually a type of electromagnetic radiation, at wavelengths which we can see. In other words, a wave can be regarded as a slightly blurred particle. Also, waves, eg, light beams, could penetrate a strong block of glass
6. Photon (a type of particle) can either be transmitted or reflected

So are you convinced that the quantum world is mysterious? But there is more. You see, the quantum world deals with uncertainty whereas physics deals with certainty. Eg, atoms could either be a wave or a particle depending on circumstances! And in quantum mechanics, there is the Uncertainty Principle which says that we cannot know exactly where a particle is and with what momentum (ie, mass x velocity) it is moving.

So a key question is: “how to build quantum computers by using technology that is so weird? Some of the main problems in the development of quantum computers that have to be overcome include:

Measurement of quantum superpositions
Occurrence in which a quantum particle is in more than one state at a time (NB. A full description of nature, at a given point in time, is called a state).

The quantum state of each particle cannot be described independently of the others. Whenever we try to measure quantum superpositions, they change rapidly and/or being destroyed.

As we know, a Qubit (which is a quantum bit, or binary bit) could exist in a superposition of two states, representing a “0” and a “1” at the same time! The traditional computers use a normal bit (representing a “0” and a “1”) but do not use superpositions.

Quantum computers in using Qubits (read: superpositions) can therefore provide enormous computer processing power. The measurement of quantum superpositions therefore is a key obstacle in the development of quantum computers.

Eg, how could we best isolate the quantum computer, with its use of complex numbers (ie, square root of -1), from its physical surroundings?

The controversy over the measurement issue has been around since the 1920s and currently many quantum experts still disagree on it. It also revolves around the fact that in the quantum world, an atom can be at several locations at once, whereas in the normal world, there is a location for everything, eg, a table!

The other problem is: “We can’t fully control or predict the future by knowing only half the story of a particle”. To fully enunciate a physical state, we often require a pair of information, eg, particle’s position and particle’s momentum.

However, quantum mechanics states that you can only elect to fully know one of them. Eg, we can elect to measure the position of the quantum particle or we can elect to measure the momentum of the particle.

The main problem is that we cannot elect to concurrently measure both the position and momentum of the quantum particle! Moreover, the Uncertainty Principle is a key building block of quantum mechanics.

The great scientist, Heisenberg believed that if it were possible to measure the position and momentum concurrently with a greater accuracy, quantum mechanics would collapse. And to this day, it is hard to find scientists who would disagree with the Uncertainty Principle. It should be noted that quantum mechanics also explains light, radioactivity and nuclear physics.

Entanglement problem

Entanglement is the phenomenon in which pairs of quantum particles can remain connected or interacted even when separated by huge distance, appearing to share the same existence.

If you'd try to measure one particle, the nature and characteristics of the other particle will change. It is of course, very difficult to maintain particles' entanglement.

At every opportunity to interact with other particles, it will; and the entanglement would usually disappear instantly. The main objective is to prevent the Qubits from interacting with their environment.

Quantum particles which are entangled pairs have great potential benefits in the development of quantum computers. Under the quantum entanglement principle, the measurement of one particle would instantly change the other particle due to entanglement; so that trying to decipher a system would automatically destroy the lock.

By using quantum entanglement we could generate random encryption keys and make the interception of keys extremely difficult. In other words, the destruction of entanglement would be instantly detected and any data communication finished prior to the leakage of data.

Therefore, quantum entanglement could be used to create instantaneous communications system. It should be noted that there have been recent overseas experiments in sending entangled photons (only for a short distance so far).

The entanglement feature could facilitate quantum teleportation which enables information required to "rebuild" a particle's state to be communicated to a remote location.

Predicting probabilities

Quantum theory is a framework for predicting probabilities. We could predict the probable final location (including the probable route) of an atom which is moving through space.

An atom has a movable location in space; it can be here or there (after a short time). In other words, the location of a quantum particle after a short time is a function of probability.

It is probable that within the next decade, quantum computing will be upon us, whether we are ready or not. Remember, a great scientist, Dr Richard Feynman (a Nobel Prize winner) once said: “If you think you understand quantum mechanics, you don’t understand quantum mechanics”.

(Disclaimer from Leonard Yong: I don’t think I understand quantum mechanics when writing this article) M.Acc, FCPA, CA, MACS(Snr) 25 February 2020 Convenor, CPA Cyber Security Forum, Chairman, Digital Economy Committee, ShireBiz

In memory of Tony Blain

I shall dearly miss my friend, Tony Blain, who had done so many good things for the Shire people. Tony was a keen believer of technology, eg, quantum technology, nuclear physics and cyber security technology, to make Australia in the forefront in the development of quantum computers.