XX Network, Messari Research & Algorand Discuss the Advancement and Threat of Quantum Computing to Blockchain Networks

Monday January 20th, 2025 4:30PM UTC

SPEAKERS

Darren Moore (Host), Rick Carback (XX Network), John Woods (Algorand), Mohamed Allam (Messari Research)

Darren Moore 00:05
Bear with me for just one second.

Darren Moore 00:19
Alright, so today we're we're just setting everything up, putting out some... waiting for some people to come into the chat, and just making sure that the links are up.

Darren Moore 00:31
But today we have a discussion on quantum technology, with everything that's happening. Willow came out and kind of caused almost like a little hype bubble. You see it in equities. There's a lot of the quantum stocks taking off, and a lot of people are asking questions about, what does this mean to the crypto community? So wanted to gather some of the leaders in the space and just speak about what, what's real, what's not and I wanted to start off with just an introduction. Rick, would you like to start off?

Rick Carback 01:07
Sure, thanks for having me. My name is Richard Carback. I am a cryptographer. I worked with David Chaum for many, many years. Helped him co found the XX Network, and right now I'm working on a stealth project, doing something in quantum, post quantum cryptography, which I am just going to be, you know, nefarious about.

Darren Moore 01:28
And John an intro for yourself.

John Woods 01:31
Yeah, sure. So I'm John Woods. I'm the CTO at Algorand Foundation. Algorand's a layer one blockchain. And my background over the last decade has really been working on software architecture engineering and applied cryptography. And so that is, unlike maybe Richard, who is a full cryptographer, where he invents new primitives, I take the output of people like Richard and I combine them together to make interesting systems. And so Algorand has some post quantum security. It's something I feel very serious about, because all of these blockchain networks typically are protecting

large amounts of dollar assets, if you like, you know, billions of dollars, hundreds of millions of dollars, in some cases.

John Woods 02:05
And so it's critical that there are hard systems that are, you know, difficult to break, and we need to be prepared for threats like quantum and other things that come down the road that threaten the modern cryptographic standards that we use today. So quite excited about it. We're doing some work on Algorand To make it even further resistant to quantum attack, and we have done some work already, so happy to talk about that later.

Darren Moore 02:28
Thanks John and Mohamed, can you give a brief intro?

Mohamed Allam 02:31
Yeah, for sure. I'm Mohamed. I work at Messari right now. I do protocol research. My background is mostly in AI. I used to work in aerospace before coming here on a lot of proprietary AI models, and quantum has kind of piqued my interest this past seven or eight months, and I've been doing a bit of research and talking with some folks at U Chicago, considering it's been a hub for quantum computing. And yeah, being in crypto over for 10 years, you worry, you know, is there a potential threat? But that's, I guess, what we're here to talk about today. So let's get into it.

Darren Moore 03:09
Yeah, so I'm wondering if it's almost overblown, the quantum hype. It's like there's so much resources that are needed for the hardware to take place. It needs temperatures below zero degrees. You need almost like a film, like an MRI for the data, because it's more than ones and zeros. So do you think this is a little bit overblown, Rick, or do you think this is more reality?

Rick Carback 03:36
You're describing the state of the world maybe 10 years ago, you've got photonics projects, I think RIKEN just released one which had error rates similar to Willow, with a, what they call is a 1000 qubit equivalent. And, yeah, most of the superconducting projects do need below freezing, you know, very cold refrigeration.

Rick Carback 04:03
But that's not outside the realm of possibility for a government or even, you know, a large university.

John Woods 04:10
Precisely. And so just to follow on that, I would just say the threats here are not some script kiddie idiot, you know, in his mom's bedroom, you know, working on a home computer trying to drain Bitcoin accounts. This, for me, is in the in the in the initial phase, it will be nation state actors. It'll be, as you know, Richard said, governments and indeed, potentially well funded agencies and but that's still a very real threat. And so, you know, it'll be a long time before we have these things as GPU, like cards that we can insert into a general purpose computer in order to speed up certain algorithms, but I think that that might come in 100 years, or something like that.

Mohamed Allam 04:45
Yeah, I think following up on Richard's mention of Photonics, it's important to consider that, you know, reaching near zero Kelvin is is very difficult task, and if you could switch to a alternate Qubit mechanism, such as photonic qubits, you would have an accelerated growth of the potential of you know what we're seeing with quantum now, just photonic qubits. The difference here is they don't need to be cooled to the absolute zeros or near absolute zeros. You can't really reach absolute zero, but very close to absolute zero. So, yeah, photonic, photonic qubits are something we should all be looking out for.

Rick Carback 05:27
I just want to touch base on the on the error rate, right? That's, that's the significant news with Willow as well as RIKEN. I encourage people to look that up. That's, that's 100x improvement. They went from, you know, 99.9 right? And they added more nines to that, which is incredible. What that does to the actual mechanism of how these algorithms need to be implemented is it significantly reduces the number of physical qubits you need to implement these gates. So, I think people get confused with qubits. They think, oh, it's like the bit size of my computer. My computer is like 128 or 64 bit. But that's not really the analogy you should be drawing. The number of qubits is more closely to the number of transistors on a computer.

Rick Carback 06:16
So we're going to see a Moore's law-like exponential scale up eventually. It's just a matter of, they got to get that error rate down to a factor where it matters. And now they're in striking distance of that. And then you're going to see the qubit density essentially explode once they figure out how to do that.

John Woods 06:34
And you know, maybe, let's just take a step back for a sec, because clearly your guests and lovely to meet you. You guys are very knowledgeable. I can tell already is this probably the best panel I've ever been on on quantum. Usually the people have no idea these guys know what they're talking about. So this is interesting, but maybe let's take a step back for your listeners and maybe frame what we're talking about a bit when we talk about error rates and all that kind of stuff.

John Woods 06:56
Normal computers like your MacBook, your iPhone, your Android phone, your Windows PC, they process data as ones and zeros, I mean. And why is that it typically? I think it probably came from the fact that, as Richard just said, they use transistors, right? And transistors use voltages, and voltages are five volts for a one or kind of zero volts, or close to it for a zero, right? And so that's why computers, they talk and think in ones and zeros, because they use voltages to represent data.

John Woods 07:22
And so what is a qubit? What is a quantum computer? And how is that different to the general purpose computer I'm used to carrying in my pocket or on my wrist? And so the answer is, you know, at a very high level, without getting too sophisticated, a quantum computer is a type of machine that harnesses quantum physics, in a nutshell, in order to do a handful of calculations extremely, exponentially faster than normal computers. Okay? Now, it's not everything. It's not going to make Doom have more frames per second. It's not going to, it's not going to, you know, make your web browsing experience smoother. This is about certain algorithms. They tend to be factoring large semi primes, factoring numbers, or indeed, searching, as the guys are well aware, searching through unsorted data sets. We have a

handful of quantum algorithms, and quantum computers just run them, but those algorithms can be applied to destroy many security systems that we rely upon today, and we can jump into that in a minute.

John Woods 08:19
And last thing I would just like to say, I said earlier, a bit is a one or a zero, a five volt, or kind of a close to a zero volt. A qubit is like a bit, except for it's kind of a one and a zero at the same time. And of course, how can that be? And the answer is, you have some blend of probability. So it's either like 50% probable, a one, 50% probability of a zero at the same time, or maybe 70/30, or 90/10, but the whole idea here is that these algorithms I spoke about before, which break modern cryptography and security, they can exploit this notion that data is in this state of like, not very sure, floating around in this (we call it a superposition), in order to exponentially speed up certain attacks and so that, just to frame it for folks who maybe are coming to this completely fresh, this is a type of computer with a very specific application, but one that's going to stick a knife inside things like Bitcoin, etc. Okay.

Mohamed Allam 09:14
Yeah, and if you want to think of it in a simplified manner, too, consider two potential mazes, one is a traditional computer and one is a quantum computer. When you're trying to get to the end with a traditional computer, you're going in through the maze, and you're tracing your way back through every potential outcome. Quantum Computer having the nature of being able to be at zero and one, at the same time, goes through that maze in a fashion to which it (think of it this way), it could split in a way that it doesn't have to go and retrace back through the maze to know what the potential next step is. It will just move through the maze exponentially faster, simply because it doesn't need that extra step to go back. So, yeah, a simplified way, I guess.

Darren Moore 10:05
So let me make sure that I have this correct. It's, it's only, only certain things that quantum is really good at. It's not like you can compare a super computer to a quantum computer or PC, it's, it's just certain problems that it's great at. Is that accurate?

Rick Carback 10:20
Yeah, like a graphics card is really good at, you know, mining and, you know, rendering, right? It's a purpose built tool.

Mohamed Allam 10:28
Can't trade the meme coins with a quantum computer.

John Woods 10:33
And this is because, I mean, Richard, actually, I do, you know, and Mohammed, I defer to you, I believe this is because we have defined quantum algorithms, like Shor's or Grover's that do, you know, factorization or searching, and maybe there's other quantum algorithms out there we haven't discovered yet for other tasks, but as we currently understand that we've only have a handful of useful quantum algorithms, right? Isn't that? Isn't that the case? Essentially?

Mohamed Allam 10:57
Yeah, yes. And they're also very expensive to develop better and better algorithms. That's been a huge roadblock, especially because a lot of this is driven by academic institutions, rather than, you know, VC

backed quantum firms, and we could get to that more. So developing these algorithms that would fit the requirements has been a bit of a task. So, yeah.

Rick Carback 11:20
There's a lot, there's a lot of simulation, chemical simulation, protein folding, that kind of thing. The nature of it has to be something where you can kind of define what the end point is, and then work backwards from there. I know that that's not completely true, but if the characterization of your problem is we know that this substance exists - how do we get there? Then, in general, you can, you can presume that a quantum algorithm can be made for that, yeah.

Mohamed Allam 11:49
Think national laboratories, right, like a Los Alamos or something of that nature, that they'll be able to make use of these in the short run to run, maybe biological based quantum simulations, or physics based quantum simulations, things that are beyond the normal use of a normal computer, I guess, right?

John Woods 12:11
And maybe, you know, Darren, maybe another thing we could maybe move to now is, well, this all sounds great, but why haven't we built this thing yet? And so, you know, maybe I'll hand over to the guys as well to discuss, you know, the difference between a logical qubit and a physical qubit. And I think this is something that people maybe don't really follow along with. As Richard said a little while ago, the number of qubits, talking about a quantum computer, is really a lot more like the processing power, a lot more like the transistor count, right? It's like the sophistication of the of the CPU, if you like, in a way. And so the thing is, things like Willow, they may be 1000 qubits, but in reality, those 1000 physical qubits may only come together to form a functional error free logical qubit that can do some interesting work. And so we need not 1000s of physical qubits, but 1000s of logical qubits in order to really attack some of the modern cryptography that we enjoy today. You know, guys, would you join and maybe talk about that a little bit from your experience?

Rick Carback 13:05
Yeah, let me hit you with a factoid that I think scares people, which is the D-Wave Advantage2, has 7800 physical qubits - you only need if they were perfect qubits, 1673 to break pretty much all cryptocurrency. Now, it turns out, because of the error rate of the D-Wave, it needs roughly 5 million or so qubits for that to actually make that - physical qubits - to make that work. But as these error rates come down, they significantly draw that down.

Rick Carback 13:40
I think if we were, if we're believing the Google Willow stuff, which I think we should, we're talking a few 100,000 now, from 5 million, that's a huge drop, right? I don't think people fully understand, because they're like, oh, it's only, only 105 qubits. It's like, no, they got the error rate working, and they have this claim, which really just changed my mind on all of this. I'm on record saying, Oh, it's still like 10 years on the optimistic side, 15-20, most likely, right? No, no, once they get this error rate going. And Willow specifically makes this claim in a couple of publications, and I really want to investigate it more, which is, as we added qubits, the error rate went down. That's true. Like the game is over. You're talking, you know, potentially two, three years out.

John Woods 14:27
Totally agree. And so, and so this is the exciting thing. So, the real innovation, as the guys have already said, with Willow, is, just simply that normally, it's like a Jenga tower, you know, the more of these things you add, the more qubits you add, the more wobbly it gets, and it falls over. It undergoes decoherence, you know, it doesn't. It doesn't stay in its magic quantum state, doing its magic thing. Whereas what Willow basically said is, hey, the more of this stuff we add, the more stable it gets, man. And so that's a profound thing to say. And I also have had no time with Willow other than the press releases, of course. But if that is true, as Richard just said, that is a profound thing, because it means, if they can scale out what they've got, it scales out stably, and it scales out in a way that they can build quantum computers with teeth, as I kind of like to say, ie, things that can do useful work, so interesting.

Darren Moore 15:15
Well, I mean, so what do decentralized communities need to do? It sounds like this is closer than most people are thinking. What do a lot of the communities need to do in order to protect themselves from the threat?

John Woods 15:32
Maybe I can start just, you know, working at Algorand and having previously worked on Cardano professionally and prior to that, Ethereum. Essentially, you can carve these blockchains, crudely up into the ledger piece, the network piece and the consensus piece. And there's bits of cryptography sprinkled here and there across most of these chains, but you got to kind of look at it under those guises and then say, well, what do I need to change in order to kind of make this thing quantum secure? And so for Algorand, just as an example, and I think it's pretty applicable across the board. You need to secure the ledger history, because that's been using regular cryptography, right?

John Woods 16:09
Some blockchains have a secure ledger already. Hedera uses SHA 384, which is, you know, strong ish, you know, 128 bit strong in the context of a quantum computer assuming kind of a rooting, or cube rooting, of the of the of the bit strength with Grover's. Then you got to look at the accounts, right? So from Bitcoin to Monero to Algorand to whatever Cardano, they all use elliptic curves. They use standard elliptic curves to find over finite fields in order to digitally sign transactions. And like a quantum computer will will shred those things like, it'll solve 256 bit elliptic curve cryptography, not in two to the 256 steps, but in 256 steps. So that's r ather than, like, quattuordecillion steps. It's like, you know, a couple of hundred steps. And that, that's very scary. Richard, you want to maybe add to that?

Rick Carback 16:56
Yeah, to clarify, there's always this question of how fast they'll be able to break them, because certain protocols would be secure. If it's, you know, good for longer than an hour or two. And that's true. It's, it's likely, given the the physical constraints, it's like, you know, nanosecond level for them to cycle these qubits, and when you run, and that works out to be like a microsecond to 100 microseconds per gate. When you, like, map that out like, the fastest you're talking is a few hours at best, more likely you're talking eight to 16 hours in that timeframe. So there's, there's going to be some time in terms of, well, we can run this protocol, and as long as, like, the quantum computer is not fast enough to keep up, then we're still safe.

Rick Carback 17:44
And that that is true for things like, oh, I want to, like, do a Bitcoin transaction... And remember, Bitcoin is now almost all Pay-to-Public-Key-Hash, right? So as long as all of my unspent transaction outputs are brand new hashes that have never been used with a public key which has been exposed, then I'm safe.

John Woods 18:03
You're saying that with Bitcoin as an example, this is a question for you. If you create a fresh account offline, right? You get the receive address. You send your Bitcoin fully to that, all your Bitcoin, and you never spend from that account. You essentially never reveal the public key. So there's no target for the quantum computer. Is that fair to say?

Rick Carback 18:19
Yeah, so there's some level of protection there. But I would argue that, you know, when you get quantum computers, they're also going to have - you're playing this game where my transaction is going to get through the transaction pool faster than the quantum computer can't get there. And I would argue, no, the quantum computer potentially has an advantage on the hashing, not a significant advantage. Hashes are still like considered post quantum, but that's better than traditional. So maybe they can make that guess faster, and maybe they can rewrite the chain going back a day, in which case that protection isn't really there.

John Woods 18:53
Right. And so, you know, here's what I would like to say... what I like better than some of this protection that Richard has described, where it's a little bit kind of by accident, or, you know, as a side effect of some property, I like more direct protection. And so that's what Algorand is kind of going for - i.e. post-quantum cryptography, the kind of stuff that cryptographers work on using new mathematical hardness, right? New trap door functions, new ways to make things hard, both for normal computers and these quantum computers. And so we have a bunch of different approaches to this, which I guess the guy could speak to maybe in more detail, having worked on it, but Algorand is using Falcon. And so Falcon is a type of lattice-based signature, and it uses the hardness of many dimensional lattices in order to make a system that's hard for regular computers and quantum computers. And so as an example, Algorand has secured the history of the ledger with these signatures. Every 256 rounds, we kind of sign the ledger to say, Hey, this is cryptographically good with this post-quantum signature, but we still have vulnerabilities, and so we're vulnerable on the accounts.

John Woods 19:57
So Algorand uses normal elliptic curves in the accounts, and they are vulnerable. Okay, we have to upgrade them to a PQ, a post-quantum scheme. And also Algorand talks a lot about its consensus giving instant finality. And so that is true, but Algorand's VRF, that allows this consensus mechanism is itself built on elliptic curves, and so it, too, needs to be upgraded to be a post-quantum VRF. And so this is the type of work that we're looking to do today.

Mohamed Allam 20:21
And taking a step back, I think, going back to Bitcoin. And that mentioned - everybody... Bitcoin is front of mind when people think of quantum whenever I have a discussion that brings about the quantum breaking, post-quantum world, people always ask, you know, well, what about Bitcoin? And it's important to address that there's three means to which, you know, Bitcoin can be potentially broken, or

for simplifised terms people to understand whether it be the hacking of the wallets the private keys becoming compromised, breaking the mining so proof of work itself, which is much less likely. And then finally, you know, double spending and manipulating the transactions on chain as well. And throwing this back to you guys, you know, on the point of Bitcoin, how do we switch the trajectory here? Because if anyone's going to hack anything, I don't think, I mean, not hack, break, I guess it's probably going to be Bitcoin, but the chances of that even happening are probably very unlikely.

Mohamed Allam 21:22
What does, what does bitcoin do? Right? What does Bitcoin do? There's no way the community comes to consensus on anything. Or there's, you know, saying, Well, we're going to use all our network power to.

Rick Carback 21:34
You say it's unlikely, I say it's most likely.

Mohamed Allam 21:37
You think so. I don't know?

Rick Carback 21:40
Binance Smart Chain, $25 billion wallet, right? You can't really do an exchange wallet and, like, unless it becomes very, very expensive where every transaction is a complete and isolated utxo, right? Like, that's not going to work. You've also got, you know, the Satoshi wallets and a bunch of the older wallets are all, you know, free pay to public key hash, yeah. So those are all just sitting there waiting to be waiting to be gone.

Rick Carback 22:10
So how do you address that to the community? Because not everybody is, you know, understanding of what quantum is, right?

John Woods 22:18
Maybe Mohamed, I just had two things to add like, one, what do you do with the Satoshi wallet as an example? Let's say it was Hal Finney or some other groovy guy, you know, and the gentleman is dead, or he's passed away, or the keys are lost. What happens then? Do you give kind of a deadline and say, if you're not upgraded by this time, you know, we just excise you from the ledger? Or do you allow it to be exploited? That's one that the community is gonna have to deal with. And the second is bitcoin's relatively slow and relatively expensive, right to move tokens compared to some of the more recent blockchains. And there's going to have to be a contention in the blocks, where blocks are not just normal transactions, but potentially upgrade transactions, right as people move their funds into new accounts and things like that, depending on how they do it, of course. And so there's going to be a time where Bitcoin is, Bitcoin is going to see a lot of flow that's quantum related. And, you know, it's not instantaneous.

Rick Carback 23:09
With respect to an upgrade path to follow on to what John has said. You know, primarily the work at XX has been on the account based side. So they have what's called the sleeve wallet, where it has a traditional ECC key, and then there's a quantum key wrapped in that, so you can prove ownership of the ECC key after you've switched to post quantum, which is a very like, I think, clean solution. I'm

hoping that other people will, you know... the sleeve algorithm's, independently reviewed, public, open source. I'm hoping other people will take advantage of that work that we've done there,

Mohamed Allam 23:40
What happens to the people that don't switch right?

Rick Carback 23:43
The network just turns off the traditional signature. So you just don't - your funds are locked forever until you decide to unlock, you know, use your quantum key.

Mohamed Allam 23:53
That's interesting.

John Woods 23:55
It's interesting. So it's kind of like a forced upgrade.

Rick Carback 23:58
Yeah, it's a smooth upgrade transition path where they can just turn it off after the fact.

John Woods 24:03
Yeah, but I guess you guys had the benefit of designing that with, you know, with, with cognizance of the issue, where, whereas Bitcoin is much more, much more nascent, I guess,

Rick Carback 24:14
Yeah, you don't have that opportunity once the cat's out of the bag. And it is for, for Bitcoin, for sure.

Darren Moore 24:21
Well, I'm, I'm interested to know if the customers of the Messari report are, like, really focused on Quantum. Is this something that you hear about a lot, or is it something that every once in a while you hear about.

Mohamed Allam 24:33
Taking, taking a step back right now, I think quantum is only a concern of like, like Binance or a really big institution, most smaller folks out there do not care about this. Most people are worried about meme coins. Like the masses are never going to worry about this quantum problem. And at Massari, we haven't had much of a discussion with, for example, an XX Network or similar protocols, because the, I don't know, the need isn't there. People only start worrying about a problem when it's right in their face, when they're affected by it, until that it's very clear that quantum is going to have a negative effect on, you know, people's bags.

Rick Carback 25:16
I agree with you completely. And in fact, I would have said the same thing. And, you know, XX Network was focused on metadata privacy and messaging privacy, and we have the problem of store now, decrypt later, right? So that's the only reason we had started looking at this post quantum stuff. But the rules have changed recently, so now I'm much more concerned about it. And also, I would argue, to the small guys, like, look, if major wallets start getting hacked, if the Binance or or other major exchange keys, and the money just gets taken from those right, what's going to happen to the market? Those

coins that you hold, you hold... you hold like five Ethereum right? What's it worth right now? What happens when a major Ethereum hack takes that, I don't know. I have, I have it written down somewhere... $184 billion Ethereum address. There's one single address holding $184 billion...

Mohamed Allam 26:19
But all the value will just disappear. I mean, there wouldn't be value in Ethereum. There wouldn't be value in Bitcoin if it gets broken, once it gets broken, across the entire spectrum.

John Woods 26:29
Right, but, and that's why this is not for me, you know, working at an L1 about protecting any particular individual, or the Algorand Treasury or whatever. It's about protecting the value, the hundreds of millions, of billions of dollars of value that is TVL on chain, right? So that's what we care about.

Mohamed Allam 26:45
And looking at this from a different perspective. Here, we're looking from a very, you know, specialized, hey, we're in crypto, this is a problem for us, but we're the least of concern. If you can break traditional cryptography. I mean, the whole world is screwed. It's a nuclear level kind of equivalent of a problem, and that's why the US, China and potentially Russia, will be in this next race, a quantum race, and whoever wins reigns supreme, or you'll have two people winning at the same time and will be at a standstill, similar with nuclear weapons, if one party had the nuclear weapons Hiroshima, but then as soon as other parties have them, then it gets, you know, more standoffish.

John Woods 27:25
And so for me, what you see with Google's Willow is, like, what you see with Google Maps, you know, when it first came out, and you could go on the street view. And I was, I personally, was like, Wow, that's incredible. I couldn't believe that it was possible to kind of go anywhere and just look on the street. But can you imagine what the military have, they have, they have that in real time, right? I mean, and so I suspect what we see with Willow is, of course, fantastic engineering. But you know, who knows what's in some Israeli or US or Russian or Chinese, you know, government lab. And this is, like the guys have just said, it's bigger than, say, $2 trillion of Bitcoin, or $3 trillion or whatever it is.... yeah, it's global.

John Woods 27:56
This is supremacy for military secrets, etc. I mean, now symmetric cryptography is not just smashed open by these things, but, you know, government agencies and government level actors will want access to this compute power.

Rick Carback 28:17
The NIST competition, in hindsight, has turned out to potentially have been very well timed. And, you know, there were some games played there. There's a whole scandal. Daniel G Bernstein has a write up, and there's a lot of bad blood between a bunch of people involved in that process. But, and I think part of that's because they, they kind of did it on an accelerated timeline than what I would have expected. I would have expected it to take 10 or 20 years. And I think they got the whole thing done in closer to four or five for the first set. And you know, that doesn't give me high confidence in like, there's sort of three major algorithm types. There's the classical like hash based signatures, the old school stuff from the 80s.

Rick Carback 29:01
There's the, I forget the name of the linear algebra version of that, which is all patented. And then the two major ones from NIST were the lattice based crypto. And then the isogenies, and the isogenies kind of got - first of all, they picked some algorithms to look at that I wouldn't have thought of because they've released too much public information, and then they didn't let certain algorithms, I would have thought CTIDH would have been in there, and it wasn't in there, and it didn't make it in, so I'm skeptical of the NIST results. But also, you know, it may have been prescient for them to have gone out and done that when they did and, yeah, my advice to people is focus on systems where they're wrapped, where you've got the classical key and you've got a post quantum key that's going to be the safest for you moving forward.

Mohamed Allam 29:58
So if we look at current let's say, let's not look at quantum computers for a second, just to understand this in contemporary context, if we look at where the biggest high performance computers are, it's always national labs, Lawrence Livermore, National Laboratory, Argonne, Los Alamos, they have the best performing high performance computer computers out there. And I don't know maybe you guys can can speak on this, but I don't see the quantum computers being anywhere else, other than in national laboratories, at least for a while, until we get huge VC pumping into the, you know, the investment side of things.

Rick Carback 30:43
The cost to run one of these at the scale you would need it is only about the cost of a flight of like, from New York to California, of like a Boeing 747, like, it's not, it's expensive. It's out of the reach of a normal person. But it's not, it's not outside the reach of, like a standard University, or even sort of a well funded company or individual.

Mohamed Allam 31:09
I'm talking at the scale to which it would break anything, right?

Rick Carback 31:14
That's, yeah. I mean, at the scale, when you multiply out the number of physical qubits that might be needed, and you kind of project it out, the costs are lower than you might think.

Darren Moore 31:26
Can like incentives from the government, I saw they're donating to Chicago and trying to push the innovation further along. Do you think that can drastically alter the timeline? Big grants? You know, if you went from, I think it was like $20 billion so if you took that number to $500 billion is that drastically alter the time line or do you think it just needs to be discovery and time that takes place?

Mohamed Allam 31:53
I mean, possibly I live in Chicago. I go to U Chicago right now. I study there. And I've been talking a lot of people on the ground, right, the professors, the students that are working on the quantum side of things, and every time I talk to them, they seem a bit discouraged on where things are going to end up. They aren't getting the funding they need, they aren't getting the application they need. So I think it would be huge if the government were to pour, pour more money into this. And especially considering the new... Do you guys remember the name of the huge quantum facility in Chicago that just was announced? It's a startup, but yeah, capital, capital inflow is going to be huge, in my opinion, for this.

Rick Carback 32:45
I agree with you completely. I mean, at this point, I think it's just a money problem. I think you could build, you know, a 10, 20 million physical qubit computer today, potentially, it's just with these error rates that we're seeing. I you know, there are engineering challenges on scaling, right? I don't want to discourage that, but I think it's, it's at this is, this point it's primarily, you know, dump enough money in, you will get a result,

Mohamed Allam 33:12
And then have the researchers that are working on quantum related tasks switch the focus from academia to business application, because as soon as businesses find that they could make money off this and use it themselves, that's when you see a huge inflow. Because AI, for example, has existed for 30/40, years in concept, right? And it's only beginning to see adoption these past five years. So as soon as businesses see the potential, that's when we make money and and grow the quantum space.

John Woods 33:43
Yeah, I think that's, that's, that's true. I was at CFC summer. It's, which is primarily a crypto conference, but I met some folks who were working in quantum there for the first time. You know, I've met... it was the first time I'd ever met someone credible who was talking about working in quantum as an industry. And so I agree with the guys and what they've just said, I also think it's telling that, like mainstream companies are adding quantum security, right? We've seen this notably. I think we, I mean, it's with open SSL and other things. But I think the two cool kind of consumer products, one is Google Chrome. So they added one of these lattice based key encapsulation mechanisms there to Google Chrome's crypto set, and also with iMessage, the iPhone based text message implementation, they've added Kyber, I think, as well the lattice based key encapsulation mechanism to make iMessage hybrid, a bit like Richard mentioned about XX, you know, using the best of both worlds, elliptic curves or whatever, plus lattices and so, you know, as I mentioned to someone last week, these companies are not adding these technologies, you know, for show, this complicates their code bases. It makes things harder to maintain, and so I suspect they're only doing it because they feel there's a credible threat, and they don't want to have the optics be bad if something emerges,

Rick Carback 34:55
It substantially increases the costs, right? You know, just the block size. it's going to have to substantially increase, because the signatures are so much bigger, right? So there's a good reason not to switch immediately, but you need to have a plan in place for when, when's the right time. I think, I think that times a couple years from now.

Mohamed Allam 35:16
The byte size goes up. I think three times with post-quantum.

Rick Carback 35:20
Depends on the signature. I mean, if you're using SQIsign, it's, it's significantly less, but, yeah, it's at least, it's at least twice.

Mohamed Allam 35:28
Yeah, I don't remember which one, but I was reading something. It's about 800 bytes for the post-quantum cryptography, versus 226, for one. So that's, that's a huge, huge difference. But I think as we

also scale up and in technology in general, that difference will continue to become minuscule, more and more minuscule as we go but yeah.

John Woods 35:53
I agree with you. I agree with you, just like the you know, the internet scales better now than it did when, you know, in the 90s or whatever. I think as well as the guys have said, one of the reasons we picked Falcon for Algorand is because the signature size is relatively small. Now, look, there's trade offs. There's like, how big is the public key? How much compute burden is there when you're, you know, rendering a signature, or creating a signature, etc. So it's not, not like, perfect, but like, it's a again, you're trying to, you're trying to optimize for the functional requirements that you need, you know.

Darren Moore 36:23
So, I mean, Bitcoin already is slow and expensive, as we said. Well, first of all, they have to deal with the governance problem. After they deal with the governance and they fork... create a quantum proof Bitcoin. I mean, now the scalability challenges really rise, and the fees, as I would imagine,would be a lot more, you know... I guess there'd be forced to use layer twos. Like, how would that look?

John Woods 36:50
Yeah, I don't really know how they're going to pull it off. I know that the guys have two different views. But, like, I do think I was around, you know, using Bitcoin, when the bitcoin cash thing happened. I remember segwit. I remember, like, you know, all that kind of stuff. And it took forever because it is quite decentralized, and there's a small team maintaining it. And by the way, as you know, as we can all attest, this stuff is really hard. This is like, specialist engineering. It's not like you can be a killer engineer, AAA person, and still not be able to invent this post quantum stuff. This is the intersection of mathematics, cryptography, applied crypto, distributed systems. It's tough, and so this is a non trivial lift for the Bitcoin team.

Rick Carback 37:25
I think they'll make it easier with op_hash and op_cat, but, you know, that remains to be seen. I think that the likely path for them is a, you know, a script that is like pay to post quantum hash, something to that effect. But what that algorithm ends up looking like? I don't know, I'm not sure.

Mohamed Allam 37:51
Something I want to throw back at you guys, because this is a question I get a lot, especially from the hedge fund and VC types, people that are holding a lot of Bitcoin, they always ask me, what is a timeline? I haven't been able to, you know, put a nail on that. I'd like to hear everyone's opinion, like, when do you guys think this is of effect? There's, there's research that says 2035, 2029, not any time in the next 100 years. But you know so many different and all of these come from reputable sources. By the way, they all come from academic institutions. So I'm kind of curious, what do you guys think? I haven't been able to come to a conclusion on that.

Rick Carback 38:30
It's hard to say, right? I would, I would say your plan needs to be, you know, two, three years out at this point, like 2027, but maybe you do the work and get ready to execute, and then you realize that things haven't progressed, right but we're at that exponential growth curve right now, but we don't know where on that line we are is where my attitude is on it.

Mohamed Allam 38:57
So also no conclusion on that, like, I've always been trying to...

Rick Carback 39:04
If you're into risk, it's like two years, two years, if you're worried about it, like, and you have money on the line, then, yeah, you should be ready to go and probably have done it already in two years, is what I would say.

John Woods 39:15
I've been saying, you know, up until a year ago, the answer to that, that I kind of parroted was 10 to 15 years. And I kept, I kept, and that never changed. It was always 10-15 years as the years went by.Now, if you ask me, and I'm pulling, I'm pulling this out of the air, just my gut instinct on it. I don't know, of course, but I would say five to seven. And I suspect five is more likely. And I agree with Richard.

John Woods 39:40

John Woods 39:41
I actually talked with Leeman Bird personally, about this at CFC. We sat and had some dinner. We were talking about post-quantum around both Algorand and hedera and other networks. And we were kind of thinking, how long would would the lift be? I mean, if you have to, if you're starting from from scratch, okay? And unlike maybe XX or Algorand, you've done nothing in this, and it's kind of just, just something fresh. It is, the lead time is two to three years. You know, by the time you you get the implementation, even if it is an API or whatever, a binding that you use, you still have to test the hell out of it. Go through test net phases, betanet phases. It's a huge lift. And so, I would say worst case, I would say five years would be my guess. I think five to seven before we have some serious shit that makes people a bit actually scared, rather than just going, ooh, that's a nice technical demo. And I would say, if your blockchain doesn't have any quantum, it needs to be like something you're looking at this year, you know.

Mohamed Allam 40:33
So how about you know, you mentioned earlier, GPU, right GPU sized Quantum. How far away from that? Because if we look at it from a government, right? Or, you know, a big tech firm, they probably aren't going to do much hacking of encrypt, right?

Rick Carback 40:53
No you just need one bored engineer over a weekend, what are you talking about? Of course!

Mohamed Allam 40:57
Well, that same bored engineer, I mean, someone at a nuclear facility is going to send nuclear launch codes. I mean, you have to have a series of...

Rick Carback 41:05
No, we have tons of examples. Like, what about the Ross Ulbricht coins that got stolen? Like, that was an FBI guy. You think, you think some bored guy is... first of all, you think that, like, all the NSA guys work 24/7? No, they don't. But like, they can go into the office on the weekend and spin up the quantum computer, which is already running, probably already costing $20,000 a day, and just use it for the

weekend. No one's gonna know. Like, what kind of monitoring do you think that the government really has in place, or something like that? That's a ridiculous statement. I'm sorry. I don't mean to get all, all on top of you about it, but like, yeah, I just like, think about, think about, like, how these things actually work in practice, like Edward Snowden was able to walk out with tons of secrets. It took a while before they figured out what was going on. You think the guy that, like, breaks Satoshi wallet in the eight hours over the weekend and then disappears to like, St Kitts is like, gonna get caught right away? I don't think so.

Mohamed Allam 42:06
I don't know. man, I thought you were being sarcastic when you first started.

Rick Carback 42:09
No, I'm ranting like...

Mohamed Allam 42:12
I don't think an individual engineer at a government organization be able to do much on that front. But I mean, we could, we could all be proven wrong. But I agree to everything with you up until this point. I don't think that's, I don't know,

John Woods 42:29
Yeah, Mohammed, my guess mate will be that - and my only frame of reference here, because I'm not, I don't work in the military intelligence or whatever industry...

Rick Carback 42:38
I have.

John Woods 42:39
Have you? Okay? Okay.

Rick Carback 42:42
For 15 years.

John Woods 42:43
Oh, really. Okay. Well, I'll go with you on that one then. But no...

Mohamed Allam 42:47
I've worked within aerospace and defense and to just run an LLM, there's, I don't know, five levels of security that you have to get across to get something.

Rick Carback 42:57
You're not wrong there. But this is a system, and I guess this is the thing that I know that other people don't. This is a system that's going to require specialist engineers and IT people, and it's not really going to have significant monitoring outside of physical access control.

Mohamed Allam 43:12
There's no on-switch that's going to turn on a quantum computer. It's not that simple by the time something is realized now. Now, if you have someone that's doing it in plain sight, right? He's working

on a particular problem to solve, and he sneaks something in there. Now we have a potential discussion, right?

Rick Carback 43:29
That's the problem here I'm describing.

John Woods 43:31
I would have thought though that governments who have access to say, let's say, for example, like, just like fiction, right? The US military has access to one of these functioning computers. Now, let's just say, okay, wouldn't they want to be really discreet with it so that they can use it in very targeted situations, you know, in order to break certain things that are military priorities. I guess it's what I would have thought, right.

Mohamed Allam 43:31
Someone sneaking through the government and getting what they want, that I think that is very highly unlikely. I would say Snowden, he did it in plain sight. It wasn't a matter of specifically, you know, like a Mr. Robot kind of situation. But...

Mohamed Allam 44:08
Go back to World War Two. I mean, most, most things were only known of when they were used. Right? They existed. The new weapons, tanks, planes, whatever they were made, the technologies, um, breaking, whatever the Germans used for sending messages. Yeah, that stuff existed, but nobody knew about it. Because if someone knew about it, they would have prepared, right? So it's kind of the same concept. I agree with you.

John Woods 44:32
It's like The Imitation Game, right? Where they let, they let ships be bombed because they didn't want to prove they didn't want to, you know, highlight the fact that they would have known where they were, right?

Mohamed Allam 44:40
Exactly, yeah, but we'll see. I mean, if we're at the point, at that point the same week, Willow announced the, you know, Google announced Willow, there's a Shao. Shao Huang, I believe, is the name of the quantum computer. It's a Chinese 506 qubit computer that was released in that same week on the low, you know, nobody knew of it, and it's on a cloud based usage front. So if they're able to announce things like this, who knows what China has, right? Who knows what the US has, it's not, it's not 506, logical, is it? I don't recall. I don't want to misquote.

Rick Carback 45:18
No, it's physical. Yeah, John, to your point The Imitation Game go, like, watch that movie and watch how much access they had to the bomb, yeah, unmonitored, yeah,

John Woods 45:32
Sure sure sure sure.

Darren Moore 45:34
I watch a lot of true crime shows on YouTube, and one common theme that I see with like dark market drug dealers is they always have their wallet seized, and like, they always swear that they never leak their private key or anything like that. So I can imagine law enforcement would want it for, you know, like John was saying specific targets, and not necessarily blow up Bitcoin, but just, you know, go after certain ones that they, you know, take the moral high stance with,

John Woods 46:06
Yeah, but, you know, here's the thing. The parallel for me is maybe this, if you take the.... and, you know, I don't, I don't have an encyclopedia in my head on this, but if you take the world's greatest super computers, right now, I believe the top one is a Chinese one. Now it used to be like, you know, blue jean back in, like, the 90s, or whatever. I don't know, but you take those computers - they can't - those computers can't arbitrarily break elliptic curves or AES or other modern cryptographic standards. It's still hard work for them. Okay, even if you had two or three of them under your control, you still wouldn't be churning through elliptic curve keys, because it's still just an absolute fucking huge space to search.

John Woods 46:39
And I think that that's what makes things like Bitcoin and other networks just like hard money or hard assets, because they are, even with global level scale, you're still not, you know, defrauding them. And so I think that that's the same place we need to be when governments have access to quantum machines. It's to know and have confidence in when you're walking down the road in that with your with your digital assets, same way you have confidence when they're in a bank that, you know, maybe it's theoretically possible, but you're pretty goddamn secure, and that's and that's why it's worth adding these post-quantum primitives.

John Woods 47:13
I don't think it's... I think, you know, for absolute government level attack, where you have a threat actor who is a government level, like, if someone wanted to get my crypto, they'll just, they'll socially engineer me. You know, at a government level, right? They'll poison me! So I don't think it's about the individual. It's just about the hardness and the network and making sure that your users have a general sense of security. Yeah.

Mohamed Allam 47:38
And to go off on a more philosophical lens, it's, does your Government ever become tyrannical? Right? Do they want to come for your Bitcoin? Do they want to come for whatever? And that's what the average Joe should be worried about in terms of protecting themselves. It's not from a hacker or first or foremost, it's the government that rules upon them. So I think looking at it from that perspective changes the lens for normal folks, because you can't just say, hey, I lost my Trezor in a boating accident, because they're already at it, yeah.

Darren Moore 48:14
Is there anything that I can add to, like, well... after quantum is, you know, a large enough qubit, could it add to the decentralized systems? Like, maybe, like a modular design of different quantum computers, kind of like, like a filecoin of quantum or, you know, maybe that I've researchers like different algorithms for consensus utilizing quantum computers. So I'm just kind of curious. You guys think there could be anything beneficial that quantum can add?

Mohamed Allam 48:49
Not anytime soon. I mean, if you look at all the you know, Render, for example, how many years has it been around - the latency issue. There's been a lot of proposals to say, Hey, this is how we're going to solve the problem. And nothing has really come up scale to which their cheaper price has intrigued all these AI developers, right? If an AI company could get cheaper compute cost to develop their models, and I know this for a fact, they would definitely go for the cheaper price, because it gets very, very costly, and then they haven't, because you haven't been able to communicate all these different resources within like, let's say, render or or the like. In the case of quantum computing, you're taking that magnitudes and magnitude scales higher in terms of communicating between quantum computers. And we're not going to be at the scale to which we could have, you know, person X, from place, whatever, communicating with another quantum computer to get a better result. I don't see that anytime soon. But again, maybe you guys have a differing opinion on that.

John Woods 49:50
Richard, what do you think?

Rick Carback 49:50
I agree with you wholeheartedly. I think that that's a like a more fundamental problem with a lot of the deep end stuff is that part of it's hard to use. Part of it's it's not actually that much cheaper once you get the implementation going. So it's just, it's difficult to see how that model would work.

John Woods 50:08
Yeah. I mean, I would agree as well. I think, yeah, maybe there's some quantum application for information, like using entanglement or something. Maybe you could send information faster or something, I'm not entirely sure. But there is a thought around quantum mining. I mean, it's quite, quite a straightforward one, the idea that, like as I mentioned earlier, hash functions are weaker to quantum computers than they are to classical computers. And I guess you could mine Bitcoin using quantum computers, and the target could be higher, I would guess, or more, or harder. And so, you know, a bit like an ASIC on drugs or an ASIC on steroids. I mean, potentially, but I really think it'll never be (sorry, never say never), but an extremely long time, more than our lifetime, before these things are commodity items that you would like you know, having a general purpose computer, I would have thought, but who knows?

Rick Carback 50:56
Yeah, I think the cost on the on doing something like that with mining is probably not going to bode well when compared with traditional computers. So yeah.

Darren Moore 51:05
I want to be mindful of everyone's time. So if there's anything that we didn't discuss that you guys want to bring up now is the time.

Mohamed Allam 51:14
One small thing. We've talked about a lot of technicals in this call, and I feel like a lot of the listeners are probably a bit confused. So if we could use these last few minutes to kind of give, I guess, a key takeaway, right? If someone were to watch the nine minutes of this video, what would be in plain English? The key takeaways, John, you want to start with that, and then maybe Richard, and I'll give my opinion at the conclusion.

John Woods 51:40
Yeah, my key takeaways would be, quantum computers are real. Our engineering is getting better at making them stable. We're still a little ways out from, you know, I would say 3, 5, 7 years before there's anything dangerous that's actually created. They're cool because they use quantum physics and quantum parallelism, but in reality, they're only good at certain things, and not just breaking cryptocurrency, but breaking modern security. And we are already doing the work, I think, in terms of the mathematical and academic work to build secure systems even with these things existing. And if you're a person who runs a blockchain, i.e. a CTO or senior engineering person you need to be looking at this today if you care about your users.

Rick Carback 52:27
Yeah, I'll add to that that if the error rate comes down, then the qubits we have in demonstrated machines today are enough to break every current classical algorithm. I don't think that's a reason for despair. I think that's a reason for thinking about all of the good things that quantum computers are going to be able to enable, in terms of very quick protein folding and solving a bunch of other problems that I think are key to humanity's survival in the future.

Mohamed Allam 52:57
My main thing would be, don't be afraid to talk about quantum computing and research, not just because you hear the word quantum. You get, you know, intimidated. I know it may seem intimidating for anyone listening, but just get into it and understand. I've been in this, you know, trying to understand about quantum for 6-8, months of consistent research, and I'm only maybe 5% of the way of where I want to be. If you understand 0.5% you're enough to be, I guess, dangerous, especially in a business setting, if you're a CTO, if you're on the business side, even you could, you could have these conversations. You could bring to people the attention, right, that's needed towards the change that is coming. So, yeah, just, just talk about quantum and get better versed in the material,

John Woods 53:46
Maybe one last quick question from me, for the for the guys, because you're, you're both very, very knowledgeable, and it's lovely to spend time on chat with you. Um, you remember when cryptography was kind of really coming into vogue, and Daniel J Bernstein made Curve25519, and kind of like, and Bitcoin uses the other curve, K1, and there was kind of like the NSA approved crypto, like, you know, P256/R1. And there was, like the Bitcoin and Cypherpunk crypto, like the Curve25519s. It feels to me like, right now, the standards that we're going with, as you mentioned earlier, super single isogeny or lattice based have all been set by the US government. And so do you think, I guess my question is, do you think that those NIST standards, which are very US "trust us, bro", a little bit... will be picked up and run with globally, a bit like Curve25519, or, do you think there'll be a kind of a push by someone like a Bernstein, again, to inject that kind of Cypherpunk version of post-quantum, which is a little bit outside of the realm of the NIST competition. I'm just interested to see what you think.

Mohamed Allam 54:48
I think the whole world right now is trying to head away from whatever the US is doing in general. I mean, look at BRICS these past few months and many other organizations around the East, right? Everybody's going to be developing their own standards, and they're going to, you know, use whatever the US has and make it better and completely ignore that they got it from here in the first place. So each entity being involved in quantum computing or will probably have their own set of standards.

Obviously, in all academic substances like this. You're taking bits and pieces, but I think it's critical for everyone to have their own standard. And just look at China. For example. China copies everything that the US does, similar to the Roman Empire, right? They copied Carthaginian ships and made them better. The Chinese are copying quantum computers, fighter jets and making them better, and they're going to copy standards and make them better. So take that and apply it across everything. Really,

Rick Carback 55:48
I will add that I'm already doing it. We're staying away from NIST at the XX Network. You know, we went with CTIDH, which is not a considered algorithm. It's from Daniel J Bernstein's group. Well, him and a bunch of other researchers, we are using the WOTS, which technically is part of Sphinx, but pre existed and predated all of that stuff by 20 years. So, you know, we're very skeptical of the of the of the NIST process.

John Woods 56:20
Yeah, that's really interesting to hear. I must research a bit more on CTIDH. Actually.

Darren Moore 56:27
Does anyone want to suggest the audience to follow any accounts? John, do you have any accounts that you want the audience?

John Woods 56:34
Yeah, sure. I'll do my my shameless plug. If you want to learn more about Algorand, you can, you can follow at Algorand Foundation. Or you can follow myself and my my name on Twitter is, or x rather, is @johnalanwoods. Happy to talk crypto with anyone. I think it's a wonderfully interesting area of computer science.

Darren Moore 56:55
Yeah, this was, like one of the easiest conversations I've ever had to host of... So I appreciate that.

Rick Carback 57:02
I want to thank everybody. I mean, I know I got a little bit of a rant there, that just tends to be my personality, but I really appreciate and have mad respect for everybody on the call. It's a really good conversation. I did not expect it to go this way. I expected nobody to know what they were doing and me to be bored. So this was great! In terms of following me, I'm @rcarback everywhere. Last name is pretty easy to remember. I got made fun of a lot in school. So let's take advantage of that pain that I went through. And then, you know, xx.network, and I'm going to be announcing stuff in the next month or so on my new project.

Darren Moore 57:37
Yeah, awesome. And Mohamed, how about yourself?

Mohamed Allam 57:41
I just got back onto Twitter. I used to post the memes and philosophy a while back, but now I'm doing little crypto thing. So I, you know, turn my Twitter back on. So it's @plague_observer. It's a bit of an edgy name, but I think it's cool.

Rick Carback 57:57
Excellent name. I love that.

Mohamed Allam 57:59
All right. Cool, cool, cool. And yeah, check out my research at Messari. Messari crypto, we always have pretty, pretty good research. So if you guys ever have any questions, research wise, Messari is the place to go.

Darren Moore 58:12
Awesome. Thanks, guys. I appreciate everyone's time. And yeah, I appreciate it. Yeah. I just want to say thank you to you, yeah, as well, Darren, I mean, you've put this together, and not many people have done this, so I'm happy that you're the one of the first to do so. So thank you. Thanks a lot for that. Yeah, appreciate that. Yeah, a lot of people aren't paying attention, like we we discussed...