Science in School
The European journal for science teachers

ISSUE 73 – June 2025

Topics Chemistry | Engineering | General science
Mathematics | Physics | Science and society

Quantum computing: is quantum mechanics the next computing superpower?

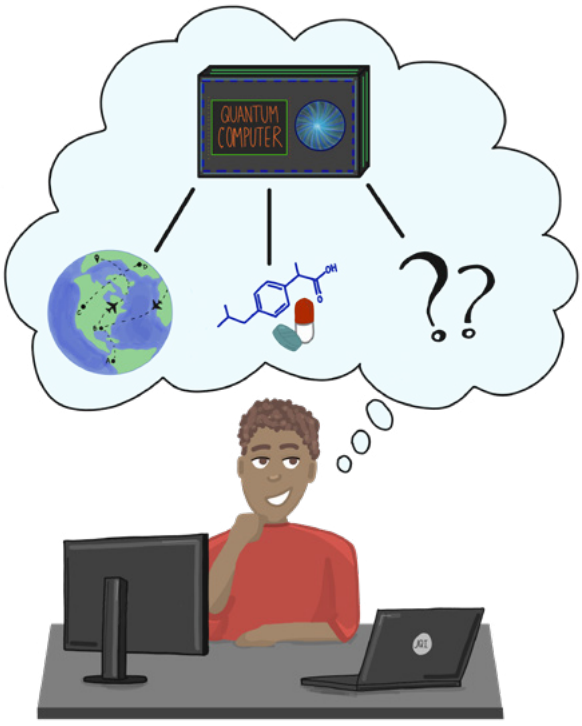
Katalin Schneider, Fabienne Marco, Vivija Čeprkalo-Simić

Stranger things: discover quantum computers, which are based on a new approach to computing powered by the strange behaviour of subatomic particles.

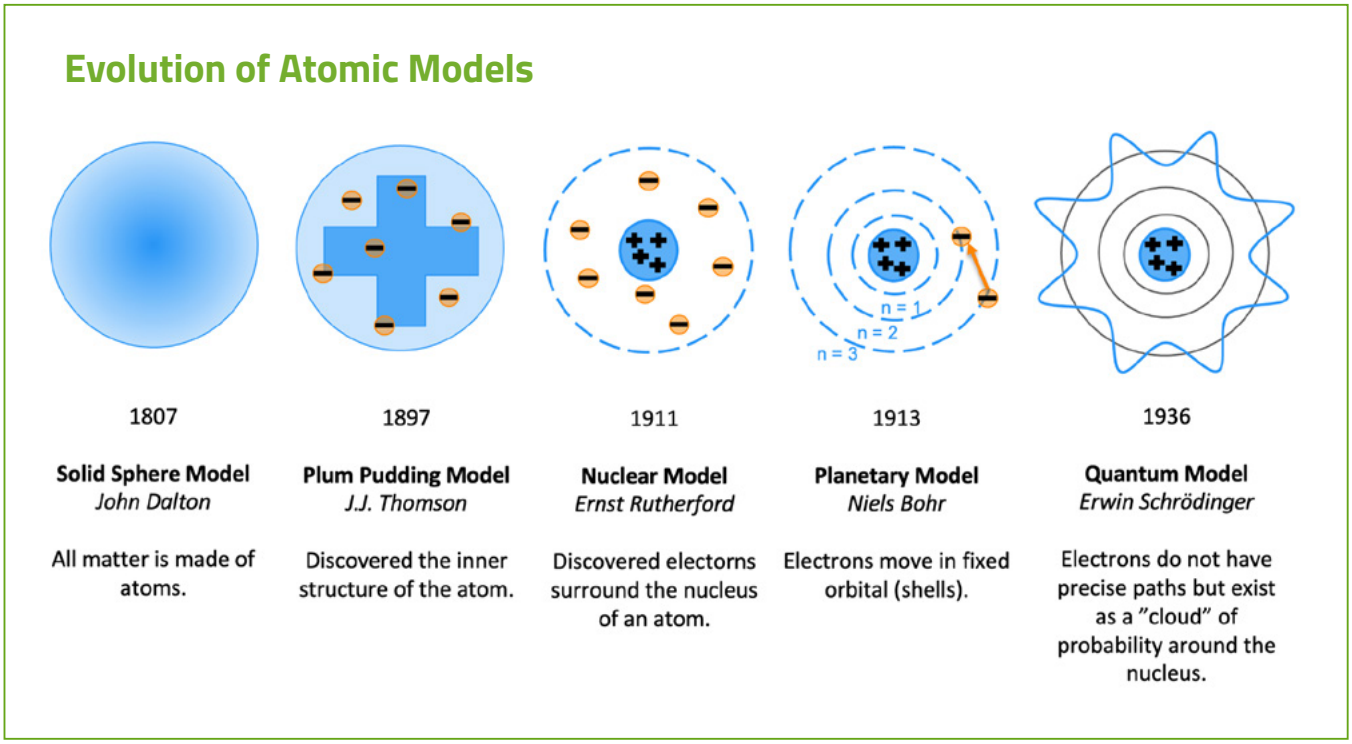
Introduction

2025 is the International Year of Quantum Science and Technology (IYQ), which recognizes 100 years since the development of quantum mechanics and aims to build public awareness of the importance of quantum science. One important application is quantum computing, but what exactly is quantum computing? How does it differ from classical computing, and why is it the subject of such intensive research around the world?

It starts with atoms, which are the basic building blocks of matter and play a crucial role in natural processes through their ability to store, transform, and release energy. The word 'atom' dates back to Greek philosophy, but around 200 years ago scientists began studying atoms and their subatomic particles – such as electrons, protons, and neutrons – in detail. As we learned more, we discovered strange and unpredictable behaviour on a subatomic scale that contradicts our experiences with matter on a macroscopic scale, that is, in 'everyday' life.



It's important to understand that it's still an open question where quantum computers will find their niche.
Image: Shivani Mattikalli/The Quantum Atlas, CC BY-NC-SA 4.0



The evolution of the atomic model over time. Scientists use models to describe reality. Scientific research constantly re-evaluates and refines these models to better understand the underlying phenomena.
Image courtesy of the authors

This apparent contradiction – material behaving differently when zooming in – led to the development of quantum mechanics, an entire branch of physics dedicated to understanding these new phenomena, which Albert Einstein described as "spooky". While current computational systems are bound by linear approaches, which creates limitations in capacity, the unusual properties of subatomic particles hold incredible potential for computing and pushing the limitations of current computational models.

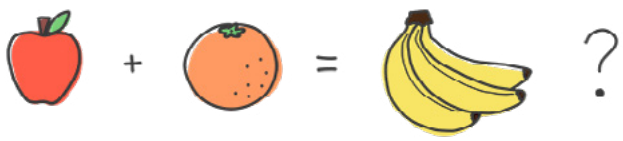
Quantum mechanical principles + computing = quantum computing

Computers are electronic devices that efficiently process, store, and manipulate data by executing predefined algorithms, performing calculations, and solving problems ranging from simple arithmetic to complex optimizations. More specifically, computers have processors that execute instructions based on changing the values of bits, which can have a value of either 0 (switched off) or 1 (switched on) and are the fundamental units of data. Sequences of bits, that is, 1s and 0s, represent information in binary code. Quantum computers represent cutting-edge technology because they redefine the core of computing by using qubits (quantum bits), which operate based on quantum-mechanical principles, rather than bits, which are limited by the rules of classical physics.

This leaves us with two questions: What are these physical properties that quantum computers build on? And how and for what applications and programs do we need these devices? Let's explore this more!

Superposition

One important characteristic of quantum particles is their ability to exist across many possible states at the same time, best described as a 'superposition' of all possible states, which means they hold different values at the same time.



In some situations, superposition can seem incomprehensibly weird, like plopping an apple next to an orange and calling the pair a banana, but it's very real.
Image: Eileen Stauffer/The Quantum Atlas, CC BY-NC-SA 4.0

In classical computing the word bit comes from 'binary unit', and it refers to the binary encoding of information with bits that can have values of either 0 or 1. Qubits, however, use the superposition of particles characteristic and can thus hold values of 0 and 1 simultaneously until measured. This makes quantum computers a lot faster when trying out different options.

In our large-scale everyday world, this would be like driving to a concert on the other side of town during rush hour and being able to take all possible paths at once to get there as quickly as possible.

Entanglement

Another characteristic of particles is that they can be 'synchronized' even when separated by large distances, which we call entanglement. Entanglement is a quantum phenomenon where two or more particles become linked so that the state of one instantly influences the state of the other, no matter how far apart they are.

Imagine you and your friend share two magical coins. Both coins could show either heads or tails. However, as soon as your friend flips their coin to find out, your coin will immediately turn to show the opposite result (heads or tails), no matter how far apart you are.

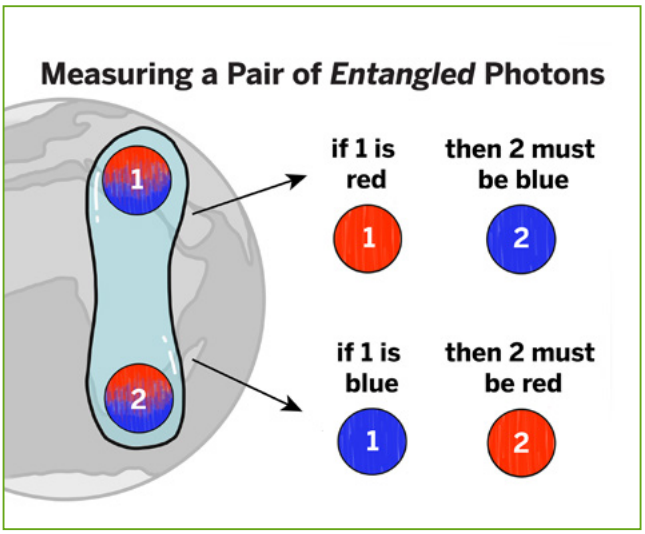


Image: Shivani Mattikalli/The Quantum Atlas, CC BY-NC-SA 4.0

In classical computers, information on how bits should be manipulated needs to be passed through the processor, where electrical signals travel through circuits to execute instructions and perform operations on the bits in chronological order. Quantum computers can surpass these extra communication steps by using entanglement: this instant effect happens even faster than light! This also makes quantum computers faster.

Quantum vs. classical computing

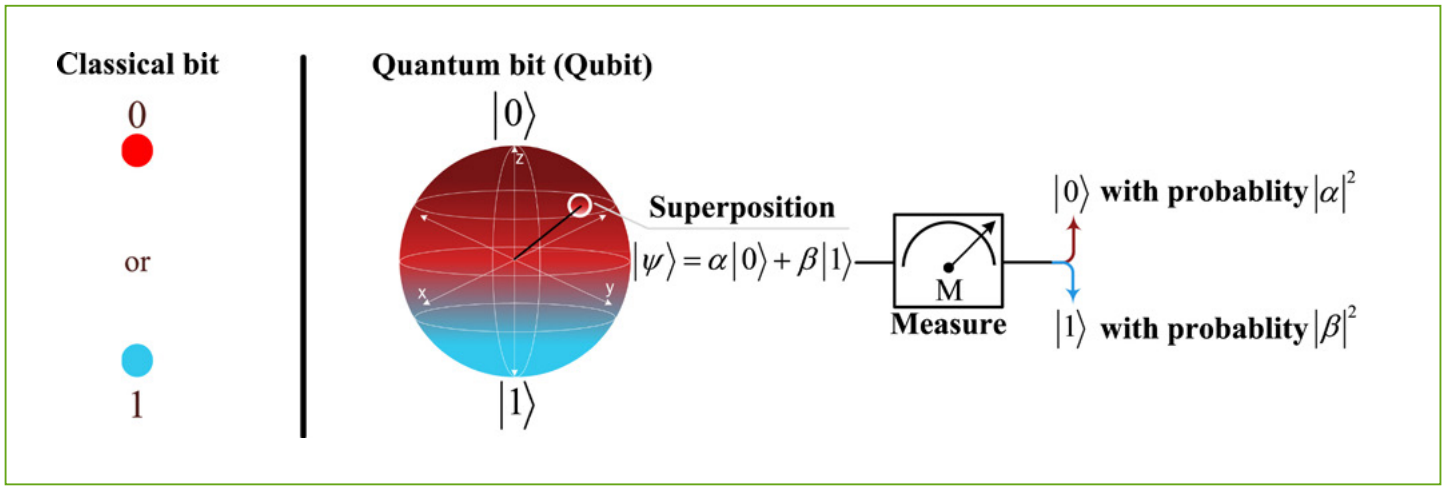
As we've seen, the qubits used in quantum computing show very different properties to the bits of classical computing.

The superposition and entanglement properties of quantum particles provide unique opportunities for quantum computing. With a shift in the fundamental principles of computing from classical physics to quantum mechanics using superposition and entanglement, quantum computers hold immense potential. The limitations on computing power in classical computing are already starting to be felt in high-intensity applications like hyperscale computing systems and neural networks. The vastly increased computing power of quantum computers means they could be used to solve problems that are currently considered unsolvable while drastically speeding up tasks that high-performance computers struggle with today, such as finding the optimal route between many stops (the so-called Travelling Salesman Problem). However, the current state of quantum technology also has some serious limitations.

Cryptography and quantum computing

Cryptography is the science of securing information. It protects our online messages, bank transactions, and passwords by turning them into secret codes. One of the most common encryption methods is RSA – named after Rivest, Shamir, and Adleman who described the algorithm in 1977 – which relies on the difficulty of factoring large numbers. However, quantum computing could change this because the advantages of qubits over bits, as discussed above, allow quantum computers to solve complex problems much faster.

One major concern is Shor's Algorithm, a quantum algorithm that can quickly break RSA encryption by finding all the prime factors for an integer. If more powerful quantum computers become reality, today's encryption methods could



The difference between bits, which can be in one of two states (blue or red), and qubits, which show superposition (a mixture of colours until measured) and entanglement (a pair of entangled particles show linked states once measured).
Image: Golestan et al./Energy reports

be at risk. To prepare for this, researchers are developing post-quantum cryptography, which includes new encryption techniques that even quantum computers cannot break.

Image: Geralt/pixabay, CC0

Despite these challenges, quantum technology also offers new ways to secure communication. Quantum key distribution (QKD) relies on the fundamental properties of quantum mechanics, such as the fact that measuring a quantum system disturbs it, to generate encryption keys in a way that means attempts to 'eavesdrop' can be detected.

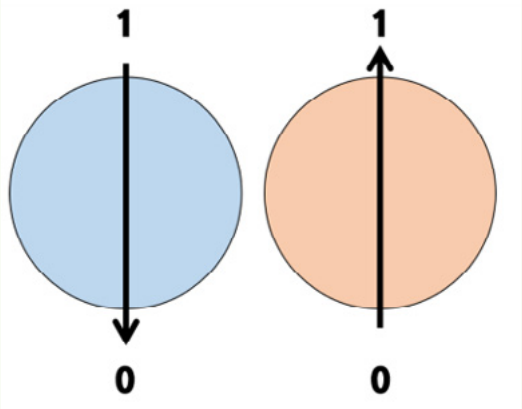
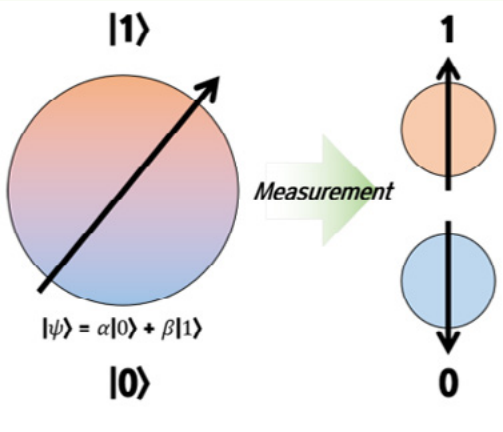
In the future, quantum computing could both compromise and improve cybersecurity. Understanding this technology is crucial for protecting digital information!

From the subatomic level back to the everyday world

Despite its immense potential, building large-scale quantum computers is an extremely challenging task.[1] As of 2025, we have devices with around 1200 physical qubits but we need devices with many thousands or even millions of qubits to solve the large complex optimization problems that we are aiming for. Physical qubits are the actual hardware-based qubits. To solve real-world problems, however, we need logical qubits. A logical qubit is a stable, reliable qubit made by combining several real qubits to protect against errors. This ensures reliable and accurate computation, but the need for logical qubits means that we need even more physical qubits.

Qubits, the basic units of information in a quantum computer, are very sensitive and can easily be disturbed by their surroundings or even by each other. This makes building larger quantum computers extremely challenging. The more qubits you add, the harder it becomes to keep them stable and working correctly together. Stable means that the qubits can hold their quantum state long enough to perform calculations without being affected by outside noise or interference. If a qubit interacts too much with its environment – such as nearby atoms, heat, or electromagnetic waves – it can lose important quantum properties like entanglement. This loss of 'quantum-ness' leads to mistakes in calculations, a problem known as quantum decoherence.[2,3]

In addition to companies like IBM, Google, and Microsoft,

Classical Computing	Quantum Computing
Classical computers operate on bits.	Quantum computers operate on qubits.
 *Image adapted from Donwoo Lee et al./MDPI*	 *Image adapted from Donwoo Lee et al./MDPI*
A bit can one of only two states: 1 or a 0. Two bits can therefore represent just one of four possible states (00, 01, 10, 11). This means that the increase in computing capacity with increasing bits is linear.	These qubits can represent the two different states of a classical bit at once. As a result, two qubits can represent four (2 × 2) values at once. This means computing power increases exponentially!
Classical computers can be used at room temperature and have low error rates.	Quantum computers need to be kept ultracold and are highly sensitive to external disturbances. E.g., fluctuations in temperature or electromagnetic interference can disrupt the fragile quantum states they rely on, which leads to high error rates.

countries such as the United States, China, and European nations are racing to build the first large-scale quantum computer with enough connected and properly working qubits to solve real-world problems.[2] They have already developed small-scale quantum computers where first applications can be tried out, where researchers can gain experience in how to use them, and where companies can test whether they work correctly.

Conclusion

Quantum computers are a new type of device that uses the principles of quantum mechanics, instead of classical physics, to speed up calculations and solve currently unsolvable problems. Quantum computers may sound like science fiction now, but they are quickly becoming a reality! If you are as fascinated as we are, you can join the United Nations in making 2025 your Year of Quantum Science and Technology. «

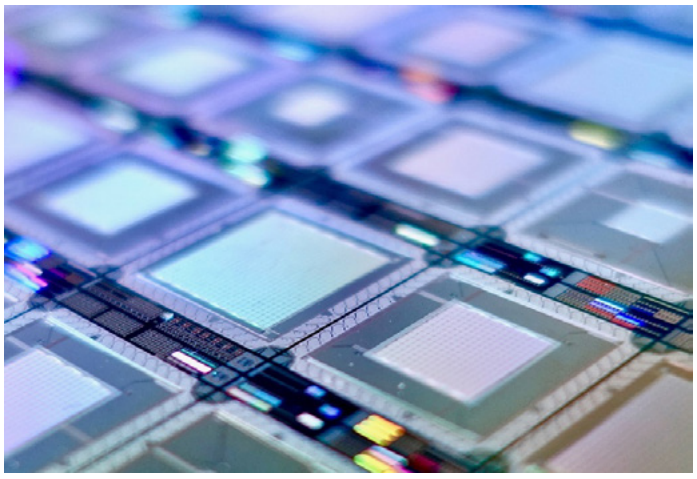


Image: Steve Jurvetson/flickr, CC BY 2.0

Here you can see Dr. Maika Takita standing beside an IBM quantum computer with a visible dilution refrigerator, featuring gold-plated, tiered components that cool the quantum processor to near absolute zero. The chandelier-like structure includes wiring, filters, and thermal shields essential for preserving the fragile quantum states of the qubits.
Image courtesy of IBM

Glossary

Bit: A binary unit, or bit, is the basic unit of information in classical computing. It can have one of two values: 0 or 1.

Qubit: A quantum bit is the basic unit of information in quantum computing. Unlike a bit, it can be 0, 1, or both at the same time thanks to a property called superposition.

Physical qubit: the actual hardware used to store and manipulate information in a quantum computer. They can be affected by noise, so many are needed to create one logical qubit.

Logical qubit: an ideal, error-free qubit for use in quantum calculations. It is built from multiple physical qubits working together to correct errors.

Hyperscale computing: very large-scale computing systems that can handle enormous amounts of data and computation, often used in big tech and cloud computing.

Neural network: a type of algorithm inspired by how the human brain works. It is used in artificial intelligence (AI) to recognize patterns, learn from data, and make decisions.

Quantum decoherence: interference from the environment causes a quantum system to lose its quantum properties, which leads to computing errors

References

[1] Mohseni M et al. (2024) How to build a quantum supercomputer: Scaling challenges and opportunities. *arXiv preprint*. doi: 10.48550/arXiv.2411.10406

[2] Rietsche R et al. (2022) Quantum computing. *Electron Markets* **32**: 2525-2536. doi: 10.1007/s12525-022-00570-y

[3] Schlosshauer M (2019) Quantum decoherence. *Physics Reports* **831**: 1-57. doi: 10.1016/j.physrep.2019.10.001

Resources

- Discover events happening worldwide as part of the International Year of Quantum Science and Technology 2025 (IYQ).
- Check out this infographic on the historical development of atomic models.
- Read this brief introduction on how bits and bytes encode information.
- Get a more detailed insight into how computers process and store data.
- Take a look at the Quantum Atlas – a multimedia approach to explore the quantum world
- Read an introduction to the principles of quantum computing, including animations to explain superposition and entanglement.
- Read a more detailed article on quantum entanglement, explained with a clever analogy.
- Watch a video from Fermilab explaining the 'spooky' effect of quantum entanglement.

- These two shorter videos from the Perimeter Institute offer clear and engaging explanations of superposition and quantum entanglement.
- Explore the most common types of physical qubits.
- Try the new particle physics course for high-school students from CERN.
- Psst! Pass it on! Teach your students binary code the easy way! Estudante A and Lourenço JP (2021) Teaching binary code with a secret word challenge. *Science in School* **52**.
- Learn about perovskites' rare magnetoelectric properties and how they could help us overcome the challenges of quantum computing: Espirito Santo C (2025) Neutrons for the quantum technologies of the future: investigating layered perovskites. *Science in School* **73**.
- Find out how magnetic 'storms' could help us achieve better, faster data storage: Chandran A (2023) Information revolution: how ultra-short bursts of light could help us improve data storage. *Science in School* **62**.
- Explain exponential growth to your students through these simple activities involving confetti: Vieser W (2021) Exponential growth 1: learn the basics from confetti to understand pandemics. *Science in School* **53**.
- Learn the basics of block coding by using a micro:bit computer and create a timer for science experiments: Bowen GM, German S, Khan S (2023) Introducing block coding: using the BBC micro:bit in the science classroom. *Science in School* **61**.
- Build a cloud chamber with your students: Barradas-Solas F, Alameda-Meléndez P (2010) Bringing particle physics to life: build your own cloud chamber. *Science in School* **14**: 36–40.
- Discover how artificial intelligence is helping to predict protein folding: Heber S (2021) From gaming to cutting-edge biology: AI and the protein folding problem. *Science in School* **52**.
- Get inspired by the science show Particle Detectives to bring fun and fascination to your classroom: Gregory M, Horvat AK (2024) Particle Detectives: boldly bringing particle physics outreach to new frontiers. *Science in School* **68**.
- Learn about how cosmic rays from space can affect electronics on Earth: ILL (2023) What does particle physics have to do with aviation safety?. *Science in School* **62**.

Books:

- Coecke B, Gogioso S (2023) *Quantum in Pictures: A New Way to Understand the Quantum World.* Paperback. ISBN: 978-1739214715
- Whurley, Earl Smith F (2023) *Quantum Computing For Dummies* 1st edition. For Dummies. ISBN: 978-1119933908

AUTHOR BIOGRAPHY

Fabienne Marco is a PhD student and head of the Quantum Social Lab at the Technical University Munich. The Quantum Social Lab aims at engaging technical developers, policy makers, and the general public in understanding quantum phenomena, quantum technologies, and their societal impacts.

Katalin Schneider is a PhD student at the Technical University Munich and works in the QuantWorld project. The QuantWorld project aims to build a learning platform based on quantum technologies and study their impact on medicine, mobility and finance.

Vivija Čeprkalo-Simić is a project manager at the Cybersecurity Training Lab of the research institute Fraunhofer AISEC. The Cybersecurity Training Lab provides hands-on training and practical education in cybersecurity and focuses on equipping professionals with the necessary skills to tackle current and emerging cybersecurity challenges.