What is Quantum Computing?

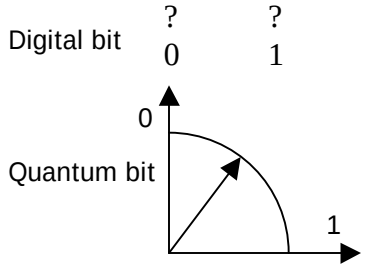
As firms continue to expand the role of IT within their corporations and demand computers that are able to handle more complex computations, technologists are arriving at the realization that the current computer architectural structure is beginning to reach its 'limits. Futurists have proposed two alternatives to overcome the current physical limitations of computers: optical and quantum computing. As was discussed in the previous technology briefing, optical computing uses light as a way to perform calculations. However, an opposing view is that computers should be conceptualized differently. Instead of processing data using bits and bytes in silicon chips, the quantum computing approach uses laser pulses to excite atoms, a process that allows scientists to harness the power of atoms and meet the demand for more complex mathematical computations.

Why Quantum Computing?

Gordon Moore predicted in 1965 that the number of transistors per integrated circuit would double approximately every 18 months (see Table to the right). A quick analysis reveals that Moore's law has successfully predicted the transistor trend through the years. So, what will happen in the next 20 years if the processor development continues to support Moore's law? The result will be that the size of the circuits on microprocessors will be measured on an atomic scale. However, as discussed in our briefing on optical computing, this decrease in size will not necessarily meet the demand for more complex computations. While optical computing can increase computation speed 1000 to 100,000 times faster than 1.2GHz processors, some researchers believe far greater speeds can be achieved with quantum computing. Furthermore, advocates of quantum computing argue that the shrinkage in microprocessor size presents an opportunity for IT that can be leveraged using quantum computing.

How does Quantum Computing work?

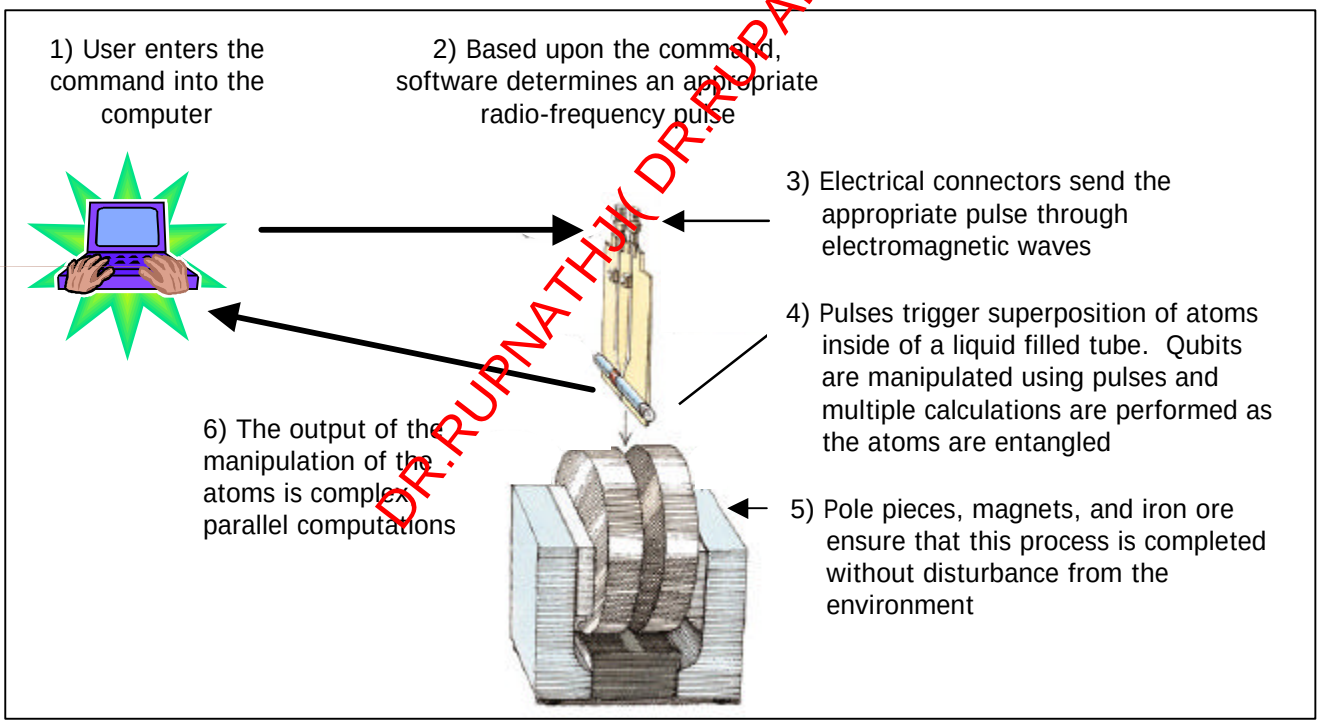
To help us understand how quantum computing works, we can start with familiar classical computing. In classical computers, data is stored in the form of a digital bit. Digital bits have only one value: true or false, on or off, one or zero; they are typically represented by the presence or absence of a few zillion electrons in silicon transistors. The chip processes one calculation at a time, sequentially, and information is processed in one direction only. Quantum computing, on the other hand, uses atoms in place of traditional processors. Each bit of information carried in quantum computers is called a 'qubit', which can represent 0, 1, and any value in between at the same time. In a graphical sense, a vector pointing in a direction intermediate between those representing 0 and 1 represents the in-between position known as superposition.



In classical digital computation, for example, a two-bit can only represents one of the following values: 00, 01, 10, and 11. A quantum two-bit, in contrast, can represent any of those numbers simultaneously. Consequently, as the number of qubit increases, the

number of superposition will exponentially increase and result in complicated numbers that current computer technology will never be able to calculate. Using superposition, scientists can use the idea of quantum parallelism in their creation of a new microprocessor.

The meaning of quantum parallelism could be interpreted as that atoms in a microscopic world are radiating to many different directions simultaneously. The essential idea is that if an atom can travel through many different routes simultaneously, a computer should be able to use atoms to perform calculations through many different routes simultaneously as well. In other words, quantum computers offer the possibility that multiple calculations can be performed simultaneously. Technically, scientists can use laser pulses to affect an atoms electronic states and evolve initial superpositions of encoded numbers into many different superpositions. Those qubits stored in the atom therefore can be manipulated and a quantum computer can perform multiple calculations in one single computational step. Furthermore, without interference from the outside world, atoms can be "entangled" in a way that if one atom spins in one direction, the rest of them will spin in some directions that could be mathematically related to each other. This process is called quantum entanglement. Using superpositions and entanglement, we will be able to harness complex algorithms for cryptography or database searching to simultaneous solving of billions of calculations. The picture to the right depicts a prototype quantum desktop computer. The behavior of quantum computer, based upon this prototype, is described in the figure below.



This picture has been reprinted from: ww.nsf.gov/pubs/2000/nsf00101/nsf00101.htm and www.sciam.com/1998/0698issue/0698gershenbox1.html

The table below contrasts classical computing and quantum computing in some primary areas that relate to computation and communication mechanism.

	Classical Computing	
Information representation	A bit: either 0 or 1	A qubit: a superposition of 1 and 0
Number of simultaneous calculations	1	Multiple
Method of calculation	Moving bits through logic gates	Altering states of atoms
Information delivered	Information can be copied without being disturbed	Information cannot be copied or read without being disturbed
Information behavior	One single direction	Spread-out to many routes simultaneously like overlapping waves
Noise tolerance	High: Information can be carried in a noisy channel	Low: The delivering channel needs to be noiseless
Security	Lower: Eavesdropper can break into the communication with high computing power	Higher: Any interruption of communication will be detected by communicating parties
Computation / Communication cost	Higher as computing or communication volume increases	Lower as computing or communication volume increases

What will be the projected benefits of Quantum Computing?

Quantum computing offers many potential benefits to the organizations of tomorrow. This new conceptualization of computing power will result in three main benefits: increases in computing power, advances in security, and the ability for firms to use the sci-fi concept of teleportation. Each of these opportunities can overcome the limitations of the current computational paradigm.

Quantum Computation: Increase in Computing Power

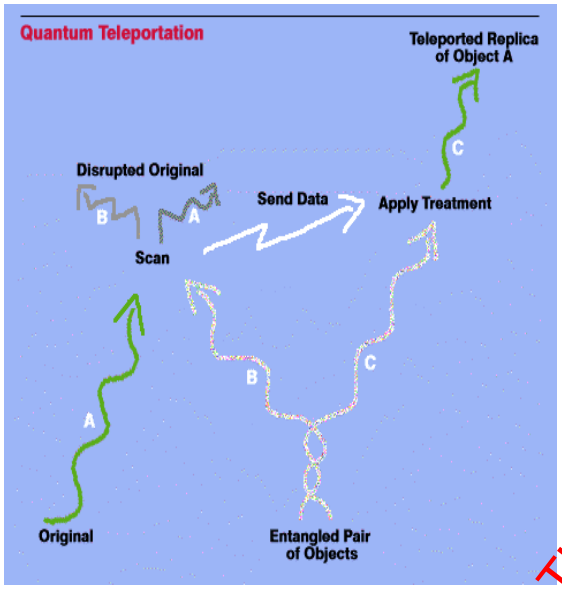
Utilizing quantum parallelism, a quantum computer can calculate or factor any huge number that is currently infeasible to be analyzed on a classical computer. For example, factoring a number with 400 digits will take the existing fastest supercomputers billions of years to accomplish. A quantum computer can obtain the answer within a year. Therefore, quantum computers well serve the purpose of searching information in unsorted databases or performing difficult mathematical calculations that are impossible using semiconductor computers.

Quantum Cryptology: Advances in Security

Linked with the first benefit (the increase in computing power) comes the possibility for advancements in computing security. Quantum cryptography allows two parties to exchange public keys in a private channel and thus secure privacy in quantum communication. The technical aspect of quantum cryptography requires tremendous amount of physics knowledge; the basic idea is that quantum mechanics will not allow any eavesdropper to obtain the private key. Two legitimate parties will reveal a random subset of the key bits and check the error rate to test for eavesdropping. In so doing, even though eavesdropping will not be prevented, any attempt, regardless how subtle and complicated, to break into the communication channel will be detected.

Teleportation

Perhaps the most astounding of the claimed for benefits of quantum computing is teleportation, the favored local transportation mechanism in Star Trek episodes. Teleportation is the capability to make an object or a person disintegrate in one place while a perfect replica appears in another. In physics, teleportation has never been taken seriously because of the uncertainty principle. According to the uncertainty principle, the duplicating process will disturb or destroy the original objects; the more an object is duplicated, the more it is destroyed. The detail information regarding how the duplication is made and how the original object is destroyed is unknown. Therefore, it will reach a point where one cannot extract enough information from the original to make a perfect replica.



However, scientists at IBM and elsewhere have discovered a way to make a perfect replica using a distinctive feature of quantum mechanics called EPR (Einstein-Podolsky-Rosen) effect (see the figure to the left: ww.research.ibm.com/quantuminfo/teleportation). In brief, they found a way to scan partial information from original object "A" while causing the remaining part of information pass to another object "C" through the EPR effect. "A" and "C" have never been in contact but somehow by applying a treatment to "C", depending on the scanned information, "C" could be maneuvered back to the same stage as "A" was before it was scanned. Since "A" has no longer been in the same state, "C" is considered as a teleportation instead of a replication. Therefore, teleportation could allow us to reconstruct all objects and place them in a different place. If information of each atom could be obtained, everything in your office or bedroom, including yourself, could be teleported to another place and displaced in front of you similarly to how it appears in Star Trek. Teleporting living beings would require a tremendous amount of information and given the constantly changing state of mind of humans, will remain science fiction for the foreseeable future. Nevertheless, quantum computing provides at least a theoretical basis for teleportation.

There are, however, three areas where teleportation, which will come from using quantum computing, might be practical sooner. First, it will allow us to picture distributed networks of quantum computers exchanging information back and forth. With exact correlation between input and output, quantum teleportation might bring opportunities for better network communication such as video conferencing with real time, real information applications. Second, it is crucial to quantum key distribution and other quantum cryptographic protocols. With teleportation's special "entanglement" effect, the information conveyed between senders and receivers can be only perfectly produced through these two parties. Any attempt to eavesdrop will be detected and result in failure. Finally, it is also a decisive factor in an efficient optical implementation of quantum computers. While classical teleportation can generate a fidelity coefficient, a coefficient to describe the correlation between input state and output state, less than 0.5, quantum teleportation could result in fidelity coefficient at 1, meaning the input state and output state are perfectly correlated. The optical teleportation, on the other hand, can yield fidelity coefficient at only 0.67. Applying quantum teleportation to optical computing, therefore, is believed to improve the efficiency of optical implementation of quantum computers.

What are the projected risks of Quantum Computing?

Although there are many proposed benefits anticipated from quantum computing, there are also potential risks. Among these are the following:

- While advancements in security will be welcome within the IT community, there is a possibility of an uneven distribution of adoption of the new technology. If some firms adopt quantum computing and others do not, those without these systems will be vulnerable to the security threats previously discussed.
- Conceptually, it is believed that with quantum technology we will be able to build microscopic machines such as a nanoassembler, a virtually universal constructor that will not just take materials apart and rebuild them atom by atom but also replicate itself. The good news of this self-replication machines means that these nanomachines will cost nothing to build and eventually make any products we might desire at zero cost. The bad news is that these HAL-like computing brains with capabilities exceeding those of humans, could redesign and replicate themselves at no cost, other than the loss of human dominance.
- Quantum computing will instigate rapid changes in computing and corresponding modifications to human life, at a time known as the point of Singularity. When that day arrives, some futurists fear that quantum computing will cause things to change so fast that it will be impossible to predict what will happen next. Or, there will be "a developmental discontinuity, an ultimate event horizon beyond which predictability breaks down totally." It sounds as terrifying as those scenarios in a science-fiction film; theoretically, nevertheless, it is the risk that quantum computing might eventually lead us to.

When will Quantum Computers be available?

It has been more than three decades since IBM Fellow, Rolf Landauer, first put forward the theory of quantum information. A decade later, David Deutsch and other research fellows proposed the concept of a quantum computer. Since then progress in the technical development of quantum computing has moved slowly. Currently, IBM has a three-bit quantum computer while Alamos National Laboratory announced a seven-bit NMR (Nuclear Magnetic Resonance) computer not long ago. Even though IBM research fellows promise that a ten-bit computer will emerge soon, a useful quantum computer will require at least hundreds and perhaps thousands of qubits. Unfortunately, it appears almost impossible to develop more than 10 qubits. This is because room temperature and other conditions will be changed exponentially as the qubits are added resulting in disturbing the atom's quantum behavior. As IBM Research Fellow Isaac Chuang, a leading scientist in quantum computing research, said *"Quantum mechanics goes away when you look at it. So you have to make sure that the computer is extremely well isolated from the rest of the world."* In other words, the commercial development of quantum computing is still limited. The real life use of quantum computers therefore will not affect our everyday life in the near future. However, Chuang is very optimistic about it: *"Quantum computing begins where Moore's law ends—about the year 2020, when circuit features are predicted to be the size of atoms and molecules"*. Other scientists estimate the birth of commercial quantum computers will be in at least another three decades.

What comes after Quantum Computing?

Once scientists can use atoms to complete complex computations, futurists claim that computers can be built in new forms, specifically smaller. Some scientists foresee the day when a computer will be the size of 1 atom. These types of machines are known as nanomachines. These new machines can be deployed in ways that are not available today. For example, a nanomachine can be built and programmed to enter human cells to fight diseases or even resusitate those who have just died. Yet, this approach will not be available until scientists can manipulate atoms using the quantum physics approaches of entanglement and superposition.

In addition to smaller machines, scientists also claim that computers can now be stored in carbon-based beings, within DNA. Scientists have long known that DNA could store information. But only when Charles Bennett, in 1973, drew attention to the computational capability that is responsible for processing genetic information in DNA did researchers begin to recognize the potential of a biological computer. The most obvious advantage of DNA computing is that molecules are so small that they offer a great potential to produce very inexpensive form of massive parallelism, also one of the major attributes of quantum computing. Scientists estimate that one pound of DNA molecules floating in 1,000 quarts of fluid could contain more memory than all the computers ever made; and a human body alone contains about a half pound of DNA. If there is a way to make DNA compute, even a small test-tube solution could contain 10^{20} number of processors. Scientists, including Aldeman at MIT, estimate that a DNA computer could perform 10^{20} operations per second - several million times faster than any supercomputers ever made. However, DNA computing is based on the foundation of quantum computings ability to manipulate atoms.

How can organizations today start to become involved in Quantum Computing?

> "The nineteenth century was known as the machine age, the twentieth century will go down in history as the information age. I believe the twenty-first century will be the quantum age." –Paul Davies

To organizations, particularly computer manufacturers or power users of computing cycles, the technical aspects and predicted capabilities of quantum computing should be of more than curious interest. To the rest of us, however, it is the potential of quantum computing to revolutionize human history that should capture our attention. While no organization can expect to productize or us use quantum computing in the near future, the discussion of this new technology allows IT to reflect upon current practices in a number of issues. While these suggestions will not directly lead to the employment of quantum computing, they are areas that the new approach illuminates.

1. Look at your current processing of data. Are you harnessing the current computational power in an efficient manner? Or, are their processes that need to be revised to be more efficient?
2. Look at your current security procedures. Do you stay aware of new and emerging threats such as, in time, the possibility of an attack from a quantum computer?
3. Look at the long run expectations of your users for computing speed and power. Do they demand and expect more than you are delivering? Do they recognize and plan for the increments in power to come? What would be possible with a hundred-fold, thousand-fold, or greater increase in computational power?

For More Information

Online resources

Find out more information about IBM new discovery of quantum mirage:
http://ww.almaden.ibm.com/alma_den/media/image_mirage.html

Learn from critics of nanotechnology and debate on related issues: http://www.foresight.org/

http://www.iro.umontreal.ca/labs/theorique/index.html.en

Find out Houston-based research resources of Nanotechnology at NASA and look at some videos showing how atoms move like a wave: http://www.nas.nasa.gov/Groups/SciTech/nano/index.html

Report from the National Science Foundation on Quantum Information Science: An Emerging Field of Interdisciplinary Research and Education in Science and Engineering:
http://www.nsf.gov/pubs/2000/nsf00101/nsf00101.htm

Learn systematic information with a variety of difficulty level on quantum computing:
http://www.qubit.org/Intros_Tuts.html

Learn about IBM's development of quantum computing: http://www.research.ibm.com/quantuminfo/

An issue about Quantum Computing with Molecules by Gershenfeld and Chuang:
http://www.sciam.com/1998/0698issue/0698gershenfeld.html

An issue about quantum cryptography by Simon Benjamin:
http://www.sciencemag.org/cgi/content/full/290/5500/2273

Learn about Hewlett-Packard's development on Quantum Computing: http://www-uk.hpl.hp.com/qip

Learn about the basic concepts of quantum computing:
www.technologyreview.com/magazine/may30/waldrop.asp

Learn how teleportation will work:
www.sciam.com/explorations/122297teleport/test.html

Report on teleportation research at California Institute of Technology:
www.cco.caltech.edu/~qoptics/teleport.html

Description of how quantum computing takes advantage of NMR (nuclear magnetic resonance):
www.sciam.com/1998/0698issue/0698gershenfeld.html

A famous talk on nonotechnology: "There's Plenty of Room at the Bottom" by Richard P. Feynman:
www.zyvex.com/nantech/feynman.html

Articles

Deutsch, D. and Ekert, A. "Quantum Computation", Physics World, March 1998.

Divincenzo, D.P. "Prospects for Quantum Computing", IEDM Tech. Digest, December 2000.

Gershenfeld, N. and Chuang, L. "Quantum Computing with Molecules", Scientific American, June 1998.

Hill, M. "Lucent Technologies Bell laboratories introduced statistical sampling algorithm which brings quantum computing closer to practical applications", Electronic Engineering Times, 75, June 05, 2000.

Steane, A.M. and van Dam, W. "Physicists Triumph at Guess My Number", Physics Today, February 2000, pp. 35-39.

Important Books To Read

Brown, J. Minds, Machines, and the Multiverse: The Quest for the Quantum Computer, Simon & Schuster, New York, NY, 2000.

Deutsch, D. The Fabric of Reality: The Science of Parallel Universes-and Its Implication, Viking Penguin, July 1998.

Siegfried, T. The Bit and The Pendulum: From Quantum Computing to M Theory—The New Physics of Information, John Wiley & Sons, Inc., New York, NY, 2000.

Research Groups Currently Working on Quantum Computing

IBM, AT&T, Hewlett-Packard, Oxford University, MIT, UC-Berkeley, and Caltech are among the institutions with quantum computing research projects underway. The National Science Foundation provides financial support for interdisciplinary research in quantum information science. Locally, NASA's Nanotechnology group may now, or in the future, be able to provide insights into this, or related new schools of computation.