

IN THIS CHAPTER

- » Adding strangeness to our agenda
- » Calculating the power of quantum computing
- » Identifying quantum computing's advantages
- » Taking stock of quantum computer types
- » Overcoming barriers to new capabilities

Chapter **1**

Quantum Computing Boot Camp

Picture flipping a coin in the air. As it's spinning, is it showing heads or tails? Well, you can't know the answer while the coin is spinning. Only when the coin lands and settles down does it display a definite result.

The uncertainty you see while the coin is spinning is like the uncertainty we capture and use in quantum computing. We put many processing elements — *qubits* — into a state of uncertainty. Then we program the qubits, run the program, and capture the results — just like when the coin lands.

Quantum computing is different from the fixed 0s and 1s, bits and bytes, used in today's devices. Quantum computing is based on quantum mechanics, a branch of physics that can be hard to comprehend. But the way in which quantum computing deals effectively with large degrees of uncertainty feels like the way we make many of the decisions we encounter in daily life.

Quantum computing is complementary to classical computing, the kind of computing we use today, not a replacement for it. By working with uncertainty, we can take on some of the biggest, most complex problems that humanity faces, in a new and powerful way. Quantum computing will solve problems for which today's computing falls short — problems in areas such as modeling the climate, drug discovery, financial optimization, and whether or not it's a good morning to launch a rocket.

Quantum computing is just getting started; many advanced quantum computers run only for a fraction of a second at a time. However, steady progress is being made. Even now, at this early stage, quantum computing is inspiring us to, as a sage once said, “think different” about the way we use existing computing capabilities. In this chapter, we introduce the power and potential of quantum computing.



TIP

This chapter presents many terms and concepts that may be unfamiliar to you. Don't worry; we explain them all in later chapters. (For instance, Chapter 3 describes quantum mechanics and how quantum computing depends on it.) Think of this chapter as boot camp for the new, quantum-computing-savvy you who will emerge after reading this book.

Understanding Why Quantum Computing Is So Strange

Quantum computers have a sense of strangeness about them, almost a mystical aura. (The 2022 movie, *Dr. Strange in the Multiverse of Madness*, captures some of the feeling that people have about quantum mechanics in general.) Why is this?

There are two main reasons. The first reason is people's fundamental misunderstanding of the nature of matter, which quantum mechanics explains. The second is the incredible power that quantum computing, when mature, is expected to deliver to humanity.

How does quantum mechanics (described in Chapter 3) change people's view of the world? The world we live in, where rocks fall down and rockets go up, seems to be dominated by solid matter, with energy as a force that acts on matter at various times. Yet matter can simply be seen as congealed energy.

Most of the mass of the protons and neutrons inside the nucleus of an atom, for instance, is simply a bookkeeper's description of the tremendously powerful energetic fields that keep these particles in place. One of the most important kinds

of particles in quantum computing, photons, have no mass at all; they are made up of pure energy.

And it was Einstein himself who told us that matter and energy are equivalent, with his famous equation, $E=mc^2$. To translate: The energy contained in solid matter equals its mass times the speed of light squared.



The speed of light is a very large number — 300,000 km/second, or 186,000 miles/second. Squaring the speed of light yields a far larger number. Plug this very large number into Einstein’s famous equation and you’ll see that there is a *lot* of energy in even small amounts of matter, as demonstrated by nuclear power plants and nuclear weapons.

The point is that, in quantum mechanics, matter is relatively unimportant; particles act more as bundles of energy. And quantum computing takes advantage of the exotic properties of these particles — ionized atoms, photons, superconducting metals, and other matter that demonstrates quantum mechanical behavior.

The second reason that quantum computers get such a strong emotional reaction is the tremendous power of quantum computing. The best of today’s early-stage quantum computers are not much more powerful, if at all, than a mainstream supercomputer. But future quantum computers are expected to deliver tremendous speedups.

Over the next decade or two, we expect quantum computers to become hundreds, thousands, even millions of times faster than today’s computers for the problems at which they excel. People can’t really predict, nor even imagine, what it’s going to be like to have that kind of computing power available for some of the most important challenges facing humanity, as we describe in Chapters 13 and 14. That future is very exciting, yes. But it’s also a bit, as Einstein described quantum mechanics, “spooky.”

Grasping the Power of Quantum Computing

To help you get started in understanding quantum computing, here are five big ideas to get your head around:

- » **Qubits:** *Qubits* are the quantum computing version of bits — the 0s and 1s at the core of classical computing. They have quantum mechanical properties. Qubits are where all the magic happens in quantum computing.

- » **Superposition:** While bits are limited to 0 or 1, a qubit can hold an undefined value that is neither 0 nor 1 until the qubit is measured. The capability to hold multiple values at once is called *superposition*.
- » **Entanglement:** In classical computing, bits are carefully separated from each other so that the value of one does not affect others. But qubits can be entangled with each other. When changes to one particle cause instantaneous changes to another, and when measuring a value for one particle tells you the corresponding value for another, the particles are *entangled*.
- » **Tunneling:** A quantum mechanical particle can instantaneously move from one place to another, even if there's a barrier in between. (Quantum computing uses this capability to bypass barriers to the best possible solution.) This behavior is referred to as *tunneling*.
- » **Coherence:** A quantum particle, such as an electron, that is free of outside disturbance is *coherent*. Only coherent particles can exhibit superposition and entanglement.

How are these terms related? Here's an example: A good qubit is relatively easy to place into a state of coherence and maintain in a state of coherence, so it can exhibit superposition and entanglement, and therefore can tunnel. (The search for “good qubits” is the subject of a lot of work and controversy today. We describe this topic in more detail in Chapters 10 and 11.)

These five terms are at the heart of the promise of quantum computing and are involved in many of the challenges that make quantum computing difficult to fully implement. In this section, we describe each of these crucial concepts.



TECHNICAL
STUFF

Classical computing describes the computers we use every day, which includes not only laptop and desktop computers but also smartphones, web servers, supercomputers, and many other kinds of devices. The term *classical computing* is used because classical computers use classical mechanics, the cause-and-effect rules of the road that we see and use in our daily lives, for information processing. Quantum computing uses quantum mechanics — which is very different, very interesting, and very powerful indeed — for information processing. We mention some quantum mechanical principles in this chapter and go into more detail in Chapter 2.

Introducing Puff, the magic — qubit?

Bits power classical computing — the laptops, servers, smartphones, and supercomputers that we use today. *Bit* is short for *binary digit*, where *digit* specifies a single numeral and *binary* means the numeral can have only one of two values: 0 or 1 — just like the results of a coin flip.

In a computer, bits are stored in tiny, cheap electromechanical devices that reliably take in, hold, and return either a 0 or a 1 — at least until the power is turned off. Because a single bit doesn't tell you much, bits are packaged into eight-bit bytes, with a single byte able to hold 256 values. (2^8 — all possible combinations of 8 binary digits — equals 256.)

A *qubit* is a complex device that has, at its core, matter in a quantum mechanical state (such as a photon, an atom, or a tiny piece of superconducting metal). The qubit includes a container of some kind, such as a strong magnetic field, that keeps the matter from interacting with its environment.

A qubit is much more complex and much more powerful than a bit. But qubits today are not very reliable, for two reasons:

- » They're subject to errors introduced by noise in the environment around them. A result of 0 can be accidentally flipped to a result of 1, or vice versa, and there's no easy way to know that an error has occurred.
- » It's hard to keep qubits coherent, that is, capable of superposition, entanglement, and tunneling.

The situation with qubits today is somewhat like the old joke about a bad restaurant: "The food is terrible — and the portions are so small!" With qubits, the error rates are high and the coherence period is short. But despite these problems, quantum computers do deliver valuable and interesting results while up and running.

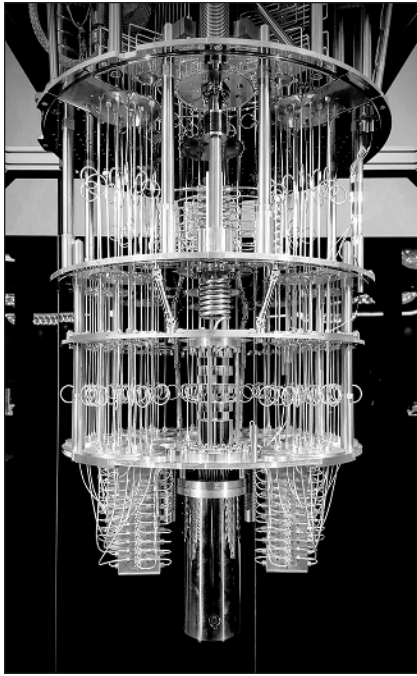
In quantum computers, qubits are much more complex and far more expensive than bits. Nor are they as easy to manage — but they are far more powerful.

Figure 1-1 shows a quantum computing module from IBM, suspended at the bottom of a cooling infrastructure that keeps the superconducting qubits at a temperature near absolute zero.

Until it's measured, each qubit can represent an infinite range of values between 0 and 1. How does the qubit hold all these values? At the core of the qubit is a *quantum particle* — a tiny piece of reality in the form of a photon, an electron, an ionized atom, or an artificial atom formed using a superconducting metal.

For quantum computing, the quantum particle at the core of the qubit must be kept in a *coherent state* — uncontrolled, like the flipped coin while it's spinning in the air. In a coherent state, we don't know whether the value of the qubit at a given moment is 0 or 1. When we measure the state of the qubit, the calculation we want to make is performed, and the qubit returns 0 or 1 as a result.

FIGURE 1-1:
A quantum
computing
processor
from IBM.



Flickr/Lars Plougmann

Much of the power of qubits comes from the fact that they behave in a *probabilistic* manner; a given qubit, running the same calculation multiple times without errors, may produce a 0 on some runs and a 1 on another. The final result consists of the number of times each qubit returns a 0 or a 1. So the result of most quantum calculations is a set of probabilities rather than a single number.

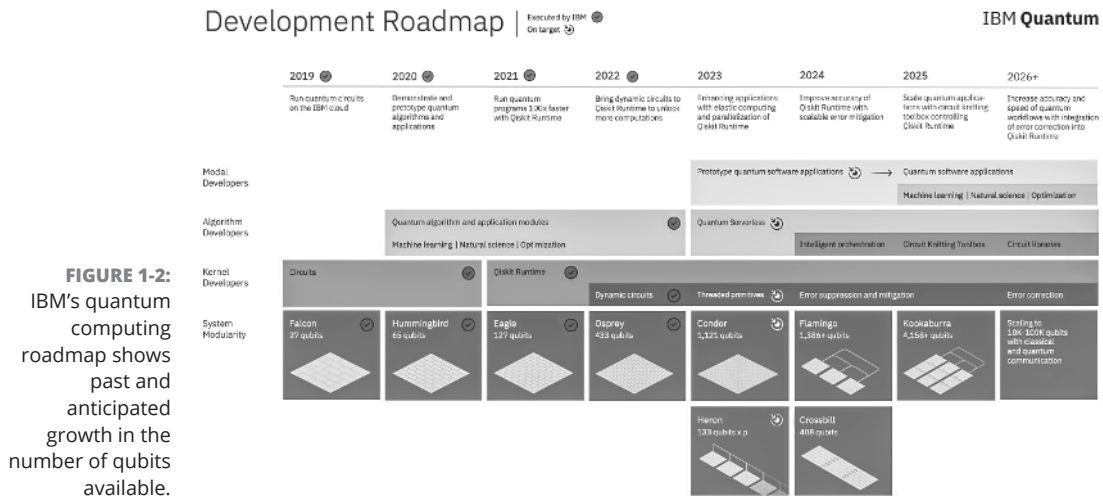
Qubits are hard to create and hard to maintain in a state of coherence; they also tend to interfere with nearby qubits in an uncontrolled fashion. Taming qubits is one of the biggest challenges to overcome in creating useful quantum computers.

A popular approach to building quantum computers involves the use of superconducting qubits, which must be kept at a temperature very close to absolute zero to minimize interference due to heat and, in many cases, to maintain superconductivity.

Classical computers are designed to work at room temperature, but they tend to generate heat and to stop working properly as the temperature rises. The need to dissipate heat prevents device makers from packing components as tightly as they would like without resorting to expensive and clumsy solutions such as water-cooling or refrigerating the components.

In quantum computing, each additional qubit adds exponentially to the power of the computer. But because qubits tend to interfere with each other, adding more is difficult.

IBM, a leader in quantum computing, has published a roadmap showing past and future increases in the number of qubits that power its current and upcoming quantum computers. A simplified version of the roadmap is shown in Figure 1-2. You can find a link to the current version of the roadmap at <https://research.ibm.com/blog/ibm-quantum-roadmap-2025>.



Superposition, the first quantum superpower

The state of possibility that's available to qubits is called *superposition*, where *super* means *many* and *position* means *possibilities*. A traditional bit can be either 0 or 1. A qubit in a state of superposition does not have a defined value because it holds many potential values at the same time. But when we measure a qubit, we just get 0 or 1 back — whichever value the qubit's energetic wave function collapsed to when it was measured.

Superposition is the first of two major pillars underpinning the power of quantum computing. The other, entanglement, is described in the next section.

In Chapter 3, we describe how the creators of quantum mechanics discovered superposition and other quantum principles during an extraordinary period of scientific creativity between about 1900 and 1930. (This period also saw the disaster of World War I and the beginning of the Great Depression.)

EXPLAINING LIFE, THE MULTIVERSE, AND EVERYTHING

Quantum computing depends on the laws of quantum mechanics, described at a basic level in Chapter 3. Quantum mechanical principles are vital to the operation of quantum computers.

One way of understanding how quantum mechanics works is that each possible state of a quantum mechanical object becomes true — in a new parallel universe that comes into existence to contain that possibility. This way of looking at reality is the basis of recent movies such as *Everything Everywhere All at Once* and *Quantumania*. But there's ongoing controversy as to whether multiple universes are real.

We don't need to get caught up in these debates as we do our daily work in quantum computing; we can, as the saying goes, “shut up and calculate.” But these seemingly wild ideas can help us understand just how strange and wonderful the quantum world is. They can inspire us in our daily work, and they may lead to seemingly science-fictional achievements such as time travel, teleportation, and faster than light travel — for information, at least, if not for objects or people.

Welcoming foreign entanglements

George Washington once warned Americans to avoid foreign entanglements. But with qubits, we welcome entanglement as an additional, powerful tool in our quantum computing toolkit.

Entanglement is a kind of connection between two or more quantum particles. For instance, quantum particles have a property called *spin*, which we can measure as either down or up (0 or 1). If two quantum particles are entangled and one of them is measured as having an up spin, we know without measuring that the other entangled particle will have a down spin. And if we influence the spin of the first quantum particle so that it changes to up when it is measured, we know without measuring that the other quantum particle will change to down.

Figure 1-3 shows the connection between two entangled qubits, which have opposing spins. Measuring the spin of one tells you that the spin of the other is the opposite; changing the spin of one qubit in one direction will change the spin of the other in the opposite direction.

As mentioned, entanglement is the second pillar supporting the power of quantum computing. With entangled qubits, influencing a single qubit can have a knock-on effect on many others.

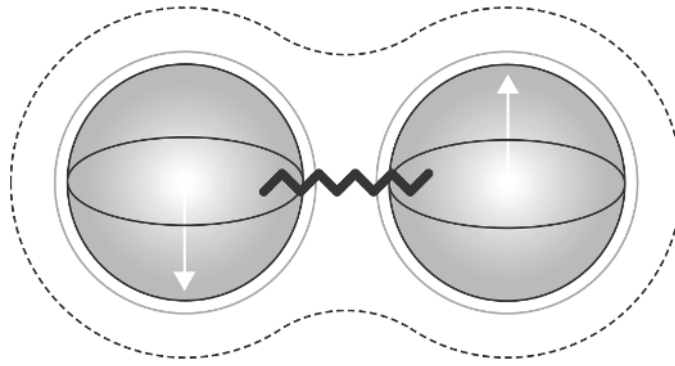


FIGURE 1-3:
Entangled qubits
influence
each other.

Entanglement and superposition work together. When an entangled qubit is in a state of superposition, each of its entangled connections is also in a state of superposition. These cascading uncertainties exponentially increase the potential power of quantum computers.

To program and run calculations on a quantum computer, the potentiality of the entangled qubits must be maintained by keeping them coherent and free from noise. We then measure the qubits (which causes them to decohere) and record the results, a 0 or 1 for each qubit.



Quantum communications is made possible by using entangled qubits for communication between distant locations. We explain this in more depth in Chapter 3.

Enabling quantum computing with coherence

Qubits can be used for quantum computing only when they're kept in a state of *coherence*, free of interaction with their environment. To do quantum computing, qubits need to follow the rules of quantum mechanics (as explained in Chapter 2), and these rules apply to only coherent qubits.



Quantum particles zipping around the universe — photons emitted by the sun, for example — are in a state of coherence. What causes them to decohere? Any interaction with excessive interference (such as vibration or a strong magnetic field), a solid object, or a measuring device.

Keeping qubits coherent is hard. Heat decoheres them, so qubits are kept cold. So do vibration (think of a truck going by on a road) and any collision with their environment. To prevent such collisions, qubits often use strong magnetic fields or targeted laser beams to prevent the quantum particles inside them from colliding with their physical containers.

BLOWING PAST C

Albert Einstein wears two hats in the history of quantum mechanics — and the two hats don't fit comfortably on a single head.

One hat comes from Einstein's discovery of relativity, published in 1905. Relativity says that speed in this universe depends on your motion relative to other observers, but that the speed of light — about 186,000 miles per second, or 300,000 kilometers per second — is always the same for all observers. This universal speed limit is called *locality*.

The other hat comes from Einstein's discovery of the photon, also in 1905. (This discovery, not relativity, is the source of Einstein's sole Nobel Prize.) The discovery of the photon is fundamental to quantum mechanics.

Einstein's problem is that quantum mechanics later asserted that quantum particles, such as photons, can be entangled with each other, so that reading the spin (for example) of one photon tells you the spin of the other. And this relationship is instantly true, without regard to the speed of light. Physicists call this an assertion of nonlocality, which is supposed to be forbidden by relativity.

Einstein hated this, calling it “spooky action at a distance.” He and his colleagues spent a great deal of effort trying to disprove it, even as Einstein continued to make breakthrough quantum discoveries, such as the identification of Bose-Einstein condensates, which are superconducting gases that can be used to create qubits.

Today's mainstream computers are subject to classical mechanics and limited by the speed of light. Quantum computers depend on quantum mechanics and, in their use of entanglement, are not limited by light speed.

The Nobel Prize for Physics in 2022 was awarded to physicists who showed that entanglement is real. So researchers in quantum computing who depend on entanglement can say, after Galileo: “And yet it computes.” (Galileo, on trial for asserting — correctly, as it turned out — that the earth is not at the center of the universe, is famously said to have whispered: “And yet it moves.”)

Decoherence is not the only disaster that can affect qubits. Temperature changes, vibration, or physical interaction may change the value of a qubit in an uncontrolled manner without causing it to decohere. This noise causes errors in the results of quantum computations. Minimizing noise and detecting errors are two of the biggest challenges facing quantum computers.

To manipulate each qubit — to program it, for instance, for quantum computing — the qubit must be controlled in such a way as to adjust its value without causing it to decohere. Magnetic fields and laser beams are among the means used to manipulate qubits without causing decoherence.

When we measure the value of a qubit, two things happen:

- » The qubit decoheres, becoming subject to the rules of classical mechanics.
- » The qubit's value collapses from somewhere between 0 and 1, inclusive, to either 0 or 1.

The qubit must be reinitialized — returned to coherence — before it can be used again for computing.



Some argue that the potential of quantum computers is very limited — that the level of coherence needed for quantum computers to achieve useful results is impossible, in theory and in fact. In the extreme version of this argument, leaders in quantum computing are accused of deliberately committing fraud, which would mean that the entire field is a massive conspiracy. Only further work will show the limits to quantum computing, if any, but the fraud allegations are just a conspiracy theory.

Doing the Math for the Power of Quantum Computing

It's challenging to fully grasp the potential power of quantum computing compared to classical computing because that power is based on quantum mechanical principles. But we can sum it up in just a bit of math.

Because the bits in classical computing can hold only one of two values — a 0 or a 1 — at the same time, the number of states that a classical computer can hold is represented by the number of bits, n , to the power of two: n^2 . But a set of entangled qubits can hold all the possible values of the qubits at the same time. For this reason, the number of states that a quantum computer can hold is represented by two to the power of qubits, n : 2^n . For example, to represent a million possible states would require 1,000 bits but only 20 qubits.

Today's computers contain billions of bits, but we have to throw a lot of them at our most complex problems to get anywhere. Today's quantum computers have a small number of qubits — a recent IBM quantum computer release clocked in with 433 — but we need only a few hundred qubits to begin tackling very complex problems.

The power of today's quantum computers is limited by errors and short coherence times. But as these factors are addressed, the results are likely to be amazing.

Examining What Quantum Computing Will Do for People

It's easy to spend time geeking out on the strangeness and power of quantum computing. But what difference will quantum computing make to humanity?

To understand the answer, we first have to address a common misconception. People today tend to worry about how powerful today's computers *are*: to worry about the power of the internet, social media, and machine learning and AI.

But there's also a big problem around how powerful today's computers *aren't*: They simply aren't up to big computational challenges in areas such as better batteries to fight climate change, better aerodynamics, better routing in complex transportation networks, and better discovery of new drugs, to name a few important examples. (See Chapters 13 and 14 for more information on the challenges that quantum computing will be able to help people to address.)

And these big computational challenges are exactly the areas where we expect quantum computing to make a big difference. Future quantum computers will be able to solve problems we can't touch today, and to do so far faster, more cheaply, and with less energy expenditure than today's computers.



TECHNICAL
STUFF

Quantum computers can only “do their thing” in partnership with computers of the kind we use today. So when you see descriptions of what quantum computing can do, understand that these accomplishments will also require a whole lot of conventional computing power.

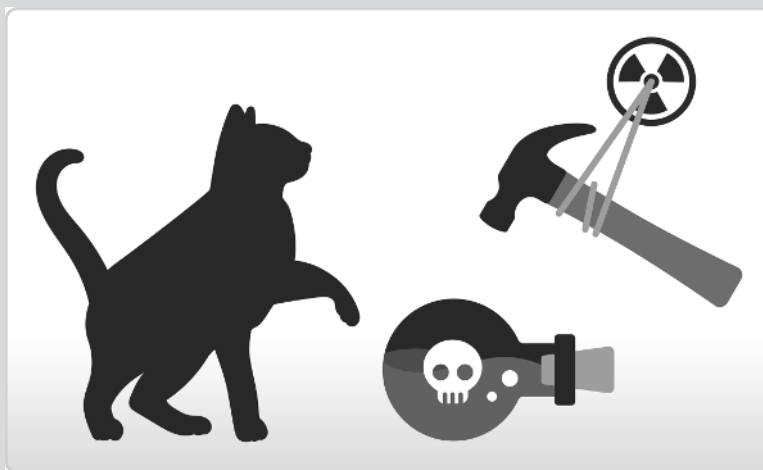
IS SCHRÖDINGER'S CAT FOR REAL?

No, Schrödinger's cat isn't real. But let's add a bit of nuance to that answer.

Quantum mechanics, the physics that power quantum computing, has been driving people batty since the core theoretical work was done between 1900 and 1930. (See Chapter 3 for details.) And nothing symbolizes this confusion better than Schrödinger's cat.

Erwin Schrödinger, the brilliant physicist behind the Schrödinger's cat thought experiment, was trying to *disprove* quantum computing when he came up with it in 1935. But he actually summed up the mystery behind all things quantum better than anyone, ever.

In the Schrödinger's cat thought experiment, a vial of radioactive poison, some decaying radioactive mass, and a cat are all placed in a box by a scientist. At some point, radioactive decay will release a hammer that breaks the flask, killing the cat, as shown in the figure. But radioactive decay is random, so no one can predict just when the hammer will break the flask.



So the scientist closes the box and goes away, and then waits several hours before coming back. During those hours, an urgent question arises: Is the cat alive or dead?

Quantum mechanics offers only a gnomonic answer: yes and no. No intelligence in the world can say for sure whether or not the radioactive decay will kill the cat at a

(continued)

(continued)

particular moment. So the cat is seen as being both dead and alive until the scientist comes back and opens the box.

This seemingly ridiculous conjecture demonstrates *superposition*, in which matter — in this case, the body of a feline — is in two states at once. Superposition, which is critical to quantum computing, has been proven to be real innumerable times since Schrödinger first came up with his thought experiment. (Cats are actually too large, and too embedded within our material world, to be in superposition, in case you were worried. And once again, NO CATS WERE HARMED. Meow.)

A related principle, *entanglement* — a mysterious connection between arbitrarily distant particles, though not cats — has also been proven, in a series of experiments that were recognized with the Nobel Prize for Physics in 2022. It was Einstein who described entanglement in particular, and quantum mechanics in general, as “spooky action at a distance.”

So Schrödinger’s cat — in the sense of actual cats being placed in mortal danger — is not real. But the principles that animate Schrödinger’s immortal thought experiment are very real indeed, as is proven every day in quantum computing.

Describing Different Types of Quantum Computing

There are three ways to do quantum-type computing, and all of them are actively being used and investigated today. They are described in some detail in Chapters 8 through 11; we briefly describe them here.

Quantum-inspired computing

Classical computers are based on logic gates, which take in electrical currents and apply binary logic to them to produce either no outgoing current (a 0) or an easily measurable current (a 1) as a result. By breaking down any mathematical or logical problem to a low enough level and running it through logic gates, you can come up with an answer.

When insights from quantum computing are used to create new algorithms that run on classical computers, or when quantum computer simulators are run on classical computers, this is called *quantum-inspired computing*, as described in Chapter 8. Quantum-inspired computing has proven to be a productive approach to finding new solutions at this early point in the development of quantum computing.

Quantum annealing

In classical computing, there's an approach called simulated annealing. It's analogous to annealing in metallurgy, in which a metal is heated to melt its internal structure, and then cooled to yield a softer, easier-to-work result. *Simulated annealing* is good for solving optimization problems, such as the least expensive route for visiting a number of cities. A similar process to this can be used to solve problems by putting a set of equations through a series of transformations until a result appears.

The quantum computing version of this approach is called quantum annealing. *Quantum annealing* doesn't use a gate-based quantum computing approach, which is more advanced but harder to implement, as described in Chapters 10 and 11. Instead, quantum annealing uses qubits as a group to solve optimization problems, which is a less demanding use of qubits.

Quantum annealers allow for qubit errors and return results that are inexact but still useful in many cases. For instance, a quantum annealer might identify a very good way to route a fleet of delivery trucks, rather than delivering the one and only best possible routing. Only one substantial company, D-Wave, makes quantum computers that use the quantum annealing approach — and they have recently announced plans to make logic-gate quantum computers as well.

Quantum annealers were criticized at one point as not being actual quantum computers, but that is no longer the case. However, gate-based quantum computers get most of the attention, research effort, and investment.

Theory says that quantum annealing should eventually be replaced by a combination of better classical computing approaches — taking over its use cases from “below,” in terms of technical sophistication — and gate-based quantum computing, taking over its use cases from “above.” We'll see.

Gate-based quantum computing

Most quantum computers use quantum circuitry to reproduce the logic-gate structure of classical computers. These computers are called, sensibly enough, *gate-based quantum computers*. Gate-based quantum computers use qubits in a specific way and are not tolerant of errors in the operation of the qubits; the quantum logic gates don't work reliably if the qubits aren't error-free. Today's qubits are not reliably error-free, which compromises the utility of today's gate-based quantum computers.



Gate-based quantum computing is so hard to achieve that we can't yet be certain that it will ever reach its full potential. But if it does, it will probably render both quantum-inspired computing and quantum annealing obsolete. In the fullness of time, gate-based quantum computing should become the best way to handle any kind of quantum-related computing problem.

Four major types of qubits are used in this type of quantum computer, based on the actual physical object kept in a coherent state to perform quantum computing:

- » Superconducting metal loops
- » Trapped ions
- » Photons
- » Neutral atoms

Each kind of qubit has its pluses and minuses, which we describe in Chapters 10 and 11. Different quantum computing companies are basing their efforts on different kinds of qubits.

KEEP YOUR ION THE BIG PICTURE

Atoms are made up of three kinds of particles: protons, neutrons, and electrons. Protons, which are in the nucleus of the atom, have a positive charge of 1. Neutrons, which are found in the nucleus as well and in the same number as protons, have a charge of 0 — no charge at all. The number of protons (and therefore also of neutrons) in the nucleus determines the atomic number of the atom and which element the atom represents. For instance, hydrogen has a single proton and neutron, whereas helium has two of each.

Electrons, which circle the nucleus, carry a negative charge equal in magnitude to the positive charge of a proton: a charge of -1 . In most states of matter, the number of electrons balances the number of protons, and the atom as a whole has a neutral electrical charge, because the charges of the protons and electrons offset each other.

In an ionized atom, electrons are added or removed. If an extra electron is captured by the nucleus, the atom now has a negative charge; if an electron escapes the pull of the nucleus, the atom has a positive charge.

Keeping qubits coherent long enough to run logic-gate operations through them is difficult, so logic-gate quantum computers tend to have relatively few qubits — a few hundred at the most, as of this writing — and to run programs for only a fraction of a second before decohering.

Addressing What's Stopping Us

We hope we've given you a taste of the power of quantum computing. What challenges must quantum computing tackle so that all this potential can start delivering more results?

In hardware, several related challenges need to be addressed:

- » **Better qubits:** Qubits with lower error rates will produce far better results. Qubits and their control machinery need to generate less noise so as not to cause cross-talk (interference among nearby qubits and the environment) and be better isolated from other noise, such as heat and vibration.
- » **More qubits:** Once each qubit behaves better, we can pack them together more densely and in greater numbers. As in classical computing, this development will greatly increase computing power while reducing costs.
- » **Cooling and supercooling:** Superconducting qubits require extremely low temperatures, but lower temperatures are better for error reduction for all kinds of qubits. Therefore, better, cheaper, easier-to-manufacture cooling and supercooling will help the other hardware challenges.
- » **Error correction:** Error correction will require multiple solutions, one of which is to combine several physical qubits into a single, self-correcting logical qubit. Colder temperatures and better control machinery will reduce the error count and ease the burden on error correction.

In software, major challenges include the following:

- » **Quantum algorithms:** Many decades of work have gone into optimizing algorithms for mainstream computers, but quantum algorithms are in their early days. Both theoretical advances and optimization in practice are needed.
- » **Hybrid quantum classical computing:** Advances in both software and hardware are needed to help quantum and classical computers share problems smoothly and with high performance; this kind of collaboration between systems is called *hybrid quantum classical computing*.

» **Error mitigation:** Software can help predict and reduce errors, making today's quantum computers more useful and reducing the burden on hardware error correction.

People power is lacking as well:

» **Scientists and researchers:** Theoretical work and advanced development are needed to move the field forward, but there are too few qualified people.

» **Software developers:** Only a small number of software developers know how to use quantum computing systems and contribute to their further development, though this share is slowly increasing.

» **Business analysts and end users:** The user community doesn't yet know what problems to try on quantum computing systems and how to ask for needed improvements that might deliver value in the near term.

Finally, quantum computing is a new way of looking at problems — and often this new viewpoint leads to better solutions for use on classical computers. Only continued work will give everyone involved a better idea as to how to use each kind of computing — and hybrid systems that use both kinds of computing — to the best advantage.

All of this may leave you wondering just where quantum computing stands today. It's actually at an awkward place: showing tremendous potential and attracting billions of dollars in investment worldwide but not yet provably superior to classical computing on important problems.

However, as this book is going to press, IBM has announced work that demonstrates what IBM calls *quantum utility*, which is the capability of quantum computers to achieve useful results that aren't possible on the computers we depend on today.

In this work, IBM used one of their more recent quantum computers, boasting 127 qubits, to simulate the interactions among 127 bar magnets — a subtle, fractal nightmare of a problem for classical computers. IBM ran the same problem across classical and quantum computer systems. Supercomputers (powerful classical computers) were able to keep up with IBM's quantum computer to about 63 qubits, half its capacity. Beyond that, the quantum computer's results seem to have exceed what's possible with supercomputers.

There's still work to do to confirm or deny this apparent breakthrough — and it's only immediately useful to anyone whose product roadmap has exactly 127 interacting bar magnets in it. But as an earnest of intent — that is, “a sort of down payment . . . a promise that you will follow through, and evidence that you can follow through,” as one website defines the term — it's pretty darn awesome.