INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 10, Issue 3 - V10I3-1159)
Available online at: https://www.ijariit.com

What are Quantum Computers and Why do we Need them?

Aarnav Chhikara
mypublishedpaper@gmail.com
The British School, New Delhi, India

ABSTRACT

Quantum computers represent the forefront of technological advancement, promising revolutionary applications across various fields. This paper explores the fundamental mechanics of quantum computing, the limitations of classical computers, and the superior capabilities of quantum computers. Additionally, it examines practical applications of quantum computing in real-world scenarios. The goal is to provide a comprehensive understanding of why quantum computing is essential for future technological progress and to highlight its potential to transform industries such as agriculture, artificial intelligence, cybersecurity, and finance.

Keywords: *Quantum, Quantum Computing, Probability, Possibility, Sycamore, Application, Shor's algorithm, Classical computers, Data, Cyber Security, Quantum mechanics, Superposition, Quantum entanglement, Quantum Tunnelling, AI, Business*

Introduction

The quantum world is rapidly developing, and as quantum computing takes over, people must understand the essentials of quantum computers. This includes understanding the mechanics they use, how they surpass classical computers, and their real-life applications. With this knowledge, individuals, businesses, and organizations can be included. Quantum computing offers numerous benefits that can be applied across various fields, from agriculture to space exploration. Its remarkable accuracy sets it apart. Consequently, billions of dollars are being invested each year in the development of quantum computing and its applications. Major companies are betting heavily on the quantum takeover of the world. It is imperative for everyone to be aware of this impending transition. Failure to embrace quantum technology or understand quantum computing can result in significant losses in the future. Early preparation, as demonstrated by companies like Google, can yield tremendous benefits. This research paper provides the necessary information for preparation and outlines the reasons for adopting quantum computing. It explores its applications and explains how quantum computing operates. The paper primarily focuses on quantum computing's "superpowers" of probability, possibility, and randomness and illustrates their beneficial use, alongside the other advantages offered by quantum computing.

Quantum computers are a groundbreaking advancement in the field of computation, leveraging the principles of quantum mechanics to perform complex calculations far beyond the capabilities of classical computers. Unlike traditional computers that use binary digits (bits) to process information, quantum computers use quantum bits (qubits). Qubits can exist in multiple states simultaneously thanks to the phenomena of superposition and entanglement, enabling quantum computers to solve problems that are currently intractable for classical machines. (Mosca and Munson)

Mechanics of Quantum Computers

Quantum computers operate on the principles of quantum mechanics. The most crucial concepts include:

- Superposition: While classical bits represent either a 0 or a 1, qubits can represent both 0 and 1 at the same time. This allows quantum computers to process a vast number of possibilities simultaneously.

- Entanglement: When qubits become entangled, the state of one qubit is directly related to the state of another, regardless of the distance between them. This interconnection allows for extremely fast information processing and error correction.
- Quantum Tunnelling: This phenomenon allows particles to pass through barriers that would be insurmountable in classical physics. Quantum tunnelling can significantly speed up certain types of computations.

Advantages of Quantum Computers

Quantum computers offer several advantages over classical computers:

1. Speed and Efficiency: Quantum computers can perform certain calculations at a speed exponentially faster than classical computers. For instance, Google's quantum computer Sycamore completed a complex computation in 200 seconds that would take the most advanced classical supercomputers thousands of years.
2. True Randomness: Unlike classical computers that generate pseudo-random numbers, quantum computers can produce true random numbers, enhancing applications in cryptography and security.
3. Complex Problem Solving: Quantum algorithms, such as Shor's algorithm for factoring large numbers, can solve problems that are currently impractical for classical computers. This has significant implications for fields like cryptography, optimization, and drug discovery.

Classical computers and their disadvantages

Before delving into the intricacies of quantum computers, it's essential to understand conventional computers and a bit of quantum mechanics. Traditional computers rely on numerous components, progressing from larger units to microchips which are made from basic modules. These modules are constructed using logic gates, which in turn consist of transistors. Transistors are the smallest units that act as switches, either allowing electricity to flow (1) or blocking it (0), forming the basis of binary digits or 'bits.' Combinations of these bits form logic gates, such as the 'AND' gate that produces an output of 1 only when both inputs are 1. By combining various gate types, complex operations and calculations can be done, which allows them to do everything from gaming to basic arithmetic like 2 + 2. (Preskill)

However, the miniaturization of transistors has led to some reaching the scale of individual atoms. At this incredibly small scale, quantum phenomena like quantum tunnelling come into play, where particles like electrons can go through barriers that would normally be impossible to go through, but due to their minute size, and the even smaller size of the electron, it allows the electron to transverse through the barrier because of quantum mechanics. This unintended electron flow, caused by quantum dynamics, presents a challenge in conventional computing. However, quantum computing emerges as the solution, working on another quantum mechanical concept known as superposition [1]. (Tabb et al.)

A good paper that delves into the mechanics behind quantum computers and why it is superior to classical computing is "Quantum Computation and Quantum Information" by Yazhen Wang.

It talks about how as time goes on according to Moore's law computers will double in power about once every two years, but now the computers have reached a point where the size of the electrical components has gotten down to the atomic level and classical computers are reaching their size limit. It talks about how quantum computers so early into their development have progressed so much that it is impossible to beat them using classical computers and how quantum computers have proven their superiority by doing things such as the Shor's algorithm. The paper tells us about the disadvantages of classical computers like how they can only generate pseudo-random numbers and how the realms of possibility and probability (which are explained further in this paper) are still far away from classical computers. The paper gives us reasons why we should focus on quantum computing more than classical computers. (Wang)

What mechanics do quantum computers use

Quantum computers are efficient because of something called superposition. But what is superposition and how do quantum computers manipulate it?

Superposition is a phenomenon wherein a single entity holds two distinct values simultaneously. Imagine Schrödinger's cat, placed in a box with a contraption that has a fifty-fifty probability of killing the cat. Until the box is opened and observed, the cat exists in both an alive and a dead state simultaneously. A similar principle applies in quantum mechanics. When a photon is fired, its charge remains undetermined until observed, at which point it assumes a specific value. This principle even applies to electrons in a magnetic field, which can be oriented upward or downward simultaneously until measured.

Leveraging the power of superposition, quantum computers can manipulate electrons in ways that challenge classical computing's limitations. Interactions between entangled electrons can affect the probability or state of a second electron, opening the door to unprecedented computational capabilities. (Tabb et al.)

To understand how quantum computers manipulate superposition we need to use this example. Suppose there is a maze a person has to go through to get to their home. Traditional computing will make the person go through every possible way to reach the house, but with the help of superposition, quantum computing is able to be every possible way to the house and when observed by the person, it gives the most likely way to the house. A maze-like this that requires hundreds of bits to solve can be solved just with one qubit as it exploits superposition.

Other than superposition, quantum computing uses quantum tunnelling and quantum entanglement. Quantum entanglement is when two or more quantum particles interact with each other. This means that the quantum state of each particle will depend on the other particles too. This, combined with quantum tunnelling, enables the quantum computers to manipulate multiple combinations of states at once.

Now to further show the quantum computers work this paper will be reviewing "Quantum Computation and Quantum Information" by Yazhen Wang again.

It talks about how, unlike classical physics which can be perfectly predicted, quantum physics is unpredictable, and even though quantum entanglement, you only have an idea of the outcomes. It tells us how anything in the quantum realm (things in the quantum realm are called quantum systems) is described as its state, and its state can be described as a vector in the complex Hilbert space. The main topics that it discusses are quantum probability and how we can use things such as the position, spin, and momentum of a quantum system can affect the result and how we can use observable information such as this to predict things in the Hilbert space and in turn the quantum realm and the quantum computers by using complex formulas such as Bayes's Theorem. It tells us about quantum circuit models, quantum entanglement and its effect on the quantum computer and the results, and the many types of algorithms used to make quantum computers like the recast quantum search algorithm. (Wang)

Benefits of quantum computers

Quantum computers are much more powerful than normal computers. A quantum computer can heavily outmatch a supercomputer. This was proven by Google in 2019 when they used a 54-qubit quantum computer named "sycamore" to do an extremely challenging simulation which would have taken the world's best supercomputer 10,000 years to complete. The simulation runs a quantum random number generator a million times to see the likelihood of different events. The quantum computer did it in 4 minutes and proved the power of quantum computing.

One big benefit of quantum computers is that they can generate completely random numbers while classical computers can only generate pseudo-random numbers on their own. This can help quantum computers to improve many areas of life such as cyber-security through encryption and doing near-impossible tasks such as finding a needle in a haystack. Quantum computers specialize in possibility while classical computers still struggle to fully understand probability. This can be really beneficial in the development of new technologies such as A.I. and can help us humans expand our limits through greater technologies.

The paper "Quantum Computing: Pro and Con" delves into the depths of quantum computing's countless benefits. (Preskill)

It talks about Peter Shor's factoring algorithm which can find the factors of any number. It is said that for a classical computer as the numbers get bigger and bigger, the algorithm will start taking a toll on the computer - increasing the time taken to find the answer. After a point, even supercomputers would take years to complete it but a nine-qubit quantum computer by IBM managed to prove Shor's algorithm. This allows quantum computers to find out prime numbers which are used almost everywhere from basic maths to complex encryption. And it's not only Shor's algorithm that quantum computers specialize in. By using its specialty of possibility and probability quantum computing can solve countless problems which may be deemed impossible and revolutionize the fields of innovation with its power. (Preskill)

How they can revolutionize businesses and the world

Quantum computing has many benefits, but they can be amplified even more if we use quantum computing in the most beneficial ways. The advantage of quantum computing is that it can use the possibility to solve problems. When this is combined with things such as AI, and farming, it can give outstanding results.

Currently, AI is booming in development and its relevance is increasing day by day Chat GPT is an example of this. But, even today it is still lacking one thing - emotion. Most technology companies are working on this very task, but their work does not amount to too much as of yet. But if AI is combined with quantum computing, it can hugely affect the progress in AI and maybe get it to understand human emotions and have some emotions of its own. This can only be possible if the speed and power of quantum computing and its 'superpower' of possibility are used correctly when combined with AI.

The same applies to farming. Today a lot of agricultural and technological companies are working on auto-farming. But this is hard to do as they have to account for every single factor that affects each and every crop. But if quantum computing is added to this field, then it can allow these companies to overcome this barrier and it can make farming fully automatic and show better results than humans can today even with technology.

A good example of the use of quantum computing has been shown in the paper "The Quantum Threat to Cyber Security" By Musca and Munson in 2019

The paper gives the example of a country - Canada and shows how the focus on quantum computing is increasing and how it can pose a threat to cyber security. The way encryption - a method used to keep data safe - works is by using public keys which are long strings of random numbers. Unless someone has a private key or knows the long string of random numbers, it is almost impossible to access the data that has been encrypted. But with the rise of quantum computing in Canada, it can be made easier to get the string of random numbers and get access to the encrypted data. Due to this cyber security has to develop itself and use some of the quantum-safe solutions provided in the paper. One of these solutions given in this paper was the collaboration of Canada's strengths in cryptography and quantum computing. This shows how quantum computing can be useful in so many fields, and even if it gets dangerous at times it is always better to work more on this technology. If used properly it can be very useful and can create a competitive advantage in business. The paper urges everyone to use quantum computing as it is more reliable against all threats - even quantum threats. (Mosca and Munson)

One of the greatest applications of quantum computing can be in financial modelling. When starting a business or taking your business into a new field, there are a lot of risky decisions that company owners have to make based on information that is already present like market data and industry trends, and a lot of times incorrect data analysis can lead to major repercussions and losses. Due to this a lot of the time companies are forced to hire data analysts and data scientists. Though data scientists and data analysts are professionals, they are still humans and because of this there are still a lot of human errors that happen, and a lot of things aren't properly accounted for. But with quantum computing, people are able to analyse and study all the data they want with perfect accuracy and speed. Quantum computers can not only analyse the data for you but also tell you things like what decisions to make and how things will work out in the future based on the data that they have collected. Due to all this, quantum computing makes the perfect financial modeler - better than any human and going above and beyond in all its tasks.

These were just a few examples, but if used properly, quantum computing can change the landscape of countless fields in technology, space, and business.

Conclusion

In conclusion, due to the shortcomings of classical computers like their size and low power, we need to switch to quantum computing if we want to keep our technologies growing and expanding. By using phenomena such as superposition it can fight back against the size limit imposed by quantum mechanics by using quantum mechanics. Apart from advancing in the places where classical computers are left behind, quantum computers have a variety of features like probability, possibility, and speed that we humans can use to finish complex, modern-day tasks with incredible accuracy and ease. The realm of quantum computers can not only add more speed and power to the things that we already do but use its 'superpowers' of possibility and probability to make accurate predictions and change the landscape of countless fields from agriculture to various fields in technology to business & finance. Quantum computing really is wonder computing and it is the future of the world. As classical computers approach their physical limits, the need for more powerful computational methods becomes critical. Quantum computers are not just faster; they offer entirely new ways of solving problems. This capability is essential for advancing technology and maintaining growth in various sectors. Embracing quantum computing is not just about keeping up with technological evolution but about pushing the boundaries of what is possible.

In conclusion, quantum computers represent the next frontier in computing, providing tools to solve some of the most complex challenges in science, technology, and industry. Their ability to process information in fundamentally new ways makes them indispensable for future innovations and developments.

Bibliography

[1]. Mosca, Michele, and Bill Munson. "The Quantum Threat to Cyber Security." *The Quantum Threat to Cyber Security*, https://www.jstor.org/stable/resrep26129.14?searchText=The+Quantum+Threat+to+Cyber+Security&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DThe%2BQuantum%2BThreat%2Bto%2BCyber%2BSecurity%26so%3Drel&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-. Accessed 11 May 2024.

[2]. Preskill, John. "Quantum Computing: Pro and Con." *Quantum Computing: Pro and Con*, 8 January 1998, https://www.jstor.org/stable/53176?read-now=1&seq=4#page_scan_tab_contents. Accessed 11 May 2024.

[3]. Tabb, Michael, et al. "How Does a Quantum Computer Work?" *Scientific American*, 7 July 2021, https://www.scientificamerican.com/video/how-does-a-quantum-computer-work/. Accessed 11 May 2024.

[4]. Wang, Yazhen. *Quantum Computation and Quantum Information*, https://www.jstor.org/stable/41714771?searchText=Quantum+Computation+and+Quantum+Information&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DQuantum%2BComputation%2Band%2BQuantum%2BInformation%26so%3Drel&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=f. Accessed 11 May 2024.