Bingecast: Enrique Blair on Quantum Computing (https://mindmatters.ai/podcast/ep110)

Austin Egbert:

Greetings. I'm Austin Egbert, director of Mind Matters News. You're listening to another bingecast, where multiple episodes are combined into a single program. This week, we talk with Dr. Enrique Blair about the weird world of quantum mechanics, what quantum computers can do that classical computers can't, and Google's claims of achieving quantum supremacy. Enjoy.

Announcer:

Welcome to Mind Matters News, where artificial and natural intelligence meet head on. Here's your host, Robert J. Marks.

Robert J. Marks:

Greetings. Quantum mechanics is the secret sauce of quantum computing. Google has announced the development of a quantum computer that has achieved quantum supremacy. What is quantum mechanics? What is quantum computing? What is quantum supremacy? We'll unpack these questions today with our guest, Dr. Enrique Blair. Dr. Blair is on the faculty of Electrical and Computer Engineering at Baylor University. He is a United States Navy veteran. He actually was canned up on a little submarine. No, it was a big submarine, wasn't it?

Enrique Blair:

Yeah, that's right, pretty big.

Robert J. Marks:

Big submarine. And has actually taught before Baylor at the Naval Academy at Annapolis. But Professor Blair teaches graduate courses in quantum mechanics and quantum computing, and he's the perfect person to talk to about quantum mechanics and quantum computing.

Robert J. Marks:

Dr. Blair, how is it to be locked up in a cylindrical tube and submerged in the ocean? I think that would get on my nerves. Did that get on your nerves, or do you get used to it?

Enrique Blair:

Oh, it's quite a different experience. The longest time I was underwater and on the submarine was about five weeks. It means that if we're on mission, we can't communicate with the outside world, so you miss things like popular songs or movies that come out. It's just, like I said, it's a different experience. I guess at the end, the levels of oxygen can get a little bit lower than what you're used to, so then when you come back up and you open those hatches and you get oxygen, people start to get oxygen happy.

Robert J. Marks:

Oxygen happy?

Enrique Blair:

Yeah. Yeah. It's really quite a thing.

Robert J. Marks:

What are the symptoms of oxygen happy? I need some of that, I think.

Enrique Blair:

Yeah. It's, maybe we're a little giddier or something. It's just fun.

Robert J. Marks:

Wow, so everybody's happy when you surface.

Enrique Blair:

Yeah.

Robert J. Marks:

I thought it would be like everybody's just happy to be on the surface.

Enrique Blair:

There's probably some of that too, yeah.

Robert J. Marks:

Okay. Let's talk about some of the things about quantum mechanics. I got a quote here. The great quantum mechanics pioneer, Niels Bohr, he was clever guy. He had a lot of great sayings. He said, "If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet." Quantum mechanics is weird. I think I understand rudimentary quantum mechanics, but even what I know is very weird. Let's talk about what is quantum mechanics. Could you tell me what quantum mechanics is from your perspective?

Enrique Blair:

Sure. Like Niels Bohr said, it's really hard to intuit this thing. It's really quite different from our daily experience. Quantum mechanics really is a description of the world at the microscopic scale. And it's really weird, because there are things that initially we thought maybe these were particles, but then we learned that they have wave-like behaviors. And there are other things that we thought were waves and then we discovered they have particle-like behaviors.

Robert J. Marks:

Was there a big debate at the time that light was a particle... no, it's a wave, it's a particle... no, it's a wave?

Enrique Blair:

I imagine there were a lot of debates on how to interpret things. I know that one of the things that comes up with quantum mechanics is that there's a probabilistic interpretation to quantum mechanics. Einstein, his work led to our present understanding of quantum mechanics. He explained the photoelectric effect. To do this, he had to assume that light came in particles, not just waves because our understanding of light as waves came first. Einstein, like I said, he didn't like some of the probabilistic interpretation of quantum mechanics, and so that's where his famous quote about God not playing dice came from.

Robert J. Marks:

In fact, Einstein won the Nobel Prize for that. He never won the Nobel Prize for relativity or his work on Brownian motion or the other great things that he did. It was for his work on the photoelectric effect. But he assumed, didn't he, that the energy of the particles coming out were quantized?

Enrique Blair:

Yes, that's right. That's right. That was his big contribution, the fact that okay, light can only be absorbed in these packets called photons.

Robert J. Marks:

So he started this out, but then he didn't like when they got probabilistic. What was the next step?

Enrique Blair:

The next step. Well, I suppose it was Max Born's interpretation. Honestly, I don't know any of the experiments that really confirmed the probabilistic interpretation, but I know that that is the generally accepted interpretation. It's the Copenhagen interpretation of quantum mechanics.

Robert J. Marks:

What's the Copenhagen interpretation?

Enrique Blair:

It's that the quantum mechanical wave function describes measurement outcomes in probabilities. You can't predict with certainty the outcome of a measurement. Which is really shocking, because in the classical world, if you have a particle and you know its position and its velocity, you can predict where it's going to be in the next second or minute or hour. Now in quantum mechanics, the really weird thing is, we say that a particle doesn't even have a position until you measure its position.

Robert J. Marks:

It doesn't exist?

Enrique Blair:

Not that it doesn't exist, but its position is not defined.

Robert J. Marks:

I was talking to our director, Austin Egbert, before you came in about an old movie called Mystery Men. It's a story about a bunch of superheroes that weren't quite up to snuff. They weren't the Captain Americas and Thors and Hulks of the day. There was the Shoveler, he was really good hitting people with shovels. But there one guy who they asked him what his superpower was. He says, "I'm invisible as long as nobody's looking at me." That kind of reminded me of quantum mechanics in a way. It was like he was quantum boy or something. He didn't have a position until somebody looked at him. I thought that was an interesting parallel.

Robert J. Marks:

The other thing that I really like is, there was a physicist named John Polkinghorne, and he was a colleague of I believe, Stephen Hawking. Polkinghorne got tired of physics. He went away, he became an anglican minister. He came back and he used physics to explain a lot of the paradoxes that he saw in places like Christianity. One of them is that there seems to be contradictions. And contradictions he said, are like light being a particle in a wave. He said, "We used to think they were particles in waves, but then we resolved that paradox at a higher level." He maintains a lot of the paradoxes we talk about such as free will versus predestination and things. Or actually, something that seems a conflict today that are actually resolved at higher levels. Polkinghorne's a really, really sharp guy.

Robert J. Marks:

Let's talk about the history of quantum mechanics. The big one that I know about, the big breakthrough was Young's double slit experiment, which again gets us into weirdness. What was Young's double slit experiment?

Enrique Blair:

Sure. Young's double slit experiment goes all the way back to 1805, where Young shot light... he had a light beam, I guess... he shot it at a couple of slits and then the light passing through the slits would show up on a screen behind that. What we got from that was, the light that goes through the slits would create an interference pattern. So you'd have peaks and valleys in the intensity of the light that showed up on the screen.

Robert J. Marks:

It was like constructive and destructive interference, when you see in waves.

Enrique Blair:

That's right. That's the only way to describe that. The conclusion there is that light is a wave... 1805.

Robert J. Marks:

And then we had... was it Planck that did the black-body radiation?

Enrique Blair:

Yes, that's right. Planck did the black-body radiation. His explanation of black-body radiation assumed that light that came from these black bodies could only be emitted in discreet chunks.

Robert J. Marks:

And then you mentioned about Albert Einstein and his Nobel Prize winning effort in the photoelectric effect.

Enrique Blair:

Right, yeah. My understanding, that is right. Planck, his work uncovered the fact that light can only be emitted in these discreet packets. Einstein theorized that light can only be absorbed in these discreet packets. That's kind of where this quantization came from.

Robert J. Marks:

Okay. I'm looking at the notes you provided, wave particle duality. That's where the light is both a wave and a particle. But what happened then next? It really gets weird here. Thus far, I think we've talked that light is quantized, that light can interfere like a wave. But then it gets really strange with this wave particle duality.

Enrique Blair:

Right. Right. Yeah. The next step here which is a lot of fun is... okay, let's consider. We take our beam of light and we're going to reduce it now because we know there are photons involved here. We can reduce a beam of light so that it's single photon. One photon is emitted at a time, and we're shooting it at our double slit again. Let's say we put up a screen, maybe it's a photosensitive plate or something.

Enrique Blair:

What happens when each particle of light goes through these slits? Well, each particle splats up against this screen, and so you can know where the photon hits. But if you do this over a long period of time, the interference pattern shows up again. You have particles hitting the screen, so we see the particle behavior. But we also see the interference pattern which suggests that okay, we've got some wave interference going on here.

Enrique Blair:

So the only way to explain both of these at the same time is that each photon which is an indivisible packet of light has to go through both slits at the same time and interfere with itself, and then the buildup of many, many photons gives you that interference pattern.

Robert J. Marks:

A particle was hypothesized to go through both slits?

Enrique Blair:

Yes, and that's the mind-blowing ramification of this thing.

Robert J. Marks:

How do we decide which slit the particles go through? Suppose we went down and we tried to measure? We put out one photon and we put it through the double slit. We've tried to measure which slit it went through. If it's a particle, it can only go through one, right?

Enrique Blair:

Right. That introduces this concept of measurement. Like you said, which slit does it go through? Now the interesting thing is, if we know which slit it goes through... maybe we set up a detector and we say, "Hey, did it go through slit one or slit two?"... we detect that, we measure it, and the interference pattern goes away because now it's gone through one slit only, not both.

Robert J. Marks:

Just by the act of observation, we are restricting that photon to go through one slit or the other. The observation really kind of screws things up.

Enrique Blair:

That's right. This is one of the things that is hard to understand about quantum mechanics, because in the classical world that we deal with every day, we can just observe something and we don't have to interact with it. So we can measure something's position or its velocity without altering it. But in quantum mechanics, observation or measurement inherently includes interacting with that thing, that particle. Again, you've got this photon that goes through both slits, but then you measure it and it actually ends up going through one once you measure it.

Robert J. Marks:

This reminds me again of Invisible Boy on The Mystery Men. The photon goes through one of the two slits while you're looking at it. Unless you look away, then it goes through both slits.

Enrique Blair:

Right. Very tricky, those photons.

Robert J. Marks:

Yeah, it really is. This gives rise to, let's see, superposition. What's superposition? What's going on there?

Enrique Blair:

Sure. There's this concept of quantum superposition, which is really a mathematical description of this. We use wave functions to describe these particles. There's a wave function for the photon going through one slit, and a wave function for the photon to go through slit two. To describe it going through both slits, we have a linear combination of those two wave functions, and so you have a more general wave function. That's the heart of quantum computing because in classical computing, we have bits like zero or one. And in quantum computing, we like to use these superpositions of zero and one. It's not one or the other, it's something of both.

Robert J. Marks:

It's kind of like Invisible Boy. When you don't look, zero and one are both there.

Enrique Blair:

That's right.

Robert J. Marks:

Now there was a big math breakthrough. I think there were two people. One of them was Schrödinger. Who was the other one, do you remember? The ones that actually presented the theory of quantum mechanics that won the Nobel Prize.

Enrique Blair:

Oh, I am not remembering this.

Robert J. Marks:

Okay. One of them was Schrödinger. But anyway, he came up with an equation that described this. What was the mathematics behind the description of all of this weird property of quantum mechanics?

Enrique Blair:

Well really, the weirdness of quantum mechanics comes in two parts. One is Schrödinger's equation, and this describes the time evolution of a system when you don't look at it and when you don't observe it. And then, there's the mathematics of measurement. That's the one where all the probabilities come out. Oddly enough, there is no mathematical definition that rigorously describes measurement. It's one we haven't quite figured out yet.

Robert J. Marks:

I remember the other guy that did it was Heisenberg.

Enrique Blair:

Okay, yes.

Robert J. Marks:

Made famous in the Breaking Bad, because that's what the head character who developed methamphetamines called himself, Heisenberg.

Enrique Blair:

Okay.

Robert J. Marks:

That was his code name. If I remember right, both Schrödinger and Heisenberg came up with a theory. Heisenberg uses matrices and Schrödinger used partial differential equations. I think they showed they were the same at some point. But both of them gave rise to something called wave functions. That's the solution to the Schrödinger's equation. Depending on what your boundary conditions are-

Enrique Blair:

Yes.

Robert J. Marks:

... and your environment and your initial conditions and things of that sort. Tell us what a wave function is.

Enrique Blair:

A wave function is an interesting thing. It's a function that describes the state of a quantum system, and it contains everything we can know about that quantum system. But we manipulate these things, or we extract meaning from them using quantum mechanical operators. These operators describe things like time evolution or the total energy of the system, or some observable quantity like position or momentum. And the wave function, like you said, it's the solution to the Schrödinger equation. It's a wave, and so that's where all these wave-like properties come from.

Robert J. Marks:

Those nerds that know what a probability density function is, it's kind of a probability density function about a property such as the position or the momentum or the speed of the particle.

Enrique Blair:

That's right. The wave function itself is not the probability density. You have to take the magnitude squared.

Robert J. Marks:

Magnitude squared, yeah.

Enrique Blair:

And then you get probabilities.

Robert J. Marks:

Okay. You have down here in your notes, this helps us discuss the notion of measurement. How does this help us?

Enrique Blair:

Okay. The wave function, like you said, when you take its magnitude squared, you get the probabilities of various outcomes for measurement when you also use an operator. But really, the stunning thing is that's all you get, is you get probabilities for outcomes you can't predict with certainty which outcome is going to result when you make a measurement. That's the subject of one of the papers we wrote recently, is just using quantum mechanics to make something that's a truly random number generator. You know well that computers can't generate random numbers because they're deterministic.

Robert J. Marks:

Which is really surprising because you see random numbers used a lot like in gaming machines, like in casinos.

Enrique Blair:

Right.

Robert J. Marks:

And they're not random numbers, they're pseudo random numbers. They actually use an algorithm.

Enrique Blair:

That's right. Nowadays of course though, I don't know how prevalent this is, but people can get a piece of hardware that has a truly quantum random number generator in it, and maybe those are used more in lotteries nowadays. I just don't know.

Robert J. Marks:

Yeah. I mentioned to you one of the greatest seminars I have been to was your colleague at Notre Dame who came here and gave a talk. What was his name?

Enrique Blair:

Craig Lent.

Robert J. Marks:

Craig Lent. He talked about randomness and the ability of quantum mechanics to generate true randomness. In fact, this is the only pure source of randomness there is. He had a random number generator, it's this little unit. He said you can buy them on amazon.com. You can go to amazon.com and buy yourself a real random number generator based on quantum mechanics that really spits out 100% random numbers. That's amazing.

Enrique Blair:

Yeah, that's a lot of fun. I actually have one of those and another type in my office too.

Robert J. Marks:

In the quantum world, when you measure something, you kind of mess around with the wave equation when you measure it. And then it collapses in accordance to its probability. Is that kind of the way it is?

Enrique Blair:

Yeah, that's true. Like I said, the Schrödinger equation describes the time evolution of the system if you don't measure it or don't look at it or don't interact with it. But then once you measure it, you get one of these probabilities and you radically change the wave function from being this thing... and it's in the state that corresponds to the result that you got. Previous to that, it's a quantum superposition of many different states.

Robert J. Marks:

And you don't know what it is. Now you mentioned the Copenhagen theory of quantum mechanics. There's also something I believe called the Many-Worlds Interpretation which I find really, really weird. It's a different interpretation of what happens in quantum mechanics. I think... correct me if I'm wrong, but it basically says anytime a quantum state collapses, that the universes separate. And you have one quantum universe going in one way where it collapsed one way, and another universe going another way which collapsed in another way. It means there's a lot of parallel universes, or is that true? Did I get that about right?

Enrique Blair:

Yeah, I think you got that about right. That would mean that you've got these branches that are taking place all the time, and millions of different universes evolving at the same time and branching off into new universes. Popular culture has really latched onto this and you see these things come out in all sorts of comic books and movies.

Robert J. Marks:

About parallel universes?

Enrique Blair:

Yes.

Robert J. Marks:

Okay, from the quantum splitting.

Enrique Blair:

Yeah.

Robert J. Marks:

I think that's really inane.

Enrique Blair:

I have a hard time with it because just from a scientific standpoint, you can't observe this. It really is just beyond the realm of science. Science is all about observation, so you can't really discuss these sorts of things.

Robert J. Marks:

On Schrödinger's equation, a manipulation of this mathematics, you mentioned an idea of an operator. How would you describe an operator to a person on the street?

Enrique Blair:

Oh, that's a hard question. An operator really is something that transforms a quantum mechanical state, so it transforms a wave function. But some operators are constrained mathematically in a certain way that they describe a measurement process, and they give you... if you use them, that they can give you the probabilities of certain outcomes. But, yeah.

Robert J. Marks:

Okay. We hear a lot in popular culture about Schrödinger's cat. Now Schrödinger was one of the guys who formulated quantum mechanics. He won a Nobel Prize for it. He was trying to explain quantum mechanics to a layperson, and he used this idea of Schrödinger's cat to do that. What's the Schrödinger's cat story?

Enrique Blair:

Oh, that is a fun story. To help out with this, I am going to quote from a translation of Schrödinger's paper. It was originally in German. I don't do German. Here's the translation. It says, "A cat is placed in a steel chamber together with the following hellish contraption. In a Geiger counter, there is a tiny amount of radioactive substance so that within an hour, one of the atoms decays. But equally probably, none of them decays.

Enrique Blair:

So we've got a 50/50 chance of getting an atomic decay. If one decays, then the counter triggers. And via a relay, activates a little hammer which breaks a container of cyanide. If one has left this entire system for an hour, then one would say the cat is living if no atom has decayed. The first decay would have poisoned it. The wave function of the entire system would express this by containing equal parts of the living and dead cat."

Enrique Blair:

The idea here is, okay, we've got these atoms and they're in a quantum superposition of decayed and not decayed, which means that if we don't look at it, maybe the detector is in a state of detected or not detected, and then the vile of cyanide is in a state of broken and not broken, and then the cat-

Robert J. Marks:

At the same time?

Enrique Blair:

Right. And then the cat is in a state of dead and alive.

Robert J. Marks:

And that's superposition?

Enrique Blair:

That is superposition taken to a very extreme which we know that's not really possible now, is it?

Robert J. Marks:

Well, I don't know. Quantum mechanics is so weird, maybe it is. But it means the cat is half dead and half not dead, right?

Enrique Blair:

Right. Maybe I shouldn't say that it's not possible, but we don't really observe something like this in real life.

Robert J. Marks:

Yeah. Before I go home and look at my dog, I don't know if that dog is alive or not alive. I don't know.

Enrique Blair:

This really relates to your previous point there about the many universes, and this is kind of one of those things where that comes out.

Robert J. Marks:

So my poor dead dog is alive maybe in some other universe if he got killed by a car or something.

Enrique Blair:

Yeah.

Robert J. Marks:

Yeah, and that begs the question, why do we never see such superpositions?

Enrique Blair:

Yeah, right. That's a really good question. There are a lot of theories behind why this is. It really gets down to the question of, what is measurement. Right? Because we would like to believe that the cat really is dead or it's really alive. But by the Schrödinger's cat paradox, if you haven't looked at it, then it's both dead and alive. What is going on here? What is measurement and how does it determine this state, is the cat dead, is it alive?

Enrique Blair:

Interestingly, there are a lot of theories behind what determines this. Some people have said, "Well, measurement is what happens when a quantum system interacts with a human consciousness." I don't know about that one because what if a dog looks at it? Is the cat still in a superposition? I don't know. It sort of reminds me of that thing, if a tree falls in the woods and no one's there, does it happen?

Enrique Blair:

Other theories say that measurement happens when a microscopic system interacts with any macroscopic system. But then you have to wonder, well, where do you draw the boundary between microscopic and macroscopic? I guess maybe in my mind, one of the leading theories is called quantum decoherence. I mean, that is the resolution here is that the quantum system interacts with the environment, and these quantum behaviors die away so you lose the ability to be in a quantum superposition. It's at a timescale so fast, you don't even have time to set up your experiment.

Enrique Blair:

It's also the case that the cat and the Geiger counter, these things are macroscopic objects. They don't really behave like this. They don't partake in quantum superpositions. Why is that? It's because they are many, many quantum subsystems and they lose their coherence or their ability to partake in these quantum properties so fast because they're so complex. We just can never see these sorts of superpositions of a live cat and a dead cat because it really has a macroscopic behavior to it, and so you just can't see it.

Robert J. Marks:

That is really, really strange stuff. In a way, just by this uncertainty existing in some environment, it reacts with the environment in some way to begin to lose its coherence in some fashion.

Enrique Blair:

That's right.

Robert J. Marks:

It isn't the observance, it's actually the interaction with the surroundings. Is that a fair thing to say?

Enrique Blair:

I think that's the way I like to think about it.

Robert J. Marks:

We've been talking about quantum mechanics, exactly what it is. We've talked a little bit about the history of quantum mechanics. And we got a little bit into the idea that Albert Einstein didn't like quantum mechanics or certain aspects of quantum mechanics. Was this argument ever brought to resolution to Einstein, or did he die thinking that quantum mechanics was a fluke? What's the history there of this interaction?

Enrique Blair:

Right. That's an interesting question because as we discussed in previous podcasts, Einstein's work really led to the... His work was integral to the formulation of quantum mechanics, but he was uncomfortable with a couple parts of it. The first part, you mentioned his quote about God not playing dice. He did not like the probabilistic interpretation of quantum mechanics so much. He wanted something that was much more deterministic. That was the first thing there.

Enrique Blair:

The second thing he was just not comfortable with was a concept called nonlocality in quantum mechanics. This idea brings up something called entanglement. You can entangle quantum systems, and you need multiple quantum systems for this, but entanglement means that each subsystem no longer has its own local quantum state. That means that we can't understand its quantum state completely in a local sense.

Enrique Blair:

Quantum state has to be understood in terms of the other systems with which it's entangled. Now this has some really interesting ramifications. Like if you entangle a couple of systems like cubits, quantum bits that are zero or one or some superposition of the other. If you entangle cubits and then you separate them at a vast distance, you can conduct operations on one cubit that affect the state of the other cubit that's very, very far away. Einstein did not like this at all. He called that spooky action at a distance.

Robert J. Marks:

Yeah. And the weird thing is I recall is that the collapse of this entanglement on one end immediately caused the collapse on the other end faster than the speed of light.

Enrique Blair:

That's right. You can have a vast separation between these two particles and the instant that someone takes a measurement on one particle, let's say she's Alice and she measures her cubit and Bob has the other entangled cubit... by the way, Alice and Bob, I like to say these are the most famous people in quantum computing.

Robert J. Marks:

Yeah. I think they are in philosophy too and psychology, because everybody uses Alice and Bob. I think that's because of A and B, right?

Enrique Blair:

Yeah.

Robert J. Marks:

I betcha.

Enrique Blair:

Yeah.

Robert J. Marks:

Okay.

Enrique Blair:

Well anyway, Alice measures her cubit. It immediately affects the state of Bob's cubit. And it doesn't matter how far these things are separated. People start to think, "Gosh, does that mean we can communicate superluminally?"

Robert J. Marks:

Okay, that's a big word. Super-

Enrique Blair:

Faster than the speed of light.

Robert J. Marks:

Okay. Okay. Got you. Is this used in quantum communication? Which we're going to talk about in a little bit. But is this something that's used in quantum communication?

Enrique Blair:

Yes. In quantum communication, you have to have entangled pairs of cubits. I'll just put out a spoiler. Sadly, no, it doesn't allow superluminal communication. We wish it did, but it doesn't.

Robert J. Marks:

Yeah, I know. I think the DOD especially spent a lot of money trying to show that you had faster than light communication. It didn't work for reasons I still don't totally understand. We know that quantum mechanics is used in quantum computers, but actually I think quantum mechanics is part of our daily life. It's all around us. What are some of the places that quantum mechanics is used?

Enrique Blair:

Oh well, in terms of human users, we use it all the time. You might even say everybody's an expert at it, even children. We're talking electronic devices... smart watches, cell phones, laptops and super computers. All of these have multitudes of transistors used for classical information processing, yet each transistor in itself is a quantum device. It uses quantum mechanics to operate. Quantum mechanics is in the operating principles of these devices, but we have to point out that we're still processing bits in a classical way. That is, we're using ones and zeros. We're not using quantum bits, these superpositions of ones and zeros.

Robert J. Marks:

I know that you're doing research in quantum mechanics now. I think probably the evidence that quantum mechanics is used everywhere is you're in the department of electrical and computer engineering, not of science.

Enrique Blair:

That's right.

Robert J. Marks:

So engineers are people that take science and reduce it to practice. Some of things that you mentioned are examples of reduction of things to practice which use quantum computing. What are some of the things that you're looking at with the application of quantum mechanics?

Enrique Blair:

I'm really working on two different areas. My first area is molecular computing. Quantum mechanics governs the operation of these molecular computing devices, but we want to process classical information. We want to do things like conventional computing. Like I said, it's in everything from cell phones to supercomputers and we want to do this in a way that is energy efficient. And oh by the way, we believe these molecules could operate at speeds thousands of times faster than the transistors we're using today.

Enrique Blair:

We like to think that if we can develop this technology, that would be really helpful for humanity in terms of reducing power consumption. Because really, the cost of computing in terms of global power production, it's pretty big. I mean, I know that in 2010, it was estimated to be about 10% of global power.

Robert J. Marks:

Say that again. 10% of global power is used for computers.

Enrique Blair:

Right.

Robert J. Marks:

Wow.

Enrique Blair:

And now you think about it. We've had this boom of cryptocurrencies, and our world is much more connected now and people want the Internet of Things. So we really need to find ways to reduce power consumption in our devices.

Robert J. Marks:

I was even told that for mining of Bitcoins, you got to crunch a lot of numbers.

Enrique Blair:

Oh, yes.

Robert J. Marks:

You generate a lot of heat.

Enrique Blair:

That's right.

Robert J. Marks:

There's actually been people that have moved to cold climates, like in Greenland.

Enrique Blair:

Right.

Robert J. Marks:

Maybe the Arctic, I'm not sure... in order to set up these bitcoin miners that use all this energy and generate a lot of heat. They do it there because they can absorb the heat because of the coldness of the environment. Okay.

Enrique Blair:

Yeah.

Robert J. Marks:

What are quantum dots? I know you did some work on quantum dots also.

Enrique Blair:

Right. A simple way to think about a quantum dot is maybe as a particle trap or a trap for a quantum particle. You're confining an electron in three dimensions to a point, essentially. There are many ways to make quantum dots. You can make them in semiconductors. Or, people have taken crystal and then manipulated some of the atoms to make atomic scale quantum dots. Like I said, I've been interested in molecular computing. There's a way you can take mixed-valence molecules. And then they have these redux centers, reduction oxidation centers, that function as quantum dots. They trap a mobile charge. We want to use those for classical or maybe even quantum information processing.

Robert J. Marks:

Okay. I don't understand everything that you're doing with the quantum mechanics, but is it fair to say that as Moore's Law continues and computers begin to get speedier and speedier and speedier, we're going to have to do things at a smaller and smaller and smaller scale.

Enrique Blair:

That's right.

Robert J. Marks:

Eventually, we're going to have to get down to quantum effects.

Enrique Blair:

That's right.

Robert J. Marks:

I think that that's the area that you're working in right now in order to recognize that those quantum effects are going to occur, and then make sure that we use them as efficiently as we can.

Enrique Blair:

That's right, yeah. It's well known that we're running out of room on the road map for scaling down our semiconductors. That's why I'm interested in new devices that depart from the transistor paradigm.

Robert J. Marks:

Ray Kurzweil, in some of his books, talks about exponential increasing. Any time you have a doubling of speed like in Moore's Law, that's an example of exponential increase. But exponential increases are never, ever sustainable. You got to get to a point where it doesn't work anymore. If you take the current exponential explosions say in the size of computers, you're going to get eventually down to things like Planck lengths, and it isn't going to work there.

Enrique Blair:

Right.

Robert J. Marks:

They're not going to be able to get smaller. Many times, this exponential explosion is actually the knee of kind of an S-shape curve where the exponential explosion comes up and eventually levels out. It's got to do that someday. I have no idea how far we are from that leveling out. I actually read an article the other day that the speed of artificial intelligence has been outpacing Moore's Law. This is not only to the increase and the speed of the computer, but the cleverness of the algorithms. So people have been doing better and better and better things.

Robert J. Marks:

Let's get to quantum computing. This is the thing that's in the news everywhere. There was the announcement that Google has built a quantum computer that has achieved quantum supremacy. What is quantum computing, for a layperson?

Enrique Blair:

Yeah, that's a good question. Quantum computing really uses quantum systems to process information in a way that our classical computers can't. Classical computers use bits, which that stands for binary digits. A binary digit can either be zero or one, and that's it, zero or one. Now quantum computing uses quantum bits. So you don't just have zero or one, you have these quantum superpositions of zero and one.

Enrique Blair:

It turns out with quantum superposition and another thing called entanglement, it turns out that you can process information in ways that you can't classically. The great hope and the great promise there is that there are going to be some applications that quantum computers can do. They can process certain things and do certain calculations efficiently that you can't do on a classical computer. There are some well known examples of this. The best known is Shor's algorithm.

Robert J. Marks:

Shor's, that's S-H-O-R-E?

Enrique Blair:

No E.

Robert J. Marks:

Oh, just S-H-O-R?

Enrique Blair:

Right.

Robert J. Marks:

Okay, Shor's algorithm. What does Shor's algorithm do?

Enrique Blair:

That is all about defeating a very widely used form of encryption. This requires factoring very large numbers into two prime numbers.

Robert J. Marks:

Oh, okay. That's the way that a lot of encryption is done today, right, with PGP encryption? It keeps your communications secret?

Enrique Blair:

That's right.

Robert J. Marks:

With Shor's algorithm, if we got that, we could throw away all those encryptions?

Enrique Blair:

That's right, yeah.

Robert J. Marks:

Wow.

Enrique Blair:

Yeah. The one that it's designed to attack is RSA.

Robert J. Marks:

What's RSA?

Enrique Blair:

Rivest, something, and Adleman. I forget who the S stands for.

Robert J. Marks:

Okay.

Enrique Blair:

Shamir, I think.

Robert J. Marks:

This is a type of encryption?

Enrique Blair:

That's right.

Robert J. Marks:

Okay. Now if I remember, Shor's algorithm is pretty old. It's been around for quite a while.

Enrique Blair:

Yeah. I think it was '98-ish. So 21 years, something like that.

Robert J. Marks:

Okay. That's one of the things that a quantum computer can do. I'd like to think of a cubit. Again, getting back to Invisible Boy on Mystery Men. That was the one that was actually invisible unless somebody looked at him. You have all of these cubits there that can be either zero or one and they're all kind of interconnected together, and it's okay as long as nobody looks at them. As soon as somebody looks at them, everything kind of collapses, just like Invisible Boy.

Enrique Blair:

Right.

Robert J. Marks:

That is just strange. They had Invisible Boy on Mystery Men because it was so comical. It was so stupid. It's application to quantum mechanics seems to be right on. Okay, so we have all of these things. We have Shor's algorithm, which is going to make all decryption obsolete.

Enrique Blair:

Yeah.

Robert J. Marks:

Common encryption.

Enrique Blair:

Yeah, that's why governments are so interested in pouring hundreds of millions of dollars into this sort of research.

Robert J. Marks:

Well, yeah. In fact, both countries and companies are just battling in order to get quantum computers. My understanding is that these different companies are using different quantum mechanisms. Not everybody is using the same approach because quantum exists everywhere, no matter what material you look at.

Enrique Blair:

Yeah.

Robert J. Marks:

They're all looking at different sort of quantum materials. Okay, Shor's algorithm. Now the good news is, which I hope we can talk about in a little bit, not now, is that once we get this Shor's algorithm running and we get all the commonly used decryption made obsolete, we can actually use quantum mechanics to do quantum encryption and actually have something which Shor's algorithm can't crack. That's the good news in the future, is that right?

Enrique Blair:

That's right. While quantum computing could take away our RSA encryption scheme, quantum communication could give us something that's provably secure.

Robert J. Marks:

Okay. Well, that's good. What else besides Shor's algorithm can a quantum computer do?

Enrique Blair:

Yeah. Well, there's also a thing called Grover's search algorithm.

Robert J. Marks:

Now, this is not the Grover on Sesame Street?

Enrique Blair:

No, not that little blue guy. I don't think so.

Robert J. Marks:

Okay. This is another guy. I wonder if that guy gets teased a lot because his name is Grover.

Enrique Blair:

Oh probably, yeah.

Robert J. Marks:

Okay. What was his algorithm?

Enrique Blair:

This algorithm is for finding one unique number that maybe it's the solution to a problem. This one number is found among millions perhaps of nonsolutions, basically. So it's a search.

Robert J. Marks:

It's kind of optimization, isn't it, in a way?

Enrique Blair:

It's not necessarily an optimization. There are other quantum computing paradigms that are more closely related to an optimization, but I wouldn't characterize Grover's search as a optimization problem. Really what behind this, it's an interference problem. It's making an interference pattern where all of the probabilities go to zero except one, and then you get that one.

Robert J. Marks:

And that's the one that's right.

Enrique Blair:

Yeah.

Robert J. Marks:

You would characterize it as a search algorithm?

Enrique Blair:

Yes.

Robert J. Marks:

Looking for a specific number that's determined a priori some way?

Enrique Blair:

Right.

Robert J. Marks:

Okay. It's kind of weird. You have these quantum computers. You have all these cubits that are okay, they're floating between zero and one. You don't know which one it is until you look at it. You have to set it up some way it seems to me so that when you do look at it, the dominoes fall down and you get the right result.

Enrique Blair:

Yes.

Robert J. Marks:

Is that a fair characterization?

Enrique Blair:

Yeah, I think that's a fair characterization.

Robert J. Marks:

Do you know if it takes a long time to set up the dominoes to knock down in a quantum computer?

Enrique Blair:

Well, I don't have a lot of experience with setting these things up, but it's not too terribly long. I mean, not like hours necessarily. I don't think so. I think it can be done in maybe the timescale of seconds.

Robert J. Marks:

One of the things is the use of quantum computers. If they ever get them to the point where they're easily usable, will they ever be in our laptops? Will our laptops and our computers ever operate totally on a quantum mechanics principle? Or is quantum computing kind of a separate way of doing things and doesn't relate to the sort of computing that we do on our computers today.

Enrique Blair:

Yeah, that's a good question. Quantum mechanics... or I should say, quantum computing certainly is very powerful. And in theory, quantum computers could do everything that classical computers can do and more. However, quantum computing is so expensive that it's really not feasible and it won't be for the foreseeable future to have quantum computers on our laps or in our cell phones.

Enrique Blair:

Some of the problems here are that to get many cubits working together, you really have to isolate them from the environment because of decoherence, which maybe we discussed before. To isolate from the environment, it means we need specialized equipment like dilution refrigerators which are massive and use a lot of power.

Robert J. Marks:

Do quantum computers use superconductivity in some sense?

Enrique Blair:

Yes. Yes.

Robert J. Marks:

Is that right?

Enrique Blair:

Many of them do, yes.

Robert J. Marks:

Superconductivity requires really, really cold environments.

Enrique Blair:

Right. Yeah, I believe I read in the Google article about quantum supremacy. They had to cool their system down to 20 millikelvin.

Robert J. Marks:

Now, millikelvin is absolutely zero. That's where nothing vibrates. If you have heat, things vibrate. And as you reduce the temperature, the vibration slows down. Zero degrees kelvin is when there's no vibration at all.

Enrique Blair:

That's right.

Robert J. Marks:

This is how cold?

Enrique Blair:

We're 20,000ths of a degree away from that.

Robert J. Marks:

Oh my gosh.

Enrique Blair:

Yeah. I don't want that on my lap.

Robert J. Marks:

Okay. Yeah, hopefully they can get something which operates at room temperature. Do you know if there's any research going on now where things are working at room temperature?

Enrique Blair:

Well, that's a good question because there are a lot of different ways to implement cubits. There are ion traps and there are... One interesting one is these defects in semiconductors. Maybe you have a diamond crystal and you pull out a couple carbons and put in a nitrogen, this gives you a nitrogen vacancy center.

Enrique Blair:

In theory, that you can manipulate cubits that are based on these nitrogen vacancy centers, you can manipulate them and read them at room temperature. But if I'm not mistaken, I think even still you have to cool them down so that you get high fidelity readings.

Enrique Blair:

Again, I'm not too familiar with all the experimental science behind that. I will be soon, hopefully. I don't know. I'm studying more about these NV centers and maybe more cost effective ways to make them, because a diamond's simply expensive. There are ways to... there are candidates for room temperature quantum computing.

Robert J. Marks:

We've been talking about quantum computing, and we touched on it last time. There's a big problem there in that we're using this really weird quantum mechanics in order to set up cubits and we have to set up all these dominoes in quantum computing, then we have to knock them down. There's all sorts of problems with maintaining coherence, making sure that everything is connected.

Robert J. Marks:

I guess one of the big problems is, how many of these cubits can you actually connect together in an entangled sort of way? That's a big problem because every time they try to do that, the quantum states start collapsing and your wave functions start going away and the thing doesn't work.

Robert J. Marks:

Google recently announced they had achieved quantum supremacy. What is quantum supremacy, and how does that relate to the quantum computer and the other computers that we use today?

Enrique Blair:

Right. Quantum supremacy, I mean, it's a pretty interesting buzzword. Maybe the first thing to mention is what it's not. I think that people might hear quantum supremacy and think that it means that now quantum computers will do everything that a classical computer can do, but better and faster. Now, that's a bit too broad. Really, quantum-

Robert J. Marks:

Yeah, we talked about this last time.

Enrique Blair:

Yeah.

Robert J. Marks:

We don't think we're going to have quantum computers in our laptop.

Enrique Blair:

That's right, yeah. Really, quantum supremacy... to achieve quantum supremacy, it's a much lower bar than that. I mean, it's still pretty spectacular, but it's not that earth-shattering. Here, to claim quantum supremacy, Google has created a task that is extremely hard for classical computers, but they demonstrated that they can do it in about 200 seconds.

Robert J. Marks:

What was the problem they were solving?

Enrique Blair:

The problem that they built really is to characterize a random quantum circuit. They had this configurable quantum circuit and they set it up in a randomized sort of fashion, and then they want to calculate the probability distribution. What I mean by that is, with a certain number of cubits, say N cubits, you get two to the N possible outcomes. They're working with 54 cubits, but one of them was broken, so they actually only had 53 cubits.

Robert J. Marks:

Ah, poor people.

Enrique Blair:

I know. But that's really a computationally intensive task to simulate classically, because now you have just numerous probabilities to calculate. They sampled the output of this quantum circuit in about 200 seconds, and that's enough to characterize the probability distribution in terms of what's its mean. To get that same characterization, an equivalent characterization classically, they're estimating that it's going to take 10,000 years.

Robert J. Marks:

Oh, if you used a normal computer?

Enrique Blair:

Yeah. And not just any normal computer, but we're talking a supercomputer at... I believe it's Oak Ridge National Labs.

Robert J. Marks:

A super duper computer.

Enrique Blair:

Super.

Robert J. Marks:

Help me out here. You say it computes a probability density, a probability density. Now, I'm familiar for example, with throwing a di. The probability density there is the probability of one pip. By the way, pip is the number of dots on a dice.

Enrique Blair:

Okay.

Robert J. Marks:

That's a new word that I learned. Very short word, but very useful if you play Scrabble. The probability you're getting only one pip showing on the throw of a die is one-sixth. The probability of getting two pips in one-sixth. And then we go all the way to the probability of getting six pips, which is also a sixth. That one-sixth, one-sixth, one-sixth, one-sixth, one-sixth, is kind of the probability density function. Is it easy to understand what they meant by the probability density function for a random quantum circuit? I guess I have a disconnect there.

Enrique Blair:

Sure. Really, what they're doing is they're randomly interconnecting these cubits and they're asking the question, what is the probability of the various outcomes? We might struggle to understand what good is this randomized quantum circuit. Really, they're saying that this could be used for generating a random number, and a list of a few other applications. But it's funny, because this task isn't incredibly useful. Nonetheless, it demonstrates quantum supremacy because it's something that's hard to do classically but you can do it with the quantum computer.

Robert J. Marks:

Well see, that's what I read in the media, that this new Google circuit actually generated a random number in some sense. I guess it generated a whole bunch of random numbers in some sort of distribution. We went back, I believe it was a previous episode, and talked about how you could buy things on amazon.com where quantum collapse could be used to generate random numbers. I'm not sure I understand what the increase and the excitement about what happened at Google is above just a normal random number being generated by a quantum collapse.

Enrique Blair:

Right. What you say is true. There are a lot easier ways to generate a random number. I guess the challenge here, the thing that Google did, is that they characterized that probability distribution quickly on their quantum computer. Whereas if you wanted to simulate that on a classical computer and to calculate that probability distribution, it's going to take a very, very long time.

Robert J. Marks:

Okay. Okay. I know that IBM came out immediately after the press release and said, "Google didn't do anything." They gave a ho-hum to the results of Google. Do you know the story behind that at all?

Enrique Blair:

Yeah. Google had this really remarkable speedup from... the quantum time was 200 seconds, the classical run time was 10,000 years. IBM made the statement, "Well, if Google did a better job of optimizing the classical computer, we think that their calculation time of 10,000 years could be done on a timescale of 10 days-ish."

Robert J. Marks:

Oh, okay. So they challenged what could be done on a normal computer then?

Enrique Blair:

Right. Right.

Robert J. Marks:

A normal super duper computer. That wasn't that big of a deal.

Enrique Blair:

Right. And really, these are only estimates because they didn't really do the full-blown calculation.

Robert J. Marks:

Okay. Well, the future of quantum computing is hopefully certain. We got enough people trying it today. Countries, businesses, are all trying it, and all trying to be the first one to actually generate this quantum supremacy. We'll see what the future brings. I do know that this quantum computer has been around, at least conceptually, since... I believe it was Richard Feynman that originally suggested it. I remember hearing about Shor's algorithm and Grover's algorithm... oh gosh, 20, 25 years ago.

Enrique Blair:

Right.

Robert J. Marks:

It's taken them this long to get the instrumentation together to even do something which is close to what we've known theoretically can happen for a long, long time.

Robert J. Marks:

The other thing is, we talked about Shor's algorithm. Shor's algorithm would make most of the encryption use today obsolete. But there is good news at the end. Because if we're able to use quantum mechanics to make encryption obsolete, we can also use quantum computing or quantum effects to actually have an encryption which quantum computing can't beat, and that's referred to as quantum communication.

Robert J. Marks:

I know there's lots of interesting quantum communication today. The NSF and the Department of Defense are throwing big bucks at it. What is quantum computing, just roughly?

Enrique Blair:

Okay. You asked, what is quantum computing? I think you meant, what is quantum communication?

Robert J. Marks:

Oh, I'm sorry. I did. I misspoke, yes.

Enrique Blair:

Sure.

Robert J. Marks:

But what is quantum communications?

Enrique Blair:

Sure. Quantum communication really is the use of quantum mechanics to share information in a secure manner. Maybe the simplest example really came out in 1984. A couple guys, Bennett and Brassard, came up with an algorithm. It's been called BB84. The idea here is that people will share entangled pairs of cubits. We're probably talking here of photons, to generate photon pairs that are entangled. We'll use these photons in such a way that we end up sharing a random number, a very large random number.

Enrique Blair:

The magic here is that if someone intercepts the photons that are transmitted, the parties on either end can know whether someone has intercepted them and tried to spoof the photons and transmitted fake photons, because the error rates will be too high. So you can know whether your random number is compromised. But if it's not compromised, then you have this long random number and you can use that to encrypt a message over a unsecure classical channel.

Robert J. Marks:

So it's taking advantage of the idea that if you look at a quantum state, it collapses. And in this communication process, if somebody peeks at what you're trying to do, quantum states collapse and you know it.

Enrique Blair:

That's right.

Robert J. Marks:

Because all of a sudden, the error rates go up.

Enrique Blair:

That's right.

Robert J. Marks:

It's taking advantage of this observation in order to detect tampering on your communication channel, which is really weird. I'm not sure of the current state of quantum communications, but I suspect it probably has the same problems as quantum computing. Specifically, coherence and keeping entangled things at far distances and things of that sort.

Enrique Blair:

Right. It has some of the same problems. What's nice about quantum communication is, we don't rely on entanglement between as many cubits. In quantum communication, you just need every pair of cubits to be entangled. But in quantum computing, you might need tens or hundreds of thousands of entangled cubits, and that's much harder.

Robert J. Marks:

Oh, so it's the same problem as quantum computing, getting a bunch of entangled quantum states.

Enrique Blair:

Yes, but it's also easier in quantum communication because you just need to entangle pairs of photons. Whereas in quantum computing, you need many, many tens of thousands, if not hundreds of thousands to be entangled.

Robert J. Marks:

And so the entanglements don't have to be coupled in any way in quantum communication, is that right?

Enrique Blair:

I guess the challenge with entangling massive numbers of quantum systems is that that entanglement becomes much more fragile. In quantum communication, you just need pairs of photons to be entangled. One with another, that's it. Whereas quantum computing, you need many, many systems to be entangled, and that's just very fragile.

Robert J. Marks:

Okay. Look in your crystal ball. What is the future of quantum computing and quantum communication? Is this something we're going to achieve or is this something we're just going to chip away at for a long, long, long time and find out that the engineering of it, at least to the degree that we would like it to perform, is not possible?

Enrique Blair:

Yeah, that's a great question. I think in terms of feasibility, I think that quantum communication is much closer and a much easier problem. I don't really know the state of the art, but I believe that we are much closer to achieving that than useful quantum computing. Like I said, this Google algorithm, it really did demonstrate quantum supremacy, but not-

Robert J. Marks:

Kind of in a trivial way.

Enrique Blair:

Yeah, in a trivial way. That's right. To do practical Shor's algorithm, we're going to need tens, maybe hundreds of thousands of cubits working together.

Robert J. Marks:

Shor's algorithm is the one that cracks encryption.

Enrique Blair:

That's right. Again, the challenge with so many cubits entangled is that it's very hard to maintain that entanglement for any useful amount of time. Right now, the state of the art is maybe 70 cubits entangled, 50 cubits entangled. We have a long, long ways to go before we can do the practical things that everybody dreams about with quantum computing. Now that said, there are other applications that are maybe closer at hand. There's a different kind of quantum computing called adiabatic quantum computing.

Robert J. Marks:

Adiabatic?

Enrique Blair:

Adiabatic, that's right.

Robert J. Marks:

I've heard that word. What does it mean?

Enrique Blair:

It goes back to the adiabatic theorem in quantum mechanics.

Robert J. Marks:

Okay.

Enrique Blair:

The idea is that if you evolve a quantum system slow enough, you can maintain the system in its lowest energy configuration. The promise of adiabatic quantum computing is that this is the one where we can solve optimization problems. Because in classical computing, there's no guarantee. When you attack an optimization problem, there's no guarantee that you're finding the absolute or the global minimum.

Enrique Blair:

Now with adiabatic quantum computing, you can evolve the system from an input state to a solution state slowly enough that in theory, you can be guaranteed to find the global minimum. This is actually already being done. There's a company called D-Wave, and they have 2,000 cubits working together.

Robert J. Marks:

That's a lot.

Enrique Blair:

It is a lot.

Robert J. Marks:

How many did IBM have, 53 or something?

Enrique Blair:

Yeah. We're talking 50 to 70. The reason they have 2,000 cubits working together and IBM and Google don't have that much is, we're talking about two different computational paradigms. One, in the adiabatic world, you don't need as much entanglement between all of the cubits.

Robert J. Marks:

So they don't have to be coupled as much?

Enrique Blair:

That's right.

Robert J. Marks:

Mm-hmm.

Enrique Blair:

And so you don't have that fragile entanglement.

Robert J. Marks:

Well, throwing money at a problem is going to solve it. I think that we're going to have quantum computing. But it seems to me, having not cracked the problem for the last 30 or even more years, that there has to be innovation which comes forward. I think that the best technology has been thrown at it, and there needs to be some sort of breakthrough. Well thank you, Dr. Blair. We've been talking to Dr. Enrique Blair. He is on the faculty of the Electrical and Computer Engineering Department at Baylor

University. And we've been talking about all sorts of things quantum. Thank you very much for joining us.

Enrique Blair:

Thank you for having me. It's been a lot of fun.

Robert J. Marks:

Excellent. Excellent. Until next time on Mind Matters News, be of good cheer.

Announcer:

This has been Mind Matters News with your host, Robert J. Marks. Explore more at mindmatters.ai. That's mindmatters.ai. Mind Matters News is directed and edited by Austin Egbert. The opinions expressed on this program are solely those of the speakers.