



[Back to Article](#)

[Click to Print](#)

# TIME

Monday, Feb. 17, 2014

## The Quantum Quest for a Revolutionary Computer

By Lev Grossman

For years astronomers have believed that the coldest place in the universe is a massive gas cloud 5,000 light-years from Earth called the Boomerang Nebula, where the temperature hovers at around  $-458^{\circ}\text{F}$ , just a whisker above absolute zero. But as it turns out, the scientists have been off by about 5,000 light-years. The coldest place in the universe is actually in a small city directly east of Vancouver called Burnaby.

Burnaby is the headquarters of a computer firm called D-Wave. Its flagship product, the D-Wave Two, of which there are five in existence, is a black box 10 ft. high. Inside is a cylindrical cooling apparatus containing a niobium computer chip that's been chilled to around 20 millikelvins, which, in case you're not used to measuring temperature in millikelvins, is about  $-459.6^{\circ}\text{F}$ , almost  $2^{\circ}$  colder than the Boomerang Nebula. By comparison, interstellar space is about 80 times hotter.

The D-Wave Two is an unusual computer, and D-Wave is an unusual company. It's small, just 114 people, and its location puts it well outside the swim of Silicon Valley. But its investors include the storied Menlo Park, Calif., venture-capital firm Draper Fisher Jurvetson, which funded Skype and Tesla Motors. It's also backed by famously prescient Amazon founder Jeff Bezos and an outfit called In-Q-Tel, better known as the high-tech investment arm of the CIA. Likewise, D-Wave has very few customers, but they're blue-chip: they include the defense contractor Lockheed Martin; a computing lab that's hosted by NASA and largely funded by Google; and a U.S. intelligence agency that D-Wave executives decline to name.

The reason D-Wave has so few customers is that it makes a new type of computer called a quantum computer that's so radical and strange, people are still trying to figure out what it's for and how to use it. It could represent an enormous new source of computing power--it has the potential to solve problems that would take conventional computers centuries, with revolutionary consequences for fields ranging from cryptography to nanotechnology, pharmaceuticals to artificial intelligence.

That's the theory, anyway. Some critics, many of them bearing Ph.D.s and significant academic reputations, think D-Wave's machines aren't quantum computers at all. But D-Wave's customers buy them anyway, for

around \$10 million a pop, because if they're the real deal they could be the biggest leap forward since the invention of the microprocessor.

In a sense, quantum computing represents the marriage of two of the great scientific undertakings of the 20th century, quantum physics and digital computing. Quantum physics arose from the shortcomings of classical physics: although it had stood for centuries as definitive, by the turn of the 20th century it was painfully apparent that there are physical phenomena that classical physics fails dismally to explain. So brilliant physicists--including Max Planck and Albert Einstein--began working out a new set of rules to cover the exceptions, specifically to describe the action of subatomic particles like photons and electrons.

Those rules turned out to be very odd. They included principles like superposition, according to which a quantum system can be in more than one state at the same time and even more than one place at the same time. Uncertainty is another one: the more precisely we know the position of a particle, the less precisely we know how fast it's traveling--we can't know both at the same time. Einstein ultimately found quantum mechanics so monstrously counterintuitive that he rejected it as either wrong or profoundly incomplete. As he famously put it, "I cannot believe that God plays dice with the world."

The modern computing era began in the 1930s, with the work of Alan Turing, but it wasn't until the 1980s that the famously eccentric Nobel laureate Richard Feynman began kicking around questions like: What would happen if we built a computer that operated under quantum rules instead of classical ones? Could it be done? And if so, how? More important, would there be any point?

It quickly became apparent that the answer to that last one was yes. Regular computers (or classical computers, as quantum snobs call them) work with information in the form of bits. Each bit can be either a 1 or a 0 at any one time. The same is true of any arbitrarily large collection of classical bits; this is pretty much the foundation of information theory and digital computing as we know them. Therefore, if you ask a classical computer a question, it has to proceed in an orderly, linear fashion to find an answer.

Now imagine a computer that operates under quantum rules. Thanks to the principle of superposition, its bits could be 1, or 0, or 1 and 0 at the same time.

In its superposed state, a quantum bit exists as two equally probable possibilities. According to one theory, at that moment it's operating in two slightly different universes at the same time, one in which it's 1, one in which it's 0; the physicist David Deutsch once described quantum computing as "the first technology that allows useful tasks to be performed in collaboration between parallel universes." Not only is this excitingly weird, it's also incredibly useful. If a single quantum bit (or as they're inevitably called, qubits, pronounced cubits) can be in two states at the same time, it can perform two calculations at the same time. Two quantum bits could perform four simultaneous calculations; three quantum bits could perform eight; and so on. The power grows exponentially.

The supercooled niobium chip at the heart of the D-Wave Two has 512 qubits and therefore could in theory perform  $2^{512}$  operations simultaneously. That's more calculations than there are atoms in the universe, by many orders of magnitude. "This is not just a quantitative change," says Colin Williams, D-Wave's director of business development and strategic partnerships, who has a Ph.D. in artificial intelligence and once worked as Stephen Hawking's research assistant at Cambridge. "The kind of physical effects that our machine has access to are simply not available to supercomputers, no matter how big you make them. We're tapping into the fabric of reality in a fundamentally new way, to make a kind of computer that the world has never seen."

Naturally, a lot of people want one. This is the age of Big Data, and we're burying ourselves in information--search queries, genomes, credit-card purchases, phone records, retail transactions, social media, geological surveys, climate data, surveillance videos, movie recommendations--and D-Wave just happens to be selling a very shiny new shovel. "Who knows what hedge-fund managers would do with one of these and the black-swan event that that might entail?" says Steve Jurvetson, one of the managing directors of Draper Fisher Jurvetson. "For many of the computational traders, it's an arms race."

One of the documents leaked by Edward Snowden, published last month, revealed that the NSA has an \$80 million quantum-computing project suggestively code-named Penetrating Hard Targets. Here's why: much of the encryption used online is based on the fact that it can take conventional computers years to find the factors of a number that is the product of two large primes. A quantum computer could do it so fast that it would render a lot of encryption obsolete overnight. You can see why the NSA would take an interest.

But while the theory behind quantum computing is reasonably clear, the actual practice is turning out to be damnably difficult. For one thing, there are sharp limits to what we know how to do with a quantum computer. Cryptography and the simulation of quantum systems are currently the most promising applications, but in many ways quantum computers are still a solution looking for the right problem. For another, they're really hard to build. To be maximally effective, qubits have to exhibit quantum behavior, not just superposition but also entanglement (when the quantum states of two or more particles become linked to one another) and quantum tunneling (just Google it). But they can do that only if they're effectively isolated from their environment--no vibrations, no electromagnetism, no heat. No information can escape: any interaction with the outer world could cause errors to creep into the calculations. This is made even harder by the fact that while they're in their isolated state, you still have to be able to control them. There are many schools of thought on how to build a qubit--D-Wave makes its in the form of niobium loops, which become superconductive at ultra-low temperatures--but all quantum-computing endeavors struggle with this problem.

Since the mid-1990s, scientists have been assembling and entangling systems of a few quantum bits each, but progress has been slow. In 2010 a lab at the University of Innsbruck in Austria announced the completion of the world's first system of 14 entangled qubits. Christopher Monroe at the University of Maryland and the Joint Quantum Institute has created a 20-qubit system, which may be the world's record. Unless, of course, you're counting D-Wave.

D-Wave's co-founder and chief technology officer is a 42-year-old Canadian named Geordie Rose with big bushy eyebrows, a solid build and a genial but slightly pugnacious air--he was a competitive wrestler in college. In 1998 Rose was finishing up a Ph.D. in physics at the University of British Columbia, but he couldn't see a future for himself in academia. After taking a class on entrepreneurship, Rose identified quantum computing as a promising business opportunity. Not that he had any more of a clue than anybody else about how to build a quantum computer, but he did have a hell of a lot of self-confidence. "When you're young you feel invincible, like you can do anything," Rose says. "Like, if only those bozos would do it the way that you think, then the world would be fine. There was a little bit of that." Rose started D-Wave in 1999 with a \$4,000 check from his entrepreneurship professor.

For its first five years, the company existed as a think tank focused on research. Draper Fisher Jurvetson got onboard in 2003, viewing the business as a very sexy but very long shot. "I would put it in the same bucket as SpaceX and Tesla Motors," Jurvetson says, "where even the CEO Elon Musk will tell you that failure was the most likely outcome." By then Rose was ready to go from thinking about quantum computers to trying to build them--"we switched from a patent, IP, science aggregator to an engineering company," he says. Rose wasn't interested in expensive, fragile laboratory experiments; he wanted to build machines big enough to handle significant computing tasks and cheap and robust enough to be manufactured commercially. With that in mind, he and his colleagues made an important and still controversial decision.

Up until then, most quantum computers followed something called the gate-model approach, which is roughly analogous to the way conventional computers work, if you substitute qubits for transistors. But one of the things Rose had figured out in those early years was that building a gate-model quantum computer of any useful size just wasn't going to be feasible anytime soon. The technical problems were just too gnarly; even today the largest number a gate-model quantum computer has succeeded in factorizing is 21. (That isn't very hard: the factors are 1, 3, 7 and 21.) So Rose switched to a different approach called adiabatic quantum computing, which is if anything even weirder and harder to explain.

An adiabatic quantum computer works by means of a process called quantum annealing. Its heart is a network of qubits linked together by couplings. You "program" the couplings with an algorithm that specifies certain interactions between the qubits--if this one is a 1, then that one has to be a 0, and so on. You put the qubits into a state of quantum superposition, in which they're free to explore all those 2-to-the-whatever computational possibilities simultaneously, then you allow them to settle back into a classical state and become regular 1's and 0's again. The qubits naturally seek out the lowest possible energy state consistent with the requirements you specified in your algorithm back at the very beginning. If you set it up properly, you can read your answer in the qubits' final configuration.

If that's too abstract, the usual way quantum annealing is explained is by an analogy with finding the lowest point in a mountainous landscape. A classical computer would do it like a solitary walker who slowly wandered over the whole landscape, checking the elevations at each point, one by one. A quantum computer could send multiple walkers at once swarming out across the mountains, who would then all report back at the same time.

In its ability to pluck a single answer from a roiling sea of possibilities in one swift gesture, a quantum computer is not unlike a human brain.

Once Rose and D-Wave had committed to the adiabatic model, they proceeded with dispatch. In 2007 D-Wave publicly demonstrated a 16-qubit adiabatic quantum computer. By 2011 it had built (and sold to Lockheed Martin) the D-Wave One, with 128 qubits. In 2013 it unveiled the 512-qubit D-Wave Two. They've been doubling the number of qubits every year, and they plan to stick to that pace while at the same time increasing the connectivity between the qubits. "It's just a matter of years before this capability becomes so powerful that anyone who does any kind of computing is going to have to take a very close look at it," says Vern Brownell, D-Wave's CEO, who earlier in his career was chief technology officer at Goldman Sachs. "We're on that cusp right now."

But we're not there yet. Adiabatic quantum computing may be technically simpler than the gate-model kind, but it comes with trade-offs. An adiabatic quantum computer can really solve only one class of problems, called discrete combinatorial optimization problems, which involve finding the best--the shortest, or the fastest, or the cheapest, or the most efficient--way of doing a given task. This narrows the scope of what you can do considerably.

For example, you can't as yet perform the kind of cryptographic wizardry the NSA was interested in, because an adiabatic quantum computer won't run the right algorithm. It's a special-purpose tool. "You take your general-purpose chip," Rose says, "and you do a bunch of inefficient stuff that generates megawatts of heat and takes forever, and you can get the answer out of it. But this thing, with a picowatt and a microsecond, does the same thing. So it's just doing something very specific, very fast, very efficiently."

This is great if you have a really hard discrete combinatorial optimization problem to solve. Not everybody does. But once you start looking for optimization problems, or at least problems that can be twisted around to look like optimization problems, you find them all over the place: in software design, tumor treatments, logistical planning, the stock market, airline schedules, the search for Earth-like planets in other solar systems, and in particular in machine learning.

Google and NASA, along with the Universities Space Research Association, jointly run something called the Quantum Artificial Intelligence Laboratory, or QuAIL, based at NASA Ames, which is the proud owner of a D-Wave Two. "If you're trying to do planning and scheduling for how you navigate the Curiosity rover on Mars or how you schedule the activities of astronauts on the station, these are clearly problems where a quantum computer--a computer that can optimally solve optimization problems--would be useful," says Rupak Biswas, deputy director of the Exploration Technology Directorate at NASA Ames. Google has been using its D-Wave to, among other things, write software that helps Google Glass tell the difference between when you're blinking and when you're winking.

Lockheed Martin turned out to have some optimization problems too. It produces a colossal amount of

computer code, all of which has to be verified and validated for all possible scenarios, lest your F-35 spontaneously decide to reboot itself in midair. "It's very difficult to exhaustively test all of the possible conditions that can occur in the life of a system," says Ray Johnson, Lockheed Martin's chief technology officer. "Because of the ability to handle multiple conditions at one time through superposition, you're able to much more rapidly--orders of magnitude more rapidly--exhaustively test the conditions in that software." The company re-upped for a D-Wave Two last year.

Another challenge rose and company face is that there is a small but nonzero number of academic physicists and computer scientists who think that they are partly or completely full of sh-t. Ever since D-Wave's first demo in 2007, snide humor, polite skepticism, impolite skepticism and outright debunkings have been lobbed at the company from any number of ivory towers. "There are many who in Round 1 of this started trash-talking D-Wave before they'd ever met the company," Jurvetson says. "Just the mere notion that someone is going to be building and shipping a quantum computer--they said, 'They are lying, and it's smoke and mirrors.'"

Seven years and many demos and papers later, the company isn't any less controversial. Any blog post or news story about D-Wave instantly grows a shaggy beard of vehement comments, both pro- and anti-. The critics argue that D-Wave is insufficiently transparent, that it overhypes and underperforms, that its adiabatic approach is unpromising, that its machines are no faster than classical computers and that the qubits in those machines aren't even exhibiting quantum behavior at all--they're not qubits, they're just plain old bits, and Google and the media have been sold a bill of goods. "In quantum computing, we have to be careful what we mean by 'utilizing quantum effects,'" says Monroe, the University of Maryland scientist, who's among the doubters. "This generally means that we are able to store superpositions of information in such a way that the system retains its 'fuzziness,' or quantum coherence, so that it can perform tasks that are impossible otherwise. And by that token there is no evidence that the D-Wave machine is utilizing quantum effects."

One of the closest observers of the controversy has been Scott Aaronson, an associate professor at MIT and the author of a highly influential quantum-computing blog. He remains, at best, cautious. "I'm convinced ... that interesting quantum effects are probably present in D-Wave's devices," he wrote in an email. "But I'm not convinced that those effects, right now, are playing any causal role in solving any problems faster than we could solve them with a classical computer. Nor do I think there's any good argument that D-Wave's current approach, scaled up, will lead to such a speedup in the future. It might, but there's currently no good reason to think so."

Not only is it hard for laymen to understand the arguments in play, it's hard to understand why there even is an argument. Either D-Wave has unlocked fathomless oceans of computing power or it hasn't--right? But it's not that simple. D-Wave's hardware isn't powerful enough or well enough understood to show serious quantum speedup yet, and you can't just open the hood and watch the qubits do whatever they're doing. There isn't even an agreed-upon method for benchmarking a quantum computer. Last May a professor at Amherst College published the results of a bake-off she ran between a D-Wave and a conventional computer, and she concluded that the D-Wave had performed 3,600 times faster. This figure was instantly and widely quoted as evidence of

D-Wave's triumph and equally instantly and widely denounced as meaningless.

Last month a team including Matthias Troyer, an internationally respected professor of computational physics at ETH Zurich, attempted to clarify things with a report based on an extensive series of tests pitting Google's D-Wave Two against classical computers solving randomly chosen problems. Verdict? To quote from the study: "We find no evidence of quantum speedup when the entire data set is considered and obtain inconclusive results when comparing subsets of instances on an instance-by-instance basis." This has, not surprisingly, generally been interpreted as a conspicuous failure for D-Wave.

But where quantum computing is concerned, there always seems to be room for disagreement. Hartmut Neven, the director of engineering who runs Google's quantum-computing project, argues that the tests weren't a failure at all--that in one class of problem, the D-Wave Two outperformed the classical computers in a way that suggests quantum effects were in play. "There you see essentially what we were after," he says. "There you see an exponentially widening gap between simulated annealing and quantum annealing ... That's great news, but so far nobody has paid attention to it." Meanwhile, two other papers published in January make the case that a) D-Wave's chip does demonstrate entanglement and b) the test used the wrong kind of problem and was therefore meaningless anyway. For now pretty much everybody at least agrees that it's impressive that a chip as radically new as D-Wave's could even achieve parity with conventional hardware.

The attitude in D-Wave's C-suite toward all this back-and-forth is, unsurprisingly, dismissive. "The people that really understand what we're doing aren't skeptical," says Brownell. Rose is equally calm about it; all that wrestling must have left him with a thick skin. "Unfortunately," he says, "like all discourse on the Internet, it tends to be driven by a small number of people that are both vocal and not necessarily the most informed." He's content to let the products prove themselves, or not. "It's fine," he says. "It's good. Science progresses by rocking the ship. Things like this are a necessary component of forward progress."

Are D-Wave's machines quantum computers? fortunately this is one of those scenarios where an answer will in fact become apparent at some point in the next five or so years, as D-Wave punches out a couple more generations of computers and better benchmarking techniques evolve and we either do see a significant quantum speedup or we don't.

The company has a lot of ground to cover between now and then, not just in hardware but on the software side too. Generations of programmers have had decades to create a rich software ecosystem around classical microprocessors in order to wring the maximum possible amount of usefulness out of them. But an adiabatic quantum computer is a totally new proposition. "You just don't program them the way you program other things," says William Macready, D-Wave's VP of software engineering. "It's not about writing recipes or procedures. It's more about kind of describing, What does it mean to be an answer? And doing that in the right way and letting the hardware figure it out."

For now the answer is itself suspended, aptly enough, in a state of superposition, somewhere between yes and

no. If the machines can do anything like what D-Wave is predicting, they won't leave many fields untouched. "I think we'll look back on the first time a quantum computer outperformed classical computing as a historic milestone," Brownell says. "It's a little grand, but we're kind of like Intel and Microsoft in 1977, at the dawn of a new computing era."

But D-Wave won't have the field to itself forever. IBM has its own quantum-computing group; Microsoft has two. There are dozens of academic laboratories busily pushing the envelope, all in pursuit of the computational equivalent of splitting the atom. While he's got only 20 qubits now, Monroe points out that the trends are good: that's up from two bits 20 years ago and four bits 10 years ago. "Soon we will cross the boundary where there is no way to model what's happening using regular computers," he says, "and that will be exciting."



**Find this article at:**

<http://content.time.com/time/magazine/article/0,9171,2164806,00.html>

---

Copyright © 2014 Time Inc. All rights reserved. Reproduction in whole or in part without permission is prohibited.

[Privacy Policy](#) | [Add TIME Headlines to your Site](#) | [Contact Us](#) | [Customer Service](#)