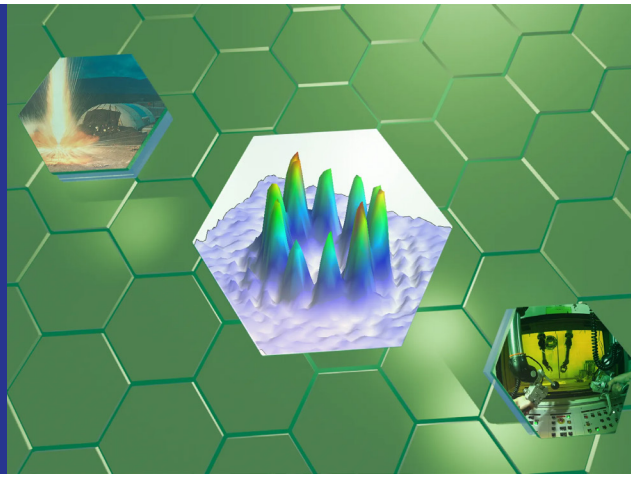
The Race to Build a Quantum Computer

KYLE DICKMAN



Los Alamos scientists turned a paradox at the heart of quantum mechanics into a pathway toward quantum computing.

Like too many other stories about quantum mechanics, this one begins with a cat in a box. According to the strange physics of the subatomic world, Schrödinger's famous cat is both alive and dead until someone opens the box. Los Alamos theoretical physicist Wojciech Zurek accepted that oddity as reality. He wanted to understand why, when the box is opened, the cat is always dead or alive—but never both.

More precisely, Zurek sought to explain how the fuzzy, probabilistic rules governing atoms give way to the definite, stable reality we experience through a process called decoherence, in which interactions between quantum systems and their environment produce classical behavior. Zurek's decades at Los Alamos were largely theoretical—whiteboards, quiet hours, long conversations about even longer equations. He didn't set out to build a quantum computer that could help design corrosion-resistant alloys, simulate complex molecules, or even secure or break cryptographic codes essential for national security. But almost thirty years after first developing his ideas, they're central to why usable quantum computers now appear within reach.

By the early 1980s, the classical computing revolution was well underway. Personal computers were entering homes and offices, while supercomputers at national laboratories were pushing the limits of numerical simulation. Moore's Law promised ever more powerful machines. Yet even as classical processors grew faster, they remained bound by the same binary logic: bits encode information as zeros and ones, and every calculation is executed through long sequences of binary steps.

Richard Feynman, the Nobel Prize–winning physicist who had worked at Los Alamos during the Manhattan Project, recognized that because of this, classical machines would always struggle to simulate the quantum world. "Nature isn't classical, dammit," he told an audience in a 1981 lecture. "And if you want to make a simulation of nature, you'd better make it quantum mechanical."

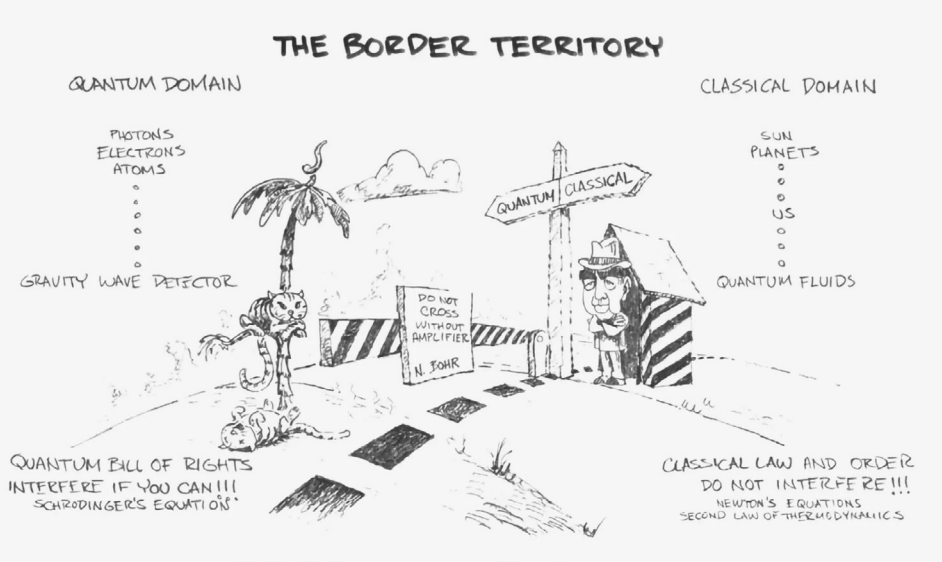
"Nature isn't classical, dammit. And if you want to make a simulation of nature, you'd better make it quantum mechanical."

At its most fundamental level, matter obeys the rules of quantum mechanics, in which physical systems, like Schrödinger's cat, can exist in combinations of multiple states at once. In the early 1980s, Feynman and British physicist David Deutsch, often called the father of quantum computing, recognized that this strange reality could form the basis of a new kind of machine. Quantum computers would

encode information in quantum bits, or qubits, which can exist in combinations of zero and one—a state known as a superposition.

When multiple qubits are linked through a phenomenon called entanglement, they become a single, unified quantum state in which each qubit's behavior depends on the behavior of the others. A quantum algorithm can then evolve that unified state, using interference to amplify certain outcomes, so that when the qubits are measured, the resulting pattern reveals the solution. Long before anyone could point to a specific application, Feynman and Deutsch understood that entangled qubits hinted at unusual computational power. As more qubits become entangled, the size of that joint state doubles with each added qubit, so that representing it on a classical computer would require resources beyond what even the most powerful supercomputers are capable of.

But there was a catch. The same delicate quantum behavior that made such machines intriguing also made them fragile. Heat, stray electromagnetic fields, and interactions with the surrounding environment can disrupt the delicate relationships that allow superposition and entanglement to persist. This disruption is known as decoherence. For a quantum computation to succeed, coherence must survive long enough for the calculation to finish. Without a way to manage decoherence, the idea of a scalable quantum computer remained largely theoretical.



A cartoon illustrating Wojciech Zurek's "border territory" between the quantum and classical worlds, where decoherence governs the transition from superpositions to everyday reality. These ideas have become central to efforts to build scalable quantum computers.

Even if decoherence could be solved, the real problem was that no one knew why it was worth solving. As the American theoretical physicist John Archibald Wheeler put it, "To encounter the quantum is to feel like an explorer from a faraway land who has come for the first time upon an automobile. It is obviously meant for use, and important use, but what use?"

That answer began to emerge in 1994, when mathematician Peter Shor of AT&T's Bell Laboratories showed that a sufficiently powerful quantum computer could efficiently factor large numbers, the mathematical foundation of modern cryptography. In a single paper, quantum computing shifted from thought experiment to strategic priority. If such machines could be built, they would be able to break or fortify many of the encryption systems that secure global finance, communications, and national defense.

Building one, however, required confronting decoherence, the same phenomenon

Zurek had been studying for decades. Soon after Shor's discovery, Zurek and his Los Alamos colleagues Emanuel Knill and Raymond Laflamme asked a practical question: if decoherence inevitably introduces errors into a quantum computation, could those errors be corrected before they accumulate and derail it? The problem was paradoxical. Errors must be detected to be corrected. But detecting them seemed to require measuring a qubit—and measurement collapses the very state the computation depends on.

The answer lay in changing what was being measured. In the mid-1990s, Zurek, Laflamme, Knill and their colleagues showed that the quantum information representing a computation could be encoded across multiple entangled qubits rather than stored in a single one. That redundancy allowed errors affecting individual qubits to be detected indirectly—without measuring and collapsing the fragile computational state itself. Their work did not build a quantum computer. But it demonstrated that scalable quantum computation was not forbidden by the laws of physics.

Over the next two decades, researchers advanced along that path. By the mid-2010s, a series of technical breakthroughs ushered in what Malcolm Boshier, a physicist at Los Alamos, calls the second wave of quantum computing. If the first wave proved quantum computing was not forbidden by physics, the second asks whether it can scale. Los Alamos now plays a central role in answering that question.

After decades studying decoherence, error correction, and quantum computing algorithms, the Lab plays a major role in the Quantum Benchmarking Initiative (QBI), a Department of Defense and Defense Advanced Research Projects Agency-supported effort to rigorously evaluate competing quantum-computing designs. Rather than build machines, QBI evaluates proposed architectures through technical scrutiny, asking a practical question: Can the quantum architecture scale to deliver performance that justifies their cost?

Today, quantum processors have grown from a handful of qubits to hundreds—and in some cases, thousands. They remain noisy and error-prone. But the conversation has shifted. The question is no longer whether they are possible, but what will it take to make them useful.

Alongside this evaluative role, the Lab continues to advance quantum science—developing precision sensors and refining the algorithms and error-correction methods that underpin computation. Yet the broader question remains open. Quantum computers are clearly powerful tools, but exactly how they will reshape science, industry, and national security is still being mapped.

How do the fuzzy, probabilistic rules governing atoms give way to the definite, stable reality we experience?

This past year, Los Alamos researchers identified another problem for which quantum computers could hold a decisive advantage: the efficient simulation of large optical circuits—networks of beam splitters and phase shifters acting on vast numbers of light modes. Such circuits underpin emerging photonic technologies used in secure communications, precision sensing, and next-generation quantum computing architectures. As these systems scale, predicting their behavior becomes exponentially difficult for classical machines, which must track a myriad of possible interference patterns. A quantum computer, governed by the same physical laws as the light moving through those circuits, can in principle simulate them far more naturally—and far more efficiently.

In a sense, the problem fulfills Richard Feynman's original challenge. If nature is not classical, he argued, then our simulations should not be either. Identifying domains where quantum systems can efficiently model other quantum systems marks one of the first clearly defined arenas in which that vision could translate into practical advantage. "At the moment, you can count such problems on two hands," says Marco Cerezo, who led the work. "That's the Holy Grail of quantum computing."

For Boshier, the story of quantum follows a familiar pattern at Los Alamos. Ideas that once seemed purely theoretical matured quietly, sometimes for decades, before revealing their practical force. “Twenty years after Zurek, Laflamme, and Knill’s key ideas were first developed, they’re only now starting to look like they can deliver a tangible product,” he says. “That’s the nature of exploratory science.”