The Quantum Leap
November 21, 2021

Quantum Quantum Everywhere

Quantum Mechanics in Everyday Life, Near Term Use and Future Quantum Computing Applications

In prior posts, I conveyed some of the underlying reasons why Quantum Computers can do things that existing digital computers cannot do or would take prohibitively long to do. In this post I will cover some of the near-term use cases for Quantum Computing, but first I want to cover how "Quantum" or, specifically, the quantum mechanics underlying the power of Quantum Computing, is already used in our daily lives, some near term applications where quantum effects are providing powerful new capabilities, and finally, where the power of Quantum Computing will likely have the most impact.

Quantum Mechanics in Everyday Life

Anyone trying to learn about Quantum Computing or quantum mechanics is likely baffled by how to picture it in your head in a relatable way. Because quantum mechanics occurs on a scale so small and the physics are wholly unfamiliar, it is an intimidating field and very difficult to visualize. However, we use and benefit from quantum mechanics every day without understanding the underlying physics. Here are some examples (Choudhury, 2019):

1. Electronic Appliances: If you notice the heating elements in your toaster, you are witnessing a quantum mechanical application of electricity as evidenced by the red glow which is the power being converted to heat.

2. Computers (transistors and microchips): The core transistors in every computer (and in the chips used in many other modern products) work via semiconductors, where the electrons behave like waves, which is a core principle of quantum physics.

3. LED's: Like transistors, LEDs are made of two layers of semiconductor, which are caused to meet and to release the energy applied by the power source, again a quantum physical action.

4. Lasers: Lasers produce their monochromatic light via a form of optical amplification based on the stimulated emissions of photons, another quantum physical process.

5. MRI's: Magnetic Resonance Imaging works by flipping the spins in the nuclei of hydrogen atoms.

6. GPS: the ubiquitous Global Positional System, where the interconnected satellites, using atomic clocks, use principles of quantum theory and relativity to measure time and distance.

7. Incandescent Bulbs: Like with the toaster noted above, current passes through a thin filament and makes it hot, which causes it to glow, which creates visible light—all quantum mechanical processes.

8. Sensors: Nearly all of us have digital cameras or use the cameras in our phones. These cameras use a lens to collect and convey photons, which the sensor, a form of semiconductor, converts to a digital image.

Hopefully, these examples give you the confidence to appreciate that quantum physics impacts your everyday life without any need to understand the underlying physics. Let's use that baseline to now explore applications of quantum physics in quantum sensing, quantum communications and, finally, Quantum Computing.

Quantum Sensing

Quantum sensing has a broad variety of use cases including enhanced imaging, radar and for navigation where GPS is unavailable. None of these uses require entanglement, so these are much nearer to actual utilization than robust Quantum Computers.

Probes with highly precise measurements of time, acceleration, and changes in magnetic, electric, or gravitational fields can provide precise tracking of movement. In this case, if a starting point is known, the exact future position is also known, without the need for external GPS signals, and without the ability for an adversary to jam or interfere with the signals, so this is of particular interest to the military.

Another application of quantum sensing involves *ghost imaging* and *quantum illumination*. Ghost imaging uses quantum properties to detect distant objects using very weak illumination beams that are difficult for the target to detect, and which can penetrate smoke and clouds (Shapiro, 2008). Quantum illumination is similar and can be used in quantum radar.

Tabletop prototypes of these quantum sensing applications have already been demonstrated and have the nearest-term commercial potential (Palmer, 2017).

Quantum Communication

The primary near-term application of quantum mechanics in communications involves quantum key distribution (QKD). QKD is a form of encryption (more on encryption below) used between two communicating parties who encode their messages in transmitted photons. Due to the quantum nature of photons, any eavesdropper who intercepts a message encoded with QKD will leave a telltale sign that the data stream was read since the act of viewing a photon alters it (a fundamental principle of quantum dynamics). For this reason, quantum-secure communication is referred to as "unhackable". This principal has already been shown over fiber optics and across line-of-sight towers (both of which have limitations on distance) and has recently been demonstrated by China via satellite. China launched the *Mozi* satellite in 2018 and beamed a completely secure QKD encrypted message between China and Austria (Liao et al., 2018). And this past month, the CAPSat, quantum communication satellite, a collaboration between

University of Illinois Urbana-Champaign and the University of Waterloo, was placed into orbit by the ISS, and is designed to test unhackable quantum communications. So long-range quantum communication is already becoming a reality (Schwink, 2021).

Quantum Computing

So far in this post I have shown you how quantum physics already impacts your everyday life as well as some new applications that are already in use or have shown success via prototypes, so will be utilized near-term. The least commercially developed feature of quantum physics, but the most profoundly beneficial, involves the *superposition* and *entanglement* of qubits in Quantum Computing [covered in detail in the prior post].

I want to make clear that "Quantum Computers" are not all-powerful supercomputers that will replace existing binary-based computers. An essential feature of Quantum Computing lies in the exponential increase in its computing power as you increase the number of entangled qubits which distinguishes it from digital computing for certain types of calculations or problems. The most fundamental areas where this exponential speedup is valuable applies to an area known as *combinatorics*. Let me provide an example to set the stage for this discussion.

Assume you manage a networking group, and you are planning the seating chart for this month's meeting where eight members are going to attend. You want to arrange the seating so that you help optimize the networking opportunities as well as respect seniority by having certain members sit facing the door, etc. (the reasons are not important, just assume that the seating chart has many nuances). You may think this is an easy exercise—for example, put Alice and Bob next to each other, but not next to Charlie since they already know each other. Put Sam closest to the door, etc. However, it turns out that there are **more than 40,000 different seating arrangements with just 8 people** (for those trying to decipher the math, it is 8! or 8 factorial, meaning place any of the 8 attendees in the first seat, then any of the 7 remaining attendees in the next seat, etc., or 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1 = 40,320 different seating combinations). This may seem more complicated than you expected, but intuitively you may feel that you could work it out if you had to.

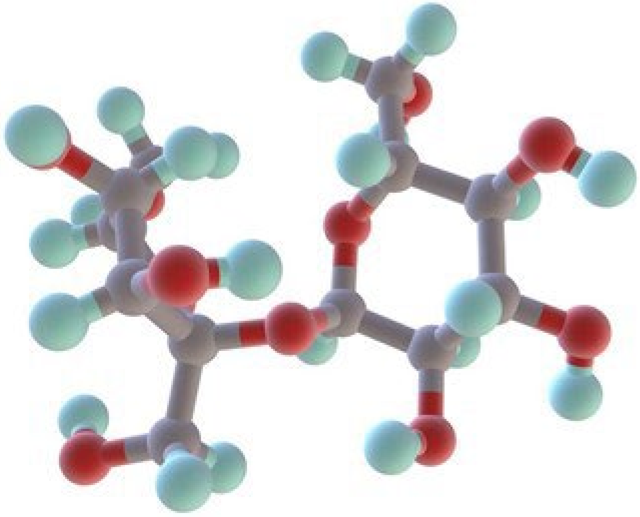
However, imagine that at next month's meeting you have 16 members attend and want to be equally diligent in the seating arrangement. For this meeting there are now **20,922,789,888,000 different seating arrangements possible, or more than 20 trillion! With just 16 people** (16x15x14x….). This defies logic but is simple factorial math. Now, I am not suggesting we need Quantum Computers to help with seating charts, but a seating chart represents a typical "optimization" challenge. For certain instances, as you increase the number of inputs, the potential *combinations* become unmanageable very quickly, hence the reference to *combinatorics*.

Where will Quantum Computers Provide Near-Term Results?

The superposition and entanglement of qubits enables Quantum Computers to consider many combinations simultaneously instead of linearly, hence the tremendous speed-up in processing. Let's now dig into two areas where Quantum Computers can use these features to provide a "*quantum advantage*" in the ability to process currently unmanageable *combinatorial* problems, namely simulation/optimization and cryptography.

Simulation and Optimization

For optimization, you can imagine our networking seating problem as analogous to molecular modeling for things such as drug development or materials science.



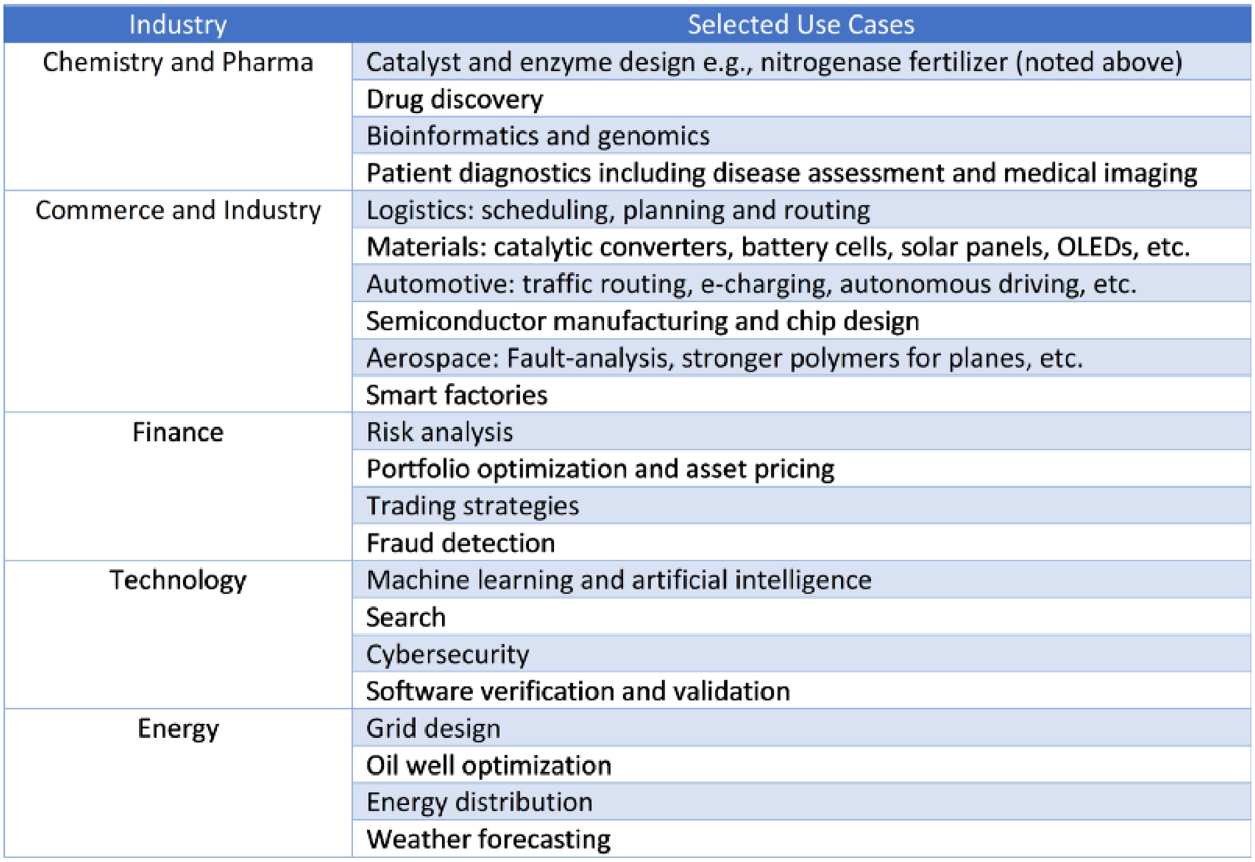
PASIEKA/Getty Images

In these cases, as you tweak the atoms or molecules or proteins you are studying, the numbers of different alignments or configurations increases quickly, like shown with the seating chart example. A powerful Quantum Computer could simulate and evaluate many potential configurations simultaneously and could dramatically accelerate advances in these fields. Here are some examples where Quantum Computers can accelerate computational problems:

· **Simulation**: Simulating processes that occur in nature and are difficult or impossible to characterize and understand with classical computers, which has the potential to accelerate advances in drug discovery, battery design, fertilizer design, fluid dynamics, weather forecasting and derivatives pricing, among others.

· **Optimization**: Using quantum algorithms to identify the best solution among a set of feasible options, such as in supply chain logistics, portfolio optimization, energy grid management or traffic control.

The table below highlights additional examples of fields where Quantum Computing speedup will manifest:



Industry	Selected Use Cases
Chemistry and Pharma	Catalyst and enzyme design e.g., nitrogenase fertilizer (noted above)
	Drug discovery
	Bioinformatics and genomics
	Patient diagnostics including disease assessment and medical imaging
Commerce and Industry	Logistics: scheduling, planning and routing
	Materials: catalytic converters, battery cells, solar panels, OLEDs, etc.
	Automotive: traffic routing, e-charging, autonomous driving, etc.
	Semiconductor manufacturing and chip design
	Aerospace: Fault-analysis, stronger polymers for planes, etc.
	Smart factories
Finance	Risk analysis
	Portfolio optimization and asset pricing
	Trading strategies
	Fraud detection
Technology	Machine learning and artificial intelligence
	Search
	Cybersecurity
	Software verification and validation
Energy	Grid design
	Oil well optimization
	Energy distribution
	Weather forecasting

Source: Bobier et al, 2021

Here are examples regarding a few of these applications along with some of the companies already deploying early quantum computing programs:

· Today, most new drugs are formulated by trial and error and the time between finding a new drug molecule and getting it into the clinic averages 13 years and costs up to $2 billion. If we can use Quantum Computers to model various drugs *in silico*, instead of the through trial and error of lab experiments, we could shorten this timeline and decrease the overall costs. Recently, healthcare giant **Roche** announced a partnership with **Cambridge Quantum Computing** to support efforts in research tackling Alzheimer's disease. And synthetic biology company **Menton AI** has partnered with quantum annealing company **D-Wave** to explore how quantum algorithms could help design new proteins with therapeutic applications.

· Fertilizers are crucial to feeding the world's growing population because they allow food crops to grow stronger, bigger, and faster. More than half of the world's food production relies on synthetic ammonia fertilizer which is created by the Haber-Bosch process which converts hydrogen and nitrogen to ammonia. However, this process has an enormous carbon footprint including the energy needed to perform the conversion (some estimate this to be 2%-5% of ALL global energy production) as well as the huge amount of carbon-dioxide by-product it emits.

Scientists believe that using a Quantum Computer, they could map the chemistry used by certain bacteria that naturally create fertilizers and uncover an alternative to the current synthetic fertilizers created by the Haber-Bosch process. In fact, **Microsoft** has already demonstrated how Quantum Computers can create better fertilizer yields and has created a Quantum Chemistry Library to facilitate such research.

· There is a global push to expand battery powered automobiles in a transition to a greener economy, but existing car batteries have limited capacity/range and long charge times. Searching for materials with better properties is another molecular simulation problem that can be better handled by Quantum Computers. That is why German car maker **Daimler** has partnered with **IBM** to assess how Quantum Computers could help simulate the behavior of sulfur molecules in different environments, with the end-goal of building lithium-sulfur batteries that are longer-lasting, better performing and less expensive than existing lithium-ion batteries.

· The "traveling salesman problem" generally describes the challenge of optimizing the routing for businesses, another area where combinatorics makes the problems exponential difficult to resolve as inputs are added. For example, a fleet of more than 50,000 merchant ships carrying 200,000 containers each, with a total value of $14 trillion dollars, is actively in motion each day. Energy giant **ExxonMobil** has teamed up with **IBM** to find out if Quantum Computers could do a better job optimizing these routes and related logistics.

In the next blog I will cover additional details on the players currently working with Quantum Computers for these and similar applications.

Encryption

Another field where Quantum Computers will have a profound impact is for encryption. Nearly every time you log into a site on your computer, perform on-line banking transactions or when governments send confidential communications between entities, such activity is "on the web" meaning accessible to others. It is protected by an encryption protocol developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 and known as **RSA public-key encryption**.

In a very truncated description, the foundation of the RSA encryption lies in the fact that it uses two very large prime numbers to create a "factoring problem". Here is an over-simplified explanation:

1. A sender uses a very large number (the product of two large prime numbers) to encrypt or encipher a message. This is known as the Public Key.

2. The encoded message along with the Public Key are sent over the Internet (in theory, anyone can see/read these).

3. The Sender and a Receiver communicate a Private Key in a secure manner. This Private Key is the two prime factors used to create the Public Key.

4. The Receiver uses its Private Key to decrypt or decipher the message.

The encoded message cannot be decoded without knowing this "private key". Said another way, finding the two prime factors of a very large number is exceedingly difficult, so if the RSA Encipher key is based on a sufficiently large number (i.e., 2048 bits which is over 600 digits long), it is practically impossible with current computers to find the two prime factors. However, in 1994, mathematician Peter Shor proposed an algorithm that could factor large numbers into their primes in much shorter polynomial time. In fact, the algorithm he created is open source and available on the Internet for anyone to download. [For those of you interested in seeing the actual code, you can visit here: GitHub implementation of Shor's algorithm written in Python calling Q# for the quantum part]. Existing Quantum Computers only have the power to factor fairly small numbers, but the code is readily available for whomever creates a powerful enough Quantum Computer to use it to break existing RSA encryption.

Cryptocurrency mining and wallets are also areas which could be vulnerable to Quantum Computers. Bitcoin and other cryptocurrencies are "mined" by computers that crunch increasingly complex algorithms which result in the creation of new bitcoins (and which is why bitcoins consume increasing amounts of power). As levels of cryptocurrency are deciphered, the code to uncover the next round of coins increases in complexity. By some estimates, the current bitcoin protocols will take another 120 years to mine the remaining coins, so once Quantum Computers are powerful enough, they could mine the remaining coins much faster. In addition, the wallets that most people hold their cryptocurrency have similar vulnerabilities as described above regarding encryption.

I hope this post helps you appreciate how quantum mechanics already affects your everyday life and to begin to appreciate areas where Quantum Computers will have a profound impact. Stay tuned for a deeper dive into this subject.

References:

Jean-Francois Bobier, Matt Langione, Edward Tao and Antoine Gourevitch, "What Happens When 'If' Turns to 'When' in Quantum Computing", Boston Consulting Group, July 2021.

Bodur, Hüseyin and Kara, Resul ,"Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application.", 2015.

Bova, Francesco, Goldfarb, Avi & Melko, Roger G., "Commercial applications of quantum computing," EPJ Quantum Technology, 2021.

Cavicchioli, Marco, "How fast can quantum computers mine bitcoin?" The Cryptonomist, May 12, 2020.

Choudhury, Ambika, 8 Ways You Didn't Know Quantum Technology Is Used In Everyday Lives (analyticsindiamag.com), October 7, 2019.

Leprince-Ringuet, Daphne, "Quantum computers: Eight ways quantum computing is going to change the world," ZDNet, November 1, 2021.

Liao, Sheng-Kai, Cai, Wen-Qi, Pan, Jian-Wei, "Satellite-to-ground quantum key distribution," *Nature*, August 9, 2017.

Palmer, Jason, "Here, There and Everywhere: Quantum Technology Is Beginning to Come into Its Own," *The Economist*, 2017.

Parker, Edward, "Commercial and Military Applications and Timelines for Quantum Technology" Rand Corporation, July, 2020.

Schwink, Siv, "Self-annealing photon detector brings global quantum internet one step closer to feasibility," University of Illinois Urbana-Champaign Grainger College of Engineering, October 13, 2021.

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.