IonQ at Cantor Convergence 2026
November 11, 2026, 9:30 a.m. EST

Jeff John Roberts: Fortune – Finance and Crypto Editor
Niccolo de Masi: IonQ, Inc. – Chairman & CEO

Jeff John Roberts:

I'm Jeff John Roberts, Finance Editor at Fortune Magazine. We have got a really interesting and a little bit scary panel today. I'm delighted to welcome Niccolo from IonQ.

Niccolo de Masi:

Want me to clap for myself?

Jeff John Roberts:

I like this panel because as a, as a reporter, I always get these pitches. They're like, "Quantum's going to destroy everything." And I've been getting these pitches for like 10 years, and it's just like, is it or is it not going to destroy everything? So, but we've actually got someone up here who can really break down the science of it.

So that's where I'm going to open. We were talking backstage about what's going to happen next and the state of quantum. So is this just like a binary thing where we're going to wake up one day and everything's going to be hacked and all the Bitcoin is going to be gone? Or just take us through. You made the analogy beforehand to the Manhattan Project, so break that down.

Niccolo de Masi:

Well, look, I want to first thank everyone for your attention. Distinguished guests, including the Premier of Bermuda, is with us here in the front row. And I, I think alarmism to me is never long-term productive, but sometimes it helps us focus the mind in the short term, for sure. The state of, as I call it, the Manhattan Project and the quantum computing sector has a very disparate spread of achievement time horizons based on who you are, where you are, and what your company is.

And what I said backstage was, if my friend from Fortune Magazine were back in time in 1942, and he asked half a dozen players how their atomic bomb project was going, he would have heard, you know, "We're 15 years out," if you were the team in China. He would have heard that we were 7 to 10 years out if you were in the Soviet Union, subject to stealing IP. He would have heard that you were 5 to 10 years out if you were the German team, subject to resources. But there was one team that happened to be ours in Los Alamos. That was two years out. And that's a wide spread, right? 2 to 20 years was a wide spread in 1942.

And there are some nations today that still don't have the bomb, thankfully. You see the same wide spread in quantum computing right now, which is there are people that will tell you they will not get there for a decade, or they will not get there for two decades. But in the case of IonQ, we've been at it for 30 years.

So we built the world's first quantum logic gate in 1994. We were the first public company in the sector in 2020. We are the largest quantum company in history today by every measure: revenue, balance sheet, market cap, patents, IP, people. We published two important papers this year. In April this year, we published the world's first shovel-ready blueprint for fault-tolerant quantum computing. And we told everybody exactly how we're building the next three generations of our machines.

And we also published two months ago the world's first down-to-gate-level specificity paper on how we can crack elliptical encryption with 20,000 qubits in our machine, which, if you look at our roadmap, is kind of roughly 2028 in the lab, which is probably '29 out in the real world.

Now, elliptical encryption obviously is used by some nation states. It's used by the blockchain. Also, RSA 2048 is the one that banks and telcos and most nation states use. Civilization as we know it relies on RSA 2048. That's probably a year after the elliptical encryption cracking when you look at our roadmap, based on the information we have today.

And the reason I say based on the information we have today is that in the last five years, every year we and the industry have been able to move down the hardware resource requirements on encryption cracking. At one point, it was a million qubits. Now it's down to five figures. And so I would not discount the very likely reality that in the next two years, you will see progress on the algorithms and software, and that will move the time horizon down sooner again.

Jeff John Roberts:

Okay. Just pausing there, break down the science first. So you have these things called qubits and you stack them. What's been the kind of impediment to the breakthrough? Is it just keeping them stable, or, you know, is it a quantity of them, or is it a raw material thing? I mean, what's the secret sauce to, to advancing this stuff?

Niccolo de Masi:

Yeah. So Richard Feynman wrote down these great postulates in the '70s. When I was an undergraduate physics student at Cambridge University in the UK, we were excited because our founder at IonQ, Chris Monroe, built the first empirical example of a quantum logic gate using what we call ion trap technology. We control ions with microwaves and lasers.

For sure, broadly speaking, broadly speaking, the challenge in quantum computing, as with quantum networking, is how long can you maintain entanglement states while you're performing your calculations? There's a whole host of other challenges around manufacturability, deployability. But IonQ has been at it 30 years. We've spent about $6 billion, and we will continue to spend money, predictably. We spend about $500 million a year on R&D.

And we do that because we fervently believe that we are running the Manhattan Project for our nation and, frankly, probably the Western world and the, and the Five Eyes. We have driven combinatorial progress on both sides of the Atlantic. Through acquisition, we have gained better architectures that are more stable, manufacturable, deployable. We're also the first quantum company in history that purchased our own quantum foundry. So we also make our chips, and our supply chain is entirely domestic in the US and totally secure.

You can read into the fact that we are one of the very few companies in the DARPA Stage C challenge, the final phase of the Department of War's 500-person diligence exercise around who they believe can deliver not just utility, but economic utility in quantum computing. Combined with the fact that we're the first partner NVIDIA has selected for their data center in Boston to deliver hybrid GPU, QPU, quantum processing unit, capabilities, that our machines are as stable as they come, as manufacturable as they come, and they also have a bill of materials that we published over a year ago that shows we're the most affordable in the fault-tolerant era as well.

So look, I always say that we are in the business of quantum. We're very focused on, yes, the R in R&D, the D in R&D, but we're also focused on the M, the manufacturing, the customer support, how we actually make sure that we're driving real-world workstreams and delivering that not just quantum utility and quantum advantage, but can you do it at a price point that delivers value for the customer?

Jeff John Roberts:

Yes. So take us to the future a bit in terms of, one day there will be a breakthrough, and it'll sort of be the, you know, aha, it'll almost be like that moment in the desert. What happens next? You know, what I would assume is the NSA and, you know, everyone kind of goes into a room with you and you figure out how to lock this down. Or is that not the right analogy? Is this something where it can be replicable easily and you're suddenly selling these things to, you know, companies and universities left and right?

Niccolo de Masi:

Well, look, we live in a free nation where technology industries, rightfully so, are cooperating and working with government agencies, departments, and so on. We're one of those. I mean, we are public about the fact that 60% of our revenue is enterprise, 40% is government, and approximately 40% of our revenue comes from partners of ours who are purchasing not just computing, but also security, networking, and sensing from us.

You know, we build the world's most accurate atomic clocks. That matters for data centers, for GPS, and quantum computers. We build the world's most secure, not just quantum networks, but networks in general. And so everybody needs to hear the June 22nd White House executive order around securing the nation against cryptographic attacks in the quantum era. And now, that is something everyone should take seriously in the classical era that we're in now.

But also realize that following the last month of hacking that we've had, not just we, nation states from Italy to France to Japan to Malaysia have had a rough month, and we've had the FBI website, the DHS website, you know, Binance, and so on. I don't see how that is going to reverse in the next year or two. And so I think that there's going to be a historically large uptick in investments in cybersecurity defenses, because LLMs are just getting started, in my mind, and LLMs are going to be smart enough to figure out that if they can get powerful quantum computers on the loop with them, they will be able to do, unfortunately, even more dastardly things. So I think, you know, November '27, November '28 will not be fewer hacks than there are now.

With regards to how, you know, the government partners with us, we're very responsible. So that elliptical encryption paper we published was in consultation with the folks at Langley, the folks at the Fort, you know, NSA, and so on. We never published the final details. We just get down to a credible point so people know that we can do it.

When I look at the GPU space, you know, we have plenty of growth ahead of us in the next three years as we move from a $500 million revenue company to a multi-billion dollar revenue company, having given precise guidance. And Troy, who covers the company, is sitting here in the front row as well.

But nevertheless, you know, we have doubled and tripled revenue the last 3 or 4 years. People probably need to sit up and listen to the fact that in '24, our revenue was $40 million, in '25 it was 130, this year it's over 500. It's a nice moment to say, as I've been saying for a couple of years, quantum is now, it's inflecting now, and this is likely to accelerate.

You know, the AI inflection points have been numerous over the last few years. You had ChatGPT-1 be a curiosity, ChatGPT-2 was a hobby, and then you had ChatGPT-3, and people went, "Goodness gracious, what should we do now?" But the actual revenue and adoption comes after that. We have been building the quantum ecosystem at IonQ, not just for enterprise, but also nation states.

And we take our responsibilities seriously in not only how we are protecting our nation and our allies, but also how we are advancing every aspect of applied science. So material science, pharmaceuticals, defense, intelligence, logistics, financial services, these are the areas where our computing business is focused. We are, at the moment, not a consumer-facing expression of a technology.

So I always jokingly say there's two things. We're not focused on banner ads, is one of them. So we're not in the banner ad business. And, and, and it's actually a serious point and a funny one, which is our QPUs are not about microsecond latency correlations. GPUs and LLMs are beautifully designed for that problem. You click on a map of Italy, how can I serve you a plane, a hotel, you know, a breakfast booking as fast as you possibly can? They're going to own that space, probably forever. It's the reason why Facebook and Google have been able to spend so much money on GPUs and grow their core business. The second thing we don't do is help kids cheat on their homework, right? So we're not in the business of like, "Can you write an essay for me?" at the push of a button thing.

Right. What, what is exciting about building the quantum ecosystem is we are a part of the conversation in every nation, nation state, and every leader of a nation state recognizes that there is a once-in-a-probably-century opportunity to work with us on how they can ensure that educational institutions and workforce development is optimized to take advantage of the quantum revolution, which is really upon us, to be blunt.

If I, if I said to you in 2020, "There's this thing, ChatGPT-1 or 2, trust me, it's going to do a lot of stuff in a year or two," I would have sat with you and you would have said, "Niccolo, when's the breakthrough? When is it going to matter?" And, and, you know, and how silly that would have looked a year or two later, right? I'm telling everyone that right now, which is, you know, we have just told everybody in April how we're going to build a fault-tolerant machine. We own the foundry. We own a supply chain. I'm a public company. I've hit not, not just financial guidance the last 5 or 6 years, but our technical guidance as well. So you should, you should hear that, because we publish our roadmap every quarter. And when people say they didn't know, I kind of go, "Well, we're, we're very public about this stuff." Like, we know exactly where we'll be next year and the year after.

Jeff John Roberts:

You know, it's clear people are bullish. I want to get into that, and also at a financial conference, so I want to get into that. But my last question, just kind of on the sort of state of the science, is, once again, how replicable is it? Because, you know, we figured out how to make a nuke almost 100 years ago, but it's still, you know, people can't do it because you need to process uranium, stuff like that. Is there some limiting mechanism that once you guys crack it and this thing is running, can everyone replicate it within the same year? Or is there kind of manufacturing or industrial or process things that limit it?

Niccolo de Masi:

So there are two questions, right? So the first one is, can I build a thousand machines if I build the first one? And the answer to that one is, and I think I thought I covered this 10 minutes ago, but like, we're the most manufacturable, lowest BOM (bill of materials), own-the-supply-chain, vertically integrated company in the world. There's no one else like us, right? I can make my chips and my machines. And obviously, with our SkyWater foundry, you know, we can make millions of machines, right?

The bill of materials is still high for quantum computing, but it's eight figures is our bill of materials, not 10. And there are, and there are people that you could sit on stage with that will say, "My bill of materials is 10 figures. I may never be able to build more than one of these, if it even turns on." That's not where we are. Our machines turned on in 2017. We've been shipping machines and cloud access since our IPO. We're the first company in the world that was on the public Google, Amazon, Microsoft cloud in 2020. So you can just go and test our machines versus everybody else's.

And by the way, we, we publish those papers. We're about 100 to 10,000 times faster time-to-solution than other cloud options that are out there, particularly on the problems that DARPA cares about, like the quantum Fourier transform, which is important for nuclear fusion research, cryptography, pharmaceuticals, material science, and so on. So for us, the state of manufacturability is the highest in

the industry. We are very focused on supply chain, manufacturing, productization, replicability, deployment. The fact that NVIDIA picked us is because our machines can sit in a data center and not get vibrated out of alignment. We might be the only person in the world that can say that.

Jeff John Roberts:

So it's a bit of an analogous to TSMC or something, that's like a very advanced foundry that it's, you know, you know, just only a handful of people can do this.

Niccolo de Masi:

Yeah. But let me tackle the second part of your question, which was, can people replicate this? And so that one's definitely no. We spend a lot of money on security, both physical and digital. We work really hard on locking down our IP. We work really, I mean, we've got maybe 2 or 3 top secret security, you know, facilities. We have a couple hundred people that have security clearances, including myself. And so we are a great partner for our nation, the Five Eyes, on a national security front. And we have no intention of letting people steal our IP at any point in the future, because we've seen this coming for quite some time.

Jeff John Roberts:

Like Jensen, that's your security? Sorry.

Niccolo de Masi:

Not that sort of security.

Jeff John Roberts:

So let's get to the Bitcoin. You're saying some pretty bleak stuff backstage. How bad is it going to be?

Niccolo de Masi:

Well, as I started 15 minutes ago, this is an important moment for enterprise and government to listen to the executive orders and to wake up that you are inside the planning horizon. I have said this for over a year. I was the first person last summer that said Q-Day is coming in from the early to mid-2030s to the late 2020s. And last summer, everybody was like, "Whoa, I haven't heard that. That sounds aggressive." This year, everybody agrees with me. Governments, you know, even the bad guys agree with us on that. What can you do about that? Fortunately, IonQ is very focused on supplying the solution, because we are not the bad guys.

Jeff John Roberts:

First, first, what's going to happen is sort of elliptic wave, or whatever it's called, gets broken. And then what happens?

Niccolo de Masi:

Well, what happens depends on everyone's reaction. Let's go through what happens if you do nothing. If you sit on your hands, yeah, you, there will be a bad moment in the late 2020s. We can argue whether it's Q4 '28 or Q1 '29 or Q4 2029, but the reality is there will not be a reduction in the cryptographic risks and the general cybersecurity risks from here on out for the rest of our lives.

I will make that bold prediction now, unfortunately, that for everyone in the room who's listening, whether or not you run a company or a country, it will not get better from here. You're, you're at the trough of cybersecurity risk you're going to experience for the rest of your life right now. And that is concerning. But it is also something that we have tackled in the past, and we must tackle.

What I like to remind us all is that the code-making, code-breaking business, it's at least 2,000 years old. Julius Caesar was doing it. Probably 5,000 years old. I would argue strenuously that in the last few months, the momentum from code making to code breaking has shifted for the first time in probably 50, 60 years. I can't remember a moment in time, other than Bletchley Park 1.0 and Enigma in the 1940s, where there was as much momentum on the offense as we have right now. And the momentum of the offense is going to increase as bad guys get access to quantum computers, not mine, but they're going to try and copy, steal, you know, catch up, etc. They are behind us, fortunately, but they're not decades behind us. Okay? They're years, hopefully. Quarters, worst case.

To be specific about the risks you face, there are three, there's three things you got to worry about. You know, network compartmentalization and, you know, authentication. Post-quantum cryptography, which is a software solution that the White House has mandated in the executive order on the 22nd, and we obviously are a big partner and provider of that supplier. And the third thing is quantum key distribution, which is the hardware solution that's as old as quantum computing, and Richard Feynman wrote about that in the '70s also. We are the largest QKD company in the Western world as well.

In tandem, those three, those three solutions will keep you safe. And so by investing today in what you can do on the network compartmentalization and on the PQC, the software front, eventually you'll need to do QKD in the core of your nodes, the core of your data center, because it's unhackable, but it's more expensive. But don't, don't sit here and do nothing, because unlike the current cybersecurity threats and breaches that we have, what is coming by the end of the decade are fundamental nigglings, if you will, on the fabric of encryption. This notion that I can take two big prime numbers, multiply them, and it's really hard for a GPU to crack that by brute force without a century to a millennium of time and a really big supercomputer, that goes away, right?

We said two months ago that we'll be able to crack elliptical encryption in 26 or 27 days, and that was sort of our first shot at it with a 20,000-qubit system. That 26 days goes down as the qubit number goes up, and then it starts to chase after, I would say, RSA 2048. Fortunately, humans are resilient and humans are adaptable. Nobody wants to live in a world, right, where we've reset the clock 50 years and you can't rely on banking, e-commerce, telecoms, messaging. No one wants to live in the, in the '70s.

Jeff John Roberts:

So let's just pause for a second. If I understand, you're like, we need to secure stuff. The mechanism and the process is out there to do it and quantum secure. But that's if things go right. What if things go wrong? And let's start with Bitcoin. Presumably we just wake up one day and see a whole bunch of movements from Satoshi's wallets. And it's, it's, but, you know, of course there's the incentive. If you had that, you probably wouldn't do it all at once, because you'd destroy the value of Bitcoin, right? Just take it inside the mind of the attacker if they get this.

Niccolo de Masi:

I, I am not the mind of the attacker, just to be clear, before we answer this question. This is not the business we're in. We're in the defense business on this topic, but I'm happy to speculate for you if you'd like. I think what you saw with Binance, obviously, is the kind of thing that you will see, which is you'll see bad state actors that are in the black market, the gray market, taking shots at various pieces of the blockchain. And when they have more access, probably later on, to RSA 2048 cracking capabilities, which the bad guys, I hope, will be getting in the 2030s if we're getting in the 2020s, you will be susceptible to more approaches in how they can steal stuff and make money.

So right now, you have the whole download-now, decrypt-later phenomenon going on. So all of us are getting stuff stolen all the time. You don't read about it in the news because they can't figure out the prime number factorization. They will be able to figure that out. And so there will be a bunch of

newspaper articles by the end of this decade talking about stuff that people weren't supposed to know about four years ago, three years ago, two years ago, five years ago, right? This has happened before in the past, but never with as much of a compressed time horizon, right?

So you'll see, you'll see that by the end of the decade. You will see, I suspect, unfortunately, portions of the blockchain where there are certain currencies that either have no ability to centralize and protect themselves, or for various reasons don't believe it's philosophically aligned, or don't get there in time. There will absolutely be people's stuff disappearing the way that it did at Binance, and you'll hear about it far enough down the line that they've monetized it, obviously. It will be a business for bad guys the same way that cybersecurity and hacking is a business today for bad guys, right?

There will be probably more panics, right? I mean, I'm impressed by the fact that the French and Italian supermarkets have lost cooling power. You've seen a horrific number of nation state attacks in Japan, Malaysia. We've had the FBI website, DHS, and we're relatively relaxed at this conference, in this room, where we are in November, because, you know, the power is still on, and there we go. But there will be a lot more of that. And so it's inconceivable to me that enterprise and nation state percentage of investment going on cyber defenses is not climbing relentlessly from here.

I do believe there'll be a spread of people that want to be secure today and want to wait till they've had a vast hair, or hair-on-fire, panic before they believe it. That's just the way humanity always works, right? It's the same as the Manhattan Project comment. Like, we got the bomb first, the Soviets stole it, the Chinese got it, other nations done it a decade later. This is what will happen in the next, not just 10 years, but 10 quarters. There'll be a spread.

The wisest enterprise partners we have have a strong security posture. They spend the most money with us on software and hardware to protect them, not just in the quantum era, but in the present classical and quantum era. And guess what? Those guys are in the news. Those guys are never in the news. Our biggest customers, never in the news. Our smallest customers, they're in the news.

Jeff John Roberts:

So, Niccolo, I'm going to cut you off, because we've only got a few minutes left and I want to throw it to the room. But very quickly, yes, no: do you think the Bitcoin people will figure it out in time and upgrade this sort of, the, the Bitcoin protocol to be quantum resistant before it's too late?

Niccolo de Masi:

Come and find me. This is a good conference. I'm here to help, and I mean that sincerely. We are friends with the blockchain, crypto ecosystem. I'm an early investor in many of these companies and the venture funds behind them. I think the smart ones will come and find me and figure it out. The ones that put their head in the sand or have no ability to get consensus are, you know, they're at risk of some panics.

Jeff John Roberts:

We have time for a question, too. Does anyone have one out here? Yeah. I'm sorry, who are you, sir?

Audience Member:

I want to thank you for [inaudible].

Niccolo de Masi:

Thank you. Very kind of you. I completely agree, by the way. Where are they?

Jeff John Roberts:

Yeah. Bermuda.

Niccolo de Masi:

Bermuda is here. Where is everybody else? You know, I agree.

Jeff John Roberts:

This should be packed. This is interesting stuff. Please, over here, and please speak very loudly. You got a mic here, Jen?

Audience Member:

Hi. I'm curious what policies you would like to see the US implement, or if there's particular agencies that you think should be taking on this challenge.

Niccolo de Masi:

So I, I am concerned, from both of your questions, and by the way that we function, that, you know, until you have the Sputnik moments and things are so terrible that there is no alternative, people don't tend to act governmentally the way that some enterprises are. What did Winston Churchill say? "You can always rely on the Americans to do the right thing after they've exhausted all the possibilities." There's a fair amount of that going on, right?

And so, look, I unfortunately predict there will be panics, because, you know, there's election cycles, people get distracted, stuff happens, you can get disagreements, gridlock, and so on. The, you know, the Chinese are 10 years ahead of us in investing in QKD, okay, on the ground and in space. The Europeans are leaning into this. And you'll all find it interesting that the Europeans that are further east are leaning in harder. We, you know, we do quantum networking in a lot of Eastern Europe, for example. And I find that really interesting, because people that are thinking about the conflicts they're either in or in the future are thinking about the not just cold war that's happening in cybersecurity, but increasingly hot war that's happening in cybersecurity.

We will need to resource all of this much more powerfully from our total budgets, not just at DoW, but across, you know, other agencies. There is always an opportunity for smart people to point out flaws and problems in every cryptographic and cyber defense on the planet. Every one of them has a vulnerability. You can do everything I said, and you still can't stop the guy with a boom microphone there listening to you typing on the keyboard. That will still be a problem in the 2030s and '40s. But nevertheless, there is a super strong correlation between posture, investment, and who is the hardest target and who is the softest target. And just like with everything in the world, you want to be the hardest target, right?

So I think it's great that we've had the June 22nd executive order. I applaud the White House administration for leading with that, because it's the first one in the Western world that I've seen out there. More needs to be done, not only to, you know, to, to raise the profile of this from an investment and policy perspective, but also to recognize that we will need to implement QKD. The question is just when and where.

It will be disappointing to me if we get to 2030, or '29, or '31, and I say, "Hey, you know, we've won the race for the Western world Manhattan Project. We've won computing. Victory is ours." And then China goes, "Doesn't matter, because I've QKD'd the whole country. I might be behind you in, you know, cryptography, but I'm ahead of you in defense." And so this is a, this is a real nation state battle, not just in those two examples, but across the globe. And people need to think about where they're going to be: spiky in computing and defense, just defense. We're spiky at both. We want to make sure that you're spiky at both.

We're here to help. Please, genuine offer, please do spread the word. Please do come and see us. We're very transparent. We're very approachable. And this is the space race, if you will, of this decade. This is the Manhattan Project of our era. And just because bodies are not piling up on the street yet doesn't mean they won't be when you start losing power to hospitals and water treatment plants go off. Like, that's when people will really focus.

Jeff John Roberts:

We're out of time. So I think the point is, go see Niccolo before the bodies pile up. That was a lot to think about, and let's give him a proper hand. That was really good. Thank you very much. Enjoyed that a lot.

Niccolo de Masi:

Keep in touch. Hey, thank you.