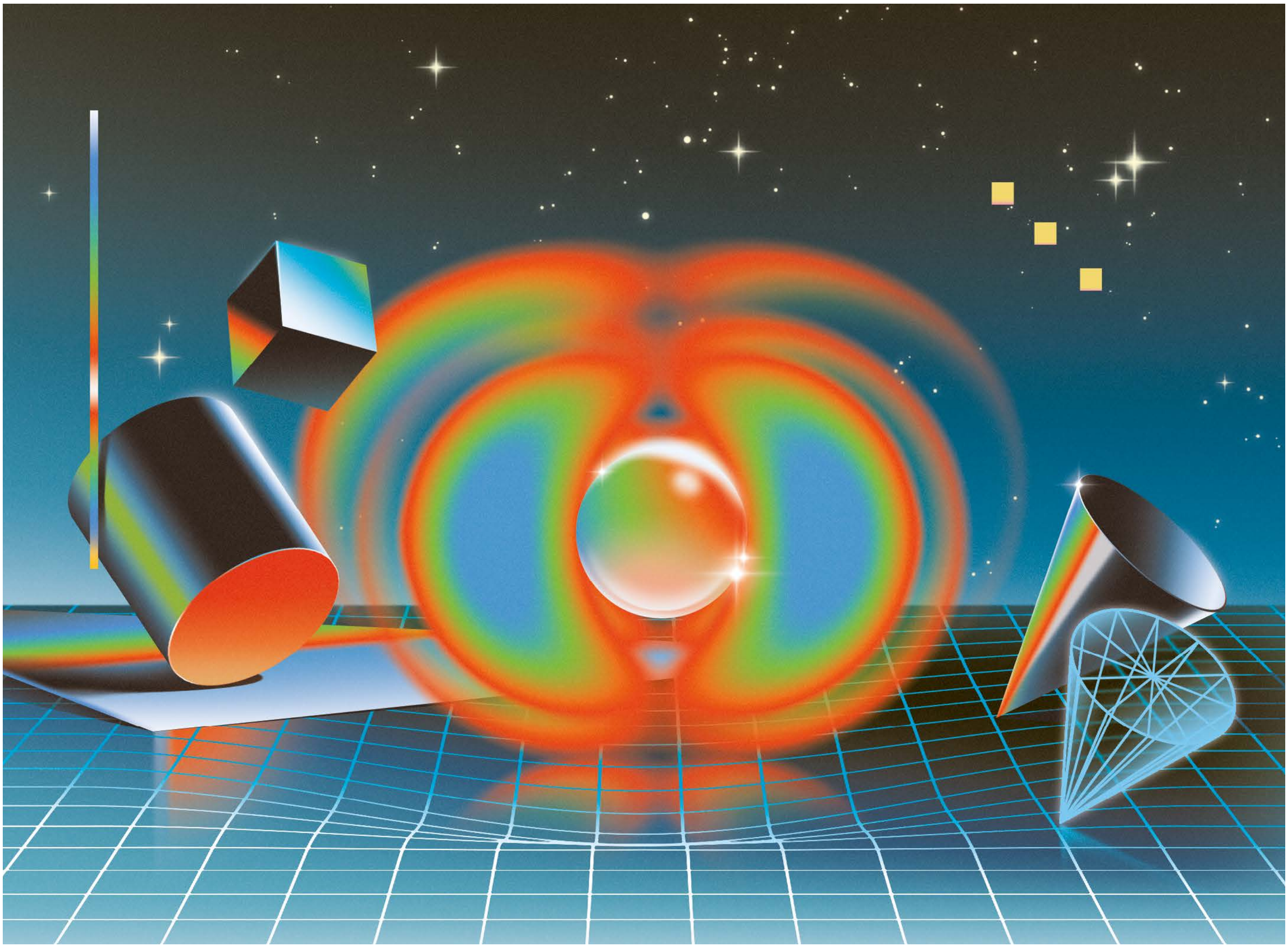


ILLUSTRATIONS: SANDRO RYBAK

Six quantum myths to wrap your head around

There's nothing intuitive about quantum theory — physicists debunk some of the most common misconceptions.

Quantum mechanics is unquestionably a robust and successful theory — so far, all its predictions have held, and scientists can build powerful technologies based on it. Yet, understanding what it tells us about the nature of reality and how we experience it has proven tricky. Physicists and philosophers have been grappling with it for a century, ironing out some of the early ambiguities, but some conceptual problems remain. And the non-intuitive nature of quantum physics makes it fertile ground for misunderstandings. Here, six physicists explore the origins of widespread myths about quantum history, theory and applications.

MARIA VIOLARIS

HAS QUANTUM PHYSICS MADE TIME TRAVEL POSSIBLE?

If you've been following quantum-science announcements in the past few years, you might think that experiments have managed to send quantum particles back in time. But despite intriguing theoretical proposals and experimental studies, that has not been achieved (yet).

The idea relies on exploiting quantum 'time loops' — hypothetical twists in space-time that allow a particle, or anything else, to come out of the loop at an earlier time than when it went in. These loops could exist in the Universe, for example through tunnels in the fabric of space-time.

The recent proposals were based on quantum teleportation of qubits, in which the state of a qubit is transported from one location to another, without physically moving between them. This can be done by using an entangled pair of qubits, one at each location.

However, to avoid violating core principles, such as no faster-than-light communication, quantum teleportation can be successful at most only one-quarter of the time. For the remainder, the receiver needs to correct its teleported qubit using information from the sender. But researchers are looking into an alternative approach, in which they discard these failed cases, keeping only the successful one-quarter.

This selective version of teleportation has been proposed as a model for a quantum universe that allows time travel. Such a Universe could have laws of physics that automatically discard any paradoxical outcome arising from something changing the past. By following a similar protocol, but instead manually discarding certain measurement outcomes, researchers have achieved a quantum advantage in the field of metrology (the science of making precise measurements).

The experimental results look identical to those that would come from a real time loop, but the behaviour has been engineered from quantum entanglement. So, no one has really sent a particle to the past quite yet. But the general theory of relativity allows for time travel – and quantum models give promising ways to resolve its paradoxes. Quantum mechanics therefore could yet make time travel possible – but I'd need to read a paper sent back from the future to be sure.

Maria Violaris works on quantum foundations as an academic visitor at the University of Oxford, UK, and on quantum computing at Oxford Quantum Circuits, Reading, UK.
e-mail: maria@violaris.com

ESTELLE INACK
CAN QUANTUM COMPUTERS GUARANTEE SPEEDIER CALCULATIONS?

The promise of quantum computers and their abilities to solve a host of intensive computational problems – from how the quantum behaviour of electrons affects chemical reactions to optimizing routes in logistics – has spurred a booming industry that is attracting billions of dollars of investor cash. As excitement has grown, so has a misunderstanding about how quantum computers work, why they are potentially so powerful and fast at making calculations and what their limitations might be. It's one thing to have a quantum computer, but another to extract the right answer for a complex calculation out of it. And it won't simply speed up every existing application – we are not likely to need 'quantum Word' or 'quantum Zoom'. Instead, they are promising tools for exploring very complex systems.

Quantum devices are sometimes said to offer power and speed by relying on quantum bits (qubits) that are both 0 and 1 at the same time; by contrast, classical bits are either 0 or 1. This is misleading. What happens instead is that a qubit exists in a superposition of 0 and 1 classical states. And each time a measurement is taken, it has a probability of being measured as either 0 or 1.

When putting many qubits together, say N of them, to form a quantum computer, their quantum superposition spans the same mathematical space as 2^N classical bits; this is often referred to as quantum parallelism with exponential speed-up. When a quantum computation is performed, the system outputs one single state from those 2^N possible ones.

The computation must be repeated many times (although fewer than 2^N times, which would be impossible when N is large) to build a probabilistic picture of the system: the outcome with the highest probability gives you the correct answer. This overhead could reduce the advantages of quantum computers over classical computers. Algorithms that increase the probability of obtaining the correct (most likely) outcomes from each calculation are crucial.

Another limitation of quantum computers is that quantum states are very fragile and need to be protected from interactions with their environment, which can disrupt them. Researchers are exploring clever ways to do this through error-mitigating algorithms.

Thus, quantum computers are indeed powerful machines that rely on quantum superposition and parallelism – but innovations in algorithms, hardware and software are also needed to harness their full potential.

Estelle Inack is a research scientist at the Perimeter Institute, Waterloo, Canada.
e-mail: einack@perimeterinstitute.ca

SABINE HOSSENFELDER
DID EINSTEIN REJECT THE IDEA OF ENTANGLEMENT?

You might have heard that what Albert Einstein referred to as 'spooky action at a distance' is technically known as 'entanglement', and that he insisted that entanglement couldn't exist. Neither is true.

The 'spooky action' quote is a direct translation of the German phrase *spukhafte Fernwirkung*, which Einstein wrote in a 1947 letter to fellow physicist Max Born. He was referring to an idea that had long intrigued him – how to interpret the measurement process in quantum mechanics, which he had earlier described as relying on a "peculiar mechanism of action at a distance" (G. Bacciagaluppi and A. Valentini Preprint at arXiv https://doi.org/p2ns; 2006).

Mathematically, the measurement process in quantum mechanics is instantaneous. Say you want to measure the position of a particle. Before you do so, the equations allow the particle to be in several places at the same time. Observe or measure it, however, and suddenly it is in only one place.

This issue of reality apparently suddenly materializing out of uncertainty when you observe it is known as the measurement problem. The update happens faster than light, seemingly violating Einstein's special theory of relativity, which says that no signal can exceed light speed. Of course, Einstein didn't like it. That is why, together with physicists Boris Podolsky and Nathan Rosen, Einstein argued in 1935 that quantum mechanics must be an "incomplete" theory (A. Einstein *et al. Phys. Rev.* **47**, 777; 1935), in which measurement is just a probabilistic description of an underlying physical reality.

That same year, Erwin Schrödinger coined the term 'entanglement' to describe a correlation between two or more objects about which one has incomplete knowledge. You could, for example, have two particles, one on the left and one on the right, that can each have a state (usually physicists consider the property of 'spin', but it could be something else, such as momentum) of either +1 or −1, and both values must add up to 0. So, either the left particle has spin −1 and the one on the right spin +1, or the other way around.

In an experiment, you can flip the spin of one particle, say the left one, even without knowing what it is. If it was −1, it is now +1; if it was +1, it is now −1. If you do that, what happens to the particle on the right side? Nothing. The other particle itself has not changed, and the two particles are still entangled – just the correlation between them has changed. You have changed an entangled system into a different, also entangled system. There is no 'spooky action' in entanglement, no exchange of information that is faster than the speed of light.

I think the reason why even some physicists get this mixed up is that in their 1935 paper, Einstein, Podolsky and Rosen used what we now call 'entangled particles' to illustrate the problem with the instantaneous update of a system on measurement. The two concepts – measurement and entanglement – became entangled, so to speak.

Einstein never claimed that entanglement, or quantum physics itself, is wrong. What he did was question the physical interpretation of the measurement: that a quantum system seems to exist in several possible superposed states but updates to a different state as soon as you observe it. That is an issue that still hasn't been resolved.

Sabine Hossenfelder is a physicist and member of the Munich Center for Mathematical Philosophy in Munich, Germany.

NORMA SANCHEZ
IS GENERAL RELATIVITY IRRECONCILABLE WITH QUANTUM PHYSICS?

Physicists have devised two grand theories to understand reality. The general theory of relativity dominates how things happen at large scales, such as across the cosmos. Quantum mechanics, meanwhile, covers atom-sized forces or smaller. Many physicists quibble that they might never be reconciled – although we have no real indication that it is not possible. In the past few years, progress and the potential for new observations, such as those of gravitational waves, gives me hope that we won't need a completely new theory to encompass both.

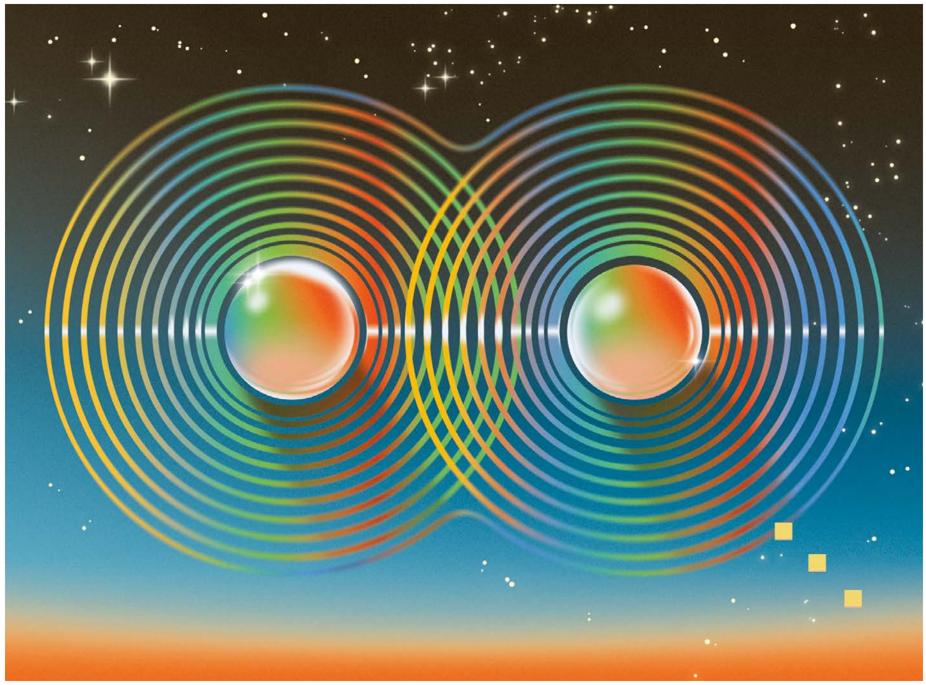
In their current form, these theories produce pictures that are completely at odds with each other, impractical or unintelligible. Gravity, for example, is well explained by the general theory of relativity as a curvature of space-time in the presence of massive bodies. But because this formalism considers particles to have non-zero mass concentrated to a single point (with zero volume), following it at subatomic scales would make gravity infinite, which makes no sense.

There have been many attempts to reconcile the two frameworks. One is string theory – in which particles and forces arise from the vibrations of tiny one-dimensional 'strings'. But this theory has run into problems: it does not explain the observed expansion of the Universe, or its structure, and no direct experiments have supported it. Other approaches that start with classical gravity and try to 'quantize' it have not succeeded either.

I'm exploring one route that starts with quantum physics and embeds gravity into it. I'm working on a type of quantum space-time – space and time that has quantum properties, with discrete mass levels that blur into a continuum in our macroscopic world, just like atomic energy levels.

Ultimately, to test this theory, more measurements are needed – on the expansion of the Universe in its early days and now, on gravitational waves from black holes and on experimental systems that would reproduce gravity in the lab. Atoms at temperatures close to absolute zero, for example, have shown condensed-matter properties that resemble the behaviour of matter near black holes. If we learn more about the Universe through observations, I hope that, together with theory, the two frameworks can be united.

Norma G. Sanchez, is the founder and director of research at the International School-Institute of Astrophysics Daniel Chalonge – Hector de Vega, CNRS-INSU, Sorbonne University, Paris, France.
e-mail: norma.sanchez@orange.fr



SHWETA AGRAWAL
WILL QUANTUM COMPUTERS BREAK ANY ENCRYPTION?

Classical encryption schemes rely on encoding plain information into unintelligible 'ciphertext' that can be read by the intended recipient who has the key to decode it. The ciphertext might also be broken open without the decryption key, but doing so implies the ability to solve some well-known problem that is thought to be mathematically 'hard' – a technical term that means it cannot be solved computationally in a given, finite time. Intuitively, the harder the mathematical problem underlying the encryption scheme, the harder it is to break open, and the more secure the encryption.

Ideally, an encryption scheme would rely on a problem that can't be solved at all by a computer in an efficient way. But researchers don't actually know whether such problems exist for classical computers that can serve as public keys (the factoring of large numbers, the problem on which the Rivest–Shamir–Adleman (RSA) encryption protocol – used widely in e-commerce and elsewhere – is based, is thought to be, but we have no proof). Our understanding of quantum computing is even more rudimentary. We know very little about what they can or cannot do.

The only thing we do know is that some problems that are thought to be mathematically hard for classical computers, and that have been used for cryptography, are now known to be easy for quantum computers – they can at least theoretically be solved efficiently in a given time frame. But there are lots of problems that remain hard for quantum computers, too, as far as we understand.

On the basis of my experience in theoretical computer science, I think we are unlikely to run out of encryption techniques to securely code information. There are many problems in mathematics and computer science that are still hard for quantum computers to solve. And if we run out, we can simply find more. Building secure encryption is like a game of chess – you just need to stay ahead of the attacker. This is a very exciting area of cryptography.

To get the best guarantees possible, we assume honest parties have access only to the regular classical computers that are currently available, while attackers have access to quantum computers. If we assume that even regular users have access to quantum computers, then we can use the principles of quantum mechanics to secure information, which yields the more powerful notion of 'quantum encryption'. An important milestone in this regime is a way to distribute unbreakable keys, something that is not known in the classical setting.

Shweta Agrawal is a professor of computer science at the Indian Institute of Technology, Madras, India.
e-mail: shwetaag@cse.iitm.ac.in

EMILY ADLAM
DO WE ALREADY HAVE A GOOD INTERPRETATION FOR QUANTUM MECHANICS?

Scientists have devised many interpretations of quantum mechanics to attempt to get their heads around what's really going on. Some physicists and philosophers think that solving its notorious measurement problem – explaining how a classical system emerges when a quantum one is observed – boils down to choosing the right interpretation from the many on offer. But it's not that simple. So far, different explanations work for different phenomena, and none explains everything.

In practical terms, solving the measurement problem means understanding where and how, in the mathematical formalisms that make up quantum mechanics, observing a superposition of states in an atomic-scale system causes it to 'collapse' into a single outcome. In philosophical terms, this brings up questions about how an observer – whether a person or a laboratory instrument – interacts with the real world. Explanations fall into two categories.

The first one leaves the current equations of quantum mechanics unchanged but disrupts the relationship between observer and evidence. For example, the 'many worlds' interpretation proposes that when we make a measurement, all the possible outcomes do occur – hypothetically (as far as we know) in 'parallel worlds' in mathematical space, consistent with the equations.

But if all outcomes occur somewhere, it shouldn't matter how often the same measurement gives the same outcome, because we know that every possible combination of outcomes will definitely occur somewhere. But the evidence supporting quantum mechanics hinges on the fact that the probabilities it predicts match the observed frequencies of the outcomes. Lasers and quantum computing, for example, depend on such precise probabilities. The many-worlds approach is at odds with this. Other interpretations that go down similar routes have their own problems.

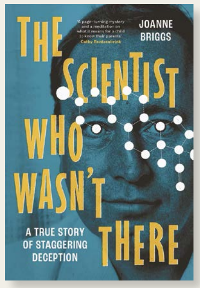
In the second category, researchers tinker with the mathematical formalism of quantum mechanics, by adding extra 'hidden variables', or more mechanisms that precipitate collapses of superpositions of states into a single outcome. But these tweaks trigger a host of technical challenges to reconcile the updated formalism with other aspects of quantum theory – raising issues in quantum field theory, which combines quantum mechanics with the special theory of relativity.

Some of these problems might be resolved in the future. As things stand, however, our most advanced scientific theory is still not consistently linked to reality in a manner that we can comprehend. In my view, for now, it's less a case of choosing the right interpretation from those available, and more of waiting for the stroke of inspiration that might open our eyes to the truth of quantum theory.

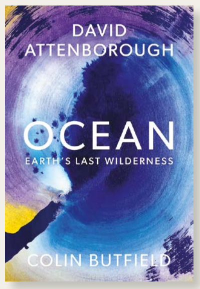
Emily Adlam is an assistant professor in the philosophy of quantum physics at Chapman University, Orange, California.
e-mail: eadlam90@gmail.com

E.I. declares competing interests; see go.nature.com/4oIov2 for details.

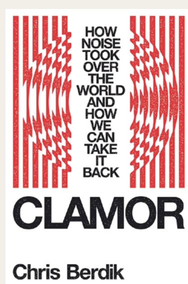
Books in brief



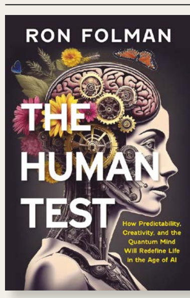
The Scientist Who Wasn't There
Joanne Briggs *Ithaka* (2025)
Once a respected NASA space scientist, Michael Briggs became a university biochemist and pharmaceutical executive who advocated for Primodos, a controversial oral pregnancy test. But Briggs was exposed for scientific fraud by an investigative journalist in 1986. He died that same year from a mystery illness. Now his daughter, barrister Joanne Briggs, has written a hauntingly frank "memoir, not a historical account" about him, relying on her and her mathematician brother's memories and copious research into their father's career.



Ocean
David Attenborough & Colin Butfield *John Murray* (2025)
During the past century — which coincides with naturalist and broadcaster David Attenborough's life — "we have discovered more about our ocean than in any other span of human history", Attenborough notes in an eloquent book, written with producer Colin Butfield. We know that the huge blue whales (*Balaenoptera musculus*) feed mainly on krill, some of the ocean's smallest animals, swallowed in a single gulp of 80,000 litres of water. Yet how whales blend their senses to traverse Earth's "last wilderness" is still a mystery.



Clamor
Chris Berdik *W. W. Norton* (2025)
The World Health Organization treats noise as one of the top environmental threats. Drawing on research in acoustics, neuroscience and urban planning, science writer Chris Berdik explores in his resonant book how "noise took over our world while we weren't really listening". Noise "can trigger a visceral, even furious response from us in the moment" but once it passes we ignore its effects. And it's tricky to distinguish noise from sound — like the high-pitched "kiss of a trout" followed by a splash while fly-fishing.



The Human Test
Ron Folman *Prometheus* (2025)
"I think I can safely say that nobody understands quantum mechanics," noted theoretical physicist Richard Feynman. Physicist Ron Folman quotes Feynman in his thought-provoking study of humans versus artificial intelligence (AI). Folman tackles a challenging question: what is the real difference between the activity in our brain and "what the single atom in my lab does when it communicates with us". Resolving the issue of randomness versus predictability will reveal whether AI can predict human behaviour.

Sand, Snow, and Stardust
Gretchen Heefner *Univ. Chicago Press* (2025)
Before the Second World War, the United States had only 14 military bases overseas; by 1960, it had more than 1,000. One such base lay beneath the Greenland ice cap, another on the Sahara Desert's edge. Engineers learnt to build a runway on permafrost and restrain blowing sand. Both proved crucial for NASA's lunar exploration in the 1960–70s, argues historian Gretchen Heefner in her pioneering exploration of how the military "acquisition of environmental knowledge turned the United States into a planetary power". **Andrew Robinson**