Scientific Research Publishing

American Journal of Computational Mathematics, 2023, 13, 619-631
https://www.scirp.org/journal/ajcm
ISSN Online: 2161-1211
ISSN Print: 2161-1203

The Future of Quantum Computer Advantage

Jimmy Chen

Senior Class, Jericho High School, Jericho, NY, USA
Email: jimmy.chen.2228@gmail.com

How to cite this paper: Chen, J. (2023) The Future of Quantum Computer Advantage. *American Journal of Computational Mathematics*, **13**, 619-631.
https://doi.org/10.4236/ajcm.2023.134034

Received: October 7, 2023
Accepted: December 16, 2023
Published: December 19, 2023

Abstract

As technological innovations in computers begin to advance past their limit (Moore's law), a new problem arises: What computational device would emerge after the classical supercomputers reach their physical limitations? At this moment in time, quantum computers are at their starting stage and there are already some strengths and advantages when compared with modern, classical computers. In its testing period, there are a variety of ways to create a quantum computer by processes such as the trapped-ion and the spin-dot methods. Nowadays, there are many drawbacks with quantum computers such as issues with decoherence and scalability, but many of these issues are easily emended. Nevertheless, the benefits of quantum computers at the moment outweigh the potential drawbacks. These benefits include its use of many properties of quantum mechanics such as quantum superposition, entanglement, and parallelism. Using these basic properties of quantum mechanics, quantum computers are capable of achieving faster computational times for certain problems such as finding prime factors of an integer by using Shor's algorithm. From the advantages such as faster computing times in certain situations and higher computing powers than classical computers, quantum computers have a high probability to be the future of computing after classical computers hit their peak.

Keywords

Quantum Computers, Qubit, Decoherence, Superposition, Entanglement, Parallelism, Hadamard Gates, Shor's Algorithm, Bloch Sphere, Moore's Law

1. Introduction

Throughout the 20th and 21st centuries, the modern computer has evolved and innovated in such a substantial sense that it plays an immense part in our everyday lives. However, this prosperity in computational innovations has been coming to an end—meaning that we are now in search of new forms of advanced

computers. One of the biggest solutions to this issue is the use of quantum computers. In recent years, companies such as Intel, Google, and Microsoft have been spending time and money on research on quantum computers [1]. These companies have done research in topics such as optimization and machine learning in order to continue innovating on the technologies related to quantum computers. Out of all the other options of computational technology, quantum computers have a substantial chance of being the next big hit in technological innovations because of their use of quantum laws and applications, making them faster than classical computers [2].

Classical computers, otherwise known as modern, everyday computers, have revolutionized the world by allowing people to enter the information age. Through this information age, we are able to search up things in a matter of seconds, and with the ever increasing number of transistors, the processing power of computers has been surging—leading to faster calculations and more capabilities. Today, the number of transistors in a microchip doubles every two years (what is known as Moore's Law), but these transistors have gotten so smal—around 7 to 10 nanometers (from companies such as Samsung, Intel, and Taiwan Semiconductor Manufacturing Company)—that, according to Moore's Law, in the near future, they could not get any smaller due to reaching their physical limits [3]. Even if we do create even smaller transistors the size of a few atoms, many problems would occur such as the silicon transistors being unable to properly manage the dissipation of heat. Hence, in this modern age, quantum computers are a possible solution to this hurdle known as Moore's Law (**Figure 1**).

Historical Overview

Quantum computers would be a solid solution to the Moore's Law issue since quantum computers are able to achieve comparable results to classical computers with the need of less time and number of bits. As an example, while classical computers run off of bits, which could either be a zero or a one and form the basis of binary logic, quantum computers use quantum bits, also known as qubits, which could be either a zero, one, or any value between them. This significantly expanded set of values a qubit can attain is enabled by a quantum property known as superposition, which states that a quantum system can be in any combination of two states, $|0\rangle$ and $|1\rangle$ (represented here using a special notation called the bra-ket notation to denote quantum states and highlight their fundamental difference from classical variables) [4]. This quantum superposition of a qubit between both a zero state and a one state is represented as a vector on the Bloch sphere diagram (**Figure 2**).

On top of that, due to their ability to be in both a zero bit state and a one bit state at the same time—a superposition of both states, quantum computers can be significantly faster and more powerful compared to classical computers. Quantum computers excel at solving complex problems since they are more efficient compared to classical computers. While some complex computational problems

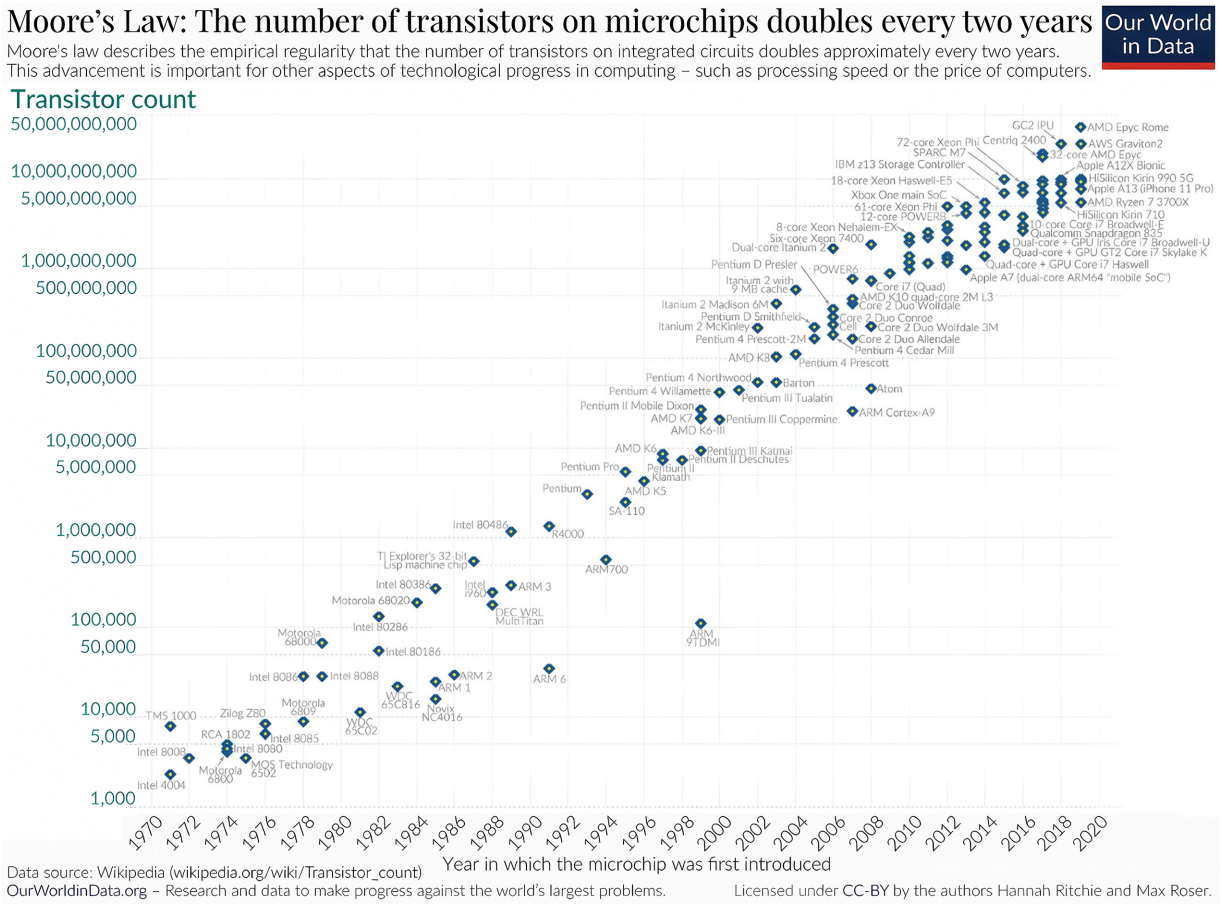

Figure 1. As shown in this graph, according to Moore's Law, the number of transistors doubles every two years: going from around 1000 during the 1970s to over 50 billion in 2020—more recently, over 120 billion in 2023.

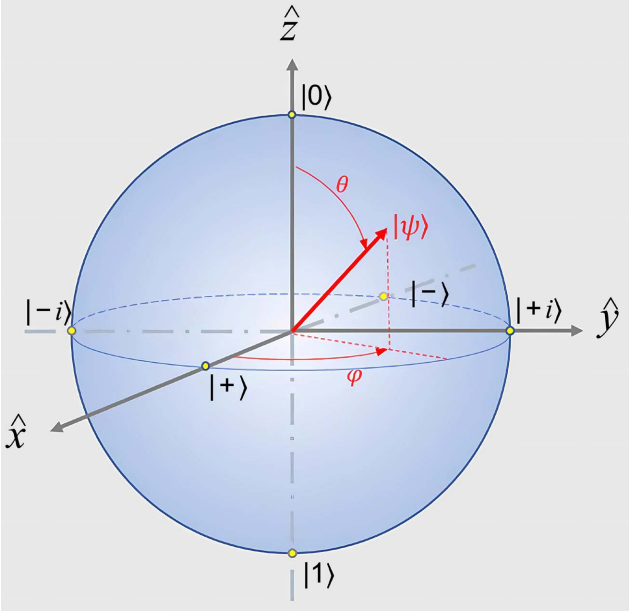

Figure 2. This Bloch sphere portrays the quantum world of a qubit. $|0\rangle$ and $|1\rangle$ represent the two distinct states of a qubit while the rest of it represents all the superpositions between its $|0\rangle$ and $|1\rangle$ states.

done by today's supercomputers might take years or even decades to solve, it would only take a matter of seconds if it were to be done by quantum computing.

Going back to classical computers, the first ever transistorized computer, TRADIC in 1954, had roughly 800 point-contact transistors while one of the highest number of transistors a computer has today is 134 billion transistors, in Apple's M2 Mac which launched in 2023. As shown in this example, the number of transistors has increased exponentially throughout this time period of about 70 years and is shown more in depth in Figure 1. Although from the graph it may seem like the number of transistors may go on forever, there is indeed a limit that we are slowly closing in on. There's a limit to the number of transistors on a circuit because as the years have gone by, the size of the transistors have become smaller and smaller (Figure 3), and as they get smaller, they dissipate an increasing amount of energy, causing their temperatures to increase, hence making it hard to create smaller or more dense circuit boards.

It's been stated that Moore's Law is slowly coming to an end, and more precisely, it will end in the 2020s. As this is an issue to the modern computer industry

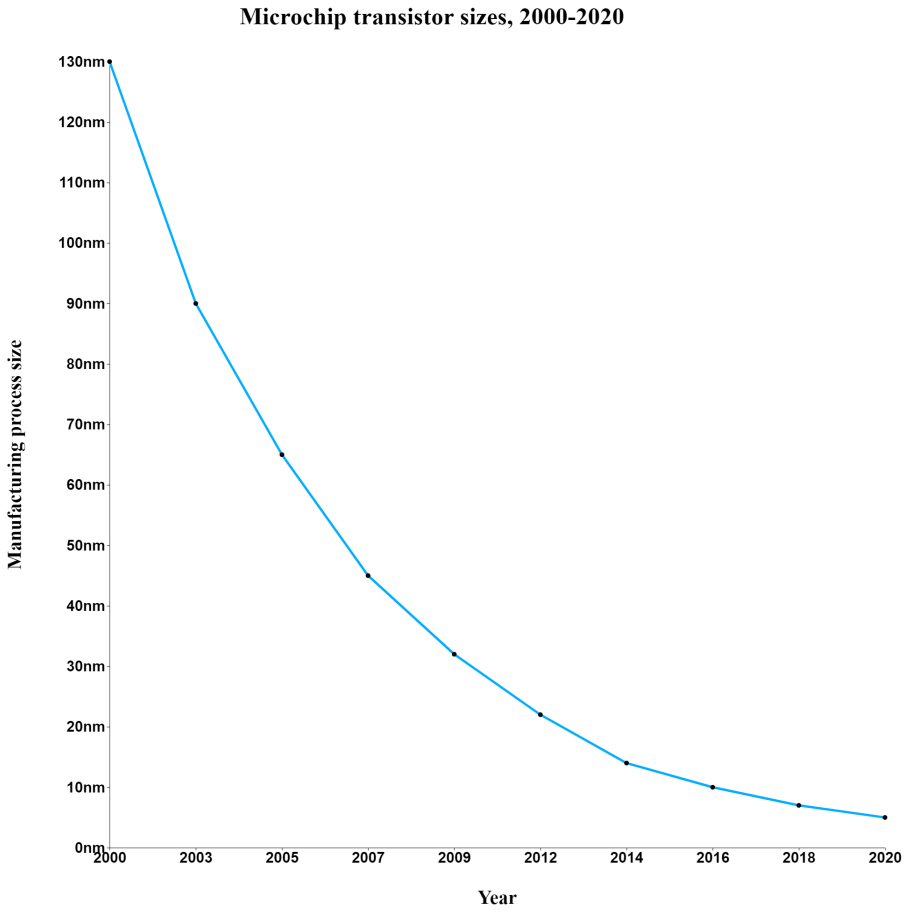

Figure 3. As shown in this graph, it shows us that as the years progress, the size of the transistors have been exponentially decreasing. But, it is clear that the size of the transistors have been reaching its physical limit.

since chips and processors will not be getting much faster, some large hi-tech companies such as Microsoft, Intel, Google, Amazon, and others, have already invested in research in the fields of quantum computing [5]. They believe that this new technology will be the future of computing due to how efficient it is and the fact that Moore's Law is coming to an end and quantum computing may overcome the limitations faced by classical computers.

2. From Classical Computers to Quantum Computers

As for the comparison between these two types of computers, they both ultimately reach the same goal of computing and outputting answers to specific operations or problems, but the difference between these two modern machines is that classical computers use bits and classical gates to perform the calculations [6]. Classical gates in a short term perform boolean functions in the computer such as AND, OR, and NOT functions which change the zeros into ones and vice versa [7]. Some may say that quantum computers are large and clunky compared to the compact modern computer, but the same was said about the classical computer when it first came out. Images of both are shown below (**Figure 4** and **Figure 5**).

These Pictures underscore the fact that both of these machines started off as big machines which are made up of large components that, over the years, have gotten scaled down and made more compact—which has been the case for classical computers. There is a lot of excitement around quantum computers because of the fact that we are still in the early days of their development, and just like when the classical computer was invented, the quantum computer has a lot of room for it to be potentially be scaled up and made more compact just like what happened to the classical computer. Moreover, quantum computers also have many advantages compared to classical computers as well. For example, the computing power of quantum computers is way faster compared to classical

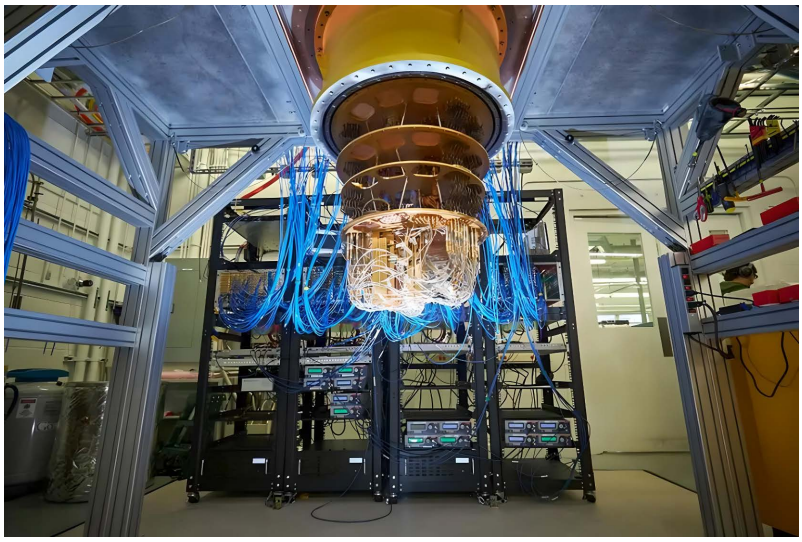

Figure 4. Image of Google's large scale quantum computer.

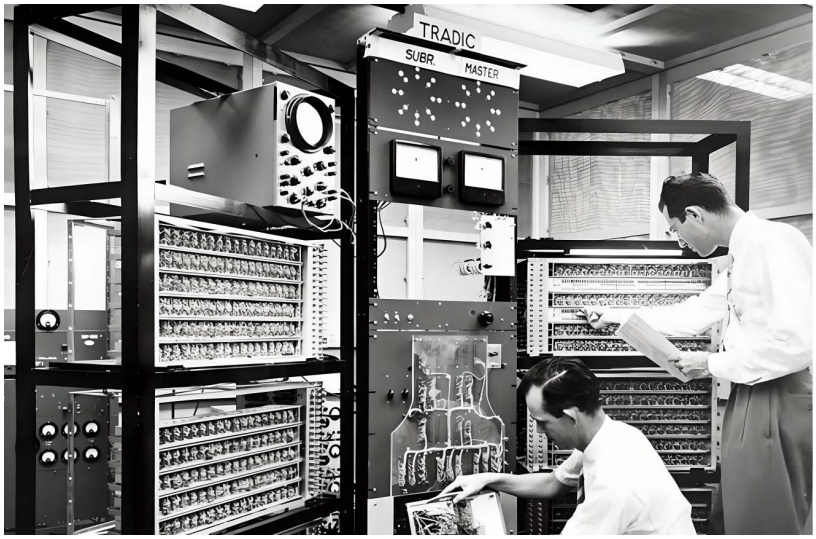

Figure 5. Image of TRADIC.

computers—more specifically, their computing power is 2^n, where n is the number of qubits used in the operation [8]. Compared to this, while the computing power of quantum computers is exponential, the computing power of classical computers is linear and directly related to the number of transistors that it contains (**Figure 6**).

While classical computers operate using bits, with their efficiency directly proportional to the number of bits, quantum computers rely on qubits. Qubits can exist in multiple states simultaneously, thanks to the principles of quantum superposition and entanglement. This property allows quantum computers to achieve faster computational times for specific problems.

In classical computers, efficiency increases linearly with the number of bits. In contrast, the efficiency of quantum computers is given by 2^n, where "n" represents the number of qubits in the quantum computer [8]. This is because a quantum system exists in a superposition of all possible states until it is measured.

As an example, in a two-qubit system, there are four possible states in bits: 00, 01, 10, and 11, resulting in 2^2, or four, potential outcomes [9].

Because of its superior computing power, quantum computers promise to offer faster computing times when compared to classical computers. Overall, quantum computers are the future of computing due to the fact that in certain instances and problems, they are already better and more efficient than the best classical computers that we have and the fact that quantum computers are just starting to emerge from the research and development efforts at several academic institutions and private companies.

3. Quantum Computers

Quantum computers implement different aspects of quantum mechanics in order to be able to compute or even work at all. The first aspect of quantum mechanics that is applied in quantum computers is the idea of superposition. The

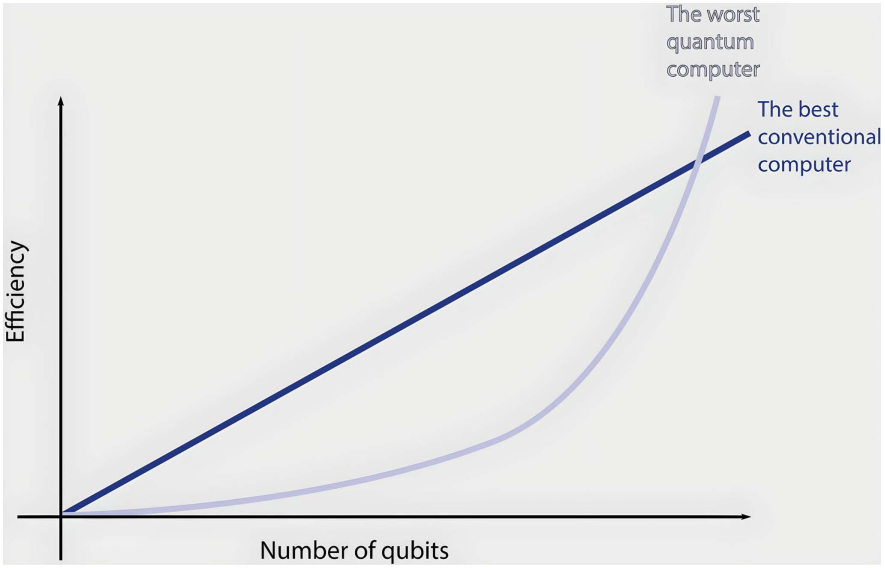

Figure 6. As shown in this diagram, the power of the computer for classical computers is a linear relationship while the power of quantum computers is an exponential relationship, meaning that it is way faster than classical computers, hence making them the future of computing since it's faster than classical computers in its early stages.

idea of superposition requires more than one quantum state, and can be realized already in a basic set of two quantum states, also known as a two level system. The set of quantum states available to a two-level system can be represented using the Bloch sphere diagram shown earlier and in **Figure 7**.

Basically, a two-level system is the superposition of two quantum states, and more specifically in quantum computers, those quantum or "pure" states are $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$, where $|\psi\rangle$ is just the notation signifying that it is a wave function and the zero and one are the two distinct quantum states. A wave function is basically a function which fully describes the state of a quantum system (e.g., a particle)—providing the probabilities and likelihood of the system being at particular positions at a certain time (**Figure 8**).

The approach for reading a wave function is by examining the amplitudes of each spike in the wave function. The larger the amplitude, the higher the probability that the particle is at that specific quantum superposition. The two-level system of the quantum computers is immensely different from classical computers because while the classical computers only have two states in total, a "0" bit and a "1" bit, the two-level system technically has an infinity of possibilities, since the generic states of the qubit are represented by a linear combination of pure states, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ [Equation (1)].

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

This expression signifies that the quantum state of a qubit can be written as a combination of $|0\rangle$ and $|1\rangle$ states—with coefficients alpha (α) and beta (β) represent the probability amplitudes, on the wave function, of each pure state.

Nowadays, many companies try to achieve the creation of an artificial qubit in

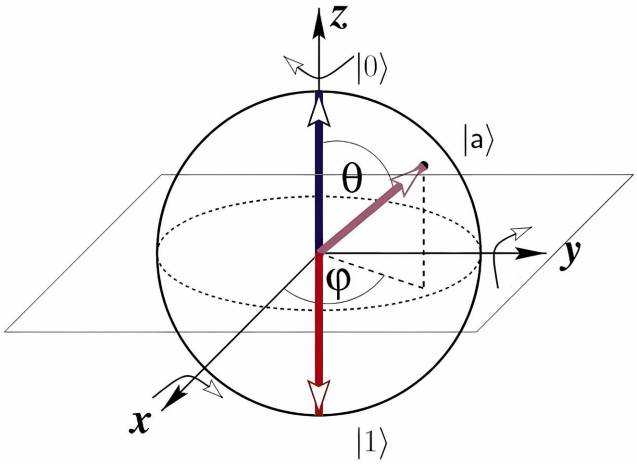

Figure 7. Image of a Bloch sphere including it's two "pure" states, |0⟩ and |1⟩. Also represented in the image is vector |a⟩ which shows the superposition of this qubit.

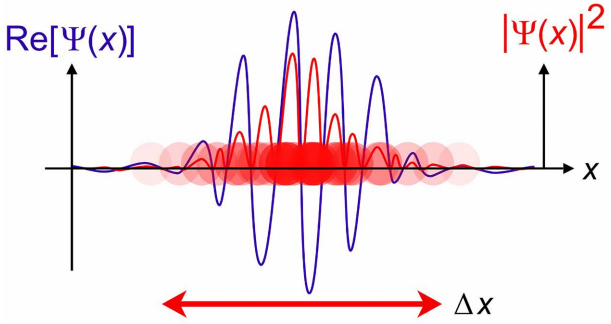

Figure 8. Image of a wave function of a qubit: shows the probability of which the qubit is at any certain superposition.

a variety of ways such as using atoms versus using particles. Some examples of these types are the trapped-ion qubits and spin dot qubits.

Creating qubits using the trapped-ion method means using particles to create a man-made qubit (**Figure 9**).

In this method, ions—subatomic particles that are charged—are suspended in an empty space where there are no gravitational and electromagnetic fields. These qubits are stored in a stable state, meaning that the qubit can remain in that state for an extended period of time without external disturbances. After the proper environment is created, quantum information is passed through into the qubits through the Coulomb force, which is a repulsive or attractive force depending on the charges of each ion [10].

Another method in creating these qubits is the spin dot method. This method primarily uses electrons from atoms. These electrons are then restricted into a static potential well in a superconductor, where the static potential well is a local minimum of potential energy for the electron (**Figure 10**).

Because it's confined to this energy level, it confers a quantized energy spectrum to the electron—a spectrum of energy where only select and discrete energy levels are present [10].

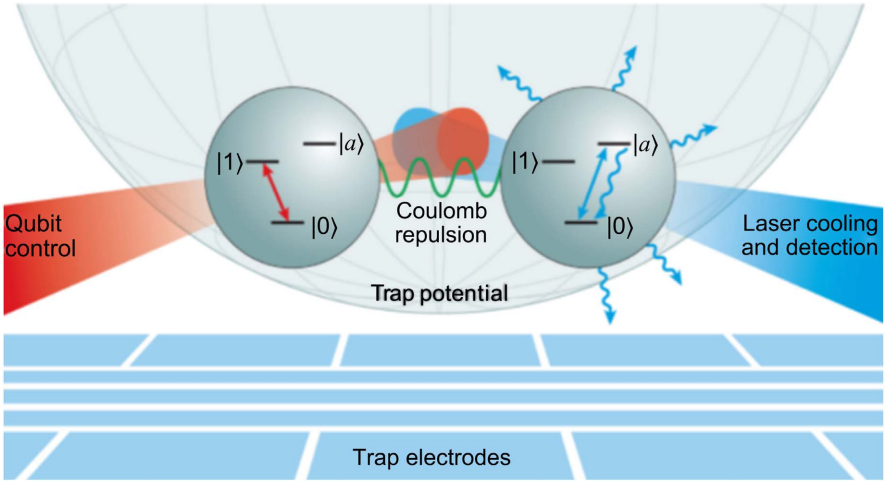

Figure 9. Image shows a representation of the trapped-ion method of creating a qubit.

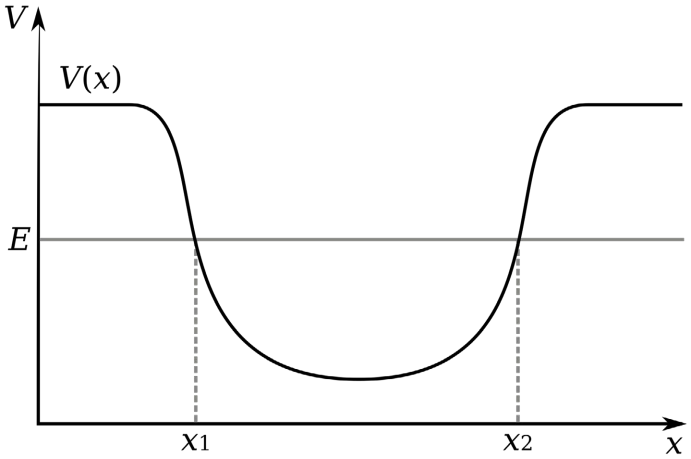

Figure 10. Graph of a function of potential energy levels $V(x)$ and a potential energy well between $x1$ and $x2$.

While a variety of different platforms seek to realize "artificial atoms" through many different methods, spin dot, trapped-ion, and others, they all ultimately seem to achieve the same outcome of creating an artificial qubit which could be modified and used for the testing of quantum computers.

3.1. Bloch Sphere

The Bloch sphere, a geometric representation of the pure state space of a two-level quantum system, has been mentioned earlier through the explanation of the two-level system (**Figure 2** and **Figure 7**).

The Bloch sphere is a visual representation of the generic superposition quantum states $|0\rangle$ and $|1\rangle$. From these two pure states, the vector, $|\psi\rangle$, representing a quantum superposition of both pure states: showing the probability amplitudes of it being in the $|0\rangle$ and $|1\rangle$ states—where $|0\rangle$ is the North pole and $|1\rangle$ is the South pole. These probability vectors on the Bloch sphere could be modified and altered by the use of quantum gates such as the Hadamard gate. The generic

combination of the equation for the superposition of the Bloch sphere as given earlier, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, can be re-expressed by replacing the alpha (α) and beta (β) terms with the angles of theta (θ) and phi (φ). This rewritten equation can be expressed through the formula, $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$—where $\alpha = \cos(\theta/2)$ and $\beta = e^{i\varphi}\sin(\theta/2)$ [11].

3.2. Implementation of Quantum Physics

Quantum computers implement many of the basic rules of quantum physics such as superposition, entanglement, and quantum parallelism.

3.2.1. Quantum Superposition

Quantum superposition is the ability for a quantum system to be in multiple states at once until the state is measured. This quantum mechanical idea of a superposition is very complicated to understand but it's way easier to think about it as a wave function. The wave function of the superposition, as stated earlier, represents the probabilities of each quantum state that the qubit could be at. So, the superposition is basically a quantum state where the state is a combination of both pure states. Quantum computers implement the idea of superposition because the qubit relies on its superposition of both the $|0\rangle$ and $|1\rangle$ states in order to compute in a faster manner than classical supercomputers.

3.2.2. Quantum Entanglement

Quantum entanglement is the idea that when you have two or more quantum particles, they could be thought about as if they are in a joint "entangled" state. This means that the knowledge about the position of one of the particles would give you the exact position of the other "entangled" particles [12]. In the sense of quantum computers, this property is sometimes used to speed up its computing times because when the state of a qubit is changed, the entangled or paired qubits would change immediately due to the property of entanglement—leading to faster computational times.

3.2.3. Quantum Parallelism

Ultimately, one of the many properties of quantum mechanics that quantum computers use is quantum parallelism. Quantum parallelism is the idea that a quantum system performs countless calculations in parallel rather than doing calculations one at a time. This property is used in quantum computers because rather than doing a single calculation at a time, quantum computers are able to perform multiple at a time, hence speeding up computational times just like quantum entanglement [12].

4. Applications of Quantum Computers

4.1. Hadamard Gates

An essential ingredient of quantum computing is the application of quantum gates. Quantum gates help with the computations within the quantum com-

puter. These quantum gates generally operate on a small number of qubits. While there are many gates which could be applied to quantum computers like the C-NOT, NOT2, and many other gates, one of the most important ones is the Hadamard Gate—also known as the square root of the NOT gate. The Hadamard Gate keeps the vector of the superposition the same but when it's used, the vector gets rotated to a certain degree. The outcome of applying the Hadamard gate to the $|0\rangle$ state is $\left(|0\rangle+|1\rangle\right)/\sqrt{2}$ and when $|1\rangle$ is passed, the gate returns $\left(|0\rangle-|1\rangle\right)/\sqrt{2}$ [13]. This is equivalent to a rotation of the vector state within the Bloch sphere (e.g., from one of the poles to the equator) After the gate has been applied onto the superposition, it rotates the state $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ to $|\psi\rangle=\alpha\left(\left(|0\rangle+|1\rangle\right)/\sqrt{2}\right)+\beta\left(\left(|0\rangle-|1\rangle\right)/\sqrt{2}\right)$ or $|\psi\rangle=\cos(\theta/2)\left(\left(|0\rangle+|1\rangle\right)/\sqrt{2}\right)+\mathrm{e}\mathrm{i}\varphi\sin(\theta/2)\left(\left(|0\rangle-|1\rangle\right)/\sqrt{2}\right)$. Moreover, since the Hadamard Gate is unitary, it's possible to get the original quantum state back by undoing the Hadamard Gate [13].

4.2. Shor's Algorithm

Another important and exciting application of quantum computers is the use of quantum algorithms that are only possible with the use of quantum computers. Quantum algorithms use the properties of quantum parallelism to be more efficient in solving problems. Because of quantum parallelism, unlike classical computers that would have to loop over several times to be able to get the answer, a quantum computer using these quantum algorithms would get the answer immediately without having to loop over anything. One of the most famous quantum algorithms is Shor's algorithm. In simple words, Shor's algorithm is used to find the prime factors of any given integer [14]. More specifically, the algorithm works in steps. As an example of the steps, if you input $N = P * Q$, and want to find the values of P and Q, the first step of the algorithm would be to automatically find a number, m, that's less than N and to find the greatest common factor between m and N. If that factor is equal to one, a function would be defined to be $fm(x) = mx \bmod(N)$, where mod() is the remainder after dividing a number by another number. Start from $x = 0$ and keep incrementing x until the output of numbers ultimately repeats and if the period of that set of numbers is equal to one, then a new value of m would have to be chosen, otherwise, the algorithm would proceed to the next step. The next step is to check if $mp/2 \neq 0 \bmod(N)$ and if that is true, the algorithm would then find the greatest common factor of $mp/2 - 1$ and N. From this step, you are able to find one of the prime factors of N, meaning that the algorithm has finished. And because quantum computers use quantum entanglement, since you have one of the prime factors of N, P, you have all the information to help you get the other prime factor of N, Q, by doing $N/P = Q$—which will ultimately output the prime values of the answer to $N = P * Q$ [15].

5. Conclusion: Future of Quantum Computers

While there is a very bright future for quantum computers and a large possibility

that they could replace classical supercomputers, there are current shortcomings and challenges that would have to be solved before it is possible [16].

5.1. Decoherence

Decoherence is a major issue for quantum computers. Decoherence is an event where the superposition of the qubit collapses due to outside interference from the environment. The superposition collapses due to an entanglement being accidentally created between the system and the outside environment. This is a major issue for quantum computers because the only way to combat decoherence is to keep the quantum particles at cool temperatures—like a fraction of a degree above absolute zero—so that the environment is immensely still, allowing a particle in its superposition to stay in its state for much longer. Otherwise, once a qubit decoheres, it loses all its information: meaning that in order to compute more complex algorithms, a qubit must be placed in an environment where its coherence state is substantially longer so that it has the capacity to run those algorithms.

5.2. Scalability

Ultimately, another substantial problem with quantum computers at the moment is the scalability issues. The largest quantum computers available today contain around 50 - 100 qubits which is way less than the thousands or millions of qubits that are required for realistic and practical computations. Scalability is a large challenge for quantum computers to overcome in order to achieve an advantage over the classical computers due to scalability issues such as cost of materials to make a quantum computer—the freezing cold environment that it needs to be in—decoherence, etc. Overall, though scalability issues are a problem of the present, just like classical computers, once this testing and birthing age of the quantum computer is over, many of these issues will hopefully be overcome, giving way to achieving a quantum advantage over classical supercomputers.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Google Research: Google Quantum. https://quantumai.google/research

[2] Tüftelakademie (2022) Quantum Computer - Quantum 1x1. tueftelakademie.de/quantum1x1/quantum_computer/

[3] IonQ Staff (2023) Quantum Computing 101: Introduction, Evaluation, and Applications. ionq.com/resources/quantum-computing-101-introduction-evaluation-applications

[4] Krambeck, D. (2015) Fundamentals of Quantum Computing. https://www.allaboutcircuits.com/technical-articles/fundamentals-of-quantum-computing/

[5] Brooks, M. (2023) What's Next for Quantum Computing. www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/

[6] IBM Quantum Learning. Composer User Guide. https://learning.quantum-computing.ibm.com/tutorial/composer-user-guide

[7] Cyril. (2020) Introduction to Quantum Logic Gates. http://einsteinrelativelyeasy.com/index.php/quantum-mechanics/153-introduction-to-quantum-logic-gates

[8] Cyril. (2020) Introduction to Quantum Computing. http://einsteinrelativelyeasy.com/index.php/quantum-mechanics/152-introduction-to-quantum-computing

[9] Mullane, M. (2023) Quantum Computing 101. https://medium.com/e-tech/quantum-computing-101-38306018d07c

[10] Grumbling, E. and Horowitz, M. (2019) Quantum Computing: Progress and Prospects. https://doi.org/10.17226/25196 nap.nationalacademies.org/catalog/25196/quantum-computing-progress-and-prospects

[11] Yanofsky, N, and Mannucci, M. (2008) Introduction to Quantum Computing: Bloch Sphere. https://akyrillidis.github.io/notes/quant_post_7

[12] Dejen, A. and Ridwan, M. (2022) A Review of Quantum Computing. *International Journal of Mathematical Sciences and Computing* (*IJMSC*), **8**, 49-59. https://doi.org/10.5815/ijmsc.2022.04.05

[13] Vos, J. (2019) All about Hadamard Gates. https://freecontent.manning.com/all-about-hadamard-gates/

[14] Wikipedia (2023) RSA (Cryptosystem). https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[15] Marchenkova, A. (2015) Break RSA Encryption with This One Weird Trick. https://medium.com/quantum-bits/break-rsa-encryption-with-this-one-weird-trick-d955e3394870

[16] Velu, C. and Putra, F. (2023) How to Introduce Quantum Computers without Slowing Economic Growth. https://pubmed.ncbi.nlm.nih.gov/37460723/ https://doi.org/10.1038/d41586-023-02317-x