The Quantum Leap
May 17, 2022

Quantum Computing is the "Manhattan Project" of This Generation

Imagine that your great-great-great…. great grandfather was alive at the beginning of the modern era. Alive at 0 BCE. Imagine he invested one penny in an account that would earn just 2% per year. Can you guess how much that account would be worth today?

That penny, compounding at only 2% per year for 2,022 years would be worth **$2.4 TRILLION dollars today**. That measly penny. This is the power of compounded interest, which is a function that grows exponentially, and I point out to emphasize how powerful exponential growth can be. Quantum Computers (QCs) have the power to provide exponential speedup in processing power.

Exponential math is difficult to appreciate so I hope the penny analogy helps provide some context. I'm not going to explain the math or the underlying QC principles that govern this power, so for the sake of this post, try and just appreciate the fact that Quantum Computers are exponentially more powerful than existing computers. (For those interested in more of the details, please see a prior post on superposition and entanglement which you can read here).

Information is Power

If we think about the advances of humankind, the societies with the most advanced technology generally out-lived or out-powered their neighboring societies. Survival of the fittest to some extent. Unfortunately, this has manifested in some barbaric says, such as with the settlers to the North American continent and those who created the slave trade by overpowering African societies. The guns and weaponry of those explorers/exploiters simply overpowered the native people. Mankind has a history of using its resources to its advantage and of one society enslaving another. This is not a pollical post and I am not intending to condemn any person or peoples (although please be clear I am not glorifying them either), I am simply pointing out that human nature has shown that societies will leverage their technological superiority in self-interested ways.

Information is Power and Power is Money

Some of you may be familiar with the acronym "HNDL", which stands for "Hack/Harvest Now, Decrypt Later." It is also sometimes referred to as the Q2K challenge because it is describing that in the not-to-distant future (some say 2-3 years, some say 5-10 years) Quantum Computers will be able to break RSA encryption. RSA encryption is the de-facto world security standard that is used continuously to make on-line interactions and payments secure. It is based on

mathematics that are too difficult for classical computers, to provide "keys" or encryption codes to secure digital assets and transmissions. Imagine for a minute that you are the first to build the QC that can break RSA. You would have the power to read nearly any secret message sent over the Internet and could hack into an untold number of digital wallets and financial accounts. Imagine the power and wealth you would have with such a machine. Bad actors are accumulating encrypted information now, with the intent of holding it until they have access to powerful enough QCs to break the encryption as soon as they are able. It's not a matter of if, it's a matter of when. In fact, the algorithm to break RSA is already written! It is known as Shor's Algorithm and it is open sourced and available to anyone from any country (don't take my word for it, you can find it here). All that is required is a powerful enough QC to run the code. The race to build that machine is on.

There is a reason China has dedicated over $10 billion to its national Quantum Computing efforts. If China or some other rogue nation or group gets access to a powerful enough Quantum Computer, you can imagine what self-interested things they might do with it. Hack all the cryptocurrency wallets, mine all the remaining bitcoin, steal money from financial accounts, steal competitor secrets, etc. There is a massive global race to create more and more powerful Quantum Computers (see the "Follow the Money" post here for more details). And while much of this post has been focused on the nefarious uses some might apply with their new QC, there are also enormously positive things that can be achieved. New medicines, more efficient solar panels and rechargeable batteries, cheaper fertilizers, more efficient logistics, plus the many, many new applications that this new computing power will enable. For good or for bad, Quantum Computers will lead to immense wealth creation and concentration.

The Quantum Computing "Manhattan Project"

The US's efforts to build the atomic bomb during WW II became known as "The Manhattan Project." The famous $E=MC^2$ equation indicated the massive amount of energy that could be released from a relatively small amount of matter (you will note that exponential power again with "C" or the speed of light being squared). The world powers during World War II were in a desperate and furious race to create an atomic bomb first. It was a national imperative and substantial resources were directed at the effort. The bomb was theoretically possible, but at the time, there was no clear path to an actual atomic weapon. However, its potential was well understood, and the underlying science and technology kept pushing the envelope. It was an existential threat. It was urgent. If the Nazi's had gotten there first (and they very nearly did), I expect we would be living in a very different society today. The power and potential for QCs is well established based on the power of quantum superposition, entanglement, and related quantum effects. The exponential speedup can already be calculated, now it is a matter of time before the machines achieve the massive speedup that is possible.

Quantum Computing is the existential threat of today. This is not hyperbole or some doomsday prediction. The power of Quantum Computing is undeniable. Having the most information and/or the most powerful processer of that information will create an enormous competitive advantage. China is pushing hard to make QCs. They already have a quantum satellite, "Micius," orbiting the planet, which has successfully demonstrated inter-continental secure quantum transmission. The power of Quantum Computing is well known and the physics of creating working machines is evolving rapidly. Actual, working Quantum Computers exist today, albeit they are not yet more powerful than classical computers. They need to scale up,

which is challenging but doable, and substantive progress is being made rapidly. There is ample motivation and over $25 billion in global investment in the space. Somebody will get there first. It will happen in this decade.

What does this mean?

It means that the world is on a path to quantum advantage. The estimated timelines to the arrival of practical, useful QCs even in the NISQ era (the N stands for "noise"), are getting shorter not longer. Advances are being made continually. It will not be a straight line. I am certain that the vagaries of the markets will cause capital flow and valuations to be spikey. And many exciting new quantum companies will not survive. Those who invest in the winners will enjoy significant outsized financial gains, and those who back the companies that do not survive, will lick their wounds. But as an industry, the race is on, the potential rewards are massive, and the clock is ticking. I sure hope that whoever wins the race uses the power to do good in the world. Stay tuned to this blog to follow the winners and losers.

References:

Nowakowski, Tomasz, "China's 'Micius' Satellite Demonstrated Intercontinental Quantum Key Distribution for the First Time," Spaceflight Insider, January 22, 2018.

O'Neill, Howard, "The US is worried that hackers are stealing data today so quantum computers can crack it in a decade," MIT Technology Review, November 3, 2021.

Coker, James, "Security Teams Should Be Addressing Quantum Cyber-Threats Now," InfoSecurity, April 26, 2022.

If you enjoyed this post, please visit my website and enter your email to receive future posts and updates: http://quantumleap.blog

Russ Fein is a venture investor with deep interests in Quantum Computing (QC). For more of his thoughts about QC please visit the link to the left. For more information about his firm, please visit Corporate Fuel. Russ can be reached at russ@quantumleap.blog.