

Will Computers Take a Quantum Leap?

SETH LLOYD: A quantum computer is to a regular computer what a laser is to a light bulb.

DAVID DIVINCENZO: Within another hundred years anyway quantum computing will be ho-hum, actually.

BIRGITTA WHALEY: Do you think they will be on your desk, and in your home?

DAVID DIVINCENZO: Yes.

BIRGITTA WHALEY: In your home, but everyone's home.

DAVID DIVINCENZO: Yes.

SHOW OPEN

SETH LLOYD: I mean, actually, you know, the world is in the midst of an information revolution, it's not a secret, okay, we don't, and one of the things that happened is that, that as computers become more and more important and information becomes important, people see the world in terms of information. So, I think that, one thing I think we're doing at a larger level is trying to construct a way of seeing the world in terms of quantum information because the world is quantum mechanical, all of these quantum systems can process information.

ROBERT L. KUHN: What is quantum computing and why is it important?

DAVID DIVINCENZO: Quantum computing is in a sense, a natural outgrowth of our progress in ordinary computers.

BIRGITTA WHALEY: People started to think about them in the early 1980s, and then there was some very important theoretical results showing that one can solve some very important problems in middle 1990s and ever since then there's been a huge activity, increasing activity in trying to build and implement some of these devices.

DAVID DIVINCENZO: We've been making bits smaller and smaller as the years have gone by and, uh, at some point that ends, and it ends pretty soon. It ends because we hit the atomic world, we hit the quantum world and so something has to give.

Will Computers Take a Quantum Leap?

SETH LLOYD: Well, I think the first problem was just conceiving of the notion of storing a bit of information on an atom, quantum means “how much” -- a quantum of light is a little chunk of light, and a bit is a chunk of information. So, quantum computing is essentially, works by mapping chunks of information or bits onto quanta, onto little chunks of elementary particles. Quantum computers, they’re not merely computers that are very, very, whose components are very, very small. They can do things that classical computers can’t. So, for instance, it’s totally okay for an electron to be both here and there at the same time, an electron is behaving almost like a wave of light and it can be in two places at once. So, if I map a bit, a quantum bit – or qubit – onto electron – then I could have a bit that, say, if I had, say, an electron over here, as a zero, an electron over here as a one, then in quantum mechanics it’s okay to have an electron that’s here and there at the same time.

ROBERT KUHN: So it can have both pieces of information theoretically at the same time.

SETH LLOYD: Yeah, in some funny, quantum sense, which nobody really understands very well, it can read zero and one at the same time.

DAVID DIVINCENZO: We have a special word for that, superposition.

SETH LLOYD: Okay, now, a bit can only store one bit’s worth of information and a quantum bit can only store one qubit’s worth of information. And the way that quantum computation works is that a bit can also be used, not merely to store information, but as an instruction for a computer. So, zero could mean telling the computer do this, and one can mean telling the computer do that. And, so, putting, if you have a quantum computer and you put in a bit, a qubit that’s zero and one at the same time – it’s saying to the computer – do this and that, and do them at the same time. And, so, quantum computation gets its advantage over classical computation by the ability of quantum computers to, in some funny quantum sense, do two things at once. And in a variety of problems from database searching to factoring, to simulating quantum systems this seems to translate into a very considerable advantage over what classical computers can do. A great example of a quantum technology that’s used all over the place is the laser, right? Now, how does a laser work? The laser takes ordinary light, which comes down in just bursts of photons randomly, if you think of it, like this water jiggling around all over the place and the laser takes all of them and puts them in the same quantum mechanical states, so all the, all the light is wiggling up and down in the same.

ROBERT L. KUHN: It’s coherent.

Will Computers Take a Quantum Leap?

SETH LLOYD: It's coherent, okay? This is a very good way to understand quantum computation. So, the light from a light bulb is incoherent, everything's coming out jiggling at all once, and the same, whereas a laser is coherent, you have a wave nature where everything fits together in these nice orderly ways. In quantum computation what you're doing is you're exploiting this coherent nature of quantum mechanics, the wave nature of quantum mechanics, so, a quantum computer is to a regular computer what a laser is to a light bulb.

ROBERT L. KUHN: What were some of these problems that now may be solvable by quantum computing? Let's take factoring, factors of sixes, three and two, or parts that can multiply together to give that number.

DAVID DIVINCENZO: It certainly is something that got IBM interested when that fact was discovered that quantum computers are very good at factoring. The reason that that's of great interest in the world of computing, in the digital world, is that factoring is a key element, or the difficulty of computing factors is a key element in our current means of making things secure, of making data secure in the world.

ROBERT L. KUHN: The electronic transmission of data.

DAVID DIVINCENZO: For example, yeah, codes on credit cards secure, or other internet transmissions secure. So, quantum computers, as Peter Shor showed, could, in a relatively small number of steps, compute factors much more rapidly than any known methods than ordinary computers can use to solve that same problem. And so factoring jeopardizes a lot of what we do currently in electronic commerce.

ROBERT L. KUHN: Makes them potentially hackable.

DAVID DIVINCENZO: Potentially, but this is far in the future, nobody's worried today or next year or even probably ten years from now. But, eventually, it increases the space for hackers a lot.

BIRGITTA WHALEY: You would need to be able to build a large-scale quantum computer in order to be able to make use of this.

ROBERT L. KUHN: And what is a large scale? How many of those qubits would you need, for example, to be able to factor a large number used in electronic transmission of data?

BIRGITTA WHALEY: A few thousand.

ROBERT L. KUHN: Now, I think a Pentium IV chip has 55 million transistors, something like that.

Will Computers Take a Quantum Leap?

DAVID DIVINCENZO: Yeah, it's something like that.

ROBERT L. KUHN: So, what we're saying is that a quantum computer with a thousand, just to pick a simple number, of qubits, can do things that a normal, classical computer with tens of millions of effective transistors cannot do.

DAVID DIVINCENZO: Even the largest super computer can't do.

BIRGITTA WHALEY: And would not be able to do, probably, in fifty years' time given the current rate of increase of the technology.

SETH LLOYD: Well, so, so, an example, not factoring, but another fun problem that you can use quantum computers for is trying to understand what's going on in the universe. So if you have a system that has, say, one atom, it will take a few bits to describe that atom, and if you take, have another atom will take a few bits to describe that atom and another atom will take a few bits to describe that atom, on a classical computer, if you have a whole bunch of atoms interacting with each other, to describe say a hundred atoms, would require 2^{100} or 10^{100} bits. So to put this in perspective, 10^{100} bits, well there are only about 10^{90} elementary particles in the whole universe. You could solve that same problem on a quantum computer with just a few hundred bits.

BIRGITTA WHALEY: It would be a wonderful tool for anyone who studies the physics or chemistry of complex systems and possibly even, down the road it might become useful also for people interested in biological problems.

ROBERT L. KUHN: How would it work for biological problems?

BIRGITTA WHALEY: Well just in the same sense that for a complex, for instance, chemical system, in order to be able to find out about one particular property that you're interested in. You have to solve the whole mess of interactions together, well, that's true of a small group of molecules acting in a cell, as well.

ROBERT L. KUHN: What is entanglement? Because that's another critical aspect of quantum physics.

DAVID DIVINCENZO: That is both a real manifestation of what makes quantum mechanics weird, and we believe at the heart of what makes quantum computing powerful. Schrödinger was the one who introduced this notion entanglement at the very same time that he introduced the notion of his dead and alive cat because in that scenario, what's going on is that the radioactive atom is getting entangled with the state of the cat. Two quantum bits get into a state where, be they two quantum bits or an atom and a cat, they are strongly correlated, um, in, in ways that are stronger than they can be correlated in any classical physics situation. is really one of the strangest things about quantum

Will Computers Take a Quantum Leap?

physics, even to professionals in quantum physics. It's a place where the mathematical laws are very strange. But this entanglement has tremendous implications, not just for the kind of computing problems that we've been discussing, it actually also has implications for privacy, because if I have a qubit and it's completely entangled with your atom, then we know that there are strong correlations between those that cannot be shared with anything else in the world. So it means, if we have managed to have two objects that are completely entangled, we share the secret, we have a secret key, for example, that we can use...

ROBERT L. KUHN: That can't be broken into, theoretically?

DAVID DIVINCENZO: It cannot, according to the laws of quantum physics, be known to anyone else, even in principle.

ROBERT L. KUHN: Well, that's good if you and I have a secret, but suppose you and I are terrorists, what does that mean?

DAVID DIVINCENZO: You know, we may win also. This doesn't guarantee a stable world, but I think quantum mechanics and entanglement in quantum mechanics really changes the rules of the game of secrecy and privacy. And it gives us new tools for doing cryptography, us and the terrorists, too.

BIRGITTA WHALEY: This sharing of secret keys has been implemented over distances of kilometers, and has been proven to be possible to do if, come up probably high enough, accuracy or fidelity to be commercially viable, and people are now exploring, communicating actually with satellites in this completely quantum fashion. And, also there are institutions, like the Bank of England, which are interested in using such a quantum scheme with complete security guaranteed to verify bank transactions within, say a small area. And this particular example is all done with exchange of photons, and so it would be easy for anyone to physically just interrupt the stream of photons which would be so-called denial of service,

ROBERT L. KUHN: And if somebody interrupted it they could interrupt it but they couldn't read it.

BIRGITTA WHALEY: They couldn't read it. There is another, a second aspect of quantum mechanics which is beneficial here to security is that, if someone does try to interrupt it, if someone tried to interrupt this stream of photons that were going through and transmitting the information, supposing they were to absorb these photons and then read the information and retransmit, the person at the other end could detect, would know that he had been eavesdropped upon.

ROBERT L. KUHN: Fascinating.

Will Computers Take a Quantum Leap?

BIRGITTA WHALEY: So it's a very powerful approach to cryptography.

ROBERT L. KUHN: Are there any other implications for practical usages beyond this?

DAVID DIVINCENZO: One area which looks very promising is, is in the area of making higher precision clocks. In fact, for the very same laboratory devices that are being explored as quantum computers, for example, this instrument is both a promising quantum computer and also a promising next generation atomic clock.

ROBERT L. KUHN: How much does it improve the accuracy, atomic clocks are, like a second in what, 20 million years.

DAVID DIVINCENZO: They're fabulously accurate, I think they could become a thousand times more accurate still.

SETH LLOYD: For instance, an application of that, one that I've been involved in, as we recently were able to show that if you take light and put it, not merely laser light, but create entangled light where all the photons are in this funky entangled state. And, when I send it from you to me and you measure when it arrives, then you can tell when it arrives to a much higher degree of accuracy than you can with ordinary light. If you combine this with super accurate atomic clocks, you can imagine, for instance, having satellites orbiting the Earth where, with this quantum GPS, or quantum positioning, you can position them to an accuracy potentially of, you know, below a centimeter and then you can use these as an aperture to make a telescope the size of the whole Earth to look up at the heavens.

ROBERT L. KUHN: How would that work, that's interesting?

SETH LLOYD: Well if telescopes for instance, if I think these are the mirrors of a telescope, I can take two mirrors like the mirrors on top of the volcanoes in Hawaii, if I know how far they are apart within to the accuracy of the wavelength of light that I'm going to use, then I can use them as a single aperture, a single mirror. So, now imagine that your mirrors are separated by the distance of the Earth and are up on satellites and here the accuracy is determined, by the size of the aperture, the size of the mirror, and the wavelength of light that you're using. And you can only do this if you can position these mirrors to the size of the wavelength of light. So, you can see what's happening is that there's this kind of feedback effect where quantum technologies have allowed us to build things like quantum computers, but by thinking about quantum information, we thought of applications like this quantum clock and then we can see how we can map this into problems of say, GPS or radar, and we can use these kind of quantum effects to create new systems with a degree of precision, which was previously unimaginable. Now

Will Computers Take a Quantum Leap?

having said that, it's going to be very hard to do, it's not that easy to do this, as we were saying before, atoms are very sensitive things and it's okay, you know, you may, if you and David were terrorists with your secret and Birgitta came along and just blew on your quantum secret, right, it could easily just evaporate like that. Because, remember if something in the environment looks at your quantum information, it tends to go away, this nice wave-length feature goes away. But in some cases it's a bug, right, and in some cases it's a feature, that is, it gives you both unprecedented capacity, it can also be easily disruptive. Who would have thought that, by using Schrödinger's thought experiment about torturing cats that you could actually make clocks run more accurately in principle.

ROBERT L. KUHN: Or build a telescope the size of the Earth.

SETH LLOYD: Or build a computer that could do a computation that's harder than you could do on a classical computer that used all the molecules or all the elementary particles in the universe. Who would have thought that, and the reason that we are able to think about such things now that we've now developed a common language about quantum information that allows solid state physicists, uh, mechanical engineers, theoretical chemists and computer scientists and mathematicians to talk to each other.

ROBERT L. KUHN: Does any of your work, Birgitta in chemistry have some of these same characteristics of being able to see problems that you never would have thought of before, or people in chemistry don't think of?

BIRGITTA WHALEY: Previous chemistry used to be done by mixing things in test tubes, nowadays a lot of it is done with lasers and, and coherent light pulses and, so, there's a lot of feedback. Anything that you can do that would allow you to make a quantum operation on, say, ten coupled qubits is something that immediately someone in chemistry, will say, oh, I can use this to make this molecule into that molecule.

ROBERT L. KUHN: In that way, quantum computing literally can help us understand the quantum and molecular world.

BIRGITTA WHALEY: Yes.

ROBERT L. KUHN: How do you look at building quantum computers, let's talk about that.

DAVID DIVINCENZO: Well, I'm first optimistic because it seems like there are many possible routes to making a quantum computer, including ones that emerge directly from our current silicon technology. And it may really be that some very different kind of system will emerge as the right system to do quantum computing. There already are functioning quantum computers. The thing that we, the reason why we're not so

Will Computers Take a Quantum Leap?

optimistic about, going to larger computers yet, that is we have ten, okay, so why not 20, and why not a hundred.

ROBERT L. KUHN: These are numbers of qubits that you would need to be part of your computer.

DAVID DIVEINCENZO: Whereas we said earlier, if you could get to a thousand then you've opened up a huge space of possible problems to solve. The systems that have been looked at so far are not so scalable, that's a key word that we use in this business.

ROBERT L. KUHN: Being able to make, enlarge it on the same, in the same way.

DAVID DIVINCENZO: To add component parts in, one at a time, you know, which is the thing that has made ordinary computing so powerful,

ROBERT L. KUHN: What would it look like in the lab or if we put it on this table, does it have to be extremely cold to avoid heat contamination, is it very large, what is the containment equipment?

SETH LLOYD: We don't really know what our quantum computers are going to look like, and the reason is that, in the same way that bits are ubiquitous, right, you know, you can store a bit in any number of ways by saying yes or no, you know, thumbs up, thumbs down, capacitor charged or uncharged, or writing a zero or one on a piece of paper. It's also true that quantum bits are ubiquitous, essentially, any quantum system, any quantum, you can, in principle, map a bit onto.

DAVID DIVINCENZO: We actually know of special kinds of systems, where you can have a collection of a thousand atoms or 10,000, and if that collection of atoms is a superconductor, for example, is a special kind of material that occurs, usually at low temperatures, then it exhibits quantum effects that may permit us to make a qubit, even in a structure that looks exactly like what you would see if you looked in a microscope at an ordinary integrated circuit today. You know, you'd see metal lines which are about one micrometer wide and they would connect together in various ways and they could, possibly, embody a qubit.

SETH LLOYD: Yeah, I was actually lucky enough to participate in one of these experiments that was run by Hans Mooij at the Technical University of Delft in which they built a superconducting qubit. Hans did an experiment where they made a little superconducting loop, actually it's quite macroscopic by the standards of our world, 1/100 of a millimeter.

DAVID DIVINCENZO: But huge on the scale of current day transistors.

Will Computers Take a Quantum Leap?

SETH LLOYD: Very huge on the scale of individual atoms, in fact much closer to us in size than it is to the size of an individual atom.

ROBERT L. KUHN: And each one acted as if it were a single qubit?

SETH LLOYD: So, by managing them carefully we were able to create a state in which we called a current going around in the loop this way (counterclockwise) a zero, and a current going around another loop this way (clockwise) a one, and we were able to create this funny state of zero and one at the same time, which is to say current other than, maybe I can do this, going around it's hard to do, they can go this way and that way at the same time around this superconducting loop.

ROBERT L. KUHN: How did you know that was occurring?

SETH LLOYD: Well, we were able to measure the current when it was going around this way and going around that way.

ROBERT L. KUHN: Doesn't measuring destroy the system.

SETH LLOYD: Absolutely. So you've been studying quantum mechanics, haven't you? Yeah, so quantum computers, quantum bits, and quantum systems in general, are very sensitive systems. You know, an atom is very sensitive. And, so particular the thing that really messes up a quantum system is being looked at, as you say, and it doesn't have to be a measurement that you make, it can be just some little electron that's floating by the environment that happens to take a peek at your quantum bit and, poof, it's history, your quantum bit. If you actually want to make a measurement and get information, then we're willing to destroy the state of our quantum bit in order to see that, and we're able to exhibit the statistics that shows that we have a state where a billion of electrons are going both this way and that way at the same time.

ROBERT L. KUHN: And that's done statistically with probabilistic...

SETH LLOYD: Right, the investigation is probabilistic.

ROBERT L. KUHN: How about the input and output, if we have a quantum computer with qubits, which is so small, how do you get information embedded on them, and then how do you read that off?

SETH LLOYD: Well, it depends on the system, of course. Look, anybody can talk to an atom, right? "Hello, I'm talking to you," right and I can make a difference with this atom just by knocking it. The key is to get it to talk back to you. There are a variety of ways and one of the most straightforward is to use the example Birgitta's quantum computers, is to use the way that light interacts with matter. So, if I think of my qubit as

Will Computers Take a Quantum Leap?

a spin, and so spinning up is zero and spinning down is one, and then I bring in light that comes along and it's a wave, the light comes along and it kind of tickles the spin as it comes there and in a field called electromagnetic resonance, or in this case nuclear magnetic resonance, if the light has just the right frequency, it's kind of like the spin listens to a particular radio station, then it likes us and it will flip for you. So you can actually flip the spin from up or down just by putting light of the right frequency on your spin. And then actually, it's also the case that small as the spin may be, the reason they can absorb this light, it's like a little antenna that's tuned to 89.7.

ROBERT L. KUHN: So that's the way you're encoding information, and then to read information out of that?

SETH LLOYD: Well, an antenna can both absorb and then, just as in your cell phone, it can radiate, as well. So, if I take a single spin, and I flip it, then it can emit a photon, a particle of light.

ROBERT L. KUHN: And you can measure that?

SETH LLOYD: Well, a single photon emitted by a nuclear spin is very hard to measure, nobody's actually ever done that except in certain optical contexts. But, in fact, if you get a bunch of them together then they can make a signal that's strong enough for you to see.

ROBERT L. KUHN: So we have the problem itself, whether it's a chemical issue or a factoring of a number in electronic commerce, then that description of the process has to be encoded within this quantum mechanical system, which we now have to build, and if that process works, then the quantum computer can be used to analyze that problem.

SETH LLOYD: Yeah, that's right.

ROBERT L. KUHN: Sounds simple.

SETH LLOYD: Simple quantum computers have been built, the first quantum logic gates, optical quantum logic gates were built back in the mid-1990s, and that was followed by Dave Corey, Jonathan Jones, Ike Chuang and others building nuclear magnetic resonance quantum computers, the kind of work that Birgitta has brought to a high pitch.

ROBERT L. KUHN: So, where will all this go in a hundred years?

DAVID DIVINCENZO: I would like to stick my neck out on that. I personally feel that within another hundred years anyway, quantum computing will be ho-hum, actually, that we will have many quantum computers and they will be in many applications at that

Will Computers Take a Quantum Leap?

stage. And that probably I would speculate that the world of cryptography and privacy will have been revolutionized as a consequence. I also think that there will still be applications, perhaps like synchronizing the satellites circling the solar system that will still be just a dream, that we will not have figured out how to do those things, but we will understand that they're possible, that quantum computers will be real, but they will not be complete, well technology is never finished.

BIRGITTA WHALEY: Do you think they'll be on your desk and in your home?

DAVID DIVINCENZO: Yes.

BIRGITTA WHALEY: In your home, but in everyone's home?

DAVID DIVINCENZO: Yes, there will be a card that is carrying quantum bits, in and out of your house on a cable that permits you to do secret things, to do things securely on whatever the internet is at that time. There's my speculation. It's safe because it's a hundred years from now.

BIRGITTA WHALEY: None of us will be around.

DAVID DIVINCENZO: My, my grandchildren will have to answer for me.

BIRGITTA WHALEY: I would venture to agree with David that there will be quantum computers. I think it's very difficult to say just what they will be doing. And I tend to agree that, in cryptography, they will probably change things a great deal and they will probably be used for communication long before a hundred years. But whether they'll be, replace the general purpose PC in your home, I'm not sure.

DAVID DIVINCENZO: Now that I don't think.

BIRGITTA WHALEY: That will depend upon what advances there are, actually in computer science over the next, say, 10 or 20 years.

SETH LLOYD: Yeah, in fact, I think that it's not necessarily desirable to have your personal computer to be a quantum computer. I mean, remember, a quantum computer is to a regular computer what a laser is to a light bulb. But we haven't taken all our light bulbs and replaced them by lasers.

DAVID DIVINCENZO: I don't see any lasers here.

SETH LLOYD: Right, that's right. Lasers are ubiquitous now, whereas 40 years ago, when they were first invented, they were very, very rare and used for only very special purposes. I think that we're very likely to have, as David says, quantum computers that

Will Computers Take a Quantum Leap?

are performing special purpose things and tasks like, well, I hope not breaking internet security codes on a regular basis, if such things exist then we will have quantum communication systems like the nice quantum internet we're trying to build, with Jeff Shapiro at MIT, to send quantum bits from place to place, and then to use that to share entanglement in secure ways to solve problems which we couldn't otherwise do. But, I think, it's also the other thing to remember about this metaphor, which is actually, surprisingly accurate, if you look at the mathematics of the laser to light bulb, is that lasers, when they first put out and, still many lasers are much less powerful in terms of the actual wattage than, you know, light bulbs are. You don't have a, not many hundred watt lasers sitting around that way. So if you were to measure quantum computers in terms of their absolute power versus classical computers is to make the improper comparison. The real question is what can they do for you and there I think that we're only just starting to discover what we might be able to do, even with the relatively simple and relatively uncomplicated quantum computers we've constructed so far.

ROBERT L. KUHN: How does each of your work contribute to the others, how do you guys communicate?

SETH LLOYD: By e-mail.

ROBERT L. KUHN: Just like everyone else.

DAVID DIVINCENZO: Web sites, I guess, pretty much the same thing.

BIRGITTA WHALEY: At meetings, at meetings, the meetings are so wonderful because they're so interdisciplinary.

ROBERT L. KUHN: What do you guys learn from each other?

DAVID DIVINCENZO: Well that's going to take awhile.