


# Quantum computers as a future technology



Maryam Lotfigolian

Oslo Metropolitan University  
ACIT 4100 – Understanding and Communication Research

## Table of Contents

On the first of August 2021, Grandpa's home .....	3
Steven's motivation .....	5
Steven's Methodology .....	6
Fundamental concepts.....	7
Qubits and Superposition property .....	7
Quantum gates .....	8
Quantum entanglement .....	10
Steven, how do you define “fast” in quantum computation?.....	11
What is the problem, Steven? .....	13
Steven, is it possible to construct quantum computers? .....	15
Is it a lie?.....	18
Do we need to be concerned, Steven? .....	18
Conclusion .....	20
References.....	21

## Table of Figures

Figure 1: Sycamore processor [14].	7
Figure 2: Classical bits can only exist in one state or the other, whereas qubits can exist in a combination, or superposition, of both states [18].	8
Figure 3: This figure shows how Hadamard gate manipulates the qubit to be in a superposition state in the unit Bloch sphere [20].	10
Figure 4: Quantum computer programming with quantum gates and visualization of a circuit [20].	10
Figure 5: A comparison of classical and quantum factoring algorithms[24].	12
Figure 6: The communication of information over a noisy channel and correcting errors [37].	15
Figure 7: Using superconducting technology, IBM designed an early 7-qubit chip [43].	16
Figure 8: Qubits made from trapped ions are impeccable [46].	17

## On the first of August 2021, Grandpa's home

"Silence and fear were all we could hear. Sailors felt the cold ocean wind on their faces. The captain's voice suddenly broke the silence, 'Now is the time.' Sailors circled the device, which was about four feet high, and entered information about shooting angles. We were using it for the first time. Battle rules were about to be changed by that device!"

'Fire!' shouted the captain. Smoke didn't take long to appear in the distance. It was crazy.

It was scary when we had face-to-face battles, and we could see the fear in the enemy's face. The last battle had taken only eight minutes once both ships got close enough. Blood was in the air. All we wanted was to see our family again" the old man kept silent and thought about how he missed going home.

"During WWII, the US Navy used computers for the first time to know when to fire torpedoes at moving targets. We return home as heroes!" said he with a smile.

Steven, his only grandchild, was listening to him talk about his memories. Since childhood, he has enjoyed listening to his grandpa's stories. Now he is a young man and wants to decide about his future.

- With this experience of using computers in war, what do you think about new arrival technology?

-Steven, it's hard to answer your question. When humans invent new technology, we usually ignore all the side effects. The first thing we do is see if it works, then we find out later, sometimes much later, what else it does [1]. For example, computers, there are no doubt computers have helped solve many problems worldwide. Companies are saving countless hours on accounting and management tasks. It allows doctors to analyze medical data and perform surgeries faster. Students learn new concepts better with them. Governments use it to map countries, plan infrastructure, and collect data. The list goes on and on. Computers have revolutionized many parts of our world; they've made daily life easier in countless ways. Modern society would not exist without them. Many organizations now rely on computers; it's difficult to imagine the modern world without them [2]. There have been a lot of changes since computers were invented. But mass unemployment, income inequality, social instability, and wars are also part of these changes.

It's great when you use technology right. But it can cause problems when you don't. There's always someone outside taking advantage of it. It's hard to imagine how the world will look in 2050, even though "everyone will still have two arms and two legs and an unpleasant smell if they don't wash" [3]. And if there's another world war, I don't know how technology will shape it!

- Progress has brought unprecedented prosperity, but I accept that it's also made it easier to harm. Despite that, the beneficial outcomes have outweighed the destructive ones [1].

-You are right. Have you heard about Darwin's theory, "survival of the fittest" [4]?

-Yes.



-As civilization has evolved, aggression has been helpful because it has definite survival advantages, and it's hardwired into our genes. Our logic and reason must control this inherited instinct. Our technology has advanced so rapidly that this aggression may result in a catastrophic war that destroys all of us [5].

- Aren't you pessimistic about technology? People will benefit from science and technology more. I also want a world that's livable, not dystopian. Let's imagine we can cure cancer with technological advancements!

- Are we going to need more people when the world is exploding?

Steven laughed loudly.

-Grandpa, computer technology does not end here. Now there is a promising technology known as quantum computers, far superior to classical computers.

- Jesus! Are we moving further than this? What type of computer?

-Quantum computer! In my opinion, it's the next generation of computers.

-Be careful with this new technology, young man! Do you intend to contribute to advancing this new generation of computers? If so, I would like to know what motivates you.

## Steven's motivation

Steven explained that at a New York City press conference in the early 80s, IBM announced their first personal computer running DOS, with 640k RAM and 4.77MHz CPU [6]. At that time, there were no networks, just floppy disks. The invention of the internet and innovations such as digital computers and smartphones have fundamentally altered record-keeping and information access. Nowadays, everyone carries a laptop and smartphone with far more capabilities than IBM's first personal computer. In recent years, mobile devices, such as smartphones, have made people more accessible worldwide than ever. This way, more information can be shared with greater ease and allows users to access a wider variety of data. Because of digital technology, information has become increasingly prevalent in today's world and has almost dominated every aspect of our lives.

In the meanwhile, the field of computer science is experiencing tremendous growth. In particular, the emergence of machine learning algorithms and Artificial Intelligence (AI) changed the game entirely in the world of data. In recent years, machine learning algorithms have been developed to extract patterns from data and make decisions, including analyzing trends and recommending courses of action based on previous data. These algorithms are used in many areas, from academia to industry. For example, we could focus on energy consumption and recognizing customer behavior patterns in the energy industry [7]. Such tasks can be accomplished by training a machine learning model with a large dataset. AI also allows the creation of models that mimic brain function and neural pathways, and many believe that AI will soon outsmart humans [8]. People create more detailed models and more lifelike simulations in their artificial intelligence applications with the help of AI. These state-of-the-art technologies are primarily characterized by data and models' computational capability.

However, the question arises, how far can we go with this amount of data and increasingly complex models, which require a high level of computational power and energy? Will it be enough to increase the number of computer servers to process our models simultaneously? Should we make tiny computer chips with billions of transistors and thousands of processors to improve our models' computational capabilities?

Adding more servers might not be the right solution. If we increase them virtually, security concerns, implementation and licensing costs, and many other problems will arise [9]. And when it comes to increasing physical servers, it is not environmentally friendly and consumes a great deal of energy.

According to Gordon Moore, CEO, and co-founder of Intel, the number of transistors on integrated circuits is expected to double approximately every two years. In the presence of these chips, there is an increase in computational speed, but there is a limitation. We can't apply Moore's law when we miniaturize chips and put more transistors on them [10]. So, what's the solution?

If a computer has the solution, it will be a revolution in the field of computer science. We may be able to resolve serious issues. For instance, in computer-assisted drug discovery (CADD), pharmaceutical companies use computers to predict the behavior of molecules that may form a new drug. Although supercomputers can simulate simple molecules, companies need more time to simulate every molecule, resulting in missed potential treatments. Researchers need to learn more about how molecules interact with proteins in the body. So, the failure rate of newly developed drugs in trials is often high and costly. Suppose we have computers capable of reviewing drugs at a molecular level with incredible speed and conducting drug trials with each compound tested against a cell model in a rapid timeframe. In that case, we can revolutionize drug discovery leading to radical improvements in treatments for cancer, Alzheimer's, and other diseases [11, 12]. Quantum computers might offer solutions to some of the world's concerns.

Grandpa looked at him with surprise!

- Are such computers available? Or is it a research project? Where did you hear about this topic?

## Steven's Methodology

- There have been some breakthroughs in developing quantum computer hardware and software. For example, in 2019, Google claimed to have developed a high-performance parallel structure quantum computing processor named "Sycamore" (Figure 1) for benchmark testing. They reported that their machine performed the target computation in 200 seconds, and they calculated that the world's fastest supercomputer would take 10,000 years to achieve a similar calculation [13]. Such progress is of great value at the research level. We see that researchers are demonstrating that this technology is feasible. To answer your last question:

First, it is an interdisciplinary subject related to mathematics, computer science, and quantum physics. I became familiar with this subject in the university's Quantum Information Technology course this semester. I aimed to gain a broad understanding of the topic by studying the fundamental concepts I needed from multiple papers. I had a literature review from Google Scholar, IBM, and AI Google blogs. I organized the articles into a taxonomy of definitions

showing how quantum computers differ from classical computers. At last, I could determine the perspective of this technology and its challenges. I intended to become familiar with the ongoing research on this topic.

I enjoy talking about it with you, Grandpa. You can understand how one technology can revolutionize our lives.

- I'm also aware of the danger! Technology is far more dangerous than its reputation. From what you're saying, I can smell more of the power imbalance around the world. It is hard to imagine how much worse the world will become if powerful countries first have access to this technology. I want you to see both sides of everything.

Okay, let's talk about how it works later. I see your excitement, but I need some rest.

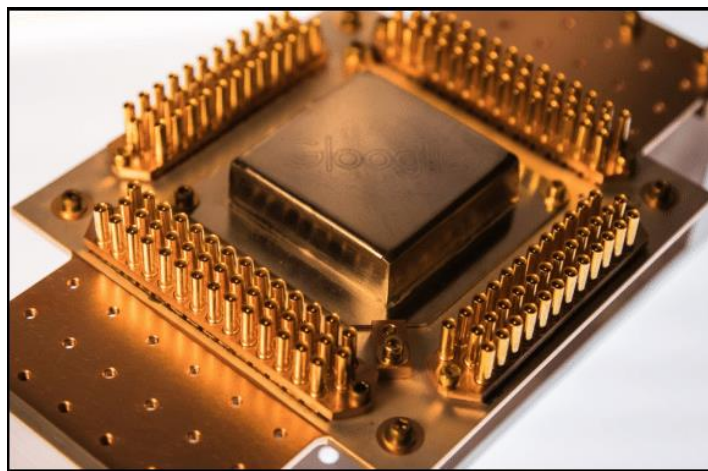


Figure 1: Sycamore processor [14].

## Fundamental concepts

Grandpa's house is where Steven studies; quiet and great for focusing. Besides that, he always has good company there to speak with. He needs to review the building block of quantum computing before the final exam. He knows these concepts are important for understanding other subjects. Taking the time to look at them many times is worthwhile. As he looks through his notes, he sees:

### Qubits and Superposition property

A qubit is an elementary unit of quantum information introduced by Schumacher in 1995 [15]. Qubits are quantum versions of classical bits. There are two states in a single qubit, such as a spin-half or a two-level atom. These two states are orthogonal and written as  $|0\rangle$  and  $|1\rangle$ . A quantum system with  $n$  qubits is inside a Hilbert space<sup>1</sup> with  $2^n$  dimensions, and in this system, there are  $2^n$  mutually orthogonal quantum states [16]. The difference between qubits and bits is that qubits can simultaneously be in both states, 0 and 1. They don't need just 1 or 0 (as shown in figure 3). This property is called superposition which has a crucial role in quantum

---

<sup>1</sup> A Hilbert space is used in mathematics for generalizing Euclidean vector spaces to infinite dimensional spaces.

computing. The information inside the qubits can be described by complex numbers and written as (for one qubit) [17]:

$$\alpha|0\rangle + \beta|1\rangle$$

$\alpha$  and  $\beta$  are called amplitudes, representing how much a qubit is in the computational basis  $|0\rangle$  or  $|1\rangle$ . Amplitudes are complex numbers. If we measure the qubit, the amplitude forces the qubit to be either 0 or 1, and the qubit will collapse in one of these two states. This means the result will be classical bits. The probabilities we observe 0 or 1 are as follows:

$$\text{probability}(0) = |\alpha|^2$$

$$\text{probability}(1) = |\beta|^2$$

The critical point is that we can control this amplitude. To design a quantum algorithm, it is essential to control amplitudes during computation to create an extremely high probability of obtaining a useful classical result [17]. The Bloch sphere provides a graphic representation of qubits. The states terminate inside the surface of the unit Bloch sphere, which is unitary, as shown in Figure 2. We can control the probabilities inside the unit Bloch sphere.

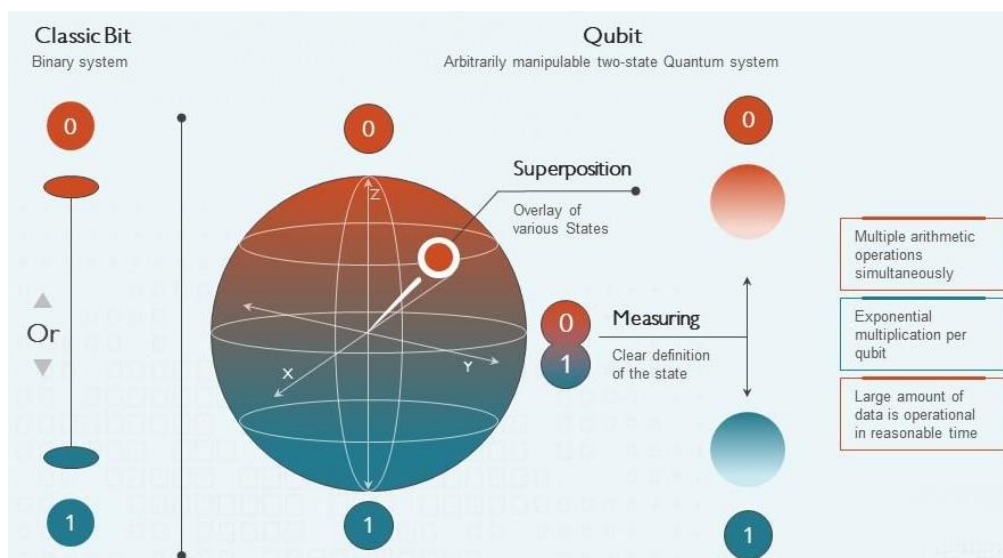


Figure 2: Classical bits can only exist in one state or the other, whereas qubits can exist in a combination, or superposition, of both states [18].

## Quantum gates

A quantum gate is a unitary operation that acts on a single input qubit to transfer information. Every single qubit evolves through these gates. A quantum logic gate is a fundamental concept in the quantum circuit that operates on several qubits in the quantum computing [19]. As classical logic gates are for conventional digital circuits, quantum gates are the building blocks of quantum circuits. For a single bit in classical information theory, there are only two logic



gates: identity and logical NOT operation. Whereas the action of some Hamiltonian<sup>2</sup> in Schrödinger's equation<sup>3</sup> produces an infinite number of single-qubit quantum gates (since they are all unitary operators) [17]. The action of these gates on a single qubit is reversible. It means that if they act twice on the qubit, its state will return to the first state.

Pauli gates are famous quantum gates, and their action is as follows:

Identity gate: Qubits will not be affected by passing through this gate.

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$$

Flip Gate: Like a NOT logic gate in classical computing, it flips the state of a qubit from 0 to 1 and vice versa.

$$X \equiv |0\rangle\langle 1| + |1\rangle\langle 0|$$

Z gate: The gate affects state 1 and sends it to state -1.

$$Z \equiv |0\rangle\langle 0| - |1\rangle\langle 1|$$

Y gate: Combination of two previous gates.

$$Y \equiv XZ$$

Two other vital gates are CNOT and Hadamard gate. CNOT flips the state if the previous state is 1; otherwise, do nothing. And Hadamard sends each state to the superposition state. With CNOT and Hadamard gates, we can construct entangled qubits.

Hadamard gate sends the state to the superposition state, which is both 0 and 1. If we measure the state after transforming through the Hadamard gate, we will see either 0 or 1 with a 50% probability (as shown in Figure 3).

---

<sup>2</sup> It is an equation that describes the motion of particles in terms of their momentum components and coordinates of space and time. It equals its total energy when time is not explicitly included.

<sup>3</sup> A differential equation is used to describe the wave-like properties of particles within a field in the context of quantum mechanics. Particles' probability density in space and time is the solution of the equation.

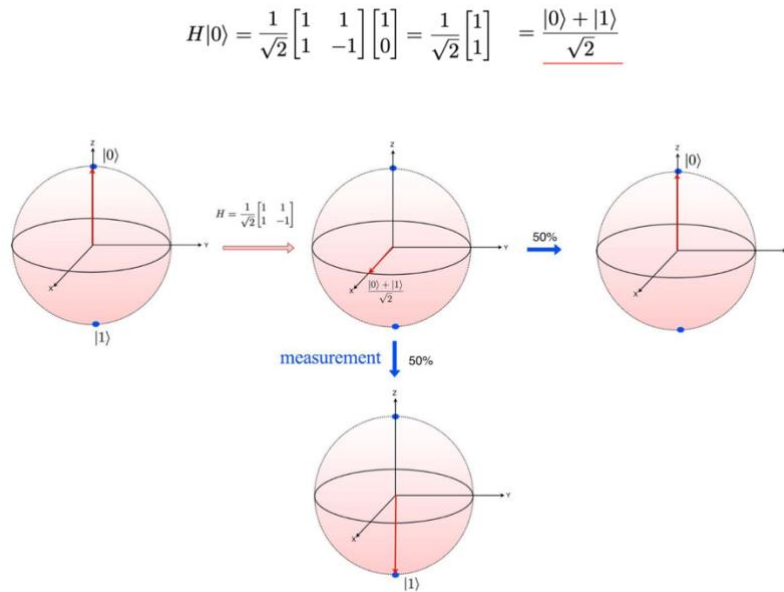


Figure 3: This figure shows how Hadamard gate manipulates the qubit to be in a superposition state in the unit Bloch sphere [20].

## Quantum entanglement

Quantum entanglement describes two particles acting based on each other as twins connected by an unobservable wave. As soon as one of the entangled qubits is measured, the other is immediately cast into its perfectly correlated state and shows its state [21]. But notice that this correlation is more robust than what we know in classical correlation, and states of the entangled qubits are not separable.

In summary, quantum superposition allows quantum computation to handle one and zero simultaneously. In contrast, the classical analysis relies on transistors to crunch the ones and zeroes individually. Additionally, quantum computers can outperform classical computers for specific challenging tasks thanks to quantum superposition and entanglement. To perform quantum computations and process quantum information, quantum computers are constructed using quantum circuits with quantum gates (as shown in Figure 4) [21].

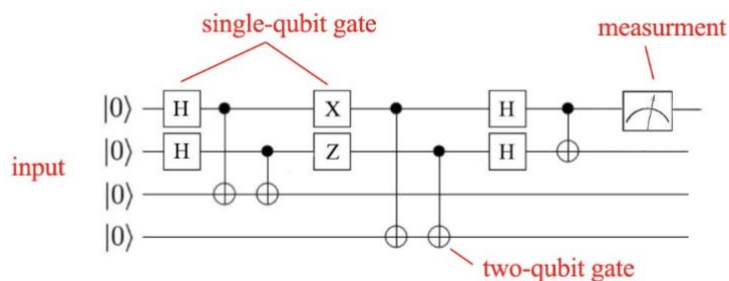


Figure 4: Quantum computer programming with quantum gates and visualization of a circuit [20].

## Steven, how do you define “fast” in quantum computation?

Grandpa sat on his old chair, looking at the fire in the fireplace. The winter was cold and dark, and Steven was enjoying his coffee beside him. Steven's enthusiasm for talking about his favorite topic makes grandpa happy. So, Grandpa started talking.

-Steven, we still haven't finished our conversation. What makes quantum computation so fast? Could you elaborate?

- Sure! Researchers have attempted to establish algorithms based on the main concepts of quantum physics to demonstrate the idea of being fast. Some algorithms outperform classical algorithms. In 1985, David Deutsch and Richard Jozsa published the Deutsch-Jozsa algorithm, one of the first quantum algorithms. This algorithm demonstrated very well the notion of a speed-up [22]. Consider a box with a function inside it. The function is either balanced or constant. In other words, it is balanced if you give it  $n$  bits, and it returns half zeros and half ones. It is also constant if it returns just zero or just one. The classical approach to processing data involves sending information bit by bit. It is as if you are shooting information piece by piece. Okay, Grandpa, how many bits should we send to see if our function is balanced?

-Well, if you send two, the first one is zero, and the second is one, then it's balanced.

-Correct, but what do you do if you get two zeros or two ones?

-we'll send the third one.

-That's precisely what we do, and if we're not lucky, we go until  $n+1$ !

-Yeah, we have to send  $n+1$  if it shows us  $n$  one or  $n$  zero.

-great, but what's the point of quantum computation? There's a concept called superposition. It is possible to have one and zero simultaneously inside a quantum bit, also known as a qubit. As a result of this property, we can shoot all the data simultaneously. This means we send everything once instead of piece by piece  $n+1$  times.

-That's awesome.

- Yeah! Do you remember when I told you about parallel servers working together in the classical approach?

-Yes, indeed.

-With the advent of quantum computers, we can now have the concept of parallelism in one device. Deutsch-Jozsa's algorithm served as the seed for other research; however, the result of the algorithm is just in theory. Following this, several algorithms were developed. People began to demonstrate that quantum algorithms can be faster in computation than classical algorithms. For instance, in 1995, Peter Shore introduced the Shore algorithm [23]. Are you familiar with the Fundamental Theorem of Arithmetic?

- Yes, I recall my time at university and my calculus course.

- As you know, the fundamental theorem of arithmetic states that every integer greater than one can be uniquely expressed as a product of prime numbers. Shor's algorithm works similarly. To factor large integers such as  $N$  into two prime factors, Shor's algorithm uses a quantum polynomial-time algorithm. This algorithm is exponentially faster than the classical algorithm. In classical computers, factorization takes exponential time as the number of digits increases, whereas a quantum algorithm returns factors in polynomial time (as shown in Figure 5).

In contrast to the Deutsch-Jozsa algorithm, this algorithm has an excellent practical implementation example. A powerful quantum computer could easily break public key cryptography in light of the algorithm. In modern cryptography, public key algorithms assure electronic communications and data storage confidentiality and authenticity. Multiplying two large prime numbers forms the public key  $N$ . In classical algorithms, factoring  $N$  becomes increasingly time-consuming as  $N$  increases. We base the security of our online transactions on the assumption that it is virtually impossible to factor integers with a thousand or more digits (specifically, no classical algorithm can factor in  $O((\log N)^k)$  time for all  $k$ ). The Shor algorithm, on the other hand, is capable of cracking public keys in polynomial time.

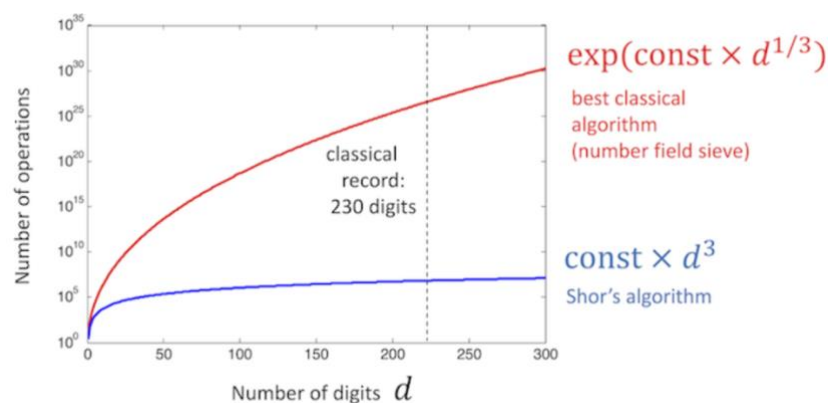


Figure 5: A comparison of classical and quantum factoring algorithms[24].

The Grover algorithm is another algorithm that helps speed up classical problems. The algorithm can be used to speed up an unstructured search problem quadratically and as a general trick or subroutine to improve other algorithms' performance quadratically. Let us examine an example of an unstructured search problem. Consider the case where you are given an extensive list of  $N$  items. One of these items has a unique property that we wish to locate. It's a winner.

- How many steps do I need to find the winner of  $N$  items, Grandpa?

- We'll see them one by one, right?

-Yes, we need  $N$  steps to find the winner in the worst case of a classical solution. With Grover's Algorithm, we can find the marked item in the roughly  $\sqrt{N}$  steps on a quantum computer [25]. When we are searching in long lists with marked items, quadratic speed-ups can save considerable time. This algorithm also provides a quadratic quantum speed-up to many other



classical problems. Using this capability, quantum computers can search large databases in a short amount of time which classical computers would take years to do.

Using the concept of superposition, people developed many algorithms that incorporate speed, for example, in machine learning and deep learning. They initially believed that quantum concepts could not be used within machine learning techniques. The tremendous success of machine learning and deep learning in classical neural networks made it particularly interesting to quantum algorithm developers. However, neural networks appeared to be an unnatural fit since they require nonlinearity to solve complex problems, which is incompatible with quantum computation's inherent linearity [26]. Later, researchers found a way to integrate the concept of nonlinearity with quantum computation during the development of machine learning and neural networks. For example, they introduced quantum Support Vector machines to demonstrate how quantum information is exploited to enhance this machine learning classifier algorithm [27]. Now, approaches range from translating classical machine learning models into quantum algorithms to developing new models based on quantum computing principles. For instance, many current financial methods, such as risk analysis, can directly derive from Monte Carlo sampling. A quantum speed-up can be achieved for Monte Carlo sampling (with a quantum amplitude estimation) [28]. A key capability of quantum computing in machine learning is its ability to parse large quantities of data in relatively short timeframes or in ways that are otherwise intractable. On the other hand, it enables applications for machine learning that might be highly commercialized in the future [29].

- Okay, so quantum computing beats classical computing every time?

- Yes, theoretically. Practically, quantum computers are prone to errors and are expensive. Quantum setups would be unreliable for simple tasks like multiplying numbers. Our classical algorithms will perform the calculation on a quantum computer similarly to classical computers. And this approach makes the calculation probabilistic. In this situation, classical computers are better at solving most of today's problems. For example, if you want to multiply two by two in a quantum computer, they will take some time, but they might ultimately tell you that it is 3.97 with a probability of 98 percent.

## What is the problem, Steven?

- Steven, why have we yet to invent quantum computers to use them as an alternative to classical computers for solving problems that take classical computers a long time to solve?

- Researchers have proposed using quantum phenomena like superposition to speed up classical problems in various algorithms. There was discussion at that time about using some of the algorithms in computers other than classical computers. Paule Benniof proposed a quantum Turing machine for this purpose for the first time [30]. A quantum computer must meet some criteria to qualify as an actual quantum computer. We need a large number of qubits. We must then find a way to entangle them and develop algorithms for moving the entanglement qubits around. Eventually, we measure the qubit; it will collapse to reveal the final state. The final state should be the one that answers your problem correctly with a high degree of probability. In other words, quantum computers aren't standalone devices. To program and read out, it needs other devices.

David P. DiVincenzo proposed some criteria in 2000 [31]. These are the criteria [31, 32]:

1. We need a physical system that is scalable and well-characterized qubit: We need a physical system that includes a collection of qubits rather than a single qubit to achieve scalability. A significant challenge facing most quantum computers is that linearly increasing the number of qubits can result in an exponential increase in the experimental setup, thus rendering any speed-up ineffective.
2. We need to initialize the qubits to a simple fiducial state: A specific computing requirement is that registers be initialized to a known value before computation begins. It means qubits should be in a well-defined state before executing a computation. Most platforms tend to choose the state with the lowest energy, and this is the meaning of being well-defined. However, achieving the lowest energy consumption means reducing the temperature of devices that are energy consumers on their own.
3. Decoherence times that are long enough to perform proper operations on the qubit: Decoherence is a property that every qubit possesses, resulting from a quantum system reverting to a classical system when it interacts with its environment. The decoherence times must be long enough to manipulate the qubit in a useful manner. If qubits affect by their environment in a short time, we might not be able to manipulate them.
4. "Universal" quantum gates: As in classical computing, we wish to create another set of gates from a set we already have. We can use this method to translate existing quantum algorithms into forms suitable for implementation on physical devices or at least into the operations we can currently perform.
5. Qubit-specific measurement capability: After performing a computation, we wish to determine the qubit's state without destroying it. Quantum Computers should be capable of obtaining accurate information in this regard.

As of now, however, there are still a few challenges to overcome before quantum computers become available.

In quantum computation, noise is inevitable when we combine the qubits, which is why large-scale computers have yet to be constructed. The noise brings us errors. Error correction needs more qubits (Figure 6). And it means more problems. For example, they tend to be not as dependent as they should be. This issue is known as crosstalk. The term has been adapted in quantum computing to describe a wide range of physical phenomena whereby one device subsystem unintentionally affects another subsystem - a qubit, a field, a control line, a resonator, a photodetector, etc [33]. However, in quantum computers, error correction is significant since efficient quantum algorithms employ large-scale quantum interference, which is fragile, i.e., susceptible to errors in the computer system and unwanted coupling between the computer and the environment [34]. As a result, large-scale quantum computation is practically impossible without error correction methods. For example, we can envision a quantum internet if we can correct errors while using quantum algorithms in quantum communication.

Several studies have been conducted on error correction. Shor and Steane were the first to discover quantum error-correcting codes. Shor demonstrated that a single qubit could be protected against general errors by using nine qubits (more qubits for error correction). In comparison, Steane described a general code construction consisting of seven qubits that accomplishes the same task [35, 36].

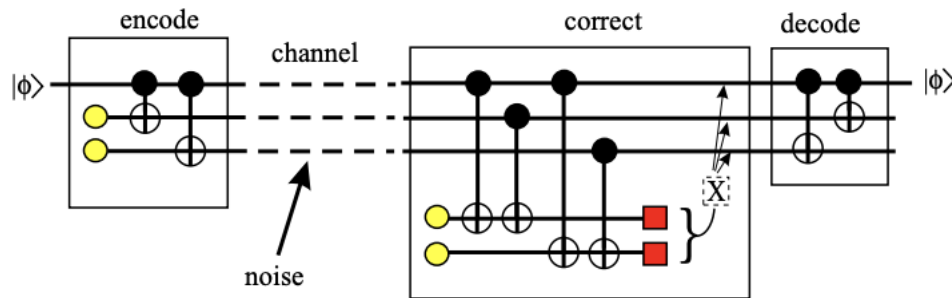


Figure 6: The communication of information over a noisy channel and correcting errors [37].

There is also a problem related to the number of algorithms available. Many are not practical and only known because of their theoretical abilities to increase speed.

Memory is another problem. It is possible to make data permanent on classical computers and move it around as needed. Disk memory can store data for an arbitrarily long period, which can then be copied and used for computation. It is also possible to send the results back to permanent storage. On quantum computers, however, the quantum data is typically only retained for the duration of the program. There are several reasons for this. According to Wootters and Zurek [38], the no-cloning theorem prohibits copying quantum states; therefore, quantum computations always operate directly on the input data. Quantum memory is also severely restricted by the physical limitations of quantum devices. Quantum states are fragile, and they naturally decay over time. As a result, it is challenging to maintain quantum information for an extended period. On the whole, several large-scale quantum algorithms heavily rely on the memory [39]. In the future, perhaps quantum memory will become more practical due to the development of quantum technology.

It is also not possible to have the property of quantum computing on classical computers as well. Neither superposition nor entanglement is possible in a classical system. This results in errors, if decoherence occurs during the manipulation of qubits and data, which is lost [40].

-Wow, you named many things, and I tried to follow you. So, we need tons of qubits that don't interact with the environment. The more time we have, the better we can manipulate them. We're trying to make qubits correlate or entangle. After that, we can move them around for algorithm processing. But more than these algorithms are needed. It's also important to know these qubits' first value, and then we want to get a classic answer from them. We also want to make another gate based on the available gates. We'll have errors when we have a lot of qubits and gates. Correcting them means more qubits and more problems. There's also a problem with memory, so there's still a lot to figure out. Considering all these problems, are there any available quantum computer architectures?

**Steven, is it possible to construct quantum computers?**

- Yes and No! Quantum versions of devices, architectures, languages, compilers, and layers of abstraction will be necessary to construct large-scale quantum computers. In most cases, the work will involve adapting classical concepts to work with quantum systems [18]. A quantum computer is not very useful if its quantum operations cannot be applied to classical data or produce classical results since humans are classical beings. Thus, the quantum system must be able to interact meaningfully with the classical world. Ultimately, a quantum computer must

be able to perform arbitrary quantum operations and be controlled and measured classically. Quantum computers produce classical information after the measurement is conducted, which is later fed back to classical computers [41]. Based on this and the criteria we have discussed, there are different architectures for quantum computers.

All of these architects support superposition and entanglement. The quantum computer community is still trying to determine which qubit design is "best," unlike classical computation, which has already settled on silicon and switches called "transistors" to manipulate 1s and 0.

Ion traps and superconducting qubits are two famous ones invented by IBM and JGU Mainz. Group Poschinger. Meanwhile, Silicon Quantum Computing company in Australia has developed atom-based manufacturing technology to create a commercial-scale quantum computer (sub-nanometer precision atom placement on silicon allowed silicon quantum computing to mimic the single and double carbon bonds of polyacetylene chains).

**Superconducting loops:** Quantum processors are the heart of superconducting computers, which are supposed to show the state of the qubits by electronic circuits. A superconducting quantum computer uses nanofabricated superconducting electrodes coupled through Josephson junctions. The IBM quantum computer contains cables that transmit microwave pulses at different frequencies and durations for controlling and measuring the qubits (as shown in Figure 7). As a result of thermal fluctuations and magnetic disturbances, the superconducting loop architecture is susceptible to decoherence, requiring the whole computer to be immersed in a special cooling apparatus and magnetic shielding [42]. This means that IBM will need to cool down its quantum processors to 10-20 mili. Kelvin temperature to isolate qubits and prevent destroying of quantum information!

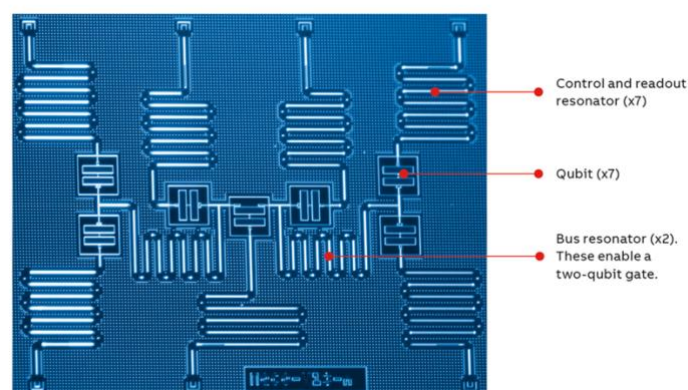


Figure 7: Using superconducting technology, IBM designed an early 7-qubit chip [43].

**Trapped ions:** The development of ion traps dates back to 1953 when Wolfgang Paul proposed his famous Paul trap [44]. An ion is a charged particle that can save information. In an ion trap, an electric or magnetic field is used to trap charged particles (as shown in Figure 8), called ions, usually in an environment isolated from the external environment. An energy pulse can be applied to a particle in the state, for example, 0, to switch it to state 1. We can manipulate the particle with a laser to read out the information, which does not affect state 0. Our iron in state 1 absorbs energy and emits it to us as a photon, a particle of light that we can detect and analyze to find the solution to a specific problem. Because trapped ions have relatively long coherence times than superconductors, qubits are long-lived [45].



One drawback in this system is, ion trapped can interact easily with their neighbors. We can resolve this problem by placing the ions in a sufficiently spaced one-dimensional array and cooling them (until their motion in space is quantized). Another significant challenge is scalability in this approach. Developing a quantum simulator that outperforms current classical machines requires scaling up the system size by several tens of qubits [45].

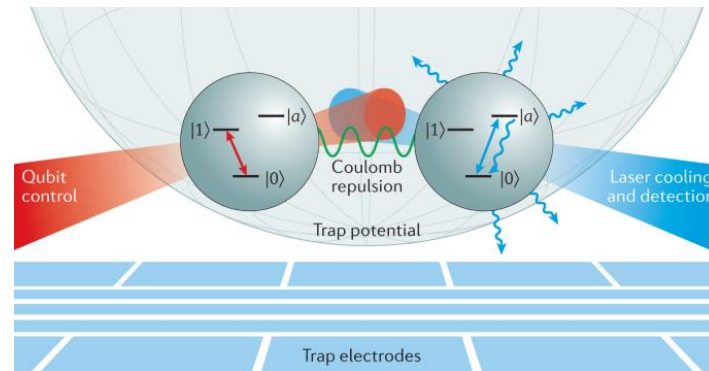


Figure 8: Qubits made from trapped ions are impeccable [46].

**Silicon quantum dots:** (A quantum dot is a semiconductor particle with an optical or electronic property that differs from a larger particle due to quantum mechanics. Nanotechnology revolves around quantum dots. And silicon is one of the most suitable neutral materials for hosting spin qubits with high sensitivity.) Imagine a classical chip containing billions of individual silicon devices such as transistors and memory elements. We want to use silicon for quantum computing and explode this technology that has enabled the modern information technology revolution. So, researchers want to use quantum dots, modified silicon transistors, to create quantum processors. The technology's proponents emphasize its ability to provide chip-scale solutions, whereas other approaches require 'building-size' equipment [47, 48]. Spin qubits, however, are delicate. It has been challenging to create an environment that can extend their coherence life and thus improve their fidelity [47].

It is expected that different companies with a great deal of investment will enter the market as time passes. Scientists are constantly presenting novel ideas about how to design quantum computers, although we have not yet been able to build them. As an example, I can cite Diamond NV's quantum approach, which is the latest idea I hear about it. It is another edition of constructing a quantum computer that has taken a different approach to implementing qubits. The NVision group from the University of Ulm, Germany, NV centers, the Institute for Quantum Optics at Ulm University (2020), Element Six (2021), and Quantum Brilliance (a venture-backed Australian-German quantum hardware company) are among those involved in this new method [49].

- Okay, I'm going to say what I understand. Correct me if I'm wrong. In our daily lives, we want classical results. Many companies, universities, and researchers are working on this to make a quantum physics-based processor. They want to reach the speed they promised. It's all about isolating the qubits and whatever else we talked about. Every time they attack from a specific angle to make better processors. They can solve some challenges at a certain level, but then there's another one. Their processors have to have the lowest energy for qubits if they

don't want their qubits to interact with the environment or each other. So they'll freeze them with big devices. They're still at the beginning of the party!

- Steven laughed and said Oh my god, this is the first time I've seen from this angle. Problems are always there! So far, nothing's worked!

## Is it a lie?

- Steven, there are two scenarios. One is that "The investment bubble will burst, and quantum winter is coming [50, 51]." I mean, quantum computer devices remain noisy and cannot achieve quantum advantages. Quantum computing is being oversold and won't change the world; it'll just have some excellent applications. Despite public and private investments in quantum technology, businesses in the field will be limited to research applications or fail. And it is a game of money. The more money flowed into the area, the more tempting it became for scientists. Companies make money from this situation by renting quantum computers to universities since the government pours money into research, which is a great way to funnel tax money into the business [51, 52].

- You think like Michail Dyakonov. In his book, he says that, instead of quantum computers, we might have special quantum devices that operate at millikelvin temperatures to perform specific tasks [52]. I agree with the word "oversell"; for example, I have heard that quantum computers can predict weather patterns better in short-term periods and even long-term effects of climate change. However, I couldn't find something that shows how a quantum computer could do that. My only observation about the weather is that it is a nonlinear system, while quantum mechanics is linear.

## Do we need to be concerned, Steven?

-We can imagine another scenario in which companies like Google and IBM were able to reach this technology; thus, no money is wasted. What countries invest in this field?

-I don't know about all of them, but I can name the US, Germany, China, Japan, Canada, Australia, India, and the Netherlands.

-Wow, there is indeed a race in the global market.

-Yes, and some people call it an "arms race [29, 53]."

-My understanding of this term is that it refers to tensions between nations. It is evident that developing scalable and error-corrected quantum computing before others could adversely affect international politics and power balances. Even within the countries, quantum computers are physically and technically complex and are unlikely to be owned by an average person or small business.

-Well, they can still benefit from it. Organizations and governments should consider how to share quantum computer-derived knowledge. It is too early to take direct action regarding ethics and quantum computing, grandad. Our journey is just beginning.

- It may be too late to wait until challenges fully present themselves. The sooner you understand the ethical traps of quantum computers, the easier it will be to deal with them in the future. A trustworthy quantum technology strategy should include ethical risk mitigation approaches. It is also an excellent time to engage wider stakeholder groups. Policymakers, industry, and academia must be aware of quantum technology's possible impacts and effects. We cannot rely solely on the tech industry to protect us. Regulations from the government can contribute to the solution, but they generally take years to implement. Quantum leaders should ensure their own and their customers' safety soon. We must share the public's views about quantum research and technologies with the quantum research community. The most significant concerns among people likely relate to the broader and less predictable aspects of quantum technology's rollout, such as uneven access, quantum as a profit-driven exercise at the expense of public interest, and the possibility of automation leading to job losses [12, 29, 53, 54].

There are some serious ethical concerns if you pay attention. If there were quantum computers, we could solve real-world problems with them. You gave me a cryptography example. What if hackers and hostile countries can break encryption protocol with a quantum computer? Several internet services, such as e-commerce and virtual financial transactions, rely on encryption. These attacks could also be against widely used blockchain technologies, like Bitcoin [29]. Are you thinking about a solution in advance, or do you wait until then?

-You are right. Quantum computation poses a severe threat to current cryptographic techniques. Most existing communication channels will be rendered insecure by breaking RSA coding. So, developers need to update their platforms to use postquantum cryptography. As soon as this technology becomes available, businesses should prepare themselves. Organizations need to quickly update cryptographic algorithms, parameters, processes, and technologies to handle new protocols, standards, and security threats as they evolve [29].

-Is there any other application you want to mention?

-Quantum computers play a significant role in health. As an example, cancer treatment. As well as providing biomedical researchers with a faster way to conduct research, they play an essential role in gene editing thanks to the ability to understand the effects of subtle genetic changes. Other benefits include the elimination of many genetic diseases. However, research in this area should remain cautious of unintended consequences [55].

The creation of new materials is another hot topic. Soon, quantum technology may enable sophisticated simulations of how small molecular changes affect materials' properties, which will be helpful in drug discovery, and chemical production.

-History shows, however, that sometimes seemingly beneficial things may end up causing harm. A lot of people were excited when plastics were invented. It is only now that we are becoming aware of how harmful they can be to the environment. The materials researchers should keep this history in mind as they work toward new material discoveries to ensure that future breakthroughs won't have similar environmental consequences [55].

How do you feel about privacy? Data collection still occurs rampantly despite restrictions. Due to quantum computers' ability to process large volumes of data faster than today's most sophisticated servers, the availability of quantum computers may also motivate organizations to collect even more consumer data.

- After the internet revolutionized technology, we are already losing control over it. The situation may worsen if we do not act quickly.

-As you see, many ethical challenges are associated with quantum technologies, including their potential use by terrorists, enhanced encryption capabilities, and the possible violation of privacy.

We must engage academia, government, start-ups, industries, and different sectors in a discussion. Ethics is all about conversation and beginning the discussion as early as possible.

It is only possible for us to fully understand what quantum computers are capable of once we possess them. Still, consideration should be given to what the power can accomplish.

But the question here is, "Is it worth taking a risk? Just because we cannot do something does not mean we should." Based on your words, I feel quantum winter is near, laughed grandpa. As a contributor to this new technology, it is your responsibility now to consider ethical concerns.

Steven looked at the fire inside the fireplace and went into silence; it might be the first time he had not been genuinely excited about quantum computers. He gained new insight from this conversation.

## Conclusion

Quantum computing is a fascinating topic based on quantum mechanics. In contrast to classical bits, qubits can simultaneously be 1 and 0. Scientists introduced algorithms that outperformed classical algorithms based on the two key concepts, superposition, and entanglement, raising the idea of speeding up. However, most of the algorithms have no practical usage. Processes of quantum information require quantum circuits with quantum gates. Several essential criteria must be met to make a real quantum computer, as outlined by David P. DiVincenzo. Having a scalable system with many qubits, initializing qubits before computation, having a long enough decoherence time for manipulating qubits, having universal quantum gates, and being able to measure the qubits are all essential criteria. Several businesses, universities, and researchers have attempted to build quantum processors based on novel ideas in physics. Despite this, it remains challenging to maintain qubits at the lowest energy level, so they do not interact with the environment. Thus, they could not achieve some ideas, such as producing an environmentally friendly quantum computer. Instead, they develop processors that require a huge cooling system to decrease qubits' energy level. The energy consumption of these huge devices is high, and they are not environmentally friendly. Thus, there is a theory that this field is nothing more than a bubble that will one day burst. Another theory suggests there will be a quantum computer, but it is unclear when it will be available. Researchers like Steven, who wish to enter this field, need to consider ethical issues related to this subject, not just think about how they can reach their goal faster. They should not - unsurprisingly - be optimistic about the potential upside of quantum technologies, especially in healthcare (which is an excellent way to oversell this technology). At the same time, there are concerns about the potential misuse of these technologies (Grandpa's concern about new technologies). They must know that a more structured conversation is needed at the intersection of quantum technology and responsible research.



## References

The first-page picture is available at: <https://futurumresearch.com/research-notes/google-claims-quantum-supremacy-but-was-it-really/>

1. Vox. Available from: <https://www.vox.com/future-perfect/2018/11/19/18097663/nick-bostrom-vulnerable-world-global-catastrophic-risks>.
2. Dutta, S., *Knowledge processing and applied artificial intelligence*. 2014: Elsevier.
3. *Technology in 2050*. Available from: <https://www.theguardian.com/technology/2020/jan/03/technology-2050-save-humanity-or-destroy-us>.
4. *Survival of the fittest*. Available from: [https://en.wikipedia.org/wiki/Survival\\_of\\_the\\_fittest](https://en.wikipedia.org/wiki/Survival_of_the_fittest).
5. *Stephen Hawking reminds us technology will kill us all and it's all our fault*. Available from: <https://mashable.com/article/stephen-hawking-technology-kill-us-all>.
6. *The birth of IBM computers*. Available from: [https://www.ibm.com/ibm/history/exhibits/pc25/pc25\\_birth.html](https://www.ibm.com/ibm/history/exhibits/pc25/pc25_birth.html).
7. Chou, J.-S. and D.-S. Tran, *Forecasting energy consumption time series using machine learning techniques based on usage patterns of residential householders*. Energy, 2018. **165**: p. 709-726.
8. Bini, S.A., *Artificial intelligence, machine learning, deep learning, and cognitive computing: what do these terms mean and how will they impact health care?* The Journal of arthroplasty, 2018. **33**(8): p. 2358-2361.
9. Wiegert, J., G. Regnier, and J. Jackson. *Challenges for scalable networking in a virtualized server*. in 2007 16th International Conference on Computer Communications and Networks. 2007. IEEE.
10. *Chips*. Available from: <https://niklasrosenberg.com/blog/2020/7/15/what-does-it-mean-to-have-60-billion-transistors-in-a-computer-chip>.
11. *Cure cancer*. Available from: <https://www.defianceetfs.com/how-can-quantum-computing-help-cure-cancer/>.
12. Srivastava, R., et al., *The commercial prospects for quantum computing*. Networked Quantum Information Technologies, 2016.
13. Martinis, J. *Quantum Supremacy Using a Programmable Superconducting Processor*. 2019; Available from: <https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html>.
14. Arute, F., K. Arya, and R. Babbush, *Supplementary information for 'Quantum supremacy using a programmable superconducting processor'*. Nat. Int. Wkly. J. Sci, 2020. **574**: p. 505-505.
15. DiVincenzo, D.P., *Quantum computation*. Science, 1995. **270**(5234): p. 255-261.
16. Steane, A., *Quantum computing, Department of Atomic and Laser Physics, University of Oxford, Clarendon Laboratory, Parks Road*. 1997, Oxford, OX1 3PU, England.
17. Salonik, R. and R. Ulya, *Quantum computing: An overview across the system stack*. arXiv preprint arXiv:1905.07240, 2019.
18. *Qbit vs bits*. Available from: <https://www.slideteam.net/quantum-computing-it-how-quantum-computer-works-ppt-powerpoint-layouts-pictures.html>.
19. DiVincenzo, D.P., *Quantum gates and circuits*. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 1998. **454**(1969): p. 261-276.
20. *How quantum computers work*. Available from: <https://qc-at-davis.github.io/QCC/How-Quantum-Computing-Works/The-Qubit/The-Qubit.html>.

21. Wang, Y. and H. Liu, *Quantum computing in a statistical context*. Annual Review of Statistics and Its Application, 2022. **9**: p. 479-504.
22. Collins, D., K. Kim, and W. Holton, *Deutsch-Jozsa algorithm as a test of quantum computation*. Physical Review A, 1998. **58**(3): p. R1633.
23. Shor, P.W. *Algorithms for quantum computation: discrete logarithms and factoring*. in *Proceedings 35th annual symposium on foundations of computer science*. 1994. Ieee.
24. *quantum vs classical* Available from: <https://quantum-computing.ibm.com/composer/docs/idx/guide/shors-algorithm>.
25. Grover, L.K., *Quantum mechanics helps in searching for a needle in a haystack*. Physical review letters, 1997. **79**(2): p. 325.
26. Schaller, G. and R. Schützhold, *The role of symmetries in adiabatic quantum algorithms*. arXiv preprint arXiv:0708.1882, 2007.
27. Schuld, M. and F. Petruccione, *Supervised learning with quantum computers*. Vol. 17. 2018: Springer.
28. Orús, R., S. Mugel, and E. Lizaso, *Quantum computing for finance: Overview and prospects*. Reviews in Physics, 2019. **4**: p. 100028.
29. Ten Holter, C., P. Inglesant, and M. Jirotko, *Reading the road: challenges and opportunities on the path to responsible innovation in quantum computing*. Technology Analysis & Strategic Management, 2021: p. 1-13.
30. Benioff, P., *Quantum mechanical Hamiltonian models of Turing machines*. Journal of Statistical Physics, 1982. **29**(3): p. 515-546.
31. DiVincenzo, D.P., *The physical implementation of quantum computation*. Fortschritte der Physik: Progress of Physics, 2000. **48**(9-11): p. 771-783.
32. DiVincenzo. Available from: <https://qc-at-davis.github.io/QCC/How-Quantum-Computing-Works/DiVincenzo's-Criteria/DiVincenzo's-Criteria.html>.
33. Sarovar, M., et al., *Detecting crosstalk errors in quantum information processors*. Quantum, 2020. **4**: p. 321.
34. Chuang, I.L., et al., *Quantum computers, factoring, and decoherence*. Science, 1995. **270**(5242): p. 1633-1635.
35. Steane, A.M., *Error correcting codes in quantum theory*. Physical Review Letters, 1996. **77**(5): p. 793.
36. Shor, P.W., *Scheme for reducing decoherence in quantum computer memory*. Physical review A, 1995. **52**(4): p. R2493.
37. Steane, A.M., *A tutorial on quantum error correction*. Quantum Computers, Algorithms and Chaos, 2006: p. 1-32.
38. Wootters, W.K. and W.H. Zurek, *A single quantum cannot be cloned*. Nature, 1982. **299**(5886): p. 802-803.
39. Rebentrost, P., M. Mohseni, and S. Lloyd, *Quantum support vector machine for big data classification*. Physical review letters, 2014. **113**(13): p. 130503.
40. Terhal, B.M., *Quantum error correction for quantum memories*. Reviews of Modern Physics, 2015. **87**(2): p. 307.
41. Oskin, M., F.T. Chong, and I.L. Chuang, *A practical architecture for reliable quantum computers*. Computer, 2002. **35**(1): p. 79-87.
42. *Superconducting loop*. Available from: [https://en.wikipedia.org/wiki/Superconducting\\_computing](https://en.wikipedia.org/wiki/Superconducting_computing).
43. *IBM superconductor* Available from: <https://new.abb.com/news/detail/74736/quantum-computing-the-hype-and-hopes>.
44. Paul, W. and H. Steinwedel, *Ein neues massenspektrometer ohne magnetfeld*. Zeitschrift für Naturforschung A, 1953. **8**(7): p. 448-450.

45. *ion traps* Available from: [https://en.wikipedia.org/wiki/Ion\\_trap](https://en.wikipedia.org/wiki/Ion_trap).
46. Brown, K.R., et al., *Materials challenges for trapped-ion quantum computers*. Nature Reviews Materials, 2021. **6**(10): p. 892-905.
47. *Silicon spin*. Available from: <https://www.factbasedinsight.com/silicon-spin/>.
48. Saraiva, A., et al., *Materials for Silicon Quantum Dots and their Impact on Electron Spin Qubits*. Advanced Functional Materials, 2022. **32**(3): p. 2105488.
49. *Diamond NV*. Available from: <https://thequantuminsider.com/2022/03/31/5-quantum-computing-companies-working-with-nv-centre-in-diamond-technology/>.
50. Hossenfelder, S.
51. Hoofnagle, C.J. and S.L. Garfinkel, *Law and Policy for the Quantum Age*. 2022: Cambridge University Press.
52. Dyakonov, M.I., *Will we ever have a quantum computer?* 2020: Springer.
53. Inglesant, P., M. Jirotko, and M. Hartwood, *Responsible Innovation in Quantum Technologies applied to Defence and National Security*. NQIT (Networked Quantum Information Technologies), 2018.
54. Stewart, D., et al., *Quantum computing in 2022: Newsful, but how useful?* 2022 Predictions: p. 124.
55. *Ethics concern*. Available from: <https://www2.deloitte.com/uk/en/insights/topics/cyber-risk/quantum-computing-ethics-risks.html>.