Quantum San Diego Convening | Hsin-Yuan Huang, CTO of Oratomic & Asst. Prof. of Physics at Caltech

41 MIN · YOUTUBE · HTTPS://YOUTU.BE/39LBTJLSIZ4
https://youtu.be/39lBtjlsIz4

SUMMARY

Robert, the CTO of Atomic, discusses the imminent threat posed by cryptographically relevant quantum computers (CRQCs) to public key cryptography systems like RSA and ECC. He outlines the progress made in quantum computing, the potential risks to global finance and security, and the challenges of transitioning to post-quantum cryptography.

- *CRQCs could break public key cryptography, posing risks to systems like Bitcoin, which relies on ECC for transaction security.*
- *The theoretical requirements for building a CRQC have decreased from 500 million qubits in 2010 to approximately 14,000 qubits today.*
- *Significant advancements in quantum error correction and logical operations have been made, enabling more efficient quantum computing architectures.*
- *The transition to post-quantum cryptography is complex and requires consensus within communities like Bitcoin, making it a slow process.*
- *CRQCs also threaten cyber-physical systems, such as medical devices and infrastructure, which rely on public key cryptography for security.*
- *The timeline for achieving CRQCs may be as close as 2028, necessitating urgent discussions on mitigating associated risks.*
- *The potential benefits of CRQCs include advancements in quantum simulations and AI, which could lead to significant scientific discoveries.*
- *Ongoing research aims to integrate various components of quantum computing to realize fault-tolerant quantum computers at scale.*

Thank you so much for um introduction and for inviting me uh here. It's a great pleasure to be here um to talk about um something that we're very excited about um and also very kind of scared about which is how close are cryptographically relevant quantum computers. So I'm Robert. I'm the CTO for atomic currently on leave um as a faculty at Keltech. So for those of you who know who don't know um hopefully everyone knows um CRQC are futuristic quantum computers uh that was envisioned in 1990 um that can break public key cryptography by running short algorithms at scale. So two of the most commonly used public key crypto systems are RSA and also ECC. So RSA is this famous uh factoring problem that is given an integer n try to find two prime numbers such that they multiply to n.

ECC actually is also widely used. For example, bitcoin uses ecc to secure its transactions. Um and ECC um is can also be solved using sha algorithm um by running discrete logarithm on these elliptic curves. and building CRQC has really long been the holy grail of quantum computing. Um since this is really the first time um that quantum computers um can solve some problems or theoretically solve some problems that classical computer cannot.

However, due to a lot of challenges that people faced um they're often thought to be many decades away. So for example in 2010 um Jones atl analyzed a full tolerant quantum architecture built out of surface code and concluded that one require 500 million cubits in order to build a CRQC in order to run sh algorithm um to solve RSA and back then the largest scape based quantum computer only has less than 20 cubit so there's a very significant theory experimental gap um in between and then eight years has passed and progress were being made. Um Craig Guinea and Martin Aera shown a 25x improvement in terms of the number of cubits. So just 20 million physical cubits, noisy physical cubit um is is needed to build CRQC and but back then um the largest gate based quantum computer um also has improved but it's still less than 200 cubit. So there's these four orders of magnitude difference between the theory requirement and also um what's experimentally possible and if we assume that 20 million um is really the theoretical limit um of how many cubits required then and and then assume that the progress remains similar. So over 8 years we improve we can scale up by 10x. Um if we extrapolate from there it would need more than 30 years um in order for one to build CRQC. So this is not so nice for quantum computing as a field.

However, this this gap is actually very good from a security point of view because even though some pe I think most many people know about it but haven't really think deeply into it but but CRQC are um actually quite dangerous um in terms of national security point of view and global financial point of view. [snorts] So some of the danger of CRQC um uh includes the following. I think the most talked about um risk um to global finance um when CRQC comes online um is BTC. Um so people talk about oh BTC now has market cap of 1.5 trillion in US dollar and um is really a very nice store of value. Uh people claim it to be digital gold. We can verify it properly.

It has all these very nice mathematical um um um properties that are created based on this uh cryptographic system that allows everyday user um to store value in this digital asset and also perform transaction um to one another. And the security of the transaction um is essentially realized by public key cryptography ECC 256 more specifically and mainly to secure against um people forging um signatures or people trying to pretend that we're someone else and try to move um the the the capital in someone else's wallet. However, as we know, CRQC can break public key cryptography and as a result um if someone's public key is revealed or exposed on the internet um then an evil actor can in principle um utilize the RQC to derive its private key and with the private key it can now forge signature and impersonate everyday user so that it can move all these uh bitcoins uh to its own wallet. And so that's one of the big thing that people talk about is that once CRQC exists it will be able to steal Bitcoin. Um there are ways to secure or to to circumvent this problem. Um um by essentially for example doing a soft fork or a hard fork of BTC. Um soft fork basically means we will be extending the addresses the wallets so that it's now secure against quantum attack. for example, by running LWE as a crypto system instead of ECC.

However, um these transitions tend to be very challenging because it requires consensus among the entire community both the miners and people holding uh BTC's and and that global social consensus extremely hard to achieve. So even though there are various known solutions um people are still just debating which solution one one should take. For example, should we burn the Satoshi era coins? um should we do a soft fork, should we do a hard fork and and all of that causes trouble and hence the migration progress has been very slow. But this is also not the the worst thing that would happen. Um especially for those of you who don't own any BTC, this would probably not be a big deal for you. Um but but more than that, so right now globally um there's transition um from traditional financial system into decentralized financial system. um big financial firms such as Black Rockck, JP Morgan, uh Visa, Mastercard are also all starting to do this. Um and one of the nice thing about it is that by moving things on chain now, one can um essentially run smart contract for example on Ethereum and that allows much faster transaction and global commerce to happen. Like for example, I'm from Taiwan. If I wanted to send money from Taiwan to United States, um under swift system, that would take uh um maybe more than a week. Um however um utilizing these uh onchain and decentralized financial technology um one can utilize USDC USDT to essentially send money in a blink of an eye. So there is a lot of uh moving towards decentralized systems and and perhaps in the near future everyone on earth will be transacting or a large portion of fin global financial system will be transacting on on onchain such as on Ethereum, Solana or other um blockchain systems and oftentimes these uh these uh technology are also developed um by software engineers and oftent times they would find bugs and need to patch them or they would need to upgrade with new functionalities and and hence they would need to essentially upgrade these uh automated market maker or automated like uh kind of transaction manager um like these smart contracts and these uh upgrade are also protected and secured by public key cryptography so that not everyone can just update these smart contracts so that it will behave differently. However, um again with CRQC um this public key crypto cryptography can be broken and allowing an evil actor um with access to CRQC to effectively hack this smart contract and now uh perform whatever action um it wants which can potentially cause great disruption to global financial system and with various adverse effects. But this is not even the worst. Um there's something even worse um which is which is in there there's now um most physical systems are now cyber physical system in the sense that they're connected to internet and can be controlled for example remotely and monitor remotely.

Some [snorts] examples include implantable medical devices um drones power grids and water supplies uh etc. And the the danger there is even greater. So for example um maybe there are some patients that have done heart surgery and have to implant uh heart pacem uh pacemaker to to essentially um that their heart pumps in a in in a regular way and oftent times these pacemaker are connected to the internet and as a result can be monitored um real time by doctors at different hospitals [snorts] and again similar to before in order to for example improve the real-time monitoring or to patch some bugs uh pacemaker manufacturer such as um um Metronics or Abot or other firms um often need to do firmware upgrade to to upgrade these pacemakers. Um and again it's protected by public key cryptography because we don't want everyone anyone to be able to mess with these implanted medical devices. Um however again um CRQC can break that um and causing evil actor to for example impersonate these manufacturer and try to inject malicious firmware into patients pacemaker. And if they successfully did that um it would be a really um dangerous world to live in where there will be these evil actors.

We don't even know who they are. We don't even know if they existed, if they already done it. um that can

basically take control of um of people's life. So in furthermore, this migration to postquantum in this scenario is extremely hard because then possibly they would need to go back and do another surgery um and then that's just not feasible. So so so due to all these danger of CRQC, it's very important to um try to understand how close we are in building CRQC. So, so far or 2018 the gap is still very large but another eight years has passed and um and there have been a lot of development in the field. So, one could ask the question what is the gap right now?

So first there are tons of theoretical advancement and also experimental advancement. On the theory side uh there are development of these high rate QDPC codes that replaces surface codes and also people have developed efficient way to perform logical operations on these high rate codes and and furthermore there's also these um optimized algorithms that have happened over the over the past eight years. In terms of high rate codes, um here is some examples um which are three instances of belonging to this co- family called lifted product codes. Um and as one can see so three of them correspond to distance 16 20 and 24 and as one can see um the encoding rate extremely high for example in order to create a thousand about 1,600 logical cubit one only need less than 6,000 physical cubits. And furthermore with proper um circuit level simulation we can see that um as physical error decreases the the block error rate basically meaning that uh whenever there's one error that happens in any one of the logical cubit we count that as an error. Uh this block error rate which is the a very strict notion of logical error rate um also decreases very quickly and um and and as as a result um we can create for example a quantum memory with error less than say 10us1 um that encodes, 600 logical cubit in just less than 6,000 physical cubits.

And these codes are also not just theoretical construct. Um they're also quite efficient. Um but but before diving into that we can also take a look at this point which in contrast if you wanted to create surface code that have distance 24 um encoding the same number of logical cubit it requires almost a million physical cubit um to do the same thing. And furthermore, when one does a proper circuit level simulation, one sees that um the block error rate of the surface code is actually uh slightly worse than these high rate codes.

And from efficiency point of view um um or from a experimental friendly point of view, they're also not too crazy. Um it's it's definitely non-trivial, but but also not too crazy. For example, here is a data block containing less than 6,000 cubits. One can count that properly. is exactly six uh 5742. Um and one can organize it for example in this specific structure. And now in order to clean up um the logical cubits stored in this physical cubit this about a thousand um 600 logical cubit all one have to do is just to bring in some check cubit block containing for example in this case about 2,000 cubits and then move them around. So we just move them around and then every time we move them around we will u perform transversal C not gate between the check cubit and also the data cubit and just by doing this um and then at the end measure out the check cubit block we can essentially um obtain the syndrome and then from the syndrome by performing proper decoding we will be able to predict what where the um logic or where the error has happened and utilize that to perform logical um correction.

And not only do these codes are very good for tolerant quantum memory, they also allow efficient logic. So in the world of falter and quantum computing um the the main the key sub routine in order to perform logical computation is the ability to um essentially measure individual logical cubit. So there is a huge number of logical

cubit inside this block 1,600 of them. But actually all of them can be measured very easily. One has to do is to bring in some additional physical cubits known as the surgery gadget system and then perform a very similar syndrome extraction round. bring in check cubit um similar to before move them around perform transversal gates and then by doing that decoding um the the check cubits um measurements one will be able to measure any logical cubid um among all of these 1,600 of them at will and together that allows one to turn essentially a fault tolerant quantum memory into a fault tolerant quantum computer. So on the memory side we will have for example [snorts] this block um which corresponds to um the the system that I just described that will be kind of um upper that that will upperbound the number of logical cubit that this computer can have. For example, if you use distance 241 it would be,600 distance 20,200 and now what how can we utilize measurements um like logical measurements in order to perform computation. Um so the basic idea is that first we can perform state teleportation by performing ZZ measurement followed by single cubit X measurement which can be done efficiently using similar to the procedure I just described to teleport the logical cubit we would like to do computation on onto a processor. It's very similar to classical computing where we have CPU and uh we have a RAM and also CPU. So this is an architecture that was presented by this work with Medi, Chen, Robbie, Lewis, Harry, Emanuel, John um and Dolph. And then after performing computation on the processor, we will do teleportation again using measurement of the logical cubits back into the memory. And inside the processor, um the the main the main thing we will have to perform is to inject magic. So there will also be a resource block that will be performing magic state cultivation. for example using the Sin7 surface code [snorts] say 10 of them and then and then after that we will distill these logical um or we'll distill magic um into BB codes um by varied bicycle codes and then during the distillation process we can create CC uh magic state and then by teleporting again just using uh logical measurement we can teleport these magic site um into the processor to implement to gates and we just teleport imported properly, implement um gates and then and then along with the additional cliff addressing um and then teleporting the logical cubit back into the memory and and just by with this very simple um architecture one will be able to um create for quantum computer that has this very dense um encoding and finally on the quantum algorithm side there's also been significant development um there's this breakthrough paper by Google quantum AI and also I think Ethereum foundation and Stanford and also in Stanford etc.

um led by Ryan Babush at Google Quantum AI where they show that ECC 2556 um can be broken um using a,200 lo cubit 90 [snorts] million tophley or slightly more lo cubit and slightly less tofle gates and now if we combine um this estimate um in this paper along with uh the result that I just described with this high rate codes and efficient logical computation um together it shows that ECC 256 can be broken with less than 10,000 um physical cubits to slightly more than 10,000 physical cubits.

So that's on the theory side. Um on the experimental side, there's also significant progress in neutral atom systems that essentially provides the key components that allows one to realize this fall tolerant architecture um that relies on these kind of moving capability. So first of all um there's this breakthrough paper led by Dalev Blucen Harry Lavine who both are um now at Oatomic. So Dolv is the CEO um while they were at u um Michelle Lukin's group um and also in collaboration with microser and Vladam volitic. So in this break breakthrough paper published in nature 2022 um they showed that these atoms can be transported um long distance without um decohering too much.

So, so that by doing so they can apply non-local gates um very similar to this moving pattern that I just showed [snorts] and not only that um in this recent work uh by Manuel Andress's group at Caltech um Manuel is also a co-founder of Oatomic uh he showed that it's possible to um essentially create 6,000 reconfigurable atomic cubits and one can move them around perform coherent operation etc And in [snorts] principle, this optical system can trap uh more than 100,000 um physical cubits.

On the fidelity side, there's also huge advancement. Uh there's this paper that was just recently put out um a few weeks ago by seven ever um who is also part of the founding team of origatomic and again from Misha Lukin's group. Uh Misha is really the pioneer in this field. um it is uh that they were able to show that the two cubit CZ gate fidelity can achieve 99.85%. Which correspond to a physical error rate of 0.15%.

So if I look back into these uh um figure that was shown here, if we go to 0.0015, we can see that with these high rate codes, it can already achieve well below 10 the minus 9 block error rate. and and with that block error rate um one it is sufficient to run this ECC algorithm that Google quantum AI has uh proposed. And finally for these atomic system um there there is one specialty special thing about it which is that sometimes cubid get lost because optical tweezers are not perfect um and and if they move if they move them too much then the cubid can fly out and get lost. So in order to continuously run these optic atomic systems, one need to have the ability to continuously load in new atoms and this has also been demonstrated um in in microscer beltic and Michelle Lukin's group um last year on published in nature.

So together um all of these experimental advances and theoretical advances shows that all the components are there um that allows us to build or that allows people um not not just us but the um everyone in the world to build CRQCs. So if we look back into this timeline um in 2010 um the gap is huge in 2018 the gap um kind of uh become smaller and now what is the gap in right now in 2026?

Basically on the theory side we need less than 14,000 cubit and then on experimental side we already had more than 6,000 cubit. So just extrapolating a little bit forward, it's not hard to imagine that maybe by the time of 2028 um they will already cross um so and and by then um when they cross uh if CRQC is real um all these danger that I previously described will happen. Um so so that's one thing that I think um the the society needs to really think about best way of addressing them. Um and and in some sense CRQC are nothing special.

They're just normal quantum computers that can run sufficient number of quantum gates on a few thousand cubits. It's not even that large scale. um like classical computer we can we have yeah huge number 10 to the 9 um or more uh bits that we can manipulate. So in a sense being cryptographic irrelevant is is just an unavoidable thing um along this path of quantum computing. Um and in a sense I think when CRQC is built we'll finally enter this new era that all the pioneers um of our field fineman Peter Shore Umesh um John Prescll Sasoy and many others have envisioned for many decades and I would say uh CRQC um even though there are negative sides towards it there's also huge opportunities and great benefit to to human society. So for example with CRQC which are essentially just quantum computers that have a few thousand cubits and can run um sufficient number of quantum gates we can also start exploring for example quantum learning agents that can run its own perform quantum simulation perform learning on quantum simulation that can discover new phases of matter

or new physical phenomena on its own. We can also start testing these ideas that were proposed in our recent work exponential quantum advantage for processing massive classical data led by my student uh Himemenzo and in collaboration with Google quantum AI to show that in data science and machine learning application a very small quantum AI model can learn and predict better than exponentially larger classical uh machines.

So together I do believe that um we should try our best to create CRQC um and try our best to mitigate all the risk that it also comes together and in terms of um building CRQC I think now given that all the components are there it's now a fascinating and also extremely hard system integration challenge that requires one to think carefully about everything um from these high rate codes to the atomic physics to how we should move the cubits around to move the atoms around to how we can utilize that to create logic to connecting into how one should compile quantum algorithms depending on the codes that we use and the atoms that we use and also designing an entire optical system um that that that can actually realize this and towards that goal um um oric was formed um that that with the all the team members currently listed on this uh on this slide and one of our mission is really to accelerate toward building fault tolerant and quantum computer um at significant scale and our our vision uh kind of more long-term vision is that by 2040 um our world will look back on CRQC and we will not treat it as some uh insurmountable crisis um hopefully we'll find clever ways to circumvent all these risk that um I previously described um and by then in 2040 it will already be a pretty old technology it would be a decade old technology [snorts] and also by 2040 we hope that CRQC will now be used um everywhere um to discover new physics routinely to train new generations of AI and power applications we have yet to conceive.

That's it for my talk. Thank you so much for listening. [applause] Thank you for your talk. Um don't know if that's on. Um I saw a someone else quote the same Google paper where you're around 10,000 uh cubits but they said given the technologies of today it would take 125 years to run. So you said 70 million to 100 millionish gates. What is your expected runtime for something like that?

>> Yeah that's a great question. So so inside this paper there's actually several different architecture is just uh changing some of these codes. um just by changing some of these codes it would have very different um runtime and slightly increase the speed. So for example if it's uh if it's less than 10,000 um versus it's slightly more than 10,000 the the runtime can be an order of magnitude different. So that's one thing and then also um this uh there is a difference between RSA and also ECC.

So in this paper the breakthrough is in ECC. So it shows that ECC only requires thus send 100 million to gate and actually RSA requires um more than an order of magnitude more um gates than ECC 2566. So actually for here um um this uh ECC 256 um if one compile it properly and uh then um for example for this uh 14,000 physical cubit it will only require say a few month um of runtime instead of 100 years. So 100 years actually kind of there there [snorts] is a very naive architecture that we laid out in our paper um just to more of use as a benchmarking and then if one also try to run RSA using that very naive um architecture then it will become compiled into 100 years but somehow people got very obsessed with that number.

>> Um this is a really enlightening presentation. it kind of changed my opinion of this area quite a bit. [laughter] Uh I do have I'm very ignorant about quantum computing. I have a very basic question. Um in addition to the

number of uh cubits also there I thought there was like how many runs you can do before the whole thing becomes decoherent. >> Yes. >> Uh I didn't see that metric anywhere in your >> uh yeah actually so that that is these uh error plots that I was basically showing here. So um one can essentially take like one over this block error rate to essentially estimate um how many um cycles or how many rounds one can essentially perform before this uh machine start to have error.

>> Thank you. >> Yeah. >> Uh I I was wondering >> wait I think I'm next. >> Hi. >> Oh sorry I didn't know. Um, yeah. So, you spent a lot of time building up the very real threat that CRQC has on our modern crypto systems. Uh, you didn't mention or you didn't discuss any of the postquantum crypto systems that are in the works, however, like lattisbased ones. Is there any reason you didn't talk about those?

>> Uh, yeah, sorry. I I yeah so like I only briefly mentioned by words but in in the LWE are ways for mitigating it but and and that's also how I think one of the key ways for how one can make for example BTC secure is that one can augment with new wallet addresses such that it's a postquantum secure it's for example running lattisbay crypto system and but then the problem there is really that there's different ways of doing it.

So there's soft fork, there's hard fork, there's decision made on um the bitcoins that have private key loss etc. And and these um kind of conflicts or these like different possibility of solution with different pros and cons um makes it extremely hard to have consensus among the entire world. um and that causes the transition to be very challenging for the context of BTC um in in ETH and and also other um real world assets on chain um there's also their own kind of um challenges in doing migration for example um it might be the case that in order to migrate to LWE one would need everyone need to go back and resign all of their contracts um and that will be an extremely um complicated process um in terms of Um in terms of pacemaker too if we wanted to migrate into for example LWE like post chronom crypto system one would need to um um yeah one would need to potentially go back and and redo the surgery in order to replace it with a with a with a hardware that is compatible with these new crypto system.

So so the migration is challenging but it is possible. I kind of just assume everyone knows LWB and data space. That's why I didn't mention it, but >> uh probably a bit of a large assumption. Um but yeah, thank you. >> Yeah, thank you. [laughter] Uh I I was wondering since uh since the uh resolution gap between uh theory and uh actuality now is so close uh and and uh classical supercomputers can uh do pretty good factoring. I I was wondering if you've thought of anything like uh like uh physically getting some kind of spin glass transition where where you use your uh quantum computing to approximate solutions and then and then get a few uh few um possibilities and and have a classical supercomput uh do the final factoring because it's getting pretty close Now >> yeah that's that's a good question. So so people are thinking about hybrid quantum and classical algorithms in order to try to make the final step but I think right now it's still um I mean in some sense the what what classical supercomputer can bring is is not that great. It can for example save some number of logical cubit um but the more you save the exponential uh growth goes up. So, >> so people I think at the vinyl stage um that might be a possibility for >> but you're you're not quite there yet.

Yeah, I was just thinking if you could get some uh nice experimental spin glass transition, you could get close

enough. Anyway, thank you. >> Yeah, that's an interesting idea. Thank you. >> Okay, so um I have a comment on a question. I think uh the gap you put at the end 6,000 versus 14,000 there are a lot of hidden assumptions there and might be not as good as it looks. I think the 6,000 cubits experiment was more of a like a memory experiment. It's not a full FTQC at that scale has not been demonstrated.

the also the assumption that goes in the calculation of uh on the order of 10,000 cubits for uh CRQC application is u based on noise models that are might be far or at least not exactly what we have today. There are also kind of potential for correlated errors like as you scale the system up and things could get a little bit tricky. Um so this is my comment. I don't know if I let you respond but I think the gap could be bigger if you do different analysis.

>> Yeah. So to be honest I I think even when even when these numbers cross it doesn't mean CRQC is built. Um because this is really just counting how many cubits but like you're saying um there's actually a lot of requirement actually one needs to put in all of it together. So for example, if you have 6,000 cubit, but then your fidelity is bad, then then then you don't have CRQC. So so um and and also if you have 6,000 cubit high fidelity, but the gates are actually quite local when you move things long distance um it becomes bad then it's also bad. So so one really need um all of these to come together and then and then it will be achieved. So, so for example, in some sense um there's also um people claiming they have 100,000 um atomic cubit but that doesn't turn it into CRQC. So, exactly. So, so, so the indeed um yeah like the numbers could cross maybe already or you already maybe has crossed um or maybe in 2028 it would be crossed but then at that point even when it crossed um a lot of things still needs to be taken care of which is >> we might it might cross at the early FTQC but you need to [snorts] get to 10 to minus 10 like rate >> which is and and for example if one look at here um even just improving physical error rate a little bit can change which also means If the physical error rate was slightly worse than one expected it would be bad. So >> yeah. So my question is about uh different class of application for the like uh application to simulating content matter system electronic structure simulation and those I I think there's not hasn't been as much effort to reduce that like overhead for those kind of application. Do you believe that those could be you know uh because right now if you do surface code error correction on um for [snorts] like focus simulation with a realistic noise model it would be 8 million cubits you know >> it's like people report 1 million but we have done the calculations much higher so I'm saying that you know and focus is the smallest things that almost simulable classically so what what do you think the electron for electronic structure or condensed matter simulation let's say a firmy hobart or transfer sizing model would be something that uh do you have any idea of what would be that >> yeah so we also thought a bit about that since in some sense the architecture that we just laid out here was a pretty general pretty general one and a universal quantum computer can in principle run anything so so one can also do the same calculation here um it depends on the physical model we would like to simulate if it's like a for example 20 x 20 so 400 cubit um um simulation of firmy hover model um I think in that context it would just be 400 logical cubits so definitely fits in here but then now the question is how many for example quantum gates do you actually need and that would translate into time pretty severely so [snorts] and and I think for some of these models um like smaller models it is possible possible to to also perform them um before CRQC is built. Um however um [snorts] for simulating actual molecules like forokco um it so far it does seems like the number of launchial cubit and also the the number of gates required in order to do it is is actually higher than than for example breaking ECC 256. Okay. So, so it could be the case that actually first one will run sh algorithm and then one will actually start doing scientific discovery. I think that's also a possibility.

>> Okay, thanks. >> Actually, I wanted to ask something very similar. So, I'll just follow up on this. Um, so with this architecture, basically what's very cool about is you really separate the memory and the and the compute, right? Um so does that mean that basically you know if I wanted to break RSA 496 instead of 448 I just add more memory and the time scales polinomally basically. >> Yeah. So so I think one would just uh um yeah increase the number of logical cubit. There's also easily tweenable things about these codes. There is this lift size. If you just scale up the lift size um the number of physical cubit and number of logical cubit just scales proportionally um with that so one can just scale it up and then and then um I think in terms of time it's a mild dependence on on the key size so >> and you can also you can also add more processors in parallel >> yeah in principle one can also have many many processor um like multi-core processor um there's also this idea called uh quantum GPUs um that was by Chen and also Chenhu and also um I think Yenziser's group um where the GPU now the processor becomes these like huge number of small processors that can perform simultaneous operation. So in order to speed time up there's actually a lot of tricks [snorts] um in the literature. Yeah, it almost seems that like we need a new model based on this and how do we it's not just like okay how many physical cubits do we have and how long it takes it's how many logical cubits we have in the memory how many processors we have and what's the clock speed and then you >> yes and also how one do IO how one perform the processing etc actually I think is really now the question is now really becoming very similar to classical architecture like classical people don't talk about how many bits they have like okay people talk about it maybe in the old time but But very quickly people started talking about the whole system design. Um and and I think we're entering that stage.

>> All right. Thank you. >> Yeah. >> Very very nice talk. Well done Robert. I think I met you just before your atomic went you know out of stealth. And I think I asked you this question. I'll ask it again. How many dollars to run in the best case scenario? How many dollars if you include depreciation and everything to run one instance? I think I think now a bitcoin is like $77,000 worth like one bitcoin, right?

>> So is it you think you can beat that with the with with say like a neutral atom? >> Yeah. So you don't Okay. I mean we're not building the business on stealing bitcoins. [laughter] >> That's not solution. >> I mean that's ultimately what sets the >> that's the evil actor. So [laughter] we're not evil. Um >> um >> [laughter] >> Um, so >> yeah, it's actually more about the biggest wallet. Um, it's not just about single bitcoin because um it's more about wallet. So, so, so if you Yeah, if you break it, you're actually breaking um one wallet and then you can take all the BTC off that wallet.

>> Okay. >> So, so one need to look at what is the maximum number of BTC in a single wallet. Um I mean these data are all open but I cannot I cannot recall from the top of my head but but it's quite a lot. Um and >> and then in terms of running uh in terms of building one of these machine it only costs less than 10 million. >> Um and then in terms of depre depreciation um not super sure. Um so so there are also slightly bigger version of these architecture um which will be there will be an update to our paper and that would describe that in a little bit more detail. Um but there's a slightly bigger version like about 20k physical cubit and by then the runtime can bring down to um like a few weeks like a week or two. So then one can for example continuously run that. So and and I do believe like I was just describing that with even better kind of architectural design and system integration one can create um even faster version of these quantum architecture.

>> So that could bring down the time a lot without really changing the cost of building one. So