Covering Crypto Livestream

Quantum computing and the future of Bitcoin

November 10, 2026

TRANSCRIPT

SPEAKERS:

Jim Armstrong Daniel Gray Matt Hogan

JIM ARMSTRONG: Could a future quantum computer crack Bitcoin? And what's in store for Bitcoin's future in general? Now, the answers to those questions are more nuanced than many of the headlines might suggest. And that's exactly what we're going to unpack today.

Hey there. Welcome to the *Covering Crypto Livestream*. I'm Jim Armstrong with Fidelity. Today, we will address those questions while trying to separate science fiction from reality. We'll discuss what researchers are watching today in this space. And we'll explore what Bitcoin's future could look like years, or even decades, from now.

To have that conversation, we've brought in a couple of fantastic guests from the Fidelity Digital Assets® team, often referred to as FDA, Fidelity Digital Assets®. You've both been on the livestream before, so thank you for coming back again. If you could, just briefly reintroduce yourselves to make sure the audience knows who you are. And, Daniel, we can start with you.

DANIEL GRAY: Yeah. I'm Daniel Gray. I'm a research analyst on Fidelity Digital Assets. I primarily focus on all things Bitcoin. So that's consensus, cryptography, and now quantum.

JIM: Excellent. OK. And, Matt, you were just in that exact seat one month ago. So thanks for coming back.

MATT HOGAN: I was. I'm getting comfortable. Thank you for having me back. My name is Matt Hogan. I'm a research analyst alongside my colleague Daniel on the Fidelity Digital Assets research team. Much like Daniel, I do focus on Bitcoin, but perhaps we differ in our certain disciplines or areas of focus, where he has more of the technical background, and mine is more in the finance and economics discipline. But I think we complement each other well in that regard, and really looking forward to the conversation today.

JIM: Awesome. Thanks again for being here. I do want to mention that we get a lot of questions from viewers during registration, and we read all of them, along the lines of what is crypto, what's the blockchain, how does crypto even work. Those are the exact right questions to be asking if you're new to this space. And these are questions that we've answered a ton in the past.

So today, we're not really going to spend any time covering the basics or the fundamentals. But keep watching, and after the show is done, we would definitely encourage you to check out Fidelity.com/LearnCrypto. And there, you will find tons of amazing resources to get those beginner questions answered.

And, with that, I'm going to turn it over, Matt, to you, for a bit of a refresher on how Bitcoin security works in general so that we can all start on the same page.

MATT: Sure. Yeah. I think it's a great place to start. I think, first, a little out of context—bitcoin is one of many cryptocurrencies today. It seems like there's a new one coming out every day. But maybe we'll start with Bitcoin because it is the first. It's the most established. It's generally the most well-known.

And we'll also focus there on the word "cryptocurrency." And so when we think about that, the "crypto" part of that is actually referring to cryptography, which is this sort of complex math that is used to secure these digital assets and the networks that they run on. And so when we think about Bitcoin and Bitcoin security, what we're really referring to is proof of work, the consensus mechanism actually securing the network, also known as mining or Bitcoin mining.

And at a high level, what this looks like is it's a trial and error sort of guessing game that requires a lot of upfront computational energy and output. It would be like if the three of us were all working on the same combination lock, and, in this example, the combination is going to be the same for the three locks. But there was no way to cheat it. We'd all have to just constantly guess over and over and over again, and it would be pretty intensive to do it that way.

But let's say, Daniel, if you found the combination first and he shared it with us, Jim, we could plug that into our respective locks and find that it was, indeed, the solution because our locks would open. So mining is a bit more complex than this, obviously, but this is what miners are essentially doing. They're expending this computational energy—again, very, very trial and error in nature. And what they are doing is competing to find the right to add transactions to the blockchain.

They add the transactions from this sort of waiting room, so to speak. They add them to the blocks. They add them to the blockchain. And that, essentially, helps secure the network. And that's really important because there's no way to cheat that. They have to use that computational energy up front. There is that upfront cost of production to make sure they're incentivized to act honestly.

JIM: And now let's talk about the cryptography part of it, which involves a public key and a private key, which, in my mind, I assign passwords and PINs.

MATT: Yeah. I love that analogy. I think that's a good way of thinking about it. Luckily for us, the naming convention there is pretty straightforward. The private key is something that you want to always keep secret. It is yours. It's individual, much like a PIN or password. You wouldn't share it with anybody else.

Whereas the public key is the shareable component, so you know who you can send bitcoin to. You need somewhere for it to go to. It is essentially shareable by nature so that you can send and receive bitcoin.

JIM: And I look at it a little bit like email addresses. I need my email address to be public. If I hope to communicate with anybody, you need to know how to get to me and vice versa. So I would want to make that public and share it. But I would never want to share my email password—that, maybe, is analogous to a private key—because doing so means not only could you check my email, you could send emails as if you were me. So the private key is my password.

MATT: Absolutely. Absolutely. In the context of Bitcoin, it's exactly what you said. If somebody had your private key, they could send bitcoin or access your funds in the same way that if they had your email password, they could access your email. But, in the context of Bitcoin, what is really unique is they have these digital signatures. And that's what, essentially, allows you to say, hey, I can actually send bitcoin using this digital signature. But what's really crucially important here is that they can use that digital signature to send bitcoin without ever revealing the private key to the network.

DANIEL: Yeah. And so what cryptography actually does is that it makes this assumption that computers have limits. We don't have an unlimited amount of time or unlimited amount of energy. So if you think of an ATM card, usually four [numbers], like you mentioned—that's 10,000 combinations. A classic computer can probably brute force that in an hour, and a stronger one could probably do it in a few minutes.

JIM: It's almost guessable too, right, if given enough time.

DANIEL: Exactly. And Bitcoin is like the other end of that spectrum, where there are so many private keys in the cryptography that the number is pretty unfathomable and so large that I don't even know the word to say the actual number.

JIM: Yeah, no, neither do we. And we spent some time trying to think about how we could explain to this audience just how unique a private key is. Because, to your point, Daniel, it's almost impossible to picture the number of possibilities there are for a private key. There are roughly—math geeks, beware—10 to the 77th power. What does that mean?

Well, imagine, for starters, every grain of sand on Earth—picture that—in every desert, on every beach, under every sea. Picture every grain of sand. That's your starting point. Take that aggressively large number and multiply it by the number on the bottom of your screen, which, by the way, is 1 trillion times 1 trillion times 1 trillion times 1 trillion times 1 trillion—a ridiculously large number.

That's roughly how many combinations of options there are for your private key. And that's why it's largely considered safe. No computer, and certainly no human, could ever guess at it or brute force it the way you could with an ATM code, potentially.

DANIEL: Yeah. So if you had a computer that was running a trillion guesses per second—

JIM: OK.

DANIEL: A trillion is a lot, right?

JIM: Sure is.

DANIEL: You start at the beginning of the universe timeline and you checked it today, you still have only effectively guessed like 0%—it's like some long 0 decimal number.

JIM: Yeah.

DANIEL: So, all to say, that there are so many private keys out there on Bitcoin. It's incredibly secure. And you're not going to randomly generate one that someone else has already.

JIM: Which should give us a great deal of security and confidence when it comes to a private key, as long as I don't give it out. As long as I don't do that. But there are still concerns about what future computers could do, which takes us to today's topic about quantum-specific discussions.

I've got a couple of great questions from a recent live chat we'll throw on the screen. One is, "Should I worry how quantum computing could crack the crypto blockchain?" And another is, "Is quantum computing a threat to crypto like bitcoin?"

So, Daniel, we have folks on this livestream in varying degrees of comfort with the topic—again, most are familiar but can't dive super deep. So keep it basic. But what do we need to know?

DANIEL: Yeah. So if we start with how classic computers work, they have something called a bit, which is either on or off. It's a 0 or a 1. I like to think of it as a coin flip. It's either heads or tails.

JIM: Yeah.

DANIEL: Quantum introduces something called a q-bit, a quantum bit, which can be both heads and tails. Or better to think of it as maybe all the numbers between 0 and 1. And so what it does is, if you think of a classic computer and you're flipping, say, six coins, you have a number of combinations, you do the computations linearly, and then quantum will do the computations while they're flipping through the air and maybe going through millions or billions of different combinations as you scale this up. And so it creates a more efficient computational timeline to try and crack some of these keys that Bitcoin uses.

JIM: So, far from binary, it's every possible combination—again, an unfathomably large number of combinations. What does that mean to investors today, though?

DANIEL: Yeah. So think of it—again, let's take a mouse and put it in a complex maze trying to find a slice of cheese. That mouse is going to try each path, find an error, come back, start again. And it's going to take some time. A quantum computer is a magical mouse.

JIM: My favorite kind of mice, by the way. I do want to say.

DANIEL: Yes. So it can clone itself. Let's say it has 100 clones, and it can go through all the different paths simultaneously until it finds the right one. You open up the maze, it has the cheese, and you know the correct path.

JIM: OK.

DANIEL: So what this means is the classic computer wasn't able to do this algorithm that could crack Bitcoin. But now, quantum computer is getting closer. And maybe, instead of taking billions of years like a classic computer, it could do it in a few years, months, days, or maybe even hours.

JIM: We don't know. Yeah, we don't know how long. One analogy that I thought—and let me know if it sounds right to you—is I've heard classic computing referred to almost as if it was a single physical key. And let's say you had the key, you would then try it in lock after lock after lock after lock around the world until you happened upon the right lock opened by that key. That's classical computing. Whereas quantum actually starts with the lock—looks at the lock and says, I know how to figure out what the key is that automatically goes in here very quickly relative to the other scenario. Is that close?

DANIEL: Yeah. So, in that example, the public key is kind of like that lock. And quantum computers can't crack a key or a lock that it doesn't know exists. And so you need that public key to act on it. And so what happened was back in the '90s, they created what's called Shor's algorithm. So just think of a function where you plug a public key in and, magically, a private key comes out. And that's what you use to spend your bitcoin.

But the problem was that it would take a classic computer a billion years to do that. And quantum is going to speed that up. But I like to think it's like you're building a time machine. You have the blueprint. You know how to do it. You've done all the math, but we don't have the hardware to actually achieve it.

And you think of it like a skill set. You're trying to learn to shoot a three-pointer in basketball. You can watch all the videos, watch NBA games, read books on how to play basketball. But, like, physically going out and doing it is a completely separate problem. And that's what researchers are trying to do.

They kind of know the math and what they can achieve, but they haven't built the hardware to actually run the algorithm. And so if that happens, then, instead of a billion years, they could do that in a few months or days.

JIM: So how does—tie it all together, I guess, to the research that you're doing on the Fidelity Digital Assets team when it comes to private keys and cryptography. Make that connection.

DANIEL: Yeah. So think of your private key as this digital blender. If I made Daniel's mysterious smoothie and I gave you a taste, you would not be able to figure out all the ingredients that went into it. And so that's this private key. You have this map on how to find the exact recipe each time. So you always can find your bitcoin.

And from that, you derive the public key, which is what you share. And it's kind of like an obfuscated version. So it's not a plaintext public key. But that's exactly what quantum computers are going to act on. They're going to see the lock. They know the public key. And they kind of reverse engineer and discover the private key. And then they can spend your bitcoin.

And so it's like, if you come back to the email example, you would not be able to exploit my email address unless you already knew it. So the key is the public key. And without that, you're not quantum vulnerable.

JIM: So making my email address, in that example, public is what would expose me to the potential threat.

DANIEL: Correct.

JIM: Got it. That was a lot in just a few minutes. And we're not done—time for your questions, too, at the end. But we do want to flash a really quick live poll for live viewers, just to make sure that you're roughly on the same page with us to test your knowledge. Again, that's just to the right of where you're seeing us talk right now.

And this is a true or false question. It's a yes or no. Today's quantum computers can currently break Bitcoin's cryptography. Vote A if you think that's true and B if you think that is false.

So, first, I'm going to check on that poll and see how people did. 90% of people said it's false. So that's good. That is correct. That is the right answer. Today's quantum computers are not powerful enough to pose this threat. And that should probably come as at least a bit of a relief to some investors.

But I guess the next question is why and when, potential. So, Daniel, let's have you talk a little bit about that. And then, eventually, in your answer, I know you brought a chart that can help tell some of the story as well.

DANIEL: Yeah. So, first, they have the time machine. They know how to build it. But they haven't constructed the hardware. And that's what's happening with quantum. We have quantum computers, but we haven't scaled it up to be efficient enough to break these computers. So let's just make an assumption that we can exploit these keys in a long time. And let's just say that's a year.

JIM: OK.

DANIEL: So the first cohort that's vulnerable is going to be these early-level bitcoin that were mined in 2010, 2011. And, remember, the public key is what the quantum computer acts on. And these early addresses were plaintext public keys. And so if you look at this chart in the light red here, they're called pay-to-public keys. And this is what Satoshi used. And these are forever vulnerable because the public key lives on the blockchain forever.

JIM: And the folks who have these, these are early-stage cryptographers, people who were experimenting with bitcoin, and, by the way, maybe collecting thousands of them over the course of their experimentation. And maybe they're just sitting in wallets and haven't moved, as you said, since 2010.

DANIEL: Yeah. They could be lost. The owners could have lost the keys. And so they're going to be forever vulnerable. But then the second cohort is reused addresses. So everything can be vulnerable if you expose that public key.

JIM: Yeah.

DANIEL: And so when you send bitcoin, you expose the public key until it's mined into a new block, and the reused addresses keep bitcoin on the exposed address.

JIM: OK.

DANIEL: Which you don't want. So the easy fix is just send all the bitcoin to a new address, and you're good to go. But then you come to the third cohort, which is what we call in-transit bitcoin. So, like I said, when you send bitcoin, you expose that public key until it's mined into a block. So every time that you want to transact, you're going to be vulnerable.

The nuance here is that let's say that it costs $1 million to run a quantum computer for 10 minutes, which it's probably a lot more today. But a quantum computer is not going to burn $1 million in order to steal $500 that we exchange between ourselves. So I see this problem much further off, something we don't really have to worry about today.

JIM: OK. Matt, sorry to leave you out for so long. We wanted to cover our bases with quantum there. What else would you add in general?

MATT: Yeah. Daniel, I think you really did a good job there of breaking it down at a technical level. I would just say probably at the highest level, it's important to know that, as we mentioned, and the viewers did a good job of picking up on this as well, is that quantum computers actually do exist today. They are just not capable enough to actually break Bitcoin's cryptography in the current state, or that of banks or the internet infrastructure broadly.

So it's a matter of acknowledging that the quantum risk is, in fact, real. We do have these quantum computers. But they are not capable now. The current hardware is not capable of actually breaking down that cryptography or posing an imminent risk or threat to the Bitcoin network or these wallet or address types in and of itself right now.

So, really, the idea is that we have Bitcoin, this decentralized community group of people, a bunch of different stakeholders involved in the network. And the idea is really coming together. And how do you actually come to consensus? How do you get people to actually agree on how do we move forward? It's all a matter of trying different solutions, seeing what the community as a whole really actually votes for or is encouraged by as a potential solution to this problem.

Because, unlike a centralized company, you might have some executives or a small group of people that could just make the decision today and say, this is what the upgrade is going to be. But, with Bitcoin, it's decentralized by nature. So it's a little more slower moving. Each proposed solution has its own trade-offs involved. So I think it's just a matter of trying and iterating and seeing what sticks.

JIM: Cool. I've got a couple more forward-looking questions that came in from viewers that I'm going to send your way, Matt. One is from Charles asking, "What's the future for Bitcoin?" So a nice big, fat, general question for you there. And then another that came in during a recent live chat asking, with the advancement of AI and quantum computing, do we think there will be increased security issues with crypto? Actually, I'd love to hear from both of you. But, Matt, we'll start with you.

MATT: Sure. Yeah, I'll start with the first. I think the future of Bitcoin is going to be much more mature and stable than what we've seen in the past. Bitcoin now is certainly the most mature digital asset out there. It has the longest track record. As we know, it's definitely been volatile in nature over time.

But, over time, we're seeing more and more maturity come to the space. And that is reflected in both price volatility, but also institutional involvement in building some solutions around it. So we have more institutional adopters, more robust custody and exchange solutions. And one thing that's really important to call out, too, is some of these spot ETP products that came to market, these are just one example of this broader institutional involvement in the space.

JIM: Incredibly popular.

MATT: Right. Exactly. In the first year alone, they combined to buy 900,000 bitcoin in these products. And that's about 4% of the total supply. And that's just in one year's time, right out of the gate right there.

And then we've also started to see these perpetual preferred equities pop up. And the cash raised from that was able to buy around 135,000 bitcoin as well, or about half a percent of the total supply. So we take that together, and we have roughly 4.5%, 5% of total bitcoin supply in these new rapidly innovating products that have just come to market in a very short amount of time.

And then we couple that with the fact that nearly 96% of all bitcoin is currently in circulation—and so this is really just to say that I think the industry, the ecosystem, Bitcoin as a whole, is really becoming more ingrained with the traditional financial system. And with that, becomes a little bit more of a mature industry. And, perhaps, we'll continue to see that going forward.

DANIEL: Yeah, and as far AI—

JIM: Yeah

DANIEL: It is going to cause a lot of security issues. I think it's already doing that today. But I think, as much as it takes away, it can also give back. And we can use AI to secure our apps and applications. And I might get some pushback for this, but I also think the quantum issue is largely solved. We have quantum-secure schemes today.

They're just a lot harder to implement on something like Bitcoin because it's decentralized. We can't just look at a CEO and say, hey, this is a problem. We need to fix it by next quarter. We have to have consensus. And I think there are a lot of threats from AI and from this quantum. But as a community, if it were timely, all of our funds are at risk, we're now very motivated to come and fix that. And I think we would.

But if you imagine redesigning a car, and you want to cool down the cabin, the easiest solution would be to take off the windshield, let a nice breeze come in. But tomorrow, if it's raining and you're driving down the highway at 60 miles an hour, that's going to hurt.

JIM: As will the bugs.

DANIEL: Yes. So that the easiest, quickest solution is not necessarily the correct one. And that's what developers are looking at. They want a solution that everybody can opt in to, pick what they want, pick and choose what applies to them. If you don't think a quantum threat is a year away, you don't have to upgrade or do anything. And if you do, you can opt in, pay a little bit more in fees. But you're going to have trade-offs.

And so I see a future, just like we saw on the previous chart, where there's all these signature schemes. You're going to be able to choose and apply what matters to you.

JIM: OK, so alongside quantum, we have unanswered questions that we get kind of a lot here on the livestream about the Bitcoin mining space in general. Bitcoin's block reward is set to halve, once again, in about two years, give or take. And that's going to put additional pressure on miners. So Matt, I'm curious how you see this issue, in general. Again, it's a pretty popular one with people who watch this show, at least.

MATT: Yeah, absolutely. And I think we have a nice chart to speak to here, as well. If we look at this chart, we see this kind of orange, squiggly line and this turquoise, bluish line, as well. And that's really in reference to the right side, the right axis there, really referencing what you mentioned, Jim, the fact that block rewards are coming down over time by design.

JIM: Right. It was built to do that.

MATT: Exactly, every four years, that's where that gets cut in half. And that is absolutely by design to be disinflationary in nature. So in Bitcoin terms, miners are earning less revenue over time. And so that poses that fundamental problem. Well, what happens when that runs out? Or what happens when that diminishes too low? I think, first, it's important to call out that the last bitcoin will ever be issued or mined or released into circulation in the year 2140. So certainly, there's a lot of time before that happens. Of course, we're going to feel the effects over time, especially those less-efficient miners.

But there's a few different ways of thinking about this, I think. One is going back to the institutional aspect of the space, the maturity of the space as a whole. If we look towards that future, and Bitcoin is really being widely adopted or adopted at scale, it's likely that the price would be substantially higher, that there will be more demand for Bitcoin. With that would drive more fees to Bitcoin that miners can actually make revenues off of those fees, as opposed to just that block subsidy. So that's certainly one aspect of it, as well.

And then I think, when we look towards the future, some of the biggest stakeholders that have the largest economic incentives might actually be willing to even mine bitcoin and dedicate resources towards mining bitcoin at a loss. And that can be custodians, exchanges, or large corporate holders that really would actually expend some of those resources, even mining, at a loss just to secure the network.

JIM: Just to keep it secure.

MATT: Correct.

JIM: OK, a couple more questions that came in from viewers. One from David, asking, "Will bitcoin and other currencies ever go away as some experts predict?" And then another from a recent live chat—when do we think quantum computing will pose a real risk to Bitcoin, and how should we hedge that risk? I'll ask both of you to weigh in on that. And Matt, we'll start with you.

MATT: Sure, yeah. I think, when we unpack the first part of that, when we think of currencies as they exist today, the majority of which are these fiat currencies issued by governments, the average lifetime of a fiat currency is roughly 27 to 35 years before being subject to hyperinflation, mass devaluation, or revaluation. So it's a lot shorter than you might think.

JIM: I was thinking about this. It wasn't that long ago that we were spending francs in France and lira in Italy. And those straight up don't exist anymore.

MATT: Sure.

JIM: That's not the currency.

MATT: Exactly. And I think you're on to something with that thought. Because I think the way that we see a lot of these fiat currencies today likely won't be the way that they exist in the future.

JIM: Sure.

MATT: And so Bitcoin is the counterargument to that or the alternative to that environment. And in a sort of Bitcoin standard type of future, you have this provably scarce digital asset where only 21 million bitcoin will ever exist. It has that fixed supply component, which all of these fiat currencies really don't have. And so with that, it's perhaps a little bit more predictable if you're looking to store your wealth or preserve that wealth in something over time. And so I think that that is certainly something that perhaps would be more attractive to people in the future.

And then when we look at, again, the overall maturation or adoption side of the equation, a lot of us use fiat currencies today because it's what merchants accept. It's legal tender. It's what you got to pay taxes in.

JIM: It's easy.

MATT: It's easy. It's convenient. It's easy. And it seems like the world is set up for it. Whereas, in that bitcoin standard, it's a lot harder to find a merchant that regularly will accept bitcoin for everyday transactional purposes. So I really think, in order to get bitcoin into that kind of everyday currency conversation, it needs to be a lot more convenient for everyday usage.

JIM: It doesn't have to be 0 sum, either. We don't have to picture a world where everybody is only ever spending bitcoin. That's not what you're saying. You're saying that there's ebb and flow to the number. Just expect changes. And I don't know what else you would add to that.

DANIEL: Yeah, I agree that state-issued currencies may be on the decline. But it really comes down to education and apathy.

JIM: OK.

DANIEL: I have plenty of conversations with friends or family or even business meetings where I can explain what is money, what's happening, and how money is being devalued. And either they don't have the time to really think about a solution, or they just don't care that one might exist. We could show you 10 different data points that show why a better money is required.

And I would encourage listeners at home, just Google how much purchasing power we've lost from generation to generation or even over the last five to 10 years. I remember, back in college, I could eat at a fast food for 4 or 5 bucks, a whole meal. And now that's going to cost you $10 or $15.

JIM: Easily. Yeah.

DANIEL: And the meals are not getting better. They're not—

JIM: They're not getting bigger. They're not tripling in size. Right.

DANIEL: It's not two or three times better, but it costs two or three times more. And I think a lot of people understand that, but they don't understand why. And so until governments stop printing money, I think bitcoin is going to remain relevant.

JIM: OK, through that lens, then, in a world in which that's the case and in a world in which there are quantum computers that could be getting increasingly powerful then, what options does Bitcoin have then?

DANIEL: Yeah, I always joke around. At the most basic level, if the quantum computer is attacking a public key, let's just toss out the public key. But that's not really how it works.

JIM: We need that.

MATT: Yeah.

DANIEL: Yeah. But there are a lot of downstream effects from adopting quantum signature schemes. One of them is larger sizes. And Bitcoin is notoriously resource constrained. We already can do seven to 11 transactions per second. If we increase the amount of the transaction size, you're going to fit even fewer into a block. But there are solutions that are being discussed. We're having this conversation now. And I think that shows, as a community, we're headed in the right direction. And the solution will be found sooner than later.

JIM: Matt, what would you add?

MATT: Yeah, I would largely agree with that. I think it's all a matter of trade-offs. Again, you have this decentralized community all working towards finding what works for everybody collectively. And so it's a lot of iterating right now, a lot of throwing out random or proposed solutions to see what people are actually essentially voting for, essentially what they actually want, what they value the most.

There's different trade-offs in terms of fees. There's different trade-offs in terms of sizing, in terms of how things are going to fit into certain blocks. And so it's really just a matter of iterating, again, acknowledging that larger quantum risk that it does exist today but leaving it up to the community to keep trying these different solutions to see how we'll go from here.

JIM: Getting a lot of—oh, sorry, I cut you off.

DANIEL: I was going to say, you could add complexity to that. I could go into a whole show about stateless versus stateful signature schemes. But users don't want to have to deal with that. And so that's what developers are really looking at.

JIM: Got it. It kind of makes my head hurt a little bit to even think about it. So we'll skip that for now. Mike's question during registration is a great one. Looking for a timeline for when quantum computers might in fact achieve the capability to access Bitcoin accounts. And let me look really quickly. I can see Andrew has that exact question in the live chat. How much longer do you believe we have before quantum makes a noticeable impact on our lives?

DANIEL: Yeah, so the issue with predicting that is innovation and breakthroughs are largely stochastic events. They're completely random. Otherwise, we'd be making a lot better investments.

JIM: Right, right.

DANIEL: But I find myself in between the quantum experts that think maybe early 2030s and then also, on the other end of the spectrum, cryptographic experts that are saying the hardware could never exist. We will never be able to scale up to that size.

JIM: Never.

DANIEL: And yeah, so I think it's OK to be skeptical. But we should be aware. And we should be prepared. And like I said, we're having this conversation. We know that there's an issue or a potential issue. And as long as we're moving towards a solution, I think one will exist before it's needed.

JIM: OK. Matt?

MATT: Yeah, agreed. I would say that, as we've touched upon, the quantum computers actually do exist today but just in such, insignificant relative capacity to be that that would break the cryptography of Bitcoin, banks, the internet infrastructure as a whole. And so I think it's important to, again, acknowledge that risk. But, also, think about it in terms of, it's not necessarily a near-term, existential threat to bitcoin or the network or to wallets right now.

Rather, it's a longer-term discussion around governance consensus—again, weighing those different trade-offs and coming to terms with, what does the community actually want? How do we try these different signature schemes and different transaction types? It's really phasing in these different ideas and how you can eventually phase in address migration and the flow of funds to more quantum-resistant addresses in the future.

JIM: Excellent. All right, and so with that, we're going to head over into the live chat. We already grabbed Andrew's question. Let me see. Here's another one. This is from Matt. What is the biggest realistic quantum computing threat to Bitcoin—mining, wallets, or cryptography?

DANIEL: So they kind of overlap there. It wouldn't be mining. That's a completely different problem. And you can look up Grover's algorithm. But it doesn't apply here.

JIM: Grover's algorithm.

DANIEL: Yes. And as far as cryptography, again, it's that public key. So the biggest threat is you've exposed a public key, either by being Satoshi and having a million bitcoin and not moving it since then.

JIM: Not me.

DANIEL: We don't know.

JIM: But it's true. I wouldn't tell you if it were. Go ahead.

DANIEL: Reusing addresses—or in that 10-minute window when you're trying to get confirmed into a block.

JIM: A question from G—going back to the earlier discussion on cryptography, can you give a high-level definition of what quote, "complex math that needs to be solved" means, please? So this is a question I think for either or both of you.

DANIEL: So yeah, it quickly gets complex. Google P does not equal QP, I think it is, or NP? But basically, you have this elliptical curve. And I'm already getting way too complex. I'm sorry.

JIM: Matt, do you want to take a swing?

DANIEL: Yeah.

MATT: Well, when we're talking about it in the context of mining, you're essentially guessing, hashing, to try to get to a certain number, a certain output. And so the complex math there—maybe under the hood it's a bit complex. But at least in the context of mining here, you're really just guessing, guessing, guessing, guessing, guessing over and over again to try to get a certain output, a certain number preceded by a whole bunch of zeros in front.

JIM: And that's what mining is. When we talk about mining, it's a very energy-intensive—

MATT: Correct.

JIM: —way to guess the right solution to verify a block.

MATT: Exactly. And that gets at their question—is that it is very complex under the hood, in terms of what the algorithms and the hashing and everything going on there. But in simple terms, you're really just guessing, using huge amounts of compute to guess over and over and over again, to try to get that output. And essentially, that output is what solves that block and then gives you the right to add transactions to the next block, add them to the blockchain, get compensated for doing that, and therefore securing the Bitcoin ledger.

DANIEL: Yeah, in the context of mining, it's literally just comparison. Is this number lower than this number? And so the network sets an arbitrary number that's difficult. And we just attempt to find a number that's lower than that. And you run that through a hash algorithm. You say, this is over or under. If it's under, someone else does it, like the combo lock we talked about earlier.

JIM: Yeah.

DANIEL: You just try the combo lock. Everybody agrees that it's lower than this number. And you can mine a block.

JIM: I'll put in a shameless plug, as well, for Fidelity.com/LearnCrypto. Because to be honest, if what we're talking about here doesn't make sense or only part of it does, that's almost not by design, but it's pretty common. It's almost like learning a foreign language after a 45-minute show. You're not going to. You're going to pick up pieces of it. But then you continue learning and reading and looking at FAQs and watching other videos. So Fidelity.com/LearnCrypto is, I think, one great way to continue that.

Kristen has a question. Does or has AI sped up the development of quantum computers? What would you say?

DANIEL: I'm not entirely sure. I would think so. We're seeing AI speed up a lot of other calculations. And on the other side, I think AI does a lot of re-creation what humans have already solved, but it doesn't do its own thinking yet. And that's where things will really, really speed up. But until then, it's just rediscovering or trying problems humans have been doing for decades now. It's not creating new ones.

JIM: So here's a great question that's a follow-up to that from a viewer named Gary. And this is something we were talking about when we were building the show. And we were thinking, do we even touch on this? But it came up in a question. So we get to.

Gary's asking, does quantum computing only exist to break Bitcoin computers? Or is there some other beneficial use for it? What's the goal for quantum computing to help develop things regular computers cannot do? Because right, the whole conversation here has been about the threat of quantum, and how real is that threat? But is there a pro side to the con argument? What could quantum do that isn't mentally going to terrify us?

DANIEL: Yeah, so I think it's going to help speed up calculations. So if we're trying to figure out a cure to cancer or chemical compounds, it's going to be able to do all those parallel computations much quicker than a classic computer. And to answer if it's built just to attack Bitcoin, no. It costs a lot of money to build these computers. And bitcoin's worth $1 to $2 trillion right now. So that's a limited takeaway.

JIM: Sure.

DANIEL: Whereas, if you wanted to attack the entire internet, encryption as a whole, that might be more profitable. Because it's just hard to tell which is worth more, a state secret or 1 bitcoin? It really matters to the end user. I'm not going to do anything with a state secret, but I might enjoy 1 bitcoin.

JIM: Same. But again, it's this idea that research takes X amount of hours or months or weeks or years. And maybe with efficient quantum computers at your disposal, you can—you talked about cancer. But what else might it be useful for? Does anything else come to mind?

DANIEL: Yeah, just I think calculating chemical compounds. So you could create new foods. I'm not sure what they're trying to do, because I really only care if they break Bitcoin or not. But I think there's a plethora of opportunities for quantum, just how classic computing opened up doorways to the internet for us.

JIM: Got it. OK, well, that makes—I got that one. Another question from Matt—not sure if it's the same Matt from before. But he's asking, what's more likely over the next 15 years: Bitcoin successfully upgrading to quantum-resistant cryptography or quantum computing advancing slowly enough that no urgent upgrade is needed?

DANIEL: Impossible to know.

JIM: Sure.

DANIEL: I would guess that Bitcoin would upgrade, just because it's better to have a solution to a nonexistent problem than to need one and not have done any of the work. So if quantum is accelerating or even moving slowly and never actually has a problem, because Bitcoin is completely opt in, you can either use a quantum-secure digital scheme and pay higher fees, or you can keep your bitcoin where it is now and be completely safe.

JIM: Got it. Are there any cases of AI being used to break the Bitcoin blockchain? That comes from Brent.

MATT: I haven't seen any specifically of breaking the Bitcoin blockchain. Maybe it's a good time to plug, too, that the Bitcoin network itself, or blockchain, has a 99.99% uptime in its entire history dating back to 2009.

JIM: And uptime means what?

MATT: Just being online, being fully functional, being completely operational. I think the one time there was just a simple bug, where there was some inflation involved. That was quickly rectified. And that was way, way in the earliest days of Bitcoin. But the idea there is that, whether it's AI, quantum, something else, Bitcoin has been highly resistant by its code base. It's simple. It's ossified. It is slower to move and innovate, because it requires more of that consensus, that community-driven response to some of these issues.

And I think, Daniel, as you mentioned, if there was that imminent threat to Bitcoin today, in terms of it breaking, that we'd see much faster migration, perhaps. But it is acknowledging

that, whether it's AI, quantum, some other risk out there, there's trial and error of throwing these solutions out and getting the community to come to some agreement on what we might like to do or have the options to do in the future. But just thinking about Bitcoin back to 2009, it's always been up and operational and functioning as intended.

JIM: All right.

DANIEL: I would add, Bitcoin's greatest feature is probably what everybody hates about it. It's boring, and it's slow, and it's simple. You can send and receive bitcoin. And that's all you can do on the blockchain. Where the attacks are surfacing now in the past even two months are layers on top of Bitcoin.

So if we built a service where we can transact bitcoin offline, not going through the blockchain, you pay lower fees, transactions are a lot quicker. But we have a bug. AI could potentially find that bug, exploit it, steal the bitcoin that were on that layer, but it could never touch the layer 1 blockchain. Because that is very simple. There's a lot fewer vulnerabilities. And it just hasn't happened yet.

JIM: Cool. So separate but related, we do have a full livestream episode that talks about Fidelity Crypto's custody and security. So if people have questions about that, we would definitely suggest you check out Fidelity.com/CoveringCryptoLivestream. That's where you'll find our full library of other shows with a much, much deeper dive on the specifics of Fidelity Crypto with regard to custody and security.

This was a big topic. And I appreciate you both being willing to try to explain it in ways that I could understand and, therefore, hopefully viewers could understand. Thank you.

DANIEL: Yeah, happy to be here.

MATT: Yeah, it was fun. Thanks for having us.

JIM: Sure thing. And thanks, also, to our viewers for signing up, for showing up, for sending in your questions beforehand, and for voting in our polls, and all the things we ask you to do. We really appreciate it.

If you do have immediate questions that you want help with, you can always also join the conversation and the community over on Reddit at r/fidelityinvestments. That's a great place to be.

On behalf of everyone behind the scenes here at the *Covering Crypto Livestream* team, thank you again for being here. And we do hope to see you again next time.

Fidelity Crypto® is offered by Fidelity Digital Assets®.

Investing involves risk, including risk of total loss.

Crypto as an asset class is highly volatile, can become illiquid at any time, and is for investors with a high-risk tolerance. Crypto may also be more susceptible to market manipulation than securities. Crypto is not insured by the Federal Deposit Insurance Corporation, the Securities Investor Protection Corporation, or any other government agency, and is not an obligation of any bank. Investors in crypto do not benefit from the same regulatory protections applicable to registered securities.

Fidelity Crypto® accounts and custody and trading of crypto in such accounts are provided by Fidelity Digital Assets, NA, which is a national trust bank.

Brokerage services in support of securities trading are provided by Fidelity Brokerage Services LLC ("FBS"), and related custody services are provided by National Financial Services LLC ("NFS"), each a registered broker-dealer and member NYSE and SIPC.

Neither FBS nor NFS offer crypto as a direct investment nor provide trading or custody services for such assets.

Views expressed are as of the date indicated, based on the information available at that time, and may change based on market or other conditions. Unless otherwise noted, the opinions provided are those of the speaker or author and not necessarily those of Fidelity Investments or its affiliates. Fidelity does not assume any duty to update any of the information.

As with all your investments through Fidelity, you must make your own determination whether an investment in any particular digital asset/cryptocurrency is consistent with your investment objectives, risk tolerance, financial situation, and evaluation of the digital asset. Neither Fidelity nor any of its affiliates are recommending or endorsing these assets by making them available.

Fidelity does not provide legal or tax advice. The information herein is general in nature and should not be considered legal or tax advice. Consult an attorney or tax professional regarding your specific situation.

This information is intended to be educational and is not tailored to the investment needs of any specific investor.

Spot crypto ETPs are for investors with a high risk tolerance and invest in a single cryptocurrency, which are highly volatile and could become illiquid. Investors could lose their entire investment. Spot crypto ETPs are not investment companies registered under the Investment Company Act of 1940 (the "1940 Act") nor are they commodity pools under the Commodity Exchange Act of 1936 (the "CEA"). As a result, shareholders of spot crypto ETPs do not have the protections associated with ownership of shares in a registered investment company nor are shareholders afforded the protections of investing in an CEA-regulated instrument or commodity pool.

Past performance is no guarantee of future results.

Diversification and asset allocation do not ensure a profit or guarantee against loss.

Fidelity Crypto and Fidelity Digital Assets are registered service marks of FMR LLC.

Fidelity Brokerage Services LLC, Member NYSE, SIPC, 900 Salem Street, Smithfield, RI 02917

© 2026 FMR LLC. All rights reserved.

1290313.2.0