Understanding Quantum Computing

Quantum computing is a difficult concept to comprehend, and this can be attributed to the complex physics and mechanics that are involved. Before delving into the specifics of quantum computing, it is important to understand how traditional computer processors work because some fundamental concepts are shared between the two. A modern-day processor consists of packing millions, and even billions, of transistors onto a die. These transistors can either be on or off, or in the binary terms a 1 or 0. The intricate layers of circuitry that connects these transistors allows bits of information to be processed with great efficiency. Intel released an excellent visual representation of the process which can be seen in Figure 1 and 2 [1].

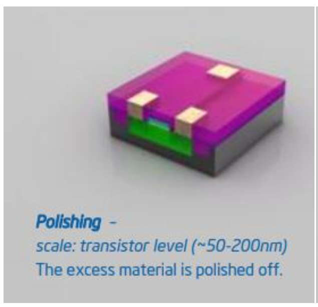

Figure 1.

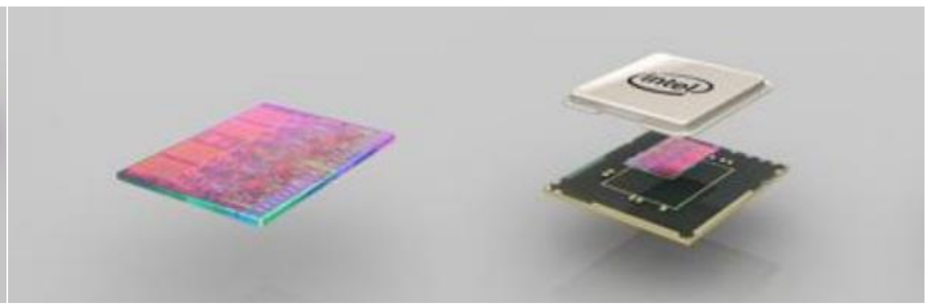

Figure 2. The making of a modern processor (Intel, 2009). Images by Intel.

As shown in the graphic above, transistors are on the 50-200nm scale; to put this into perspective, the width of a human hair is about 60,000nm [2]. These transistors are about 300 to 1,200 times smaller than said hair and going any smaller would prevent them from functioning properly. The argument of simply increasing the size of the chip or die is viable, which can be seen in larger processors that fit 4 or more of these dies, however not viable forever. At some point in time, processors will peak and become limited by a combination of several factors including but not limited to size, heat, power consumption, efficiency, cost, and more. Quantum processors circumvent this by harnessing quantum mechanics to process information at speeds unheard prior.

Quantum Physics and the Qubit

The speed of a conventional processor can be increased by combining multiple processors, or cores, in parallel. However, as stated previously this is limited by physical space. Quantum computers are different in that the amount of parallel processing that can be accomplished increases exponentially relative to their size [3]. Where a conventional processor uses physical transistors to process zeros and ones, a quantum system can harness properties of particles like photons to perform the same tasks [4].

A qubit, or quantum bit, is used to describe the chosen particle to manipulate. The qubit is defined as a unit vector in a two-dimensional complex space, and the polarization of a particle in this space determines the value of a qubit to be a 1 or 0 [3]. This complex space also relates to the concept of superposition. In terms of quantum mechanics, superposition is the principle that any number of qubits can be combined and will result in another completely valid quantum state [5]. It is this principle that allows a qubit to be in infinitely many states at any moment in time.

Although qubits represent an infinite amount of states, only a single bit of data (1 or 0) can be retrieved at once. Furthermore, when extracting data from a qubit the state is then altered as a result [3]. This presents challenges that will be discussed later in the report.

Groups of qubits are also subject to entanglement. Entangled qubits cannot be deconstructed into meaningful information for each qubit individually. This phenomenon has no comparable counterpart to traditional computers, which leaves the possibilities for its use, if any, up to the engineers.

The Relevance of Moore's Law

Moore's Law is the idea that computer processing power will double every two years. This rule has held true until the 2000s, when progress on increasing processor speed began to decline. The frequency a processor operates at, commonly measure in gigahertz, began to remain in the same range, but the processors were still improving in other ways. In order to continue relevance, the law was revised to describe the doubling of the number of transistors every two years instead of just raw power [6].

This revision led to some companies abandoning the concept, while others continue to accept it. However, quantum computing will likely invalidate the law altogether. Not only do these computers operate without the use of transistors, but the processing power won't just double, but multiply by the hundreds or thousands. Another revision, or new law entirely, may have to be required in order to account for quantum computers.

The Progression of Quantum Computing

As with any new technology, the initial implementations tend to be inefficient or rudimentary. The goal is to get a working configuration in any way possible, then make improvements moving forward. Quantum computing is no exception concept. In 1994, Peter Shor discovered important algorithms that enabled logarithms and factoring for a quantum computer. Shor's factoring algorithm was extremely fast at finding the prime factors of any number, even large ones, which has many uses; most notably is the ability to crack modern cybersecurity measures, like string passwords, with ease [7]. Naturally, this generated quite a buzz around quantum computing. The idea had not yet been realized, but scientists and engineers believed in its possibility and continued to innovate.

The Birth of Quantum Computing

In 1997, Daniel Loss and David DiVincenzo from the University of Basel and IBM respectively proposed the Loss-DiVincenzo quantum computer, which implemented qubit gates from the mechanic that allows rotation to change states [8]. Soon after in the following year, the first tangible and successful quantum computing experiment took place. This version of quantum computing utilized nuclear magnetic resonance (NMR) and molecules of a chloroform solution to create a system that had four possible states.

Figure 3. A typical molecule sample.

Figure 4. An NMR spectrometer. Images obtained from USCB [10].

Using this system, the scientists were successfully able to implement a search algorithm in fewer steps than a traditional computer and read the result afterwards [9]. A physical working prototype proved the possibility and potential of quantum computing, which meant it was full steam ahead for scientists and engineers. In the next few years, slow but fundamental progress was being made; for instance, IBM's demonstration in 2001 of the first quantum computer to fully implement Shor's algorithm, which was also built in a test tube [11]. However, as knowledge spread and interest grew, innovations began to occur faster than ever before. Determined minds from around the world began to fully implement and realize quantum computers, and the idea was no longer just that.

Modern Quantum Computers

Seemingly starting in 2006, progress on quantum computing began to grow significantly. Physicists devised an efficient way to generate and manipulate photons at low temperatures to potentially be used for quantum computers or cryptography [12]. This was done by combing multiple precise layers of silicon to create a perfect mirror for reflecting light; an important milestone which potentially reduces requirements for strictly controlled operating environments.

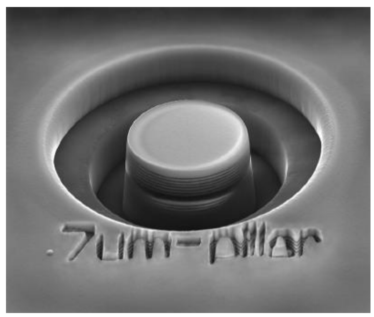

Figure 5. A multilayer micropillar capable of producing a single photon (Soft Machines, 2006). Image by Wen-Chang Hung.

Later that year, physicists for the U.S. department of Energy developed a new theory that allowed the spin of particles to be manipulated without using powerful electromagnets [13]. Not only would this would allow new quantum computing technology to be far more efficient, but also potentially decrease the physical size of the machines.

In the following years, the wave of innovation continued. The idea of memory for quantum computers began to take shape when scientists were able to store the state of a photon for 8 microseconds, then read it again [14]. A short amount of time such as this may seem insignificant; however, it is crucial because prior to this point the state of a qubit could not be read without altering it. Not long after, physicists from Bristol University were able to build the first NOT gate controlled by a single photon [15]. This photon gate was also embedded onto a silicon chip, which allows many to be used in unison for a multitude of different applications and configurations. The idea of these “building blocks” can be loosely compared to the transistors of traditional computers; as they decrease in size more of them can be combined to increase speeds. Professor Jeremy O’Brien, who led the group of researchers, stated that this “is a crucial step towards a future optical quantum computer, as well as other quantum technologies based on photons” [15].

D-Wave Systems, a company specializing in quantum computing, took notice of the growing interest and innovation and began developing machines of their own that would be commercially available. The D-Wave One was announced in May 2011, which boasted a 128-qubit processor [16]. However, there was a major limitation of this quantum computer; it was designed for optimization problems only, which prevents its use as a general computer. This system may not have seen much commercial success, but it was an important step towards bringing quantum computers to the mainstream.

The Industry Standard

As the technology and research marched onward towards present day, D-Wave continued to release updated quantum computers with each revision a vast improvement over the last. Large companies like Lockheed Martin, Google, and even NASA began purchasing D-Wave computers after realizing their incredible potential. Ned Allen, Lockheed Martin's Chief Scientist, "sent D-Wave a sample problem to run on its system. It was a 30-year-old chunk of code from an F-16 aircraft with an error that took Lockheed Martin's best engineers several months to find. Just six weeks after sending it to D-Wave, the software error was identified" [17].

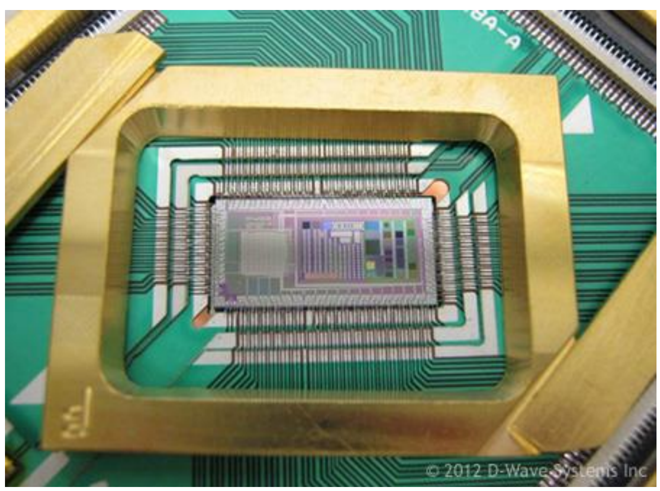

Figure 6. A quantum processing unit being bonded to the circuit board (D-Wave Systems, 2012). Image by D-Wave Systems.

It was not long before the major tech companies such as IBM, Google, and Intel saw the potential in the market as well, and announced plans for commercial quantum computers of their own.

References

[1] Intel, “From Sand to Silicon: The Making of a Chip Illustrations,” May 2009. [Online]. Available: www.intel.com/pressroom/kits/chipmaking. [Accessed May 7, 2019]

[2] “Diameter of a Human Hair,” 2011. [Online]. Available: https://hypertextbook.com/facts/1999/BrianLey.shtml. [Accessed May 7, 2019]

[3] E. Reiffel and W. Polak, "An Introduction to Quantum Computing for Non-Physicists," *ACM Computing Surveys*, September 2000. Available: Computer Database, http://link.galegroup.com.libproxy.oit.edu/apps/doc/A74089509/CDB?u=s8375154&sid=CDB&xid=f7ed33b9. [Accessed May 1, 2019]. [Accessed May 7, 2019]

[4] Wikipedia, “Qubit,” March 2019. [Online]. Available: https://en.wikipedia.org/wiki/Qubit. [Accessed May 10, 2019]

[5] Wikipedia, “Quantum superposition,” April 2019. [Online]. Available: https://en.wikipedia.org/wiki/Quantum_superposition. [Accessed May 10, 2019]

[6] “Moore’s Law.” [Online]. Available: http://www.mooreslaw.org/. [Accessed May 12, 2019]

[7] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *35th Annual Symposium on Foundations of Computer Science*, 1994. Available: https://doi.ieeecomputersociety.org/10.1109/SFCS.1994.365700. [Accessed May 14, 2019]

[8] D. Loss and D. DiVincenzo, "Quantum Computation with Quantum Dots," January 1997. Available: https://arxiv.org/abs/cond-mat/9701055. [Accessed May 14, 2019]

[9] I. Chuang, "Experimental Implementation of Fast Quantum Searching," *Physical Review Letters,* April 1998. Available: https://pdfs.semanticscholar.org/6c05/5053f4f1605fdc0bd474c7a350dcd01f627d.pdf. [Accessed May 14, 2019]

[10] University of South Carolina Beaufort, "Nuclear Magnetic Resonance Quantum Computing (NMRQC)." [Online]. Available: http://web.physics.ucsb.edu/~msteffen/nmrqc.htm. [Accessed May 14, 2019]

[11] IBM, "IBM's Test-Tube Quantum Computer Makes History," December 2001. [Online] Available: https://www-03.ibm.com/press/us/en/pressrelease/965.wss. [Accessed May 14, 2019]

[12] R. Jones, "The best of both worlds – organic semiconductors in inorganic nanostructures," *Soft Machines,* March 2006. Available: http://www.softmachines.org/wordpress/?p=215. [Accessed May 15, 2019]

[13] Argonne National Laboratory, " Spinning new theory on particle spin brings science closer to quantum computing," September 2006. [Online]. Available: https://phys.org/news/2006-09-theory-particle-science-closer-quantum.html. [Accessed May 15, 2019]

[14] "Scientists succeed in storing quantum bit," *EE Times,* September 2006. [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1249860. [Accessed May 17, 2019]

[15] CMP Media, "Physicists Build First Single-Photon Logic Gate; Bristol University physicists advance the field of quantum computing with the successful miniaturization of a high-performance, optical 'controlled-NOT gate.'," *InformationWeek*, April 2008. Available: http://link.galegroup.com.libproxy.oit.edu/apps/doc/A191319614/CDB?u=s8375154&sid=CDB&xid=8cd9190b. [Accessed May 17, 2019].

[16] S. Anthony, "First Ever Commercial Quantum Computer Now Available for $10 Million,"*ExtremeTech*, May 2011. [Online]. Available: https://www.extremetech.com/computing/84228-first-ever-commercial-quantum-computer-now-available-for-10-million. [Accessed May 19, 2019].

[17] D-Wave Systems. [Online]. Available: https://www.dwavesys.com. [Accessed May 19, 2019].