RTI INTERNATIONAL

Quantum Computing Market Research Brief

Lab 58 Market Research Brief

June 2022

Quantum computers (see Figure 1) can perform certain tasks much more quickly than traditional computers. For example, IBM's quantum computer, Eagle, completed a random-number generation problem in just 3 minutes; for comparison, today's supercomputers would have needed 600 million years to complete the same task.[1] To date, quantum computing's potential has not been reached because scientists are still in the process of building a fully scaled quantum computer. Based on developed theories, quantum computing can have widespread effects across multiple industries; we are limited only by our own effort. In the next decade, quantum computing—both the industry and the technology—will experience significant growth. This growth could affect companies in multiple ways. The Lab 58 team thinks corporations will most likely need to develop internal plans for the post-quantum world; additionally, companies should continue to monitor scenarios in which their leaders can utilize quantum computing to accomplish work that aligns with their mission statement.

Figure 1: In this photo, the Minister of Finance of South Africa, Tito Mboweni, is seen observing an IBM quantum computer built by scientists working for IBM and Wits University.

Hon. Tito Mboweni, Minister of Finance of South Africa | Flickr

KEY TAKEAWAYS

Quantum computing is far from its potential, but industry growth in the next decade could lead to some real-life applications for quantum computers.

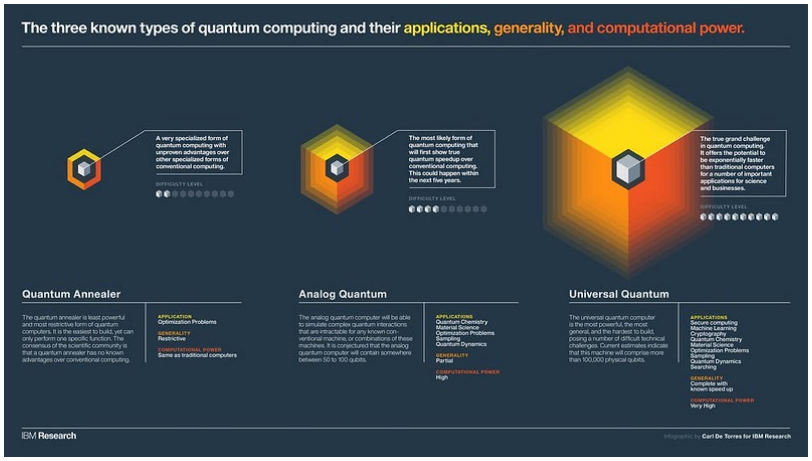
IBM, Google, and Microsoft are the three largest companies involved in the quantum computing sector.

Companies may need to develop internal plans for transitioning to a post-quantum world as the quantum computing industry grows.

[1] Pascual, Manuel G. (2021, November 19). IBM unveils the Eagle, the quantum processor set to revolutionize computing. *EL Pais.*

Quantum Computing Basics

Quantum computing and quantum mechanics are closely related. Quantum mechanics articulates the motion and interactions of subatomic particles through mathematical theories and equations. Using this understanding of quantum mechanics, scientists have learned how to perform calculations using subatomic particles. In quantum computers, these particles are called qubits, which provide quantum computers with far greater computational power than today's supercomputers. However, as Figure 2 shows, harnessing qubits' computational abilities is a multistage process. Quantum computing as mainstream technology is a milestone that will take time to accomplish.



The three known types of quantum computing and their applications, generality, and computational power.

A very specialized form of quantum computing with unproven advantages over other specialized forms of conventional computing.

The most likely form of quantum computing that will first show true quantum speedup over conventional computing. This could happen within the next five years.

The true grand challenge in quantum computing. It offers the potential to be exponentially faster than traditional computers for a number of important applications for science and businesses.

Quantum Annealer

The quantum annealer is least powerful and most restrictive form of quantum computers. It is the easiest to build, yet can only perform one specific function. The consensus of the scientific community is that a quantum annealer has no known advantages over conventional computing.

APPLICATION
Optimization Problems

GENERALITY
Restrictive

COMPUTATIONAL POWER
Same as traditional computers

Analog Quantum

The analog quantum computer will be able to simulate complex quantum interactions that are intractable for any known conventional machine, or combinations of these machines. It is conjectured that the analog quantum computer will contain somewhere between 50 to 100 qubits.

APPLICATIONS
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics

GENERALITY
Partial

COMPUTATIONAL POWER
High

Universal Quantum

The universal quantum computer is the most powerful, the most general, and the hardest to build, posing a number of difficult technical challenges. Current estimates indicate that this machine will comprise more than 100,000 physical qubits.

APPLICATIONS
Secure computing
Machine Learning
Cryptography
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics
Searching

GENERALITY
Complete with known speed up

COMPUTATIONAL POWER
Very High

IBM Research

Infographic by Carl De Torres for IBM Research

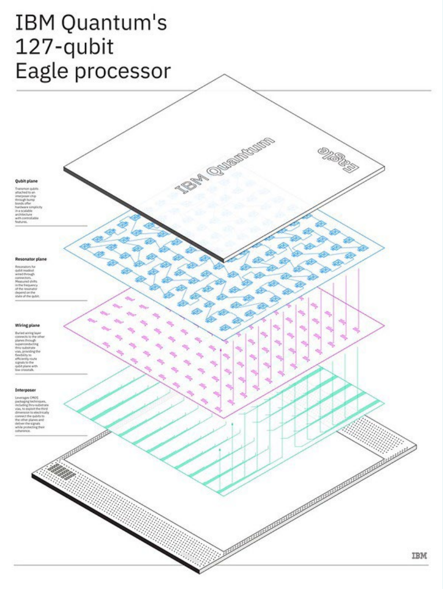
Figure 2: This graphic shows the stages of quantum computing and the possible applications for quantum computing in each stage. To view full image, click the link below:

Three Types of Quantum Computing - IBM Infographic | Flickr

History and Progress

In 1994, Dr. Peter Shor proved that a fully scaled quantum computer could break many of the encryptions used to protect public data online.[2] This revelation drew the attention of many and sparked the industry's growth. A quantum computer's computational capacity directly relates to the number of qubits the computer uses. However, the process of constructing processing chips with qubits is difficult, so progress has been slow. In 2021, IBM revealed the world's largest quantum computer, Eagle.[3] Eagle uses a 127-qubit processor chip (see Figure 3), making it the first quantum computer to exceed the 100-qubit barrier.[3] This is a great accomplishment; however, Eagle is far from a fully scaled quantum computer, which requires an excess of 1 million qubits.[4]

Building a fully scaled quantum computer will take time and a great deal of money, but the process should be exciting to watch. In the next decade, the global market for quantum computers is expected to flourish. The value of the industry's global market is expected to reach $64.98 billion by 2030, which is considerably higher than its 2021 evaluation of $62.4 million.[5]



IBM Quantum's
127-qubit
Eagle processor

Qubit plane

Transmon qubits attached to an interposer chip through bump bonds offer hardware simplicity in a scalable architecture with controllable features.

Resonator plane

Resonators for qubit readout wired through connectors. Measured shifts in the frequency of the resonator depend on the state of the qubit.

Wiring plane

Buried wiring layer connects to the other planes through superconducting thru-substrate vias, providing the flexibility to efficiently route signals to the qubit plane with low crosstalk.

Interposer

Leverages CMOS packaging techniques, including thru-substrate vias, to exploit the third dimension to electrically connect the qubits to the other planes and deliver the signals while protecting their coherence.

Figure 3: A description and visual representation of IBM's 127-qubit processor chip Eagle.

2D Schematic of IBM Quantum 127-Qubit Eagle Processor | Flickr

[2] Aaronson, S. (2008, March). The Limits of Quantum. *Scientific American*. 62–69.

[3] Chow, J., Dial, O., & Gambetta, J. (2021, November 16). IBM Quantum breaks the 100-qubit processor barrier. *IBM*.

[4] Fridman, L. (2020, February 17). *Scott Aaronson: Quantum computing | Lex Fridman Podcast #72* [Video]. YouTube.

[5] Global Industry Analysts. (2021, August 10). Global quantum computing market to reach 411.4 million by 2026. *PR Newswire*.

Additionally, in the next few years, major tech companies—such as IBM and Google—are hoping to make great advancements in the industry. At the beginning of 2022, IBM announced it was in the process of developing a 433-qubit chip named Osprey and a 1,121-qubit chip named Condor.[3] These milestones are part of IBM's ultimate goal of creating a quantum chip of practical value within the next 2 years.[6] Meanwhile, Google has announced its desire to build an error-corrected quantum computer by 2029, which would represent a major leap toward building a fully scaled quantum computer.[7] During this period of growth, large companies may benefit from actively monitoring the journey of quantum computing to determine future use cases as the technology becomes more powerful.

Technical Barriers to Progress

Decoherence

The process of building a quantum computer is incredibly complex and slow moving (see Figure 4). Of all the challenges, the largest technical obstacle is most likely a phenomenon called decoherence, which is any "unwanted interaction between a quantum computer and its environment."[2] Unfortunately, decoherence cannot be easily avoided. Even trace levels of radiation can cause decoherence, and the situation becomes more difficult as more qubits are added.

Luckily, scientists have identified a way to solve the decoherence issue, but the solution is not an overnight process. Researchers have developed error-correcting codes that limit how decoherence affects qubits, essentially allowing the qubits to self-correct most decoherence-related issues. These qubits are called error-correcting qubits. Quantum computers that are able to use a large number of error-correcting qubits have not been built yet; however, Google's Quantum AI facility was built with the intention of constructing an error-correcting computer by 2029.

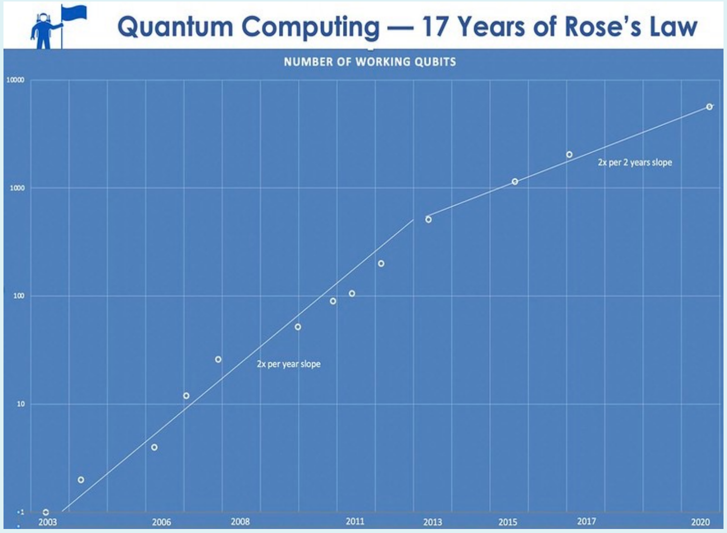


Figure 4: In 2003, Rose's Law was introduced as a means of predicting quantum computers' future qubit capacity. The Y axis shows the number of working qubits predicted by Rose's Law, and the X axis shows the timeline in years. As the graph shows, we have fallen behind the predictions, and 100,000 qubits—the maximum of the graph—are not nearly enough to power the quantum computer that scientists want to build.

Jurvetson, S. (2020, September 30). Scaling quantum computing: 17 years of Rose's Law.

[6] Nellis, S. (2021, November 14). IBM says quantum chips could be standard chips in two years. *Reuters*.

[7] Lucero, E. (2021, May 18). Unveiling our new Quantum AI campus. *The Keyword*.

Major Companies in the Quantum Computing Market

Google

Established: 1998
Application/Division: Google Quantum AI

In May 2021, Google revealed its new Quantum AI campus in Santa Barbara, California. Scientists are planning to build the first-ever error-corrected quantum computer by 2029 on this campus.[7] This type of computer uses error-correcting qubits, which are essentially better versions of the qubits that are currently available. To build a quantum computer that meets Dr. Shor's expectations, scientists have concluded that error-corrected qubits will be required. Therefore, Google's success would be a great achievement. Google also expects the computer will house 1 million qubits, which is a tremendous increase compared to the 127-qubit Eagle quantum.[7]

Microsoft

Established: 1975
Application/Division: Microsoft Quantum

Microsoft has a team that is focused on all aspects of the quantum stack. The company is trying to create hardware that allows for the control of thousands of qubits without overheating the computer. Microsoft's quantum capabilities allow users to integrate computational power with their cloud-based computing platforms. Microsoft has named this development tool Microsoft Azure, which is one of the earliest attempts to deploy quantum computing solutions at scale.

IBM

Established: 1911
Application/Division: IBM Quantum Network

IBM, like its counterparts, also has a full-quantum stack that allows partners to explore quantum solutions. IBM uses their IBM Cloud to offer quantum systems, simulators, runtimes, and programming tools. According to IBM's website, they have a "fleet" of quantum computers, and the company offers a quantum developer certification program.[8] In 2021, IBM broke the 100-qubit barrier by creating a 127-qubit processor.[3] In the next 2 years, the company is hoping to create processors with more than 1,000 qubits.[3]

Future Use Cases

Quantum Simulations

According to Scott Aaronson, head of The University of Texas at Austin's Quantum Information Center, the "biggest practical application of quantum computing, that we know about, by far, is simply the simulation of quantum mechanics itself."[4] Remember, quantum mechanics describes how the subatomic particles interact and move with each other. If researchers can simulate those interactions, the potential exists for researchers to develop new chemical processes, new raw materials, new medicines, and much more.[4] Simulating interactions could affect industries thought to be disconnected from computing, such as industrial fertilizer. Fertilizer is made through a process of chemical reactions. Therefore, by studying those chemical processes in a new way, a more in-depth quantum simulation could provide researchers with knowledge that permanently alters the way fertilizer is made. In fact, Google wants to create a fertilizer that does not produce carbon emissions, a goal they announced for their new Quantum AI lab.[7]

Cryptography

As previously mentioned, Dr. Shor proved in 1994 that a quantum computer of a specific complexity could break most of the encryptions used to protect public data over the internet. Since then, scientists within the post-quantum cryptography field have researched other ways to encrypt data, ways that are immune to quantum computing.[4] One of the most popular proposals for post-quantum internet security is lattice-based cryptography, but the future remains blurred.[4]

In 2016, the National Institute of Standards and Technology (NIST) began reviewing over 50 approaches for protecting data from attacks from quantum computers.[9] The group of 69 submissions was cut to 15 in 2020, and a final decision is expected sometime in 2022.[8] The report will provide a much clearer outlook for the future of post-quantum cryptography.

The current competition at NIST is symbolic of a broader government effort to prepare for a post-quantum world. In 2018, Congress signed The National Quantum Initiative Act, in which the federal government pledged $625 million in funding for quantum computing and information sciences.[10] Such an investment is unmistakable evidence that the U.S. government (1) believes a post-quantum world is plausible and (2) wants to be one of the industry leaders in data encryption and more in the post-quantum world.

[8] Asfew, A., Ferguson, K., & Weaver, J. (2021, March 29). IBM offers quantum industry's first developer certification. *IBM Research Blog.*

[9] National Institute of Standards and Technology. (2020, July 22). *NIST's post-quantum cryptography program enter 'selection round.'*

[10] Vincent, J. (2020, August 26). US announces $1 billion research push for AI and quantum computing. *The Verge.*

Suggestions and Possible Timetable for the Future

Quantum computing is something to be excited about, but we will need to exercise patience while we observe its growth. Google has set 2029 as a landmark year, the year the world's first useful quantum computer will be built. And in 2022, we are expected to get two new significantly upgraded quantum computer chips from IBM. The quantum computing industry will continue to grow, and the Lab 58 team thinks two specific questions could be relevant to companies in the future: (1) What do companies look like in a post-quantum world? (2) How soon can quantum computing be used to benefit companies and their missions?

Given the vast investment in the industry, both by the federal government and private entities, it seems plausible the world will have multiple, fully scaled quantum computers at some time in the next 10 to 15 years. If this occurs, the world will need to change how it encrypts all data on the internet. At this moment, it seems as though lattice-based cryptography is the most popular option, but things could easily change, especially once NIST creates national standards. Companies have plenty of time, but it might be wise for them to be proactive rather than reactive in their approach to a post-quantum world to ensure proper data protections.

Finally, organizations may choose to closely monitor any progress related to quantum simulations. Scott Aaronson, a leader in the field for at least a decade, anticipates quantum simulations could be the first practical application of quantum computers to affect our world, and these simulations will be the focus of the large companies involved in quantum computing over the next decade.[4] Quantum simulations could be performed by 100–200 qubit quantum computers, which is well within the range of the quantum computers we will build over the next 2–3 years.

Quantum simulations have the power to redefine industries. The possibility exists for industries to use the findings of quantum simulations in ways that we could have never imagined previously.

Work With Lab 58

Thanks for your interest in our work! We want to help you explore opportunities to work with quantum computing.

Please email us at Lab58@rti.org. We will set up a 30-minute, one-on-one chat to discuss opportunities and answer any questions. We are interested in partnering with you to find a solution that meets your needs.

For more information, contact Lab58@rti.org.