# This Cryptographer Has a 10-Year Plan for Zcash - Zooko Wilcox

48 MIN · YOUTUBE · HTTPS://WWW.YOUTUBE.COM/WATCH?V=6G2GTYCKGM0
https://www.youtube.com/watch?v=6G2GtyCkgM0

SUMMARY

*The discussion centers around the evolving landscape of Zcash and its response to emerging technologies, particularly quantum computing and scalability solutions like Crosslink and Tachyon. The speaker emphasizes the importance of responsible innovation within the Zcash community, highlighting the need for a balance between maintaining security and adapting to new challenges.*

- *Quantum computing poses risks to cryptocurrencies, including Zcash, which is not yet quantum-safe.*
- *Zcash has a culture of responsible innovation, allowing for gradual improvements without jeopardizing user security.*
- *Crosslink aims to enhance Zcash's consensus mechanism by adding irreversible finality while maintaining proof of work.*
- *There is a focus on sustainability in Zcash's economic model, addressing potential future security budget issues.*
- *The Zcash community is encouraged to evolve and adapt, contrasting with Bitcoin's more rigid approach.*
- *Tachyon promises scalability improvements, but its implementation will require significant changes to wallet infrastructure.*
- *The speaker advocates for a modular approach to development, allowing for iterative testing and community feedback.*
- *Future visions for Zcash include widespread adoption, with the potential for billions of users benefiting from its privacy features.*

quantum computers are increasingly, you know, coming along and, you know, with new breakthroughs and new papers coming every week. It's not fair to say it's the quantum safe coin because it's it's not actually safe against quantum computers as it currently stands. I was like an OG Bitcoiner. What we're building here is something that is planetary for like hundreds of millions of users. This is a dangerous risky technology. I don't really separate money into store value and medium of exchange. I think it's like two sides of the same coin. Price is going up.

Everyone says don't change anything and ruin it. Don't ruin it. Yeah. Like don't touch it. >> And when the price is going down, everyone says devs do something. >> Yes. >> You are a Cypher Punk adviser. Why join Cypher Punk? Why be an adviser? >> Well, they invited me to be an adviser and it seemed like a good idea at the time. I thought Cippher Punk was going to be a DAT and even then I thought a DAT was probably a good idea to give various parties the ability to get price exposure to Ze that >> they otherwise couldn't get because of their organizational rules or structure.

>> Yeah, for institutions it's very useful. Yeah. >> And I trust Tyler and Cameron's intentions. They have the they have the right goals >> that I I share. So, and I get Cippy Punk like stock options or some some kind of pay, some kind of indirect pay for doing it. >> so, I agreed to be an adviser to Cyberpunk, which is one of only basically two professional obligations I've agreed to do at this point. >> The chief product officer at Shielded Labs and an adviser to Cypher Punk. One of the big topics that's been you know the main the current thing in the Zikash ecosystem has been quantum computing. As you may be aware quantum computers are increasingly you know coming along and you know with new breakthroughs and new papers coming every week. Some have like positioned Zcash as like the quantum safe coin.

Do you have any thoughts on that? like what's your perspective of like Zcash's position on the quantum problem? >> It's not fair to say it's the quantum safe coin because it's it's not actually safe against quantum computers as it currently stands. The best thing about Zcash is that there's a culture and a tradition of responsible innovation. >> Yeah. >> Like we don't move fast and break things, but nor do we like try to hold absolutely still.

>> Yeah. Yeah. Yeah. Yeah. Which is very important. >> and Zcash has a lot of really good cryptographers and security engineers who've been thinking about this since long before it became the current thing. And we've got some defenses against certain kinds of problems already built in. And some of the other cryptographers, not me and not Shielded Labs, but some of the other teams working on Zcash have developed a roadmap to to further protect the users against quantum computers over the coming years in a like responsible incremental fashion that doesn't disrupt or put everything at unnecessary risk, but also makes progress.

>> Yeah. Yeah. So, that's what I like about Zcash, but it's it's overselling to say that Zcash is the quantum safe coin because it's currently not. No, no major coins currently are. >> and they've all started like trying to move that direction or at least all of them except Bitcoin have started trying to move that direction. >> Yeah, we're not there yet. I think what's promising about Zcash is there's a lot of work being done about it. It's taken very seriously. If a quantum solution is is is put forward, my guess is that it would likely be adopted just because of the culture of Zcash, whereas you could argue that for Bitcoin that is much less certain due to a lot of like, you know, divisiveness in like the Bitcoin community. Do you have any thoughts on that? Like, yeah.

>> Yeah, I agree. Let me put it positively. I have this p practice I'm I'm practicing, which is don't say what's bad about a bad thing. Instead, say what's good about a good thing. >> for one thing, double negatives confuse me. But also it makes everyone focus better. So what's good I'm thinking about bad things about Bitcoin. Yeah. >> But let me express it as good things about Zcash. So a like we just said the Zcash community is willing to evolve like >> at the right pace carefully and responsibly but with intention.

>> Y >> and the other thing that you just mentioned is that the Zcash community is largely more like win-win oriented. Y >> like we may not agree on everything but we have a lot of shared values and shared goals and we can cooperate. I think that's really valuable long run for for building there's a concept I saw a lot with the original with with the Bitcoin culture. I don't know if you know but I was like an OG Bitcoiner. I don't know if you know but I'm the author of the first blog post ever written about Bitcoin.

>> I know. I know. and there's a there was there developed a culture there of it's sort of like took the network level and cryptographic level principles that you want to minimize trust, right? You want you don't want to be vulnerable or to take the word of another node over the network. Instead, you want to be able to verify everything and sort of defend yourself >> as a node. >> Yeah. And for whatever reason, people also applied that to the human level, like you're not going to trust any other humans, you're going to distrust them. It's like the the culture in which sort of bad faith is should be the assumption.

>> Yes, >> the assumption is bad faith. And that was a lot of people thought of that as they would say like Bitcoin is so important >> that we can't be like namby paming around with being nice. >> It's so important that we need to be mean. And I always thought, yeah, but like being nice works better. Like it's so important you want to be you want to get stuff done. >> Yeah. and human trust and cooperiveness and and focusing on the win-win opportunities gets stuff done in a way that distrust doesn't.

>> I guess we just got on to that cuz you mentioned >> something about the Zcash culture. >> I I agree. I agree. I I think one of the big positives I think we were speaking speaking of that earlier for for Zcash is really the the culture, right? This openness to innovation. I mean there's still like conser you know a conservative aspect a conservative aspect which I think is very important for store of value but the fact that we are open to innovation and open to the ideas of others is very important for quantum for maybe at some points potentially replacing proof of work for like these types of of things. so yeah, I agree.

>> yeah. >> Yeah. The world is never going to stop changing. Yeah. >> The needs of the people are never going to stop changing. >> I agree. Speaking of proof of work, so like one of the major focuses of of Chile Labs is is cross link. maybe let's first cover what cross link is because I think like the proposal has like changed quite a bit since like the original first IDs came about. and then we can you know go over like you know the the case for it some of the critiques and yeah discuss more about it if that's okay.

>> Cross link is a proposal to change the Zcash consensus algorithm by keeping the current proof of work in place and adding a finality gadget. >> Y >> so I kind of think metaphorically like proof of work which was Satoshi's big breakthrough contribution right. It's kind of like an engine, a self-powering engine that's always pushing forward. >> Yeah. >> Which is amazing and very useful. And then the finality gadget, which used proof ofstake technology to make the finality gadget work. And what finality is doing is like a ratchet that prevents backsliding.

>> Yeah. >> Okay. U proof of work by itself doesn't have a notion of when a thing is is permanent. >> Mhm. >> it can always be undone by by the engine pushing in a new direction. >> It's it's probabilistic. >> right. Well, that's what people say. >> And I actually think at like a a mathematical level that's a misnomer. >> you can't think about you shouldn't think about security as probabilistic if it's worth enough to the attacker.

>> Yeah. >> If they have the opportunity >> and they have the means and the motive >> Yeah. >> to take advantage of you. >> Yeah. >> It is just going to confuse you and mislead you if you think to yourself, there's a probability that they'll take advantage of me. Yeah. >> It's not a probability. It's whether they decide to and

whether they can't. >> Yes. Yes. Yes. Correct. Yeah. Yeah. That's always a risk. I mean, and we've seen like these reorg attacks like for example last week with Litecoin.

it does happen. But like I I I guess one of like the main arguments then brought forward by you know the other camp is well why not just improve proof of work currently because there's a lot to improve. like I mean until I think a month ago Zcash had just like one big minor via BTC. now we have Foundry as well. I is this maybe like a first path we should explore before like exploring cross link or or are these like >> not mutually exclusive?

>> Yeah, they're not I think they're compatible and they help in different ways. There are a bunch of other potential improvements to the proofof work component. Yeah. that the Valor team is now proposing like reducing the times between blocks other kinds of performance improvements >> and all of those are totally compatible with the cross link design because it's it's very modular. Like cross link keeps our current proposal, our design and the prototype that we've implemented which we're now experimenting with. You can you you can join the the channel and play with cross link and help us break break it. It's very broken right now and that's why we do this anyway. But the design is extremely modular like any any improvements including the new mining pool foundry and the reduced block times and and pro and like improved peer-to-peer networking so that blocks can get communicated and transactions can get communicated faster between nodes. All of that is perfectly compatible with crosslink. What cross link adds is primarily, let me try to think of the most important things. It's got like quite a few different benefits that I think it offers, but I'd say the two most important ones are irreversible finality.

>> Y >> so that when >> you can know if someone has deposited a million dollars worth of Zach >> guarantee >> into your exchange or or your deex like near. So this is what happened in year. Well, >> yeah, with Litecoin, they actually lost a lot of money. >> They lost $600,000, I think, in that event. And >> it's kind of confusing whether irreversible finality would or wouldn't have >> fixed that. In that case, >> transaction would have occurred. Yeah.

But in any case, in general, if you're operating a DEX or a CEX or you're accepting large transactions over the network, irreversible finality tells you that there's not a probability here. It's just that once once it has the stamp of finality on it, you know, it cannot be undone. >> Yeah, >> that's a much simpler and safer guarantee to reason about as a operator. >> Correct. Correct. Yes, that makes sense. And the other the second biggest advantage of cross link is that it magnifies the security budget in a sense >> and we we have a more precise technical definition of this number but people call it informally they call it the security budget >> and that's a thing which in Bitcoin and in Zcash it's tied to the issuance. Yep.

>> Right. And the issuance ticks down over time, >> of course. Yeah. >> And like with quantum, this is a thing where I I think it will be a problem for Bitcoin and I don't know if they have the right culture to be willing to make changes to address the problem. >> And in Zcash, it's got the same problem because Bitcoin and Zcash are the two coins that want to maintain a hard fixed cap on the supply.

>> Yes. There's only ever 21 million bitcoins, only ever 21 million Zcash. And almost everyone agrees to that.

>> That's the global. >> Very few people want to to change that. But there's substantial maybe 10 or 20% of all the Zcashers would be happy to change the supply in order to gain the >> sustainability. >> Yes. So at Shielded Labs we have two projects and one of them is cross link >> which we think can provide the sustainability and thus sort of harden the assurance that the supply will remain limited.

>> Yeah. >> Whereas with with Ethereum they long since accepted a variable supply in return for various other trade-offs. And in Bitcoin, I don't know what their plan is. It's like they're committed to the fixed supply, but they don't know how they're going to provide the sustainability. >> Yeah. >> So, two of Shielded Labs' project network sustainability mechanism and also Crosslink both contribute to sustainability while hardening the 20 million supply cap. >> Yeah, that makes sense because like the problem with Bitcoin is and and it's such a logical problem. I I I I fail to understand how people cannot see that it's a problem is if you're allocating like a security budget every year to mining which the inflation on Bitcoin is effectively and you're hving that security budget every four years you need the price to catch up and compensate which at some point it might not and when it does not when it doesn't you're going to be in big trouble because your security budget effectively hves and so at some points. It's practically guaranteed we'll need like an alternative system.

>> Seems like it. And there's transaction fees. >> Yes. But those are not enough. It's like a bitcoin. It's very low. >> Questionable. Yes. >> A thing about crosslink. One of the two biggest features or benefits of cross link is that if you take your security budget, your issuance, which can come from unissued coins, right? Because we're still below 21 million, so we can issue more. And it can come from past fees because with Shielded Labs's network sustainability mechanisms, 60% of the fees get burned.

>> So 40% of the fees goes to the current minor of the next block. >> Okay? >> And 60% of the fee gets burned. >> And in the network sustainability mechanism, everything that's ever been burned can be reincarnated months and years later to add to the sustainability. But maybe a dumb question, but wouldn't that then reduce the security budget for mining? I mean, I'm guessing that you're then rewarding miners less >> the fee burning or the issuance part.

>> Well, for the fee burning, like the fees you're burning previously, I'm assuming they went to minor, >> right? Currently, 100% of the fees go to minor. Yep. And in the NSM proposal, which is going up for some kind of governance vote shortly, >> but it's already been voted on once and everyone approved this part of it the last time around. But anyway, in that proposal, 60% of each fee gets burned. >> Okay, >> that only leaves 40% of the fee for the current minor.

>> Okay. >> However, that's enough to incentivize them to include that transaction >> because it's it's very cheap for them to add a transaction in. >> Yeah. Yeah. So your bet is that they will do it anyway and okay >> they're still motivated to include transactions. at the current levels like with Bitcoin the fees are very little. >> Yeah. >> in real money terms yeah compared to inflation it's >> but this is we're very like long-term and sustainability and like economic balanceoriented at Shielded Lab. Almost all of our projects are focused on like if we got this into place, got everyone to agree to it >> and then the world radically changed, how would the network do in that situation?

>> Yes. Yes. Yeah. Yeah. And I think it is very important to plan for like the future where like what we're building here is something that is planetary for like hundreds of millions of users. That's the plan. That's the goal. Yeah. we don't want to you know like it's nice to have our little community of like you know a few hundreds maybe a few thousands of people who are very committed to Zcash but the end goal is millions of users millions of transactions every day and yeah which will >> increase the fees increase the load >> increase all the sort of like stress on makers of software and services and everything and >> correct >> those hundreds of millions or however many users They make it much harder to change things.

>> Yes. Yes. Yes. >> I'm hoping to get these things in now because I think they're like longterm >> because later on it will be much harder. Yeah. >> Probably. Hopefully. >> Yeah. Hopefully. Hopefully. Indeed. Indeed. I guess to to close on the cross link chapter like one of the other critiques I I think Mert has given this critique. I I myself do resonate with it as well is that it might make the protocol too complex or too complicated.

Yeah, >> because you're introducing a lot of like new variables like proof of work is great because it's pretty simple like it's really just very simple like the miners guess like a nonsense >> turns out to be pretty complicated in practice but yes even simple things turn out to be really complicated so I really resonate too with that factor that critique that like complexity is definitely >> the enemy >> especially for store value. Yeah. >> Yeah. Right. because we want confidence, reliability, safety even in face of attack, attempted exploitation, all kinds of attacks from different parties.

I totally agree with that. There's an aspect of our current crosslink design which is kind of targeted that way. I'm not saying they're wrong to critique it. Like it's definitely two things is way more complicated than one. Like more than twice as complicated, right? >> two things is a a lot. Yeah. but there's an aspect of it which I'm pretty satisfied with and we've solicited some sort of independent analysis from like economics mechanism design >> to try to double check if we're we're getting this right but >> there are different components and each component only has one job >> y >> and so in a way that simplifies things like in the current in Bitcoin and in Zcash currently >> the proofof work miners People are counting on them both to keep making progress and including transactions.

>> Yeah. >> And not to backslide too much. >> Yeah. >> So they kind of have two sort of competing goals. >> Yes. >> and then they normally do this well, but of course it gets more complicated when due to load due to like bugs that are coming out from the cyber security AI >> wave, things like that. it it the complications compound. >> Yeah. >> And a thing that I really like about the current cross link design is now there's two components, but each one only has one job.

>> Yeah. >> The the the proofof work miners can't backslide or undo anybody's transaction. >> Mhm. >> even if they tried and they don't need to worry about that because the the finalizers it's called validators in other >> blockchains but >> in cross link they don't validate anything. All they do is put the stamp of approval that this thing cannot be undone. The irreversible Yeah. stamp. Okay. >> And so the finalizers, they just have one job. Just put the irreversible stamp on things and and never undo it. They as a component, they can be simpler.

They're not responsible for including transactions, dealing with all the other like >> Yeah. They do one thing, they do it well. And yeah. >> Yeah. So I agree. Complexity is the hard part and we're always fighting against complexity at all levels. >> Let's move move forward to a new topic like you were speaking about you know the other proposals of shielded labs being NSM and dynamic fees. Any update on those my understanding is that both passed both were put forward in the last NU7 I think voting proposal.

>> I think the voting was confused. >> Okay. Because the actual ballot said for for each of there was many questions like 12 or something different questions or 10 >> and the ballot said things like do you generally like the idea of fees being based on market conditions or adapting or whatever. >> Yeah. But then sort of the accompanying extra information said this question is about this specific protocol in a draft Zcash improvement proposal in like GitHub.

>> So now it's ambiguous. Are you voting for and against the general idea or are you voting for against this specific preliminary protocol? Anyway, a bunch of the like interest groups, the the there's a a a voting body that's all the core devs >> and there's like the Zcash Brazil community and then there's like the Zcash Foundation's long-standing advisory panel that's been doing this for like eight years or whatever. I think they all voted in favor of the dynamic fees item >> and then 80% of the coin holders voted against the dynamic fees item.

>> Okay. >> and one guy Dave from the Valor group posted his rationale on Twitter as to how he why he voted how he voted. >> Yeah. >> He voted against dynamic fees saying the reason was he disagreed with some specific detail of the >> draft protocol. Anyway, I don't know. I guess there's going to be another vote. Yeah, >> some like other people are organizing that stuff. >> I think there's also like still a lot of room for like the you know voting to be improved whether it being available in you know in Saddle in Zingo and other Zash wallets.

>> but also obviously like the questions should be like very very clear and simple so you know everyone knows what they're actually voting on and what they're not, >> right? Well, at least they're all voting on the same question as each other for starters. >> Yeah. Because Yeah. In in this case, for example, it's very hard to actually learn >> actionable information from it because we actually don't know what the reasoning was behind it. >> Yeah.

>> Like if actually people understood the right like the question and >> Yeah. >> Yeah. which question as you said they voted on. >> Yeah. It'd be interesting if there was some process. I don't know. I'm speculating here. It's not really my department, but it'd be cool if there was something that were more deliberative or people had to post their ration along with their votes or something, then we'd learn a lot more because just a a yay nay vote on a specific question could be interpreted a lot of different ways.

>> Yeah. or or maybe as as I think you you had mentioned in an earlier discussion have sub questions where it's yes to this specific outcome no to this specific like yes to this other specific outcome or like just no kill it and let's just not do this for example like you know for insurance curves like this curve this curve or just no curve at all like we don't change anything and I think that you that would be way more actionable and yeah just way more

useful >> makes sense and and this is an example of like responding to the previous vote by asking a more specific or clarifying question or or seeing if some people are going to shift and converge between then and now or something. So, it's more I don't know a interactive process than a oneshot vote.

>> I think you had had some conversations with Dyra Emma about conwed voiding and I think she was generally against it. You were in favor? >> I don't remember this conversation last year. or was this on the forum? >> I I'm guessing. Yeah. Like what's your position right now on coned voting? Like what's you know are you in favor of it? >> Historically there there was a time when most people who were active in the Zcash community were against it >> for for valid reasons. one of them was Vitalic Peterin who was always a Zcasher in addition to being an Ethereum person. And others were like Peter Van Valkenberg who's now who at the time he was on the Zcash Foundation board of directors. He subsequently stepped down from that in order to become the executive director of Coin Center.

>> Yeah, that makes sense. Y >> but Vitalik and Peter and others expressed concerns about like the risks or downsides of coin weighted voting and my position at the time was well yeah but those are risks if the coin holders have like all of the power. >> Yeah. >> All all the decision. >> And currently they have like zero power or zero voice at all. Like nobody even knows what they think much less will >> give them any credence.

>> Yes. And my position at the time was so I think they should have somewhere between like 1/3 and 2/3 of the power >> and then that's probably not going to run into those like total risks on that side and probably not the total risks on this side. This is >> typical of me to figure like the extremes are more risky and the muddled middle ground is probably safer sometimes. Okay. Well, >> I still think that I still think coin holders should have between 1/3 and 2/3 of the political power.

>> Yeah. It's totally unclear to me how much they currently have. >> I think it's technically a third, but like it's all in just like culture, right? Like I mean, >> right. Like that's the funny thing about political power is >> if you convince someone you have it and there's no point >> Yes. >> in resisting you, then you have it. >> Yeah. There you go. Yeah. Now, the one technical thing that I can tell without trying to infer a culture is that coin holders control I think it's 60% of the funding.

>> Yeah. >> Because 60% of the funding goes to retroactive grants determined solely by the coin holder votes. 40% of the funding goes to other kinds of grants controlled solely by the Zcash community grants committee. >> Yeah, I think of the 20% that is going to the defund, it's 12% that is going to one and 8% going to the other. Yeah, that's correct. >> Same numbers. >> Yeah, same similar numbers. >> so that fits nicely within my 1/3 to 2/3 range.

>> Yeah, one of the, you know, aside from cross link, one of the other hot topics in the Zcash community has been Tachon, which you know has been for a lot of people very exciting like you know the promise of like near infinite scalability. >> >> any thoughts or updated thoughts on on Tachon? First of all, I love the idea. >> Yeah. >> I love the founder, Sean Bo. this is not the first time he's come up with a breakthrough idea that seems >> Hello, too. Yeah.

>> Literally sort of incomprehensible to other people at first. Like Sean was the only one who got it at first. >> Yeah. >> Takan is very much like that for me. It's kind of hard to even understand how that's possible or how it would work. so I'm really excited and in addition to coming up with these breakthrough ideas, Sean is one of very few people who both the vin diagram of people who come up with novel scientific breakthroughs and the people who engineer stuff until it works and ship it is a very small sliver of a vin diagram.

>> Yeah. >> so that's it's all very encouraging. I definitely think Tachion like cross link and like all these changes that we've been talking about it's going to be a really good test of the Zcash culture of responsible evolution. >> Yeah, >> responsible upgrade. It's going to be very very difficult to get all the users and all the software implementations and and everyone to cooperate to deploy a new thing while you know maintaining a sufficient level of stability and safety for all the current users.

>> Yeah. >> Etc. etc. Especially because my understanding is with wallets with Tachion wallets will need to be completely I mean rebuilt essentially right I mean they need >> I think I don't haven't thought that much about it but yeah my instinct is yeah the >> everything changes >> everything about the and and the wallet is sort of the focal point right like the >> it's kind of like the wallet is the center of the universe and the blockchain is just one of these peripheral pieces that serves the wallet >> but I think one of the exciting thing with Tachon is that we'll have sufficient we'll have the ability to make postquantum Zcash scalable because you know with postquantum cryptography is very heavy it will make the transactions way way bigger which means that if we don't change anything in terms of scalability we will be able to do even fewer transactions than we are able to do today >> right >> so yeah any thoughts on that and like where you know Tken can help >> I may misunderstand understand some of this stuff like Tachon is not my I'm just like a fanboy of Tachon, right? My jobs at Shelder Labs include cross link network sustainability mechanism, dynamic fees, and supporting a bunch of mining pools and CEXs and deexs to like help them not get hacked.

>> Yeah. >> So, I don't like to sound off on things that are not my business, get in other people's way. Y >> Zachon moves a bunch of state management and transmission of data >> off of the blockchain. So that's great. That's a huge improvement. Although it immediately raises the question of okay then who does all that state management and transmission >> but even if we can if the Tachon team can solve all that we can get it deployed get all the wallets or some wallets to support it >> that extra bandwidth can be used for postquantum signatures and encryption.

>> Mhm. But that doesn't protect against a quantum computer counterfeiting Zcash, which is almost like the would be if you could just pick one thing to protect to prevent quantum computers for doing >> preventing them from counterfeiting Zcash would be a great pick. >> Yeah. Yeah. >> That's the thing they would probably want to do most if if they could do stuff to you. >> Yeah. and it makes sense the way the Tachon team and the Valar team have what little I understand of how they've been sketching out this road map is to sort of do the things that we know how to do now that we could do sooner >> and the things that protect privacy against future quantum attackers because >> if they want to violate your privacy they can look back in time to violate your privacy. So those are really good things to schedule first.

>> Y >> but it's like the end of the road map is sort of like a big question mark on the last step. And now we invent a way to prevent quantum computers from counterfeiting Zcash. >> Yeah. >> And Pachon doesn't help with that as far as I understand. >> My understanding is that that's also like a much harder problem which will which will take probably I'm guessing years. You know speaking of the initiatives of of of Shila Labs I think you mentioned Shil Labs has recently been helping miners exchanges etc to you know run on Zcash build on Zcash you know can can you say more about that? we are offering like professional support services >> and like it's like enterprise software support y >> right >> so we're prioritizing companies that are willing and able to pay us to do this so we can afford to spend all the time to do it >> and our dream and I don't 100% know how like if these companies are going to want to do this and how well it will work for all the other orgs in the Zcash ecosystem but I imagine >> it'll good for all the orgs that shielded Labs becomes the point of contact for like you know staying up all night responding to security concerns and then other people can focus on their building instead.

>> Okay. so we have like three more questions to go. So first question is I think last year two years ago you did a podcast with Arjun Kimmani and Josh Swehart. in that podcast at some point you guys had a a disagreement on the addresses >> whether or not they should be deprecated. My understanding if I recall correctly is that >> Josh was in favor of deprecating them and just fully go fully shielded. I think you like the optionality of having T addresses. any updated thoughts on that? yeah. Well, this is also not one of my jobs at Shielded Lab, so I don't want to interfere with other people's work. But also, it's a really good example of how like my opinions or other people's opinions, you you can go to the higher level and say the users, the devs are not in control.

>> Yeah. Right. >> Which is great. Let's >> like Yeah. It's a it's a a fascinating surprising thing about blockchains and open permissionless systems unlike the previous few decades of software where basically the devs could do anything they wanted and the users >> had no choice in the matter other than stop using that software. That was your your one option. >> Yeah. >> but now suppose all of the devs there's a bunch of different >> Zcash development organizations now which is pretty awesome. like I'm starting to lose count. There's like six or seven >> funded, skilled, dedicated Zcash focused >> development orgs, which is amazing. And wow. okay. So, imagine hypothetically all seven or however many got together and said, "Let's turn off T addresses." And suppose whatever we can keep going. The Zcash Foundation's advisory panel all voted 80% were in favor of turning off Z addresses. The coin holders all voted 80% in favor.

Okay. Suppose new full nodes and wallet software got uploaded to the app store. Y >> and the difference is when you install this one, >> all your money that is in a T address is now >> shielded. Yeah. >> No, I was going to say it's now inaccessible. >> Oh, okay. >> Right. Like you can't let's just say whatever like >> Yeah. Hypothetically >> the easy way to do it is just make T addresses invalid in the blockchain.

>> Yeah. which effectively means burning everyone's money that's currently in T addresses. >> Yeah, >> there's no way to like force shield it all. >> So let's just say for the sake the point of this story is the devs cannot take away a feature from the users, >> right? So if we did all that, we went through that process, we uploaded all that software, >> any users who still wanted to keep their money that was currently in a T address or they still wanted to be able to send and receive with T addresses, >> they just wouldn't install that software. they'd keep using the software they currently have which currently works for them. Like I do think there's like a a very

important aspect of T addresses for like institutions for exchanges where for example as we were speaking of earlier you wouldn't necessarily want an entity like Cippher Punk for example to have their coins shielded because that would prevent transparency so users would not be able to audit >> that Cippher Punk does indeed hold these tokens.

>> Yeah, transparency is good for some purposes. Yes. and that optional, you know, and especially for exchanges who want to, you know, stay within the law. well, >> they may be forced to, you know, >> the law, but also if they're custodying someone else's funds by someone else. >> Yes. >> I mean, I would rather they did that transparently so we can all watch >> on the other end.

>> that would be less that would be sort of a mixture. It How would that be better? >> I mean, I guess you could then say, "Oh, we're fully shielded." But if you want transparency, you can use a view key. It's kind of like the same thing. But >> it's the same thing. It's just more more steps. It's transparency with more steps. And more steps is bad because that makes it harder >> for the users. It makes it easier for people to get confused or to get scammed or tricked. So anyway, >> yeah, >> I agree with you or I agree with what you were saying that transparency has its uses >> and also just in general like if the users I I really like a certain kind of humility like >> if I think 80% of the people out there should behave differently than they do.

>> Yeah. >> It's like I'm not wrong, the children are wrong, right? like maybe they know something I don't about their lives and their priorities and their situation. >> Second question is regarding cross link. I mean as I'm guessing you're well aware there's been a lot of back and forth around that in the community of people in favor of people against it. like you know we were speaking earlier in this conversation about like some critiques and and as in the case forward obviously what's the realistic political path for cross link to get to mainet do you have any timeline what are the next plans the road map yeah >> I don't know about the political future like how will people's feelings change I could guess or speculate like one thing I really think is >> coin Prices influence people's feelings.

Like when the price is going up, everyone says don't change anything and ruin it. Don't ruin it. Yeah. Like don't touch it. >> And when the price is going down, everyone says devs do something. >> Yes. >> And also the a lot of the opposition to cross link and and a lot of the other recent like governance and strategic and mimetic debates within Zcash have been about comparing Zcash to Bitcoin. that that whole movement was the Zcash equals encrypted Bitcoin movement.

>> And so that's where I think as long as the Bitcoin price languishes, that movement will lose >> steam. >> It'll be less and less exciting to people to be like encrypted Bitcoin. If Bitcoin is not going up, if Bitcoin starts going up again, then everyone's going to start saying, "Let's be like more like Bitcoin." >> But okay, so I don't know about politics. Hard to predict whatever what we're doing spending a lot of effort on.

And I and I'm excited about how I think it will be also useful for Tachion and other things in the future. >> Yeah. >> Is assume you don't know about politics. Assume >> Yeah. >> there's conflicting opinions or opinions change over time. >> Yeah. >> But you can develop and test and get people to start using the thing. >> Yeah. The

more you do that then the more knowledge and understanding people have the more mature the thing is and the more you and others can judge what are the actual tradeoffs >> of this >> there might or might not be a future so that's what we're currently doing with crosslink we've got this prototype that we've implemented it's very buggy which is very good opportunity to find bugs and learn how things can go wrong >> and we've got a very active community of developers who are like building their own block explorers and patches and stuff and just users who want to run it and see how it runs. so there's a really good feedback loop both like we're learning from them and they're learning from shield labs etc etc etc.

>> I think that's a really good process. in the past we had the opposite process in Zcash which was like the whole community will decide if this is a good idea. having made that decision then some developers will go off for the next few years and implement the thing >> and I think that's the wrong way around >> and a good example is like three years ago the entire Zcash community except for me >> said that's a great idea we should definitely prioritize that as one of the most important priorities so now a bunch of developers have spent three years and millions of dollars implementing that thing >> at which point some faction or >> one-thirds or two3 thirds or whatever of the Zcash community said actually we don't want that thing but like it's both too late and too early. We don't even know how ZAS would work in practice because no one's ever implemented a wallet and ever >> to my knowledge maybe someone has but I've never seen a wallet that could actually use a ZSA for anything.

>> U but it's also too late because we've already spent millions of dollars and many years of a skilled team's time to implement it anyway. So, we're trying to do things in the other order with cross link where you implement it first, you can see how it works, what it does and doesn't do, what the trade-offs are, >> and then either the Zcash community changes their well, the ones who currently oppose it change their minds and say, "Actually, that doesn't look so bad."

>> Yeah. >> And then we could collectively, the whole Zcash ecosystem and community could upgrade the main the central mainet to add cross link. especially because we've designed it to be very like modular and sort of deployable. >> Y >> or if they're still not into it, then we have this interesting situation where you've got this like it's kind of like a side chain. It doesn't have the >> the economic linkage to real Ze, but it has like the community and the functionality.

>> I don't know. There may be some way to like keep it keep it growing >> on the side. Anyway, I wouldn't be surprised if this same sort of process turns out to be good for Tachion. >> Yeah. Yeah. I I speaking of the side chain, I think one of the proposals someone has floated around was the was the idea of having like some sort of like canary network as they call it, >> you know, sort of like polka dot as like Kuzama I think it's called. where like we can kind of like go crazy and like I mean go crazy you know within certain bound >> fast and break things you know in a safe space >> to so that we can be maybe more conservative on the main chain >> and then only really implement like the really you know very very solid stuff and yeah that that's a very interesting >> that's really interesting and it relates to turn styles one of my other favorite technologies also underappreciated for for many years but now Now people appreciate them because they've saved our bacon multiple times and >> and it's one of those Zcash innovations that I hope >> other cryptocurrencies and technologies will sort of start >> like I think they'll eventually realize once they're once they have the hard experience themselves of oh if only

we had had a turn style here. Wouldn't that be great?

>> and turn styles like these side chains and this canary network. It's like you could imagine hypothetically, I don't know how this would work, but you can imagine we're going to make a pool >> that is going to be interoperable with the Zcash main chain, but this is a dangerous risky technology. So, it has a turn style and there's like a limit. You can't have more than 10,000 Zcash in this pool at a time. >> Yeah.

>> Or or you can't move more than 100 Zcash a day into this pool or something like that. Then if this one has a catastrophic failure, it's not going to hurt everyone else who who chose to not risk it. >> Exposure is limited. Yeah, >> it's interesting. I I don't know. There's a lot of possibilities for their future. >> Yeah, it it's definitely something that should be considered. for sure. I agree. Yeah. last question is for the future of Dcash. What's what's your vision? I I I know you wrote this blog post was it a year or two ago about like honoring the the holder? what's your you know your vision of Zcash for the next decade or so how how do you vision envision Zcash I know a lot of people have now you know started really thinking of Zcash as a store of value but I mean there's like cash in the name Zcash >> so as you know >> >> have you a particular opinion about that about the use cases about the you know your your vision of Zcash has that changed >> I think of I don't really separate money into store value and medium of exchange. I think it's like >> two sides of the same coin or whatever.

The chicken and the egg, >> it's really the same thing. >> >> my vision is Zcash continues to grow in distribution, users. >> Yeah. and security and sustainability. >> Yeah. >> because like people's expectations or confidence level about what might happen 10 or 20 years from now >> is an important part of >> correct >> the of this this product this concept.

>> >> I think you asked me about 10 years. I can imagine Zcash steadily growing to have more and more users who are thus empowered and it's way more useful and way more valuable with a network effect. The more different kinds of people use it, the more people use it, the more useful and valuable it is to everyone. >> Correct. >> Yeah. Yeah, that makes sense. Do do you like 10 years from now, how many you know, let's let's do some numbers. How many millions of users would Zcash have? like what are what are the goals like how you know what would you be happy with what would be your success >> 10 years from now so we have to assume that tachon works or tachion 2 works or something >> yes >> solves that fundamental problem >> y >> and then I'm allowed to go into science fiction here you asked a science fiction question I'm allowed to give a science fiction answer >> I think I can imagine everyone using Zcash except for the like enslaved humans who are not allowed to do anything without the permission of their >> AI masters serving like Kim Jong-un or whoever the ruler of the universe is by then. But the other few billion humans.

>> Yeah. >> or tens of billions on all the different planets. They all use Zcash because it's got the network effect. >> Yeah. where that's the that's the thing that's that's safe and that they know will work for any other person they want to >> cooperate with anywhere. >> That makes sense. That makes sense. yeah. Well, it was a pleasure talking to you. Thank you for >> and yeah, maybe let's do an episode in the future again. Was a pleasure.

Thanks.