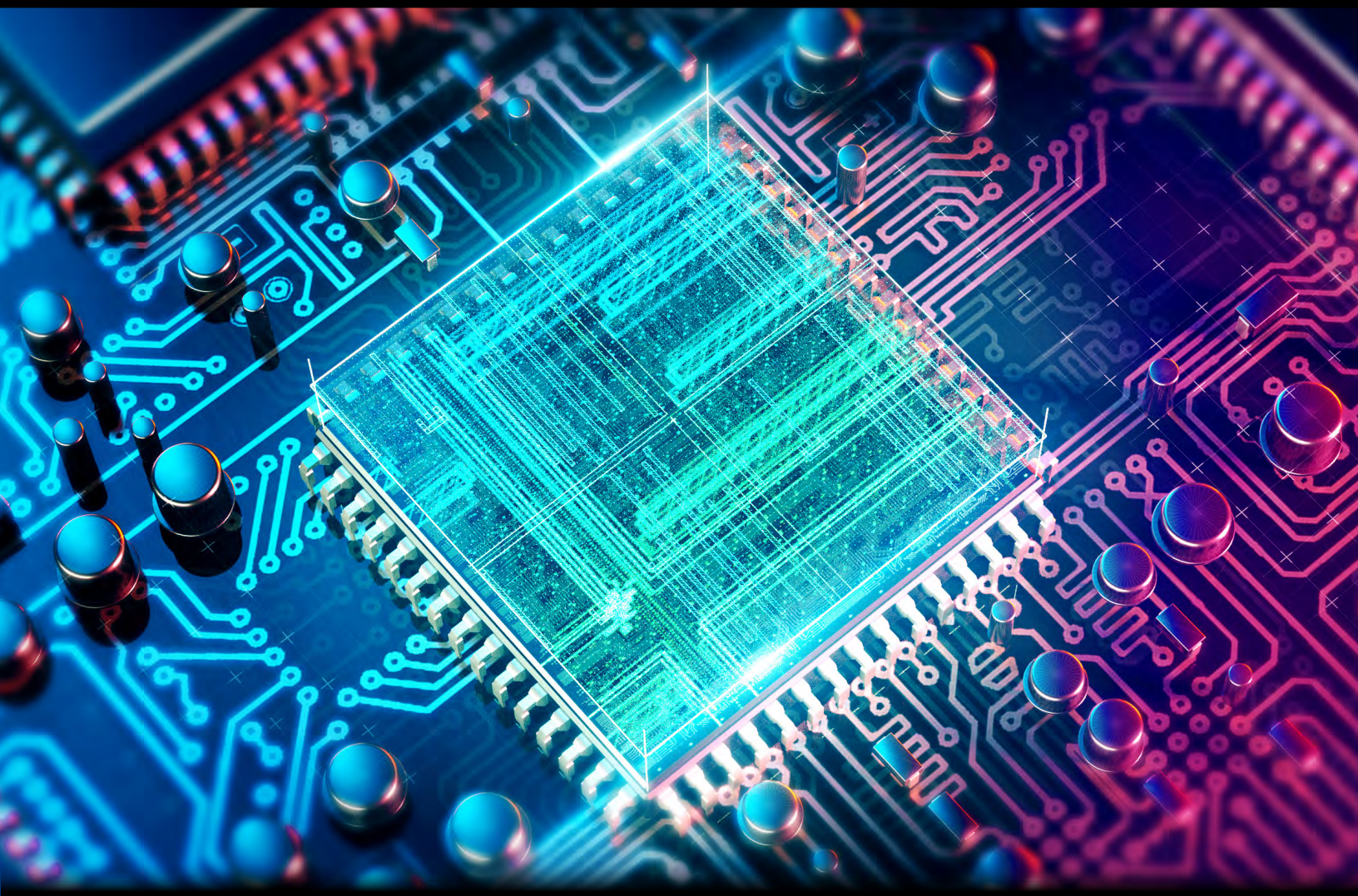
GlobalLogic®



Quantum Computing: The Next-Gen System

Authored by
Amit Gupta and Yasa Khan

Contents

Introduction

With an exponential rise in data sources and the scarcity of time to turn that data into meaningful action, the gap between what we desire to accomplish and what we can actually achieve is widening. Clearly, we need a new kind of computer.

Quantum computing is a major innovation since the invention of the microprocessor.

Quantum computers are much faster and powerful than today's computers. These systems are still in the developmental stage, but research is ongoing to develop quantum computers for security, business, and civilian purposes.

Today's computers (PCs, laptops, tablets, smartphones, etc.) are based on classical physics and carry out all their operations in the forms of bits that are 1 or 0 because this is the only language they can understand.

However, in quantum physics, the state can be either 1, 0, or both. Therefore, instead of using binary digits, quantum computing uses quantum digits (also known as qubits). This means a qubit can be in multiple places at once, and a quantum computer can be in many different states at the same time.

Today's computers try every possible solution one at a time, and it may take millions of years to solve big problems. Alternatively, quantum computers can find all possible solutions at the same time. In principle, a 300-qubit quantum computer could perform more calculations at once than there are atoms in the observable universe.

Quantum Computing

Quanta

In the past, classical physics could not explain the behavior of atoms or why radiation emerges from hot objects. In 1900, Max Planck coined the term “quantum” and its plural form “quanta.” When the theories of his time could not explain a phenomenon known as cavity radiation, Planck gave up classical physics dogma and said that cavity radiation is emitted only in bundles that he termed quanta.

Qubits

Today’s computer uses bits. Data travels and is stored in the form of these binary bits. Quantum computers use qubits, which are subatomic particles like photons or electrons. Managing and generating qubits is a very challenging scientific and engineering process because a qubit can be 0, 1, or both 0 and 1 at the same time.

Superposition and entanglement are the properties of qubits that provide more processing power than the same number of binary bits.

Superposition

When two waves meet, they overlap and interact. Sometimes they add together to make a bigger wave, sometimes they cancel each other out, but often it’s a combination of both. This phenomenon is known as superposition.

Qubits can have any possible combination of 1 and 0 at the same time until they are measured. The property where qubits can hold multiple states simultaneously is also known as superposition. After measurement, it then falls to one of the basis states that form the superposition, thus destroying the original configuration.

Entanglement

Quantum entanglement can be described as the physical relationship of a group of qubits in which each qubit knows what happens to the others. It matters how large the distance is between them, but together these qubits are treated as a system with a single quantum state. When one qubit is measured, it collapses its superposition to a single state. Then, other qubits also lose their superposition state and change to a single state in the system.

How Quantum Computing Works

Quantum computing works because of superposition and entanglement. It is these two properties that allow a quantum computer to process a vast number of calculations simultaneously.

Today's computer solves a problem like escaping a maze by trying every possible corridor. When it reaches dead ends, it turns back and tries another way until it finds the way out. With superposition, a quantum computer can try all paths at once.

Today's computer (two bits) has four possible states (00, 01, 10, or 11) but can process only one of them at any time. This limits the processing power of computers.

A quantum computer (two qubits) has the same four states (00, 01, 10, or 11), but due to superposition, all four states can be represented at the same time by qubits. It is the same idea as if four computers were running side-by-side.

Today's computer would take around four hundred years to go through 264 states at a speed of 2 billion per second, which is modern PC speed. In the quantum world, qubits represent all 264 states simultaneously. All the qubits have to be linked together, and once one qubit is measured, the state of all other qubits is known. This gives a quantum computer an exponentially faster speed to process data.

A natural candidate for the qubit is the electron spin because the only two possible spin orientations (upwards and downwards) correspond to the basis states of exactly one qubit. Scientists are trying to achieve this by using the quantum dot concept.

A quantum dot can be described as a spherical volume whose diameter is very, very small and located inside a solid. A free electron, which is not bound within an atom, is "locked inside" the sphere. Semiconducting materials like silicon and germanium surround that sphere.

These semiconducting materials are cooled at extremely low temperatures (one-tenth of a degree above absolute zero). Through semiconducting materials, an electric field is created and the free electron is held in place using electrical fields. In this environment, the electron spin can be switched "down" and "up" electrically. Therefore, the spin of an electron can be used to store one of the smallest units of information (0 or 1).

Like a classical computer's circuit, a quantum computer's circuit is based on quantum registers and quantum gates. Relationships between states of qubits are established through quantum gates. The qubits in a quantum computer are conceptually grouped together in the qubit register. Qubits that are entangled on their way into the quantum gate remain entangled on the way out, keeping their information safely sealed throughout the transition.

Quantum computers do not work by breaking a problem down into small pieces that can be tackled separately. Instead, the register must be initialized to represent all inputs to the problem. Then, the contents of the register evolve in accordance with relationships dictated by the arrangement of gates.

This is the fundamental difference between classical digital computers and quantum computers: to process a large dataset, a classical computer must examine data points one at a time and keep records of what it has seen.

A quantum computer, in contrast, loads all data points into the quantum register and then performs operations on the superimposed data. Once the correct operations have been performed, the contents of the quantum register are outputted, and each qubit will read either 0 or 1 according to the register state with the highest probability.

Applications of Quantum Computing

Chemical Industry

Molecule simulation is a critical field in biology and chemistry. The structure of molecules and how they interact with each other can be explained by simulation, and it can also help scientists discover new molecules.

Today's supercomputers have limitations in simulation due to the complexity of molecules. Quantum computers do not have such limitations and can perform such tasks effectively.

Artificial Intelligence and Machine Learning

Artificial intelligence (AI) is currently a major focus for the tech industry. Artificial intelligence makes machines smarter and act more like people by using human-like decision-making processes. Using various machine-learning algorithms, machines can predict and give suggestions to users. However, to make decisions or predictions, machines must have huge amounts of quality data and the capability to process that information quickly.

Because quantum computers can process huge amounts of data in a very short time, they will be a game-changer for AI.

Quantum Cryptography

In a cryptosystem, the key distribution is the main focus for quantum cryptography. Two pairs of entangled qubits are used. In this process, one qubit is sent to the recipient and another qubit is kept with the originator. These entangled qubits are in a superposition. If one of the entangled qubits is measured, it changes the state of the other qubit.

Qubits cannot be copied. When someone tries to copy a qubit in motion, it means the qubit is measured. Therefore, the sender's qubit state would change due to entanglement and the sender would know that someone has copied the qubit. The result is that eavesdropping becomes impossible.

The idea is to send a stream of these qubits along with the key that needs to be transmitted. This makes key distribution absolutely safe, and it cannot be broken.

Weather Forecasting

Currently, existing supercomputers take a long time to analyze weather conditions. Sometimes they take longer than the weather takes to change. Several parameters (temperature, air pressure, air density, etc.) are considered. These parameters make it difficult for weather to be predicted accurately with current computer technology. Because quantum computers can process huge amounts of data in a short time, they allow scientists to predict changing weather patterns quickly with accuracy.

As climate change affects the world, it becomes essential to predict weather in a short time. Quantum machine-learning applications would improve pattern recognition, and scientists would be able to predict extreme weather events. This would give time to mitigate emergency situations, and thousands of lives could be saved.

Threat to Existing Cryptographic Security

"The irony of quantum computing is that if you can imagine someone building a quantum computer that can break encryption a few decades into the future, then you need to be worried right now."

Current cryptographic techniques, based on algorithms like RSA, are responsible for providing security in today's cyberspace. Networking, information transfer, real-time communication, and online financial transactions, etc., are protected by them.

Encryption techniques are based on two aspects: keys and encryption algorithms. Imagine a number that is a product of two prime numbers. Let's say 35. Here, the encryption algorithm is simple multiplication, and the keys are the prime factors of the number, 5 and 7 in this case. This process forms the basis of the RSA algorithm. Pretty easy, right? But this is just a two-digit number for explanatory purposes.

What if there's a 7-digit number with just two prime factors? Would you still be able to produce the answer that quickly? In real-world cyber-security, RSA uses numbers of a magnitude that large (2048 bits) that current computers cannot break within a normal human's lifetime! Hence, our RSA encrypted data is pretty safe from security breaches.

However, what if quantum computers try to break it? Though current ones aren't yet capable of doing so, we may have superior ones (better algorithms, hardware, and greater number of qubits) within three decades, as per the current trends. This is henceforth a threat to prevailing security systems.

Shor's Algorithm

This is a quantum algorithm developed for factoring a number. This algorithm can break public-key cryptography by using a quantum computer. Shor's algorithm works on probability and produces the correct answer with high probability. If the algorithm is repeated, the probability of failure can be decreased. Shor's algorithm was demonstrated in 2001 by a group at IBM. They factored 15 into 3 and 5, using a quantum computer with seven qubits.

Challenges in Building a Quantum Computer

Building a quantum computer has been very challenging work. It has been very difficult to assemble the qubits and write/read information on them. Also, transmitting qubits without error has been difficult work because it requires perfect isolation and temperature. The slightest vibration can cause qubits to lose their superposition state.

Even if someone succeeds in making high-quality qubits and building a quantum computer using these qubits, building new software and hardware abstraction to interact or migrate information from current computers would be very challenging.

A quantum state cannot simply be copied. If someone takes any measurement of a quantum state, it collapses to a set of classical bits, bringing computation to a halt. Therefore, debugging software and hardware would be challenging work. New approaches need to be built to solve this problem.

Summary

Quantum computers remain largely theoretical since the concept developed nearly 30 years ago. There has been some encouraging progress, like the first five fluorine atoms were used to make five-qubits quantum computers in 2000. In 2011, D-Wave Systems declared they had success in building a 128-qubit machine.

In October 2019, Google announced it had achieved "quantum supremacy." Google built a 53-qubit quantum computer and resolved a problem that a classical supercomputer might take 1,000 years to solve, though IBM disputed the claim.

Big investments have already been made to build quantum computers by many countries and businesses. One thing is certain — quantum computers are the future.

About the Author

Amit Gupta is a Sr Consultant at GlobalLogic. He has vast experience in product transformation from on-premise to cloud.

References

Why Google's Quantum Supremacy Milestone Matters
Quantum Computing Security & Threats

GlobalLogic®

GlobalLogic is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating strategic design, complex engineering, and vertical industry expertise, we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the communications, automotive, healthcare, technology, media and entertainment, manufacturing, and semiconductor industries.



www.globallogic.com