005 Applying Quantum Computing for Federal Challenges

Tue, 4/5 10:57AM • 33:50

SUMMARY KEYWORDS

quantum, quantum computer, quantum computing, algorithm, cybersecurity, black swan, people, classical computers, technology, continuum, problems, nist, computer, test, world, starting, talking, years, attack, keys

My name is John Gilroy and I will be your moderator. Our guest today is Duncan Jones, head of cybersecurity at a company called Quantium. Qu a NTINUUM. Is that correct? Duncan?

04:17
Yes, that's right. Yes, it's easy to say easy to spell.

04:23
Well, well, we're gonna talk about a big trending phrase here in the United States. I don't know if it's trending over there in the UK. But, you know, quantum computing is kind of the thing that's almost a conversation around the coffee table. The evening is in the house, you know, people are talking about artificial intelligence and quantum computing and, and all of a sudden, it's kind of trending. And if you go to Google Trends, you find out that this term has been around for a while. And I think finally we're at with software developers would call a maturity level, where maturity level we actually can deploy some of the aspects of quantum computing and and I thought it'd be good to have you in give you maybe get a dispassionate view from the other side of the pond. and help our federal audience understand what quantum computing can do for them. So, so let's say you're, you're in the tube, talking to someone over there, and you have to describe this whole idea of quantum computing. So Sahaj describe it to, you know, to the great unwashed, like me.

05:17
So the other day, I was speaking to my father, and he was asking me unprompted about quantum computing, which I think suggests that we've reached a level of public awareness that is quite high. So how would I describe quantum computing, it's very different to computing as we know it today. So the computers that we have in our pockets that we call phones and the laptops that we use. In my industry, we now call those classical computers. And they operate on binary, they run programs, zeros and ones, and it's the stuff that we've had for, you know, 60 years or so. Quantum Computing, its origins are, you know, decades old, is based on the idea of quantum mechanics. And in the 70s 80s, people were starting to think, Well, if we want to be able to simulate or run really complex experiments to reflect the complexity of nature itself, then we can't hope to do this on classical computers, we need to actually operate in the same way that nature does, we need, we need a quantum computer. And one of the main differences between today's classical computers and a quantum computer is that we move away

from this idea of just having binary zeros or ones. And we move to a world where we can operate on every possible combination of zero and one. So instead of it's like, hugely parallelizing, for hardware to say, like continuum parallelizing computer operations, so if you want to solve a problem, you can potentially explore running a function on every possible input at once, and you get an answer out the other end. And if you repeat that several 1000 times, you may end up having solved a problem that a classical computer couldn't even couldn't even approach something, you'd have to have a classical computer, the size of the universe to be able to answer certain problems, that we expect quantum computers to be able to solve relatively quickly, in the years ahead, is very, very different, very exciting, a lot of opportunity for approaching, you know, world changing issues that we just can't do classically.

07:56
Tomorrow, I'm having a meeting with a software developer two o'clock, and, and I'm trying to talk about quantum not frogs, and then so, so I'm trying to set up a parallel here. So the abacus is to a classical computer, as a classical computer is to quantum is that something we can say?

08:15
Ah, I just say it's even greater than that. Whoa, really? Yeah. Because because, say classical computer, versus an abacus is, is sort of a it's an increase in performance. Definitely what we can do with a classical computer versus a, an abacus is, is a huge clearly, but I think the difference between what we can do on a classical computer and, you know, powerful quantum computer in the future will be orders of magnitude greater. It's like having probably infinite advocacies that you could experiment with it's, yeah, I think it's really going to be more different than we can imagine.

08:56
Okay, so we set the stage for the discussion here, we have a different way of computing and it's much more powerful, give you many more options. So if someone is sitting over at NIH, and they're listening to this or scratching their head and going well, you know, what's in it for me or people at FEMA? What's in it for me, people treasury? What's in it for me? And we can take different specific use cases, I guess, for the federal government, I guess, I think of NIH, I think of research and development and doing studies. So is this an application for our listeners?

09:26
Yeah, absolutely. Quantum is going to have an impact in a wide range of fields. So for example, continuum, we have different groups focusing on some of the areas that we expect to have impact in the next, you know, 235 10 years. And they include things like quantum chemistry, so the ability for scientists to predict what is going to happen when we build when we design medicines and how they will interact with the human body. For example, Those questions are incredibly difficult to answer when they're impossible really to answer on classical computers, because there's so many, so much data to crunch, you know, so many possibilities of how a molecule may attach to some part of the human body and so forth. With a quantum computer, we hope in the future to see that we can actually simulate these things in advance and hugely accelerate the process of drug discovery or, or bring new medicines to market far more effectively and cheaply. So that's one example. Another example is in the field of machine learning, which touches what we master is a technology rather than a sector. And almost every industry is using machine learning one way or another. And we expect over the years

ahead, starting relatively soon that machine learning algorithms will be more efficient to compute on a on a quantum computer than they would be on racks and racks of, of, you know, NVIDIA GPUs or something like that. And in the years ahead, we'll probably be able to tackle problems that are just out of reach of classical machine learning. There's like natural language processing, which is going to be of great interest to a number of your listeners. Now that one's slightly further out, that's probably something that will bear fruit in 10 years, maybe rather than two years. But we genuinely hope that with the power of quantum computers, we will be able to understand what language means and then be able to process it. And you can imagine all the use cases that would entail everything from our voice assistants in the home, I won't name any in case it sets off people's people's devices, right the way through to intelligence and understanding what's being written and said by the people around the world. And then, of course, the area that my group focuses on, is cybersecurity. And that's the nearest term use case. And in fact, the first use case that is really live, we're able to do things today, with quantum computers that can improve cybersecurity. So that's, that's the closest use case that already in the market.

12:19
So in a chess match, I move upon you move upon, I'm moving Knight, you move a knight. And so if people are worried about near peer adversaries using quantum computing to break cryptography here, then the counter move would be for the opposition or another organization to use quantum to defend right, so So is this a little game we see things like back and forth is is quantum computing to use for preventing attack from another quantum computer?

12:49
Yeah, partially. So the there is definitely a well understood threat that quantum computers pose to cybersecurity. And that threat is that powerful quantum computers the likes of which may arrive, as soon as 10 years from now, we'll be able to solve the mathematical problems that we rely upon to keep our cybersecurity systems safe today. So you and I are talking over an internet connection, which is encrypted. And the reason why it's safe today is that an attacker cannot break cannot solve these problems that the decryption relies upon. In 10 years time, an attacker may indeed be able to solve those problems on a on a quantum computer. And so the whole world is about to go through a big transition towards different encryption methods, effectively very similar. They just use different mathematical problems. And they are problems that we don't think quantum computers will be any better than classical computers in solving. And this effort is largely being orchestrated by NIST. And in fact, in the next handful of weeks, we're expecting them to make some announcements about what are these chosen algorithms that we'll all need to migrate to over the next few years. As you mentioned, though, quantum is not just a threat, it can also strengthen cybersecurity. And people are investing and exploring. How can we do things with quantum where we move away from this idea of we have a hard math problem and the reason that everything is safe is because nobody's figured out how to break that math problem yet, towards systems that rely instead on This is secure, because this is how the universe works. And somebody can't break into this particular part of the system, because to do so they would have to break the laws of physics. And we don't believe that's possible at the moment. And this is really exciting because I would argue the threat is should motivate people to act. And people should probably be acting faster than they are. But it will come and go, and we'll forget about it in due course, we'll all move to these new algorithms, and it will be in the rearview mirror. I think in the wholeness of

time, we'll actually see that quantum has given us a gift for cybersecurity. And it will allow us to build things that are secure in a way that can't be undone in 10 or 15 years time by some new advances in computing, for example.

15:58
I want to ask you a question about NIST and something called Rainbow. But first, one of the best ways to keep up with the fast changing world technology is to attend webinars, your only your schedule, and you get continuing education credits, the best webinars are from Fed insider.com. And they're free. As a matter of fact, Duncan, their last webinar, they had a guy from the UK, a military guy, a Brigadier General, and they had a general United States talk about digital transformation and sharing information on the international stage sounds like some appropriate time for talking about this. So all kinds of stuff, we're fed Insider. So let's go back to NIST, my friends up at n i s t up the road from me here. So you've recently written and you're all over LinkedIn, by the way, all kinds of articles, and I don't know what you're doing, but you're all over LinkedIn. There's an article that mentioned you talking about this rainbow algorithm and NIST, maybe you could give us a quick nutshell description of what this is all about and what this means for what's going on in the next couple years. Yes, sure.

16:54
So I think some useful background context here is the idea that we use these cryptographic algorithms, encryption algorithms and other algorithms. And we use them not because we think they cannot possibly be broken, we use them because the best known attack against them is not feasible to actually carry out. So you know, academics are always poring over these algorithms, looking for ways to do a slightly more efficient attack on them. But as long as that attack requires 10 million years and 1 trillion computers to implement, then we're not too worried because nobody has that. And so every algorithm that mist is considering as as replacements as quantum resistant replacements, what we use today, they all have known attacks against them. They are just reassuringly infeasible to actually carry out. Except recently, somebody made a bit of a leap forward on how we can attack a particular algorithm called Rainbow. And what that meant was that something that we thought was infeasible suddenly became feasible. In fact, the paper that announced this had a an amazing title, which I'm going to paraphrase, but it's something like how to break rainbow in a weekend on a laptop. You know, the horror story that no no cybersecurity professional wants to read. But what this, this researcher managed to do was to take a big step forward in the efficiency of attacking this algorithm. And what this means is that rainbow is now becoming less and less attractive as an algorithm, because the natural response to a increase in in attack sophistication, is to basically make everything bigger and harder to break. So the keys themselves that are used with with rainbow, if you just make them larger, they're harder to break. It's a bit like having a you know, you probably have a four digit PIN on your ATM card. Yeah. It's intuitive. If you have a 10 digit PIN, it would be that much harder for somebody to guess what it is. And in that same vein, the reaction to this attack for Rainbow has been to say, Well, okay, what we'll do is we'll just make all the numbers a bit bigger. So this thing is we're back to where we were still difficult to attack. However, the impact of that is that this algorithm is just becoming less and less attractive to us, you know, as you make things bigger, make keys larger, for example, they're just harder to use in the systems that we have today. And there's always a concern that someone is going to make another breakthrough. You know, once you've had one break through sometimes, you know, other academics build on that. Or maybe this, the same person is getting into their stride and starts to

do even more attacks. And there's always this question mark over what could come next. And so my suspicion, which we'll we'll, we'll know for sure, in the next few weeks is that rainbow probably won't be one of the winners of this competition now.

20:24
But it was a fair fight. I mean, they they all they offer it up as a test. And it's like a wrestling match. And And next, when you find someone that's better, I think it's, I think that's almost the scientific method, isn't it is that, you know, we'll test over here, see if the same things apply, and then test and test and test and test and test and then maybe make a weak statement? Keep on testing, huh?

20:46
Yeah, this this is, this is a good thing, really, we want, we want the academic community to scrutinize these algorithms, and find the problems now. So that we can standardize on algorithms that we believe will be compromised in the field. But the problem is, and this comes maybe back to the whole quantum thing, again. Anytime that we are relying on complexity, you know, relying on the idea that somebody can't break this, because they don't have a big enough computer, yet, we run the risk that there's going to be a huge breakthrough. And, and, and the things that we think are secure, could become insecure, you know, overnight. And that's one of the motivations behind exploring quantum as a tool for for cyber is that we can move away from those assumptions and back towards, you know, solutions based on the laws of physics. Now, I should say, because this gets people quite hot under the collar, that even solutions based around quantum aren't perfectly secure the quantum part of it might be but it these are real world systems that we have to build. So there are no silver bullets anywhere. But there are places an example of this, which my team focuses on is, is generating these keys in the first place. How do you make a unpredictable, you know, super strong, cryptographic key? Well, we can approach that with quantum and we can say, Well, look, we we, we know from the way that the universe operates that if we generate a key using the unpredictability of quantum nobody will be able to predict that regardless of what computer they invent in the future. You know, it's the laws of physics are what is securing that not? The sort of complexity assumptions. So this is why people are intrigued and there's a growing interest in quantum cybersecurity.

22:52
I have three grown kids for Christmas. I just get most of books to buy me and so I want to reread The Black Swan. So I'm rereading you know, Tellabs book, I think you're familiar with a black swan. So my question to you there, Mr. Smarty Pants. So is this a is this a Black Swan? Is this something it's really a complete game changer Quantum? You're talking about 10 years out? Is this going to be just like, turn everything upside down? Is it a Black Swan? And what would leap say what I agree with you.

23:19
It's definitely game changing. I think one of the properties of a black swan is that nobody saw it coming yet. In hindsight, yeah, so obvious. And I think what's notable about quantum across the board, is that everybody can see it coming and your investment and the interest is going through the roof. I can't remember the last time that a technology has seen such such discussion at the highest levels of government, we're seeing, you know, pacts appearing between countries who are agreeing to invest in this technology to throw billions of dollars behind it. So I think it will have an impact on humanity. The

equal of any black swan event in history, perhaps greater than that. But the good news is we can see it coming and everybody is starting to gear up and get ready to embrace it.

24:17
What's fascinating is that if you look at interviews with this guy, Nassim Taleb, he thinks that COVID, they should have seen that comment. So it's not black swan. So similar to because you can see these things building. And if you go to Google Trends, like I did, and you'll see artificial intelligence, and quantum been around for a while. And so it's not like a something that came out of the blue. There's other events that have happened here recently that maybe qualifies black swan events, but we're not going to go there. We're going to talk a little bit more about cryptography and your company. So how can a federal agency use you guys before 10 years from now when it gets more mature? So can they engage with you? Do they use your system? Do they have a truck and pull up on your computers to use Amazon or how can they use you

25:01
And I think thanks for asking, it's it's a common misconception that simply because a product is enhanced by a quantum computer that you therefore, couldn't possibly use it today, or that you would need to be a physicist, or you'd need to spend $25 million on a quantum computer. Now, unfortunately, none of those things are true. Our product that we launched in December, is the first product that uses a quantum computer to do something that a classical computer can't. And one of the reasons why this is in the market today is simply because we don't actually need very much from the quantum computer. This particular use case has only modest requirements from a quantum computer, something that is already met by the vast majority of computers in the field. And so the product we launched is called Quantum origin. And if you were to embed this into your existing infrastructure, you wouldn't actually need to know anything about quantum physics. Obviously, we will tell you about why what we do is highly secure. But it acts It's looks and smells like other technology, it plugs into the technology we all already use. So a typical use case, for example, is that you have a cybersecurity solution, and you want to strengthen the cryptographic keys that it uses. And you can just pull keys from our service. And they can be easily integrated into the systems that you already have, with the key difference being. And one of the problems of selling keys is you keep using the word key at the wrong time. And it gets everything ready for viewing. But one of the important differences is that because of the way quantum mechanics works, we can mathematically prove that these are the strongest keys but they've ever been created. So I think it's a interesting example of how quantum technology is beginning to trickle into the world. And yet, it's already accessible, you know, cuz this technology as a whole is not going to be successful. If everybody needs a team of quantum physicists, we need to create products and services that are easy to consume that are enhanced by quantum. And that's something that our company continuing is striving to do to make these to deliver the benefits of quantum to the world without everybody having to become a quantum physicist.

27:35
I tried to draw automobile analogies, I've got a hand as 2000 sit in my driveway there, I can drive up and get low for bed and come back. Now, I probably couldn't take that water pump out and redesign a new water pump. But that's not the objective. I'm hungry. So it's not the water pump technology, worried about worried about going to the store and back. And so if you get involved in what exactly

quantum technology is, you've got to bring in some brainiacs and physics majors. And then you're 10 years down the road and you're 50 pounds heavier and you understand it. And you could have gone to the store back and forth many times. So it seems like it's a theoretical trap. And maybe someone as smart as Nasim Talib can sit with you for three hours and talk about what quantum is what it isn't. But I think it has practical applications for the federal government that they have to just, they're not going to have a choice because there's countries outside the United States, as you mentioned, they're banding together. And if the American government doesn't keep up, they're going to get blindsided.

28:31
Absolutely, and I think a common concern in the industry is around skill shortages. So as as I presented a slightly idealized version of the future where you get all these content benefits without knowing nothing about quantum mechanics. And that that future is probably some way away with the exception of the product that we decide the product we just discussed. And between now and then a lot of large companies and a lot of government agencies are really going to have to wrap their head around what quantum could do for them. And they need to start now, you know, if they, if they invest in five years time, or in 10 years time, they are five or 10 years behind the competition, whether that's governments around the world, or whether that's, you know, for the private sector as to what your your nearest competitor is doing. Starting to embrace this now is the only way that you won't fall dramatically behind in a few years when the quantum speed up, if you will kicks in and your competitor can suddenly predict the prices of stocks, you know, 100 times better than you can well that's gonna be a that's gonna be a existential threat to your business if you haven't started to explore it already. And so when you combine that with the idea that there is a finite but great I mean number of people who really understand this subject. It's it's fatal not to move now.

30:07
Yeah. And, and I mentioned British military earlier. They have to embrace it. Everyone's embracing it. Everyone from the satellite manufacturers, to oil producers to banks. Cryptography is getting interesting as have to be more and more explained in the future. Well, unfortunately, Duncan, we are running out of time here. You've been listening to the federal tech podcast with John Gilroy. Like thank my guest, Duncan Jones.