Quantum Operating Systems: Opportunities & Challenges

Eric Paulz
Clemson University
Clemson,
South Carolina, USA
epaulz@clemson.edu

Abstract. As quantum systems become more commonplace it is important for us to apply the best practices we have learned from traditional computers to the quantum realm. Challenges that we face in traditional computers will likely be a factor in quantum as well, but the way we deal with them will almost certainly be quite different. Creating a useful quantum operating system may be far down the road, but by exploring some of the individual components of current OSs we can dissect and understand what to consider when developing these next-generation systems.

INTRODUCTION

With every passing day we are getting closer to achieving a goal that has been theorized and conceptualized for decades: the fusion of quantum physics, computer science and computer engineering to create a practical quantum computer. Current quantum computers show promising results, but there is much more work to be done to make this technology readily available to scientists, researchers and everyday people. Companies, organizations and universities around the world, including the CIA, Google, NASA and Cambridge, are investing large sums of money into developing quantum technologies, making it one of the biggest investments in modern disruptive technologies [1].

However, all this promise does not come without some drawbacks. Quantum computing is thought of by many as high-risk, high-reward due to the complex and unpredictable nature of quantum mechanics. In this paper, I will outline some of the opportunities and challenges (mostly challenges) that come with developing these quantum systems. Specifically, I will focus on and compare aspects that relate to traditional operating systems.

QUANTUM OPERATING SYSTEMS

The first electronic computers were expensive and slow. They were primarily only useful to the military for code-breaking and weapon design. Similarly, current quantum computers are expensive and slow. Also, when they become remotely practical, they will likely be initially used to break classical cryptosystems such as RSA [4,5]. However, just as electronic computers have become smaller, cheaper and faster over time, quantum computers will likely follow suit. When this happens, we will surely turn to operating systems to make these computers safer and optimized for everyday use.

FAULT TOLERANCE

One of the challenges that scientists face in creating fault tolerant quantum systems is how to detect errors. From a theoretical standpoint, this problem has already been solved due to a discovery of fault-tolerant quantum computation [2]. However, theory and reality don’t always add up the way we would like them to.

Traditional computers use bits which represent information as 0 or 1. Quantum computers, on the other hand, use qubits which can represent information as 0, 1, or both at the same time (superposition). When a qubit represents 0 and 1 simultaneously, there is a relationship between the 0 and 1 value. This relationship is called phase. This concept is demonstrated in Figure 1.

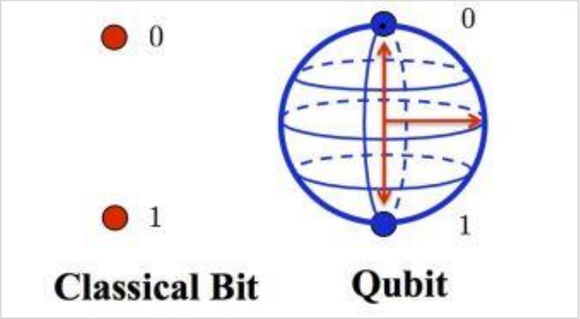

Figure 1: Qubit representations [1]

Sometimes qubits can flip without warning, but we have learned to mitigate this issue since regular bits experience it as well. The problem is that qubits can also experience phase flips; that is, the relationship between the 0 and 1 representation of the qubit changes. Until recently, scientists could only detect one of these errors at a time. However, IBM has developed a new circuit composed of four superconducting quantum bits, configured in a square lattice, that allows detection of both types of quantum errors simultaneously [3]. This is an important step towards developing fault tolerance quantum systems. Fault tolerance is vital to modern data centers and super computers, so if we are aiming to replace or supplement current systems with quantum capabilities, they must be able to recover from errors efficiently.

SECURITY

An FPGA is a programmable integrated circuit that is used in a variety of different applications today. Quantum FPGAs (qFPGA) maybe be a long way off, but we can speculate as to what types of applications they could be useful for. A quantum circuit is similar to a Boolean circuit except it uses quantum gates instead of standard logic gates [4]. A conceptualization of a classical processor and a qFPGA working in tandem can be seen in Figure 2.

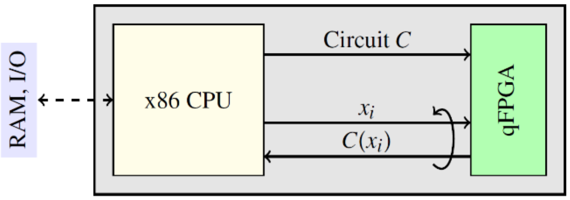

Figure 2: A classical processor connected to a qFPGA [4].

One potential use for a quantum circuit such as this would be password cracking [6,7]. Most current password-cracking methods involve simply creating an extremely large dictionary (*D*) of potential passwords and trying each one until it works. This process takes electronic computers time linear to the size of *D*. One of the prospects of quantum computers is that they will be able to perform many more tasks simultaneously than traditional computers, meaning in this context that they could attempt multiple passwords from the dictionary at the same time. Thus, such a computer would be able to try all guesses in the dictionary much faster than a traditional computer (predicted $\sqrt{len(D)}$)[4]. From this we can see that the power of quantum computing could potentially be used for insidious purposes.

Another thought on this matter is that when traditional computers were making their debut, computer hackers were not really a thing. It didn't take long for people to learn to use the power of computers for less desirable purposes, but nonetheless it took some amount of time to catch on. Today, we have extremely sophisticated hackers and even entire organizations and government agencies with branches dedicated to computer attacks. This likely means that as soon as quantum technology is made available to the world, these entities will have ways of exploiting it. For this reason, we must take extra care to make these systems as safe and friendly as possible from the beginning.

SCALING

In order to measure a quantum computer's power we need two metrics. The first is its qubit count. In short, the more qubits you have the more computational power you have. However, this power must be kept in check. This brings us to our second metric which is error rates. In order for a qubit to be useful we must make sure that the work it does is accurate. The combination of these two metrics gives us quantum volume. Quantum volume measures the relationship between number and quality of qubits, circuit connectivity, and error rates of operations [8]. As we continue to develop more advanced quantum systems, quantum volume will (potentially) increase to the point where these systems are more useful than traditional computers.

CONCLUSION

If done right, quantum technologies could completely change the world and effectively revitalize Moore's Law which has been dwindling as of late. This new age of computing could unlock countless new opportunities, some of which cannot even be fathomed given our current understanding. However, as always, with great power comes great responsibility. We must do our best to be sure that these systems are used for the greater good. A formal quantum operating system would help to ensure security and practicality for mass use of quantum technologies.

REFERENCES

[1] Anthony Cuthbertson. 2015. *Quantum revolution: UK strategy outlines research into 6G smartphones and quantum computers.* (March 2015). Retrieved November 29, 2018 from https://www.ibtimes.co.uk/quantum-revolution-uk-strategy-outlines-research-into-6g-smartphones-quantum-computers-1492896

[2] A.Yu. Kitaev. 2003. *Fault-tolerant quantum computation by anyons.* Annals of Physics 303. (2003).

[3] George Rajna. 2015. *Operating System for Quantum Computing.*

[4] Henry Corrigan-Gibbs, David J. Wu, and Dan Boneh *Stanford University*. 2017. *Quantum Operating Systems*. In Proceedings of HotOS '17, Whistler, BC, Canada, May 08-10, 2017, 6 pages. https://doi.org/10.1145/3102980.3102993

[5] Peter W. Shor. 1997. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. Siam j. Comput. 26, 5 (1997), 1484-1509.

[6] Joseph Bonneau. 2012. *The science of guessing: analyzing an anonymized corpus of 70 million passwords*. In Symposium on Security and Privacy. IEEE, 538-552.

[7] Robert Morris and Ken Thompson. 1979. *Password security: A case history*. Commun. ACM 22, 11 (1979), 594-597.

[8] IBM. *Scaling quantum systems.* Retrieved November 29, 2018 from https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/