Matt Russotti
AU23 CSE2501
Word Count: 990

The Ethical Implications In The Development Of Quantum Computing

Matt Russotti
AU23 CSE2501
Word Count: 990

Section 1

In this essay we will ask, Is it ethically justifiable to develop quantum computing despite its risks to data security? Competing views on this topic include supporters who believe it is ethically justifiable due to the advancements we would make in drug discovery, materials science, and solving optimization problems. The opposition believes that the threat of developing a quantum computer to existing encryption methods poses a risk to data security that is greater than the benefits it would provide. I believe that it is necessary to develop this technology due to the benefits as mentioned earlier, but also to support the development and adoption of quantum encryption algorithms and proper legislation to hedge the negative impact quantum computing could bring. An implication of my answer to that ethical question is the need for a global framework for quantum computing development to ensure ethical considerations.

Section 2

Recent advancements in quantum computing from labs such as Google and IBM have brought the concept closer to practical realization. Given the profound implications of this technology, especially for data security, is it ethically justifiable to pursue its development?

The internet currently relies on encryption in many ways. Some examples are to protect data as it’s sent across the internet, to create digital signatures to verify the authenticity of a message or piece of information, SSH, and most importantly SSL and TSL protocols which secure most of the data sent over the internet (Golden).

Matt Russotti
AU23 CSE2501
Word Count: 990

This critical infrastructure relies on the fact factoring large prime numbers is computationally difficult and if you follow US Government recommendations it would take a classical computer thousands of years to break that encryption. However, due to the unique properties of quantum computers, they can factor those numbers in a fraction of that time, compromising the encryption. This is possible because of Shore's algorithm (Golden).

As you can see the research and development of quantum computers poses a threat to internet security as we know it. What needs to be done and who is responsible for doing it?

Section 3

The first answer to our ethical dilemma is to focus on the benefits that developing quantum computing will bring. It would enable us to discover all kinds of drugs to cure diseases, improve quality of life, and increase life expectancy (Bova). Advancements in material science will allow us to develop better, cheaper, and more sustainable materials. This is especially important as climate change and sustainability are at the forefront of some of the issues today. Another important development would be improved batteries. That addresses the issue of finding an efficient way to store electricity and would overall lead to less harmful waste from current disposable batteries made from rare earth metals that are gathered in unethical manners. Another example the benefits from developing quantum computers are optimization problems. This could mean anything from "reducing materials waste on a production line, scheduling delivery fleets

more efficiently, and minimizing risk while maximizing gains across a financial portfolio" (Tyrrell). Improving the efficiency of our societal systems allows for the better utilization of finite resources which is generally considered a good thing. Better financial models can help hedge against unforeseen market forces and reduce the impact of recessions on our economy.

The most common argument to oppose the development of quantum computers is the threat to internet security. To fully understand this threat we must understand what encryption is, why its important, and how it is at risk. Encryption, put simply, is the process of converting information or data into a code to prevent unauthorized access (Rafter). The importance of encryption is pretty obvious, not all information on the internet should be accessed by everyone. If this were the situation, online shopping would become untenable, anyone could access the passwords safeguarding your accounts, and the concept of privacy would essentially vanish. In an age where we rely on the Internet for so many things, not having internet privacy isn't feasible and is something to be concerned about. In the late 90's a mathematician named Peter Shor developed an algorithm that can theoretically break public key encryption which is the basis for internet communication, e-commerce, and encryption protocols like SSL, TLS, and HTTPS (Golden). While an argument can be made for both positions I prefer to take a more moderate approach.

Section 4

Matt Russotti
AU23 CSE2501
Word Count: 990

I believe it is possible to get the benefits of quantum computing while minimizing the downsides through quantum encryption. I justify this by appealing to the utilitarian (Shafer-Landau). The potential benefits from developing this far outweigh the negative impacts and we can take steps to reduce those. I will use the ACM code of ethics to defend my opinion. First, it is our duty to contribute to society and human well-being. The potential benefits as described in the previous section show the magnitude of good quantum computers can bring, from saving lives in the medical industry, producing cheaper and more sustainable materials, and improving the efficiency of processes quantum computing has immense benefits (ACM Code Of Ethics). The second code is to respect privacy. This is why quantum-safe encryption technology is necessary if we are to develop quantum computing, we cannot sacrifice people's privacy (Hanacek, ACM Code Of Ethics). Finally, this will create many new opportunities for all levels of computer science since we are developing a new field previously only existing in academia which combines physics and computer science to bring us new jobs, companies, and career paths for many individuals (ACM Code Of Ethics).

Section 5

Now we accept my proposed solution what are the implications? First of all, we need to invest more resources to influence quantum-safe encryption adoption across the internet as well as put resources into re-encrypting soon-to-be-unsafe data. This process has begun by the NIST but it is critical that these algorithms are operational before quantum computer use is widespread (Hanacek). This will avoid any technical backlash from insecure systems that are lagging behind.

Matt Russotti
AU23 CSE2501
Word Count: 990

Work Cited

Association for Computing Machinery (2018). "ACM Code of Ethics and Professional Conduct". Retrieved January 9, 2023, from https://www.acm.org/code-of-ethics

Bova, Francesco. "Quantum Computing Is Coming. What Can It Do?" *Harvard Business Review,* 23 July 2021, hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do.

Golden, Deborah, et al. "Preparing the Trusted Internet for the Age of Quantum Computing." *Deloitte Insights*, Aug. 2021, www2.deloitte.com/us/en/insights/topics/cyber-risk/crypto-agility-quantum-computing-security....html.

Hanacek, N. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST." *NIST*, July 2022, www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

Rafter Dan, *What Is Encryption? How It Works + Types of Encryption – Norton*. us-stage.norton.com/blog/privacy/what-is-encryption.

Shafer-Landau, Russ (2020). The Fundamentals of Ethics, Fifth Edition. Oxford: Oxford University

Tyrrell, James. "What Are the Benefits of Quantum Computing?" *TechHQ*, 15 Nov. 2022, techhq.com/2022/11/what-are-the-benefits-of-quantum-computing.