Quantum Computing: Time for Change?

By: Jordan P Lydon

With the advent of modern computing and the desire to always have more compute power and faster access to data, some companies are beginning to look towards different options to potentially be on the forefront of the future of computing. A lot of big names in the technology industry, such as Microsoft, IBM, Intel and Alphabet, are investing in quantum computing looking to be the first to bring the technology to the mainstream computing world. The return on investment for these companies could be potentially enormous if quantum computing becomes viable for long-term mainstream use in server or workspace environments. The potential advancements that stand to come from moving to quantum wafers also come with their own set of risks, costs, education and security considerations.

To understand the potential benefits of an alternative data computing method, we first need to establish a basic understanding of modern traditional compute methods, namely, traditional silicon processing chips. The architecture currently used to mass produce central processing units (CPU)'s relies on silicon-based wafers with a large number of transistors. Throughout the process copper is added to the wafer to increase conductivity and lay a path for electricity to flow and power the finished die. Once a die has been completed and passed through testing, it is attached to a substrate with a heat spreader. The heat spreader is used in conjunction with a CPU cooler in a completed machine to transfer the large amount of heat generated by the die away from the CPU itself and out into the surrounding environment.

Quantum wafers differ from standard CPUs in a few ways, the main difference being the way that quantum processors handle data. Standard CPUs use strings of 1's and 0's to compute and calculate data, this way of computing data is less efficient than quantum computing. Quantum wafers also operate on a more subatomic level by manipulating electrons magnetically to process data versus relying on transistors in standard CPUs. Quantum computing uses something called

"Qubits" in place of bits and bytes found in normal computer processing. We will delve into Qubits in the next paragraph and how they differ from standard CPUs and make computing more powerful and more efficient overall.

With standard CPUs, the processing scheme is broken into bits. As previously mentioned, bits are a string of 1's and 0's that are used to transport instructions between the CPU and the rest of the computer. While this approach is reliable, it is old and outdated compared to the way quantum wafers handle data. A wafer computes data in such a way that allows it to detect or use values that fall between 1's and 0's. This allows more data to be passed through the wafer and computed making the process more efficient and gives faster access to data that needs to be computed. However, such a boost in efficiency does not come cheap.

One consideration that has yet to be discussed is the difference in cost for businesses and consumers alike that want to adopt quantum technology. Since quantum wafers are not yet in full mass-production or available in a retail storefront the pricing is mostly speculation. The speculated price is somewhere in the three to five-million-dollar price range for an entire system built based on quantum technology. As time goes on and the production processes are refined, and more quantum machines are produced this cost will drop but early adopters will have to pay a premium. Currently the adoption of quantum computing is slow if not completely non-existent, due to the cost, but the first companies to really roll out quantum technology will see some return on their investment as they will be able to work more efficiently, process more data and allow for a higher amount of revenue due to the increased computing power. Now that you have a better understanding of quantum computers, another question is what can they do in the security space?

Many people in the security space feel that quantum computing could pose a large threat to security, saying things like "Quantum computers pose a security threat that we're still totally unprepared for" (Giles, 2018) Many professionals think that we are far behind the curve of security when it comes to the implementation of quantum computers stating "it could take at least 20 years to get quantum-proof encryption widely deployed." (Giles, 2018) and while I don't think this thought is outlandish, I'd like to play devils advocate and examine the potential good quantum computers could do in the security space. While I know there is no way to guarantee that something like a quantum computer is only used for good, what would it mean if they were? These machines compute data at such a fast rate, they could potentially identify threats before one had time to manifest itself. A quantum computer could also theoretically actively scan every single file entering and exiting a network or device without there being any notable slow down or performance decrease. "No matter how much computing power is dedicated to solving quantum-based security implementations, they'll still provide a safe conduit to send data through." ("How Will Quantum Computing Impact Cyber Security? |", 2018) I think this quote is extremely pertinent to the discussion of quantum computers because they will provide a safe avenue for data to travel once they have been implemented and had time to be develop new security hashing algorithms. Once new security methods have time to be researched and implemented the computing world would almost certainly continue down the same path it is currently on. The only difference would be the amount of data that could be processed and how fast certain types of work could be done. Now, unfortunately this does not completely detract from the potential of quantum computer use for nefarious purposes.

Quantum computers could stand to potentially be used for nefarious purposes like hacking or cyber warfare against other nations. These computers are so powerful, they could cripple any system that relies on computers to properly run. These systems in the United States include traffic control devices, power management systems, security systems, internet backbone servers, phone providers, etc. While all of these systems are currently protected with normal security measures, those measures could easily be negated by a quantum computers raw power. If another country who does not like the United States were to come into this technology first, they could pose a very real threat to our nation or any nation of their choosing. This is one of the biggest fears behind quantum computer adoption, the big what-ifs of data security should these machines become a common use item.

Cyber-attacks and cyber warfare have been increasing steadily against the United States for quite a while now. With more companies here developing products and safeguarding trade secrets in the United States, the potential for a big score is there and many hackers know that and that is what they are after. Most of these attacks originate in Russia and China. If a quantum computer were to get into the hands of one of these countries, the United States would become very vulnerable very quickly and that would be a tremendous issue. It wouldn't just put citizens personal information at risk, an attack could potentially leave America at a standstill. Our power grids could be tampered with, phone networks, emergency radios, the internet could be taken control of by a foreign attacker and cripple our economy. In December of 2018, the United States along with other countries around the world found that China had been conducting cyber espionage for almost 12 years trying to steal trade secrets. Not all of the attempts were successful, but had the Chinese had something as powerful as a quantum computer, that outcome would almost certainly be different.

With all of that said, these computers could potentially be an amazing resource for every country in the world, but in the wrong hands they could also mean terror and destruction. The adoption of quantum machines will be a balancing act for all that choose to make use of the devices, making sure that the devices are in good hands and being used for good rather than bad.

I think that these machines stand to do a lot of good in almost every avenue of business that they are used in, but we do need to be cautious of how fast the technology is adopted and who we know has access to machines these powerful.

Works Cited

Deagon, B. (2019, February 22). Quantum Computing Companies Aim Technology Higher. Retrieved from https://www.investors.com/news/technology/quantum-computing-companies-aim-technology-higher/

Giles, M. (2018, December 05). Quantum computers pose a security threat that we're still totally unprepared for. Retrieved from https://www.technologyreview.com/s/612509/quantum-computers-encryption-threat/

How Will Quantum Computing Impact Cyber Security? |. (2018, March 28). Retrieved from https://www.technative.io/how-will-quantum-computing-impact-cyber-security/

Nguyen, T. A. (2009, July 18). Intel Shows How A CPU Is Made. Retrieved from https://www.tomshardware.com/picturestory/514-intel-cpu-processor-core-i7.html#s29

Significant Cyber Incidents. (n.d.). Retrieved from https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

(n.d.). Retrieved from http://www.cpushack.com/MakingWafers.html