An Introduction into Quantum Computing

Cameron Mims

***Abstract* – This paper provides a broad and entry level view into the study of quantum computing. Basic concepts, types, etc. will be discussed in full without the necessary need of understanding the mathematics, physics and quantum mechanics behind the making and ideas of quantum computing. The scope of this paper is to mainly give light to an exciting field that is still in its infancy and will be a main topic of discussion in the coming of years as we search for faster, stronger and better computers.**

I. Introduction

In its most basic definition, we can describe quantum computing as the harnessing and exploitation of the laws of quantum mechanics to process information. While we are most familiar with the traditional models of computing such as the Turing Machine, the massive amount of processing power generated by computer manufacturers has not yet been able to satisfy the need for speed and computing capacity in our world today. With the harnessing of atoms and molecules to perform memory and processing tasks, quantum computers have the potential to perform certain calculations significantly faster than any silicon-based computer ever could. If Moore's law states that the number of transistors on a processor doubles nearly every two years, we will find ourselves soon dealing with circuits on a microprocessor on an atomic scale leading into the inevitable next step of quantum computers.

II. Superposition

In traditional computing we represent information in the form of bits or a string of bits. A bit can be characterized as a 0 or 1, meaning that there are only two possible states for representation. Instead quantum computers encode information as quantum bits or qubits, that encodes the 0 and the 1 into two distinguishable quantum states. Qubits represent atoms, ions, photons or electrons and their respective control devices to act as computer memory and a processor. What makes qubits so different between bits, is the concept/system of superposition. Superposition is a system that has two different states that can define it and its possible for it to exist in both. As a physical example, an electron has two possible quantum states; spin up and spin down. When an electron is in superposition, it is both up and down at once, being a combination of both. Only when measured does it drop out of superposition and adopt one position or the other. With this quantum mechanics system, we can do away from binary constraints that are found in our traditional computers

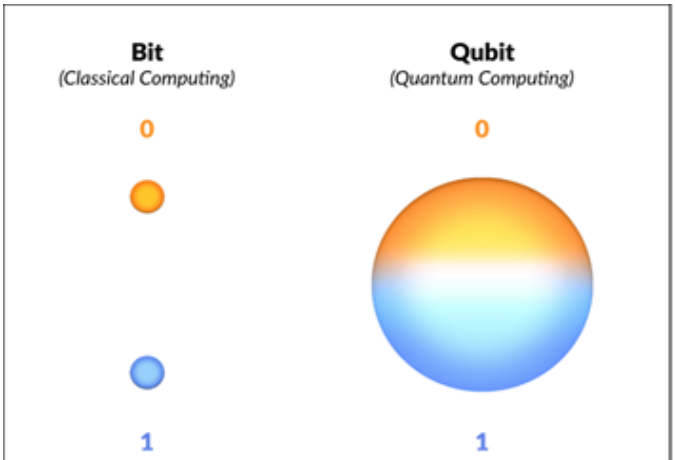

Fig 1. A visual representation between a classical bit found in traditional computing, and the qubit found in quantum computing. Note how the qubit can be both 0 and 1

III. Entanglement

A problem with the idea of quantum computers, is that if you try to look at the subatomic particles, you could in turn "bump them", and thereby change their value. If you look at a qubit in superposition to determine its value, the qubit will assume the value of either 0 or 1, but not both. This in turn will overhaul the concept/system of superposition and will effectively turn into a mundane traditional computer. To make a practical quantum computer, scientists needed to devise a way of making measurements indirectly to preserve the systems integrity. Luckily scientist have been able to capitalize on the quantum mechanics fundamental of Entanglement. Quantum entanglement is a label for the observed physical phenomenon that occurs when a pair or group of particles is generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the pair or group cannot be described independently of the state of the others, even when the particles are separated by a large distance. As an example, if left alone, an atom will spin in all directions. The moment it is disturbed or "bumped" it will choose one spin and or value; and at the same time, the second entangled atom will choose an opposite spin and or value. This allows us to know the value of qubits without looking into them, preserving the quantum computers integrity

IV. Types of Quantum Computing

There are three types of quantum computing with each type differing by the amount of processing power (qubits) needed and number of possible applications, as well as the time required to become commercially available.

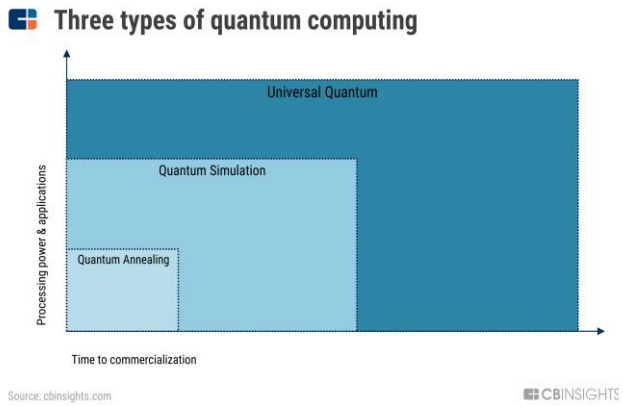

Fig 2. A graph representation between the amount of time the quantum machine would take to commercialize, and its processing power/applications it would be used for

A. Quantum Annealing/Quantum Annealer

The Quantum annealer is the least powerful and most restrictive form of quantum computers. It is the easiest to build, though can only perform one specific function. The consensus in the scientific community is that a quantum annealer has no known advantages over conventional/traditional computing. Quantum annealing processors naturally return low-energy solutions. Some applications require real minimum energy, and others require good low-energy samples. This makes annealing best for solving optimization problems and probabilistic problems. In an optimization problem, we search for the best of many possible combinations. These types of problems include scheduling challenges, such as finding the most efficient route for the traveling salesman. Sampling from many low-energy states and characterizing the shape of the energy landscape is useful for machine learning problems where we want to build a probabilistic model of reality. These samples give information about the model state for a given set of parameters, which then can be used to improve the model. Probabilistic models handle uncertainty by accounting for gaps in knowledge as well as errors in data sources. Probability distributions represent the unobserved quantities in a model and how they relate to data. Sampling is a computationally intensive task, but due to how the D-wave system solves problems, it is an excellent match.

B. Analog Quantum/Quantum simulation

The analog quantum computer will be able to simulate complex quantum interactions that are intractable for any known conventional/traditional machine. It is thought that the analog quantum computer will need to contain somewhere between 50 to 100 qubits. To compare, the most qubits in a quantum computer is IBM's new 53-qubit quantum computer. Quantum simulation/simulators explore specific problems in quantum physics that are beyond the capacity of traditional computers. The act of simulating complex phenomena is an important application of quantum computing. As an example, modeling chemical simulations on many particles, which we call quantum chemistry. Other applications can be material science, optimization problems, sampling and quantum dynamics. Unlike a quantum annealer and its generality being restrictive, the analog quantum would be partial in comparison, meaning the system can achieve multiple things.

C. Universal Quantum

The universal quantum computer is the most powerful, the most general, and the hardest to build out of all the other types of quantum computers, posing many difficult technical challenges. A true universal quantum computer would estimate the need of around 100,000 qubits, where some are even speculating 1M qubits. In comparison to IBM's 53-bit quantum computer, this can be considered a testament to how much the study is in its infancy. While we may be a long way out from being able to achieve such a feat, we can still formulate an idea of what this computer should be able to achieve. The basic idea behind the universal quantum computer is that you could direct the machine at any massively complex computation and get a quick solution. Theses computations can range from solving annealing equations, simulating quantum phenomena, and many more. Researchers have designed many algorithms that are only possible to be solved on a quantum computer. Of course, this is not limited to classical algorithms as well, for example RSA encryption which utilizes prime factorization as a means of security. So, in theory a universal quantum computer should be capable of universal quantum computation. Can be applied to all classes of problems and capable of computing whatever a classical computer can compute, in addition to anything a quantum computer can compute, including simulation of real physical quantum systems. It is important to note that universal refers to each of the discrete operations which can be performed, and not necessarily the amount of data which can be processed or its structure.

V. Quantum Networking

In its broadest definition, a quantum network facilitates the transmission of information in the form of qubits between physically separated quantum processors. A quantum processor is a small quantum computer that can perform quantum logic gates on a given number of qubits. Quantum networks and classical networks have many things in common, the main difference being that like quantum computing, quantum networks will be able to solve problems faster and better than a traditional model. It is very important to note that quantum networking is still in its infancy, and most of the concepts surrounding it currently are more theory based.

A. Computation

Networked quantum computing/distributed quantum computing works by linking multiple quantum processors through a quantum network by sending qubits in between them. In doing so, we create a cluster that creates more computing potential. This is parallel to how we connect several classical computers to form a cluster in classical computing. This system will also be scalable, being able to add more and more quantum computers to the network. Quantum processors currently are only separated by short distances.

B. Communication

Quantum communication can be directly correlated to how regular network communication is established. The idea is that one wants to send qubits from one quantum processor to another over a long distance. This way local quantum networks can be intra connected into a quantum internet. Like our traditional internet, a quantum internet will be able to support many applications which derive from the creation of quantum entangled qubits. Making it so information can be transmitted between remote quantum processors. Over long distances the main method of operating a quantum network is to use optical networks and photon-based qubits. Optical networks have a reduced chance of decoherence, meaning a loss of quantum coherence where two wave sources do not have the same frequency or waveform. Optical networks also can re-use optical fiber. Other communications lines are fiber optic networks and free space networks.

C. Repeater

In theory a true quantum repeater will allow the end to end generation of quantum entanglement, and the end to end transmission of qubits. A quantum repeater will allow entanglement and can be established at distant nodes without physically sending an entangled qubit the entire distance. In a trivial case, a repeater is composed of two sources of entangled particles. The four particles go in four different fibers arranged in a way that one particle of each source go to a quantum measurement device, and the other two remaining particles will go in opposite directions. The quantum measurement device will check if the two particles are identical to the two particles arriving at the same time. If this measurement succeeds, the two other particles are entangled together and the state representing this entanglement depends on the result of the measurement. With this measurement, we have established the entanglement of two particles which are separated by a distance larger than the one reached using a single source of entangled particles. This means that a quantum repeater can increase the distance over which entanglement can be distributed.

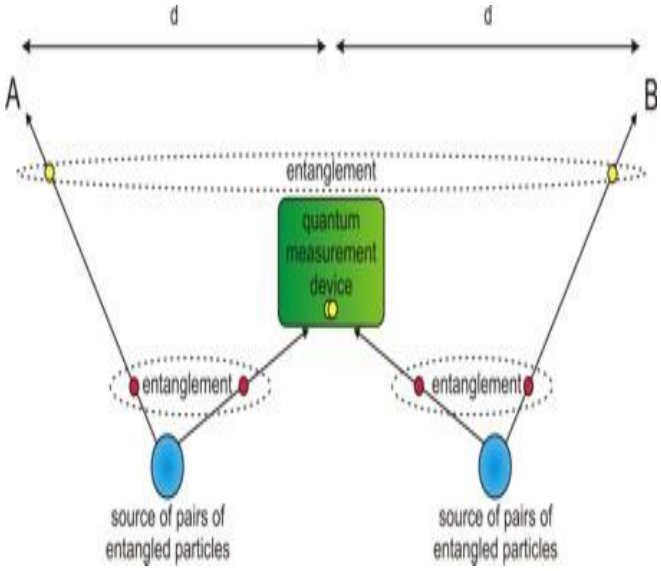

Fig 3. Visualization of how a quantum repeater and quantum measurement device establish the entanglement of particles and distance they can be distributed

D. Quantum Key Distribution

Quantum Key Distribution (QKD) is the act of generating a private key shared between two parties using an insecure quantum channel and an authenticated but not private classical channel. The private key can then be used to encrypt messages that are sent over an insecure classical channel. Where traditional cryptography security is usually since someone is unable to solve a certain mathematical problem, QKD achieves its security through the laws of physics. This means that if an eavesdropper were to try an intercept a quantum communication, traces will inevitably ne left behind that will be detected. A QKD implementation includes the following components:

I. A fiber or free-space quantum channel to send quantum states of light between the transmitter (Alice) and receiver (Bob). This channel does not need to be secured.
II. A public but authenticated communication link between the two parties to perform post-processing steps and give a correct secret key.
III. A key exchange protocol that exploits quantum properties to ensure security by detecting eavesdropping or errors, and calculate the amount of information that has been lost or intercepted

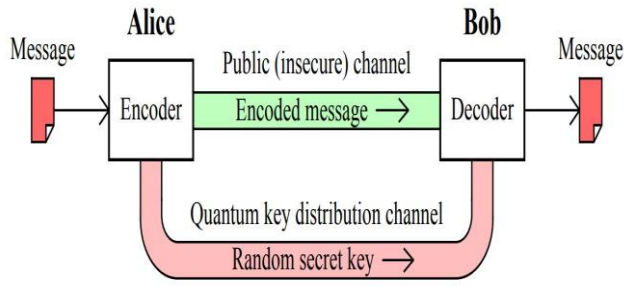

Fig 4. Broad example of QKD and the two channels used, one being an insecure public channel, the other an authenticated but not private QKD channel

While harder than QKD, sometime in the future it will be possible to encrypt data using quantum computing techniques that are particularly resistant to eavesdropping and various forms of hacking. The most prominent approach to this is the Kak protocol, which is a quantum version of the double-lock algorithm allowing two users to securely exchange data without sharing keys.

VI. Conclusion

While we may be a little way away from a fully functioning quantum computer, many fundamentals and practical discoveries have been made in the name of quantum computing. Quantum technologies are already in use, with QKD being commercially available. Such tools will be invaluable to the development of a true quantum information processor or universal quantum computer. The revolution of the computer world has already begun, and the possibilities that lie ahead are seemingly endless.

VII. References

[1] Institute for Quantum Computing. (2019). *Quantum computing 101 | Institute for Quantum Computing*. [online] Available at: https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101 [Accessed 5 Dec. 2019].

[2] C. Fisher, "q-site", *q-site*, 2019. [Online]. Available: https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/. [Accessed: 05- Dec- 2019].

[3] H. Garden, HowStuffWorks, Tech, Computer, Hardware and Desktops, "How Quantum Computers Work", *HowStuffWorks*, 2019. [Online]. Available: https://computer.howstuffworks.com/quantum-computer1.htm. [Accessed: 05- Dec- 2019].

[4] D. Cardinal, "How Does Quantum Computing Work? - ExtremeTech", *ExtremeTech*, 2019. [Online]. Available: https://www.extremetech.com/extreme/284306-how-quantum-computing-works. [Accessed: 05- Dec- 2019].

[5] "How does quantum computing work?", *plus.maths.org*, 2019. [Online]. Available: https://plus.maths.org/content/how-does-quantum-commuting-work. [Accessed: 05- Dec- 2019].

[6] M. Giles, "Explainer: What is a quantum computer?", *MIT Technology Review*, 2019. [Online]. Available: https://www.technologyreview.com/s/612844/what-is-quantum-computing/. [Accessed: 05- Dec- 2019].

[7] "What is superposition?| Explore | physics.org", *Physics.org*, 2019. [Online]. Available: http://www.physics.org/article-questions.asp?id=124. [Accessed: 05- Dec- 2019].

[8] D. Voorhoede, "Superposition and entanglement", *Quantum Inspire*, 2019. [Online]. Available: https://www.quantum-inspire.com/kbase/superposition-and-entanglement/. [Accessed: 05- Dec- 2019].

[9] "Qubit", *Joint Quantum Institute*, 2019. [Online]. Available: https://jqi.umd.edu/glossary/qubit. [Accessed: 05- Dec- 2019].

[10] "Visualizing bits and qubits", *Medium*, 2019. [Online]. Available: https://medium.com/qiskit/visualizing-bits-and-qubits-9af287047b28. [Accessed: 05- Dec- 2019].

[11] *Cl.cam.ac.uk*, 2019. [Online]. Available: https://www.cl.cam.ac.uk/teaching/1617/QuantComp/slides1.pdf. [Accessed: 05- Dec- 2019].

[12] "Entanglement Made Simple | Quanta Magazine", *Quanta Magazine*, 2019. [Online]. Available: https://www.quantamagazine.org/entanglement-made-simple-20160428/. [Accessed: 05- Dec- 2019].

[13] "Quantum entanglement", *ScienceDaily*, 2019. [Online]. Available: https://www.sciencedaily.com/terms/quantum_entanglement.htm. [Accessed: 05- Dec- 2019].

[14] K. Artist, "How Quantum Entanglement Works (Infographic)", *livescience.com*, 2019. [Online]. Available: https://www.livescience.com/28550-how-quantum-entanglement-works-infographic.html. [Accessed: 05- Dec- 2019].

[15] J. Emspak, "Quantum Entanglement: Love on a Subatomic Scale", *Space.com*, 2019. [Online]. Available: https://www.space.com/31933-quantum-entanglement-action-at-a-distance.html. [Accessed: 05- Dec- 2019].

[16] "What Is Quantum Computing?", *CB Insights Research*, 2019. [Online]. Available: https://www.cbinsights.com/research/report/quantum-computing/. [Accessed: 05- Dec- 2019].

[17] J. Desjardins, "The 3 Types of Quantum Computers and Their Applications", *Visual Capitalist*, 2019. [Online]. Available: https://www.visualcapitalist.com/three-types-quantum-computers/. [Accessed: 05- Dec- 2019].

[18] "Introduction to Quantum Annealing — D-Wave System Documentation documentation", *Docs.dwavesys.com*, 2019. [Online]. Available: https://docs.dwavesys.com/docs/latest/c_gs_2.html. [Accessed: 05- Dec- 2019].

[19] "What's the difference between quantum annealing and universal gate quantum computers?", *Medium*, 2019. [Online]. Available: https://medium.com/quantum-bits/what-s-the-difference-between-quantum-annealing-and-universal-gate-quantum-computers-c5e5099175a1. [Accessed: 05- Dec- 2019].

[20] "What Is a Universal Quantum Computer?", *Medium*, 2019. [Online]. Available: https://medium.com/@jackkrupansky/what-is-a-universal-quantum-computer-db183fd1f15a. [Accessed: 05- Dec- 2019].

[21] "Quantum gates", *Quantiki*, 2019. [Online]. Available: https://www.quantiki.org/wiki/quantum-gates. [Accessed: 05- Dec- 2019].

[22] "What are Quantum Networks and How Do They Work? | QuantumXC", *Quantumxc.com*, 2019. [Online]. Available: https://quantumxc.com/what-are-quantum-networks-and-how-do-they-work/. [Accessed: 05- Dec- 2019].

[23] "Quantum network", *En.wikipedia.org*, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Quantum_network. [Accessed: 05- Dec- 2019].

[24] *Quintessencelabs.com*, 2019. [Online]. Available: https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf. [Accessed: 05- Dec- 2019].

[25] T. WIRED, "The Future of Security: Zeroing In On Un-Hackable Data With Quantum Key Distribution", *WIRED*, 2019. [Online]. Available: https://www.wired.com/insights/2014/09/quantum-key-distribution/. [Accessed: 05- Dec- 2019].

[26] "Quantum Key Distribution (QKD) - Quantum Technology", *Quantum Technology*, 2019. [Online]. Available: https://qt.eu/understand/underlying-principles/quantum-key-distribution-qkd/. [Accessed: 05- Dec- 2019].

[27] "Quantum key distribution", *Quantiki*, 2019. [Online]. Available: https://www.quantiki.org/wiki/quantum-key-distribution. [Accessed: 05- Dec- 2019].

[28] "Quantum Repeaters - Quantum Technology", *Quantum Technology*, 2019. [Online]. Available: https://qt.eu/understand/underlying-principles/quantum-repeaters/. [Accessed: 05- Dec- 2019].