



The Quantum Leap January 17, 2022

Ten Fundamental Facts about Quantum Computing

I've covered some of the key aspects of Quantum Computing in prior posts, including details about things like qubits, superposition, and entanglement. I thought it would be helpful to readers to now synthesize and consolidate some of the fundamental properties of Quantum Computing to provide a bigger picture of the promise and potential of the industry.

However, I want to be on alert for overblown claims or statements disconnecting fact from reality. Some speak of a “Quantum Winter” where the hype gets overblown, and people get fed up with the promise and divert their attention (and resources) elsewhere, such as the case with nuclear fusion as a power source. So, I will be careful to be as fact-based as possible. As with all these posts, I hope that readers without any formal physics or computer science training can still appreciate and understand the information presented. Feedback is always welcomed and encouraged.

1. *What is a Quantum Computer?*

Quantum Computers (QCs) use incredibly tiny particles (e.g., atoms, ions, or photons) to process information. The physics that governs the behavior of particles at this minute size scale is quite different from the physics we experience in our much larger “people-scale”. QCs control and manipulate the individual particles as “qubits” which hold and process information analogous to how “bits” control our computers and electronic devices. However, the quantum mechanics at work at this scale allow QCs to process more information much more quickly than ordinary computers. Also, because of the different physics at play, different questions can be processed, and physical systems can be more accurately modeled, suggesting significant new advances as the machines continue to scale in size and power. The following table highlights some of the differences between existing digital/classical computers and QCs:

	Classical Computer	Quantum Computer
Bit Dimensions	1	3
Core Operators	3	6
Logic Direction	One-directional	Bi-directional
Logic Type	Deterministic	Probabilistic







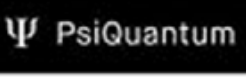



Think about these differences as enabling a Quantum Computer to do more per step, which is another way of saying it can process information faster than a classical computer. As it turns out, this speed advantage is phenomenal, which is why there is such enormous potential for Quantum Computers. See [here](#) for a prior post with additional details.

2. How are Qubits made?

There are several different ways people create and manipulate qubits, each with an array of strengths and weaknesses. The overarching challenge for each method is the desire to maintain a constant environment for the qubit, shielding from light, electromagnetism, temperature fluctuations, etc., (i.e., non-disturbed) while at the same time maintaining exquisite control of the qubit. Any tiny disturbance in the environment can throw off the qubit and create “noise” in the calculations. On top of this, is the challenge of achieving precise control of such tiny elements, often in a cryogenic environment. The power of the qubits resides in the ability to manipulate or rotate them very precisely. This is a difficult engineering requirement that is increasingly being met by the players in the industry. While there are a growing number of methods of creating and controlling qubits, here are some of the most common:

- **Superconducting Qubits:** Some leading QC players including Google and IBM are using superconducting, achieved at near absolute-zero temperatures, to control and measure electrons. While there are a few different ways these qubits are created (charge, flux, or phase qubits) it generally utilizes a microwave resonator to excite an electron as it oscillates around a loop which contains a tiny gap, and measures how the electron crosses that gap. Superconducting qubits have been used for many years so there is abundant experimental knowledge, and they appear to be quite scalable. However, the requirement to operate near absolute zero temperatures adds a layer of complexity and makes some of the measurement instrumentation difficult to engineer due to this low temperature environment.
- **Trapped Ions:** Ions are normal atoms that have gained or lost electrons, thus acquiring an electrical charge. Such charged atoms can be held in place via electric fields and the energy states of the outer electrons can be manipulated using lasers to excite or cool the target electron. These target electrons move or “leap” (the origin of the term “quantum leap”) between outer orbits, as they absorb or emit single photons. Trapped Ions are highly accurate and stable although are slow to react and need the coordinated control of many lasers.
- **Photonic Qubits:** Photons do not have mass or charge and therefore do not interact with each other, making them ideal candidates of quantum information processing. Photons are manipulated using phase shifters and beam splitters and are sent through a maze of optical channels on a specially designed chip where they are measured by their horizontal or vertical polarity.
- **Semiconductor/Silicon Dots:** A quantum dot is a nanoparticle created from any semiconductor material such as cadmium sulfide, germanium, or similar elements, but most often from silicon (due to the large amount of knowledge derived from decades of silicon chip manufacturing in the semiconductor industry). Artificial atoms are created by adding an electron to a pure silicon atom which is held in place using electrical fields. The spin of the electron is then controlled and measured via microwaves.

The following table highlights some of the features of these strategies along with companies currently working on QCs with these qubits. See [here](#) for a prior post which provides added details.

Qubit Type	Pros/Cons	Select Proponents
Superconducting Loops	Pros: High gate speeds and high gate fidelities. Can leverage standard lithographic processes.	  
	Cons: Requires cryogenic cooling; short coherence times; microwave interconnect frequencies still not well understood.	
Ion Traps	Pros: Extremely high gate fidelities and long coherence times. Extreme cryogenic cooling not required.	  
	Cons: Slow gate times/operations and low connectivity between qubits. Lasers very hard to align and therefore scale. Ultra-high vacuum environment needed.	
Photonics	Pros: Extremely fast gate speeds and promising fidelities. No cryogenics or vacuums required. Small overall footprint	 
	Cons: Noise from photon loss; each program requires its own chip	
Quantum Dots	Pros: Leverages existing semiconductor technology. Strong gate fidelities and gate speeds.	 
	Cons: Requires cryogenics. Only a few entangled gates to-date with low coherence times. Potential interference/crosstalk. Purification of silicon not very advanced.	

3. *What are Superposition and Entanglement?*

Nearly every introduction to Quantum Computing includes an explanation of Superposition and Entanglement, because these are the properties that enable qubits to contain and process so much

more information than digital computing bits and enable the phenomenal speed-up in calculations. While these are profound properties that are difficult to conceptualize with our common frame-of-reference on the macro-scale world, they are well established quantum physical properties.

- **Superposition:** classical computers use a binary system, meaning each processing unit, or bit, is either a “1” or a ”0” (“on” or “off”) whereas Quantum Computers use **qubits** which can be either “1” or “0” (typically “spin up” or “spin down”) or both at the same time, a state referred to as being in a **superposition**. This is a bit more subtle than it sounds because to use qubits for computational purposes, they need to be measured and whenever you measure a qubit you will find it collapsing into either the 1 or 0 state.
But *between* measurements, **a qubit can be in a superposition of both at the same time**, which imparts more information per processing unit than a classical bit.
- **Entanglement:** Quantum entanglement is a physical phenomenon that occurs when a group of particles are created, interact, or share proximity in such a way that the particles are “connected,” even if they are subsequently separated by large distances. Qubits are made of things such as electrons (which spin in one of two directions) or photons (which are polarized in one of two directions), and when they become “*entangled*“, their spin or polarization becomes perfectly correlated. It is this feature of quantum mechanics that largely underpins the awesome power of Quantum Computers because it enables the information processing to scale by an **exponential factor (n qubits = 2^n bits)**. The following table showcases this feature:

# of Qubits	Required Bits to Match	Equivalent Classical Computer RAM	Equivalent Classical Computer Processing Time
10	1024	128 bytes	2.6 μ s
20	1,048,576	131 KB	0.26 ms
30	1.1 billion	134 MB	0.27 seconds
40	1.1 trillion	137 Gigabytes	4.6 minutes
53	9.0×10^{15}	1 Terabyte	625 hours
63	9.0×10^{18}	1 Petabyte	73 years
100	9.0×10^{30}	1 Exabyte	10 trillion years
1,000	9.0×10^{301}	1.3×10^{232} Exabytes	8.5×10^{283} years

To give this some context, 100 qubits is the equivalent of an Exabyte of classical computing RAM which is a million trillion bytes (18 zeros). It would take a powerful classical computer nearly the lifetime of the universe to process that amount of data! The corollary is that quantum computers can perform certain complex calculations phenomenally faster than classical computers, and this concept of entanglement is a key to performance superiority. See [here](#) for more details on superposition and entanglement.

However, the sobering reality is that this chart assumes the qubits can be perfectly controlled for the duration of the calculations and that all the qubits can entangle with each other. We are still quite far away from being able to achieve these parameters at a meaningful scale, although

progress and advances are being made continuously. The other key to understanding and appreciating this, is to distinguish between “logical qubits” which this table describes, versus “physical qubits”. You may hear of companies using quantum computers with over 1,000 qubits but in the current NISQ (noisy intermediate-stage quantum) environment, many of the physical qubits are dedicated to error-correction as opposed to logic/calculations and often the qubits lose their superposition or entanglement properties (decoherence) very quickly, before the algorithms can be completed. So, discussions about the number of qubits in a given quantum computer need to have the proper context to understand the computing power implications.

4. Is the Power of Quantum Computers Magical?

You may be hearing claims of phenomenal powers of Quantum Computers (including from yours truly) along with descriptions of “quantum” as doing things surreal or supernatural (e.g., Schrodinger’s cat being both alive and dead). Features of Superposition and Entanglement are very difficult for a lay person to understand or appreciate, let alone believe it can be used for computing purposes. Some even describe quantum mechanics as “magical.” Most people, when they think of magic, conjure up parlor tricks or optical illusions, so it would be natural to doubt the veracity of the claims of QC. This, combined with the fact that nobody has created a QC that can perform real-world useful computations (yet) that can’t be performed on a classical computer.

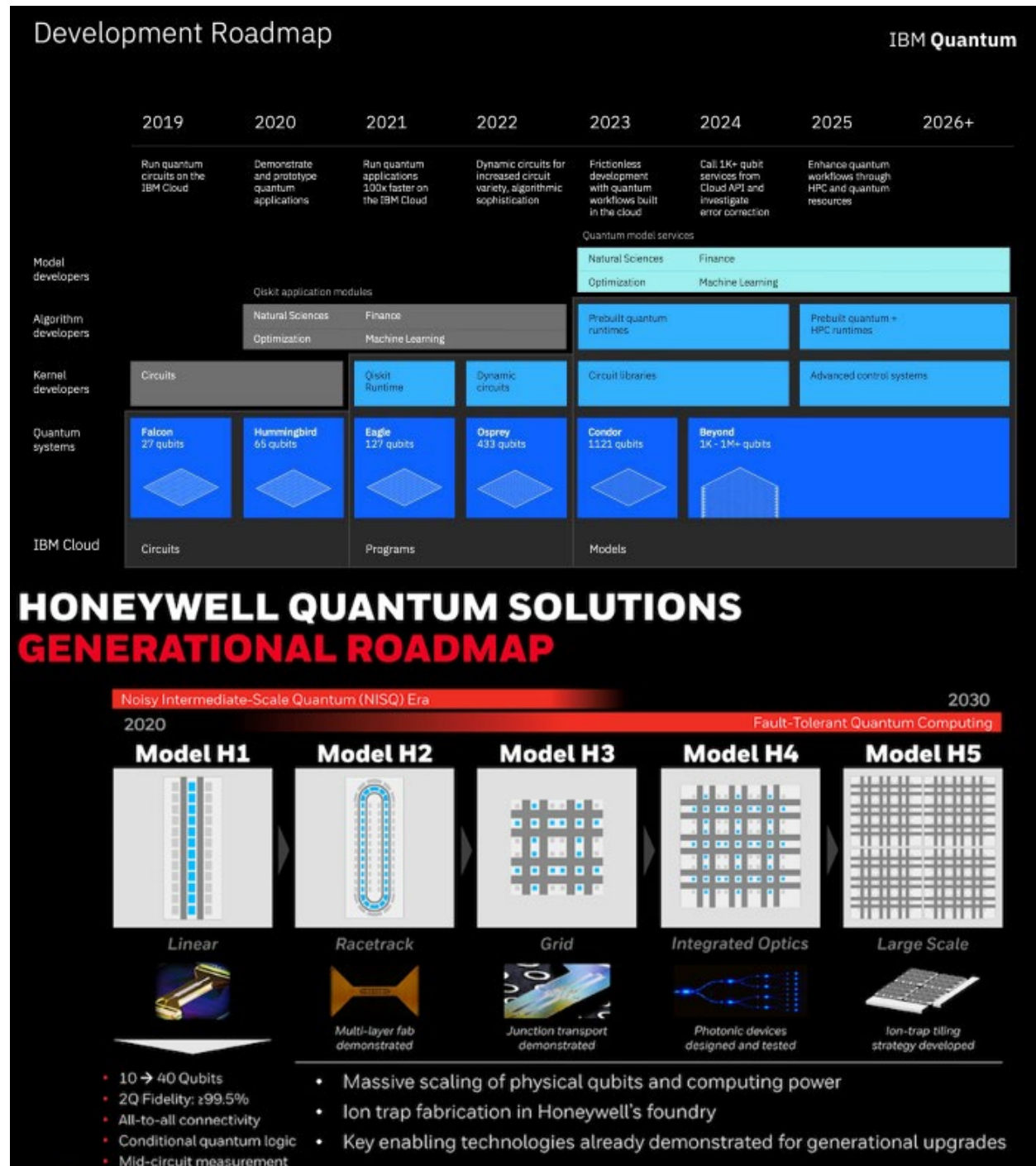
However, while the underlying mathematics is advanced, there is clear and agreed science concerning the construction and performance of Quantum Computers. The mathematical principles of manipulating qubits and using them to create logic gates are based on well-established linear algebra and trigonometry. Innumerable quantum algorithms are being written and will perform useful and important calculations once quantum machines scale to match the required power needed. At this point, it is difficult to predict precisely when such scale will be achieved, but those in the field will confirm that this is an engineering challenge not a theoretical challenge.

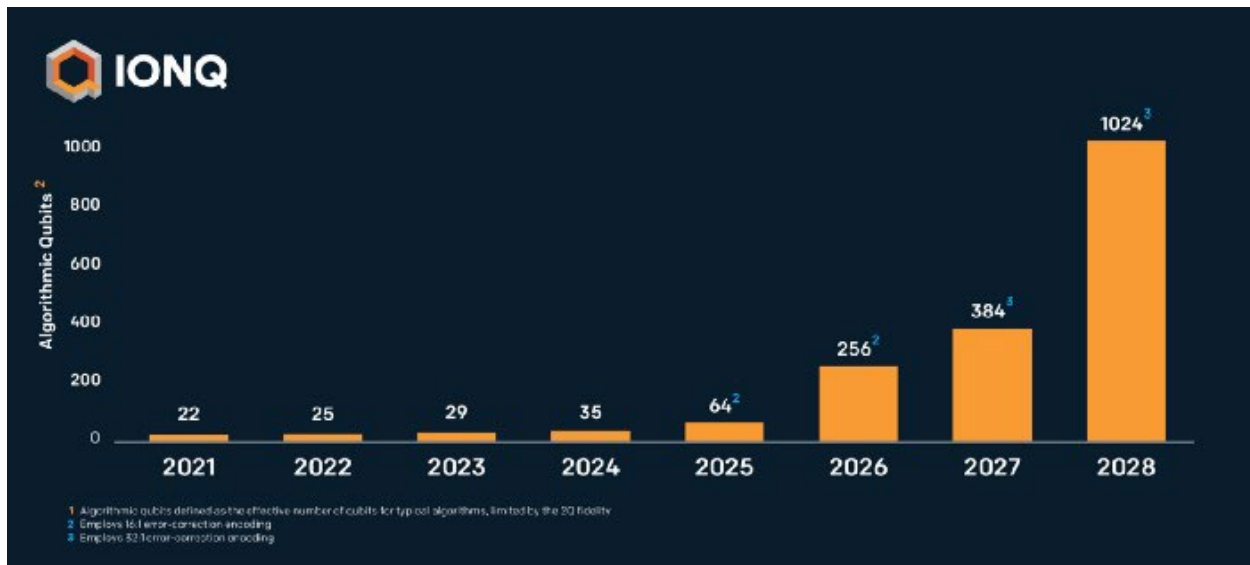
5. I Hear True Quantum Computing may be Decades Away. Is that True?

This is very difficult to answer with precision. My first “computer”, bought in 1980, was a Sinclair ZX80 with only 8k of memory, a puny amount compared to today’s PC’s. It certainly could not perform any applications or calculations that were of practical use at the time, although I was able to write some very basic code (ironically “Basic” was also the software language it used). But I could truthfully and accurately say in 1980 that I was using a personal computer to execute commands. A similar statement can currently be made by users of existing QC’s and many people are using cloud-based Quantum Computers today to run simple algorithms. While they are not yet capable of performing calculations that ordinary computers can’t perform, it is a dynamic and evolving situation.

At the same time, companies like D-Wave have “quantum” computers that use annealing, which leverages certain aspects of quantum mechanics, but cannot yet perform typical gate functions. They have many customers performing useful optimization calculations today, although not full-fledged QCs in the typical sense.

While there are no crystal balls, there are several high-profile quantum computing companies publishing their development timelines, which generally **suggest a large-scale product (i.e., more than 100 logical qubits) before the end of this decade**. See below for IBM, Honeywell (Quantinuum) and IonQ versions:





Many predict consistent Quantum Advantage (when Quantum Computers can consistently perform real-world calculations) in the next 5–10 years. The key thing to follow as the industry advances, will be to monitor which players are successful in meeting their timeline milestones. As more and more companies achieve important stated milestones, this timeline should become more precise.

6. Can We Measure Quantum Computing Power?

Unfortunately, there is no universally recognized measurement standard for the power of a Quantum Computer. There are several characteristics that are important including the number of qubits, the fidelity of the qubits, the length of time entanglement can be sustained, the numbers of gates that can be utilized, the numbers of connections between qubits that can be controlled, etc. Recently, IBM proposed a metric called “quantum volume” which is intended to consolidate many of these features although not all players are utilizing this standard. Barring any established metric, be careful to understand and appreciate the claims made by Quantum Computing companies realizing that the power of the computer is not necessarily directly correlated to the numbers of qubits it uses. See [here](#), for a prior post which covered performance measurement.

7. Are People Really Using Quantum Computers?

This is a bit of a trick question. The truth is that dozens of providers have made actual working Quantum Computers available for use via the Cloud. Some basic machines are available for no charge, some are available free for academic use, and some can be utilized for a modest cost. You could finish reading this article, and assuming you were familiar with basic Python programming, download a development kit from IBM (Qiskit), Microsoft (Q#), Google (Cirq), Amazon (AWS Bracket) or others, and begin writing quantum algorithms, and then establish an account with one of the QC cloud providers and either wait in the queue for your turn on a given machine, or acquire time to have the algorithm run on one of dozens of machines available remotely.

A recent study by Zapata Computing revealed that many companies are also using or planning to use QC in their businesses. Specifically, the study indicates that “69% of enterprises across the globe reveal they have adopted or are planning to adopt QC in the next year,” with those already having adopted some form of QC amounting to 29% of their survey respondents. In addition, you may read of many companies using Quantum Computers today to begin various optimization analyses. The following highlights some of the companies currently exploring QCs for various business applications:

Product Design/Logistics



Consulting/Info Tech/Finance



8. Where with Quantum Computing Provide Early Impact?

The superposition and entanglement of qubits enables QCs to evaluate many dataset items simultaneously instead of linearly, hence the tremendous speed-up in processing. One area where QCs can use these speedup features to provide a **quantum advantage** is in the ability to process currently unmanageable *combinatorial* problems (simulation and/or optimization). To visualize this, consider that a simple seating chart for 16 people involves over 20 trillion possible configurations [see [here](#) for prior post describing this in more detail]. Imagine the complexity of trying to design new chemicals or materials or medicines or optimized financial portfolios. The numbers of atoms, chemical bonds, or securities involved makes computer simulations practically impossible with existing classical computers, and the trial-and-error of experimentation is costly and time consuming. Therefore, problems involving combinatorics are the likely first uses of QCs. The following table highlights some of these use cases:

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

9. Are My Bitcoin Portfolio or Encrypted Bank Transactions Vulnerable to Quantum Attack?

The short answer is, not really. While it is theoretically true that powerful enough Quantum Computer could mine all remaining cryptocurrency and break standard RSA encryption (used for most secure messages and transactions communicated over the Web), this is a well-known issue

that is seeing substantial remedial attention. NIST (the National Institute of Science and Technology), a government entity which oversees certain standards and measurements, is in the final round of approving candidates to deploy a post-quantum cryptography standard. There are four Round 3 finalists with Public-Key Encryption and Key-Established Algorithms, and three Round 3 finalists with Digital Signature Algorithms, so new approved protocols which are “quantum safe” are imminent. In addition, there are other ways to secure on-line transactions besides RSA encryption, such as two-factor authentication, so more and more users are establishing enhanced protections. As for bitcoin, that is a bit more nuanced. Since most cryptocurrencies rely on increasingly complex mathematics for the mining of new coins, there is a finite number of bitcoins that can be created, and with existing computing power, it is anticipated that the discovery, or mining, of new coins will continually take longer and longer until it reaches its final amount (estimated at ~100 years at the current pace). So, if quantum computers are built which can mine faster, this end date may be accelerated, but the total number of possible bitcoins won’t change.

10. How can I Learn More?

There are many excellent resources available including articles, papers, on-line tutorials, books, and other resources. Please sign up to receive this blog as new posts are written and/or visit [this section](#) of the Quantum Leap blog for links to some additional resources.

Disclosure: *I have no beneficial positions in stocks discussed in this review, nor do I have any business relationship with any company mentioned in this post. I wrote this article myself and express it as my own opinion.*

References:

[IBM’s roadmap for scaling quantum technology | IBM Research Blog](#), retrieved January 16, 2022.

[Scaling IonQ’s Quantum Computers: The Roadmap](#), retrieved January 16, 2022.

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. [Harnessing the Power of Quantum Computing | Honeywell Beyond 2021](#), accessed January 9, 2021

“[Starting the Quantum Incubation Journey with Business Experiments](#)”, Digitale Welt Magazine, accessed January 16, 2022

[The First Annual Report on Enterprise Quantum Computing Adoption](#), Zapata Computing, July 5, 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.