TFTC 446

**Matt:** [00:00:00] If your phone catches fire, then maybe, you know, you had to have it on the cloud somewhere, and have a live backup. That doesn't change with L2, right? With L2 you get, that data doesn't grow unbounded, it doesn't like keep increasing in size, it's just fixed size. But you still have to do that same, that, that step that adds all this latency and adds all this complexity, you still have to do it.

And the reality is, even though the data today grows unbounded in size, it's just not that big. Um, and so, like, it, to my, to me it doesn't solve that, that hard part of the problem. And

**Marty:** something like VLS solve that in a more creative way?

**Matt:** No, I mean VLS has the same problem. Also, anytime it does an update, it has to, like, durably save the fact that it's about to do this update to disk somewhere.

Um, or to the cloud, or, you know, live backup, whatever [00:01:00] the, your, your storage solution is backing your lightning node. You know, you always have to, every time before you do an update, you have to do these live, these durable writes. What does fix it?

Nothing. I mean, it's not like the hardest problem in the world. Like, it's fine. We can do durable writes. This is a solved problem in computer science. It's just a thing we have to do. And, like, that's the, to my mind, that's the annoying part of lightning storage. Not this, like, oh, the size grows unbounded.

It, like, keeps growing and growing and growing. That isn't the hard part to me. And, in fact, with splicing... You know, if people start using splicing, once you splice, you can throw away all your old state. So it's like, oh yeah, it kept growing unbounded, and then we spliced, and then we threw it away, and now it's back to zero, and we start again.

So it's like, okay, well, you know, that's not a lot of data, I don't...

**Marty:** Alright, let's get into it. We're already recording. Did you hit go? [00:02:00] Oh, we hit go already. Oh, alright, that's

**Matt:** all hot mic? That was all hot mic.

**Marty:** Alright. We got Matt Carallo back in the studio for the first time, and... First time in person since Williamsburg when it was me, you, Val, Eric, and

**Matt:** Matt.

Yeah, it's been a minute. That was

**Marty:** a while ago.

**Matt:** Yeah. Thanks for having me back.

**Marty:** Thanks for coming back. I left New York, you left New York, I'm in Austin. I'm in

**Matt:** SF. How is SF these days? It's good. It is, it is good. Um, don't go downtown, but that's true of a number of cities. Um, but aside from that, like, you know, the city's back, there's a lot of people there.

As always, SF has great nature, lots of places to go. Go walk, go be in a forest. Um, yeah, it's good. Do you

**Marty:** miss New York at

**Matt:** all? Yeah, I like the energy, but my wife likes, uh, likes SF, so.

**Marty:** I don't want to, uh... Derate the [00:03:00] Austin bit devs because it's an incredible bit Dev, but the OG bit devs, I do

**Matt:** miss. Yeah. It's hard to beat the New York bit devs.

They just celebrated their 10 year anniversary. They've been doing bit devs in New York for 10 years. Yeah, it was the 200th

**Marty:** bit devs, wasn't it? That

**Matt:** was a while back. Was it 10 years? Was a month ago. Mm-hmm. , or not even, it was like

**Marty:** two years ago. Yeah. Yeah. Um, well, anyway, Logan Ninja launched us into hot mic.

We were discussing. The original question I asked, talking about all the potential soft forks that people are discussing right now, whether it be drive chains, OpCTV, OpVault, in APL, that's what we were talking about was APL. Yeah. Somebody working on LDK. I was running with the assumption that maybe APO would be appealing to you.

**Matt:** Yeah, I mean, I think, you know, A, I'm really excited that the people are working on Covenants. I think we need some kind of Covenants scheme. You know, obviously Covenants, the word is a little overloaded now. All of these things actually do subtly different [00:04:00] things. Um, have very different properties in terms of what you can build, what you can build easily, what you can build cleanly.

Um, but I am excited for the future of things. People are talking about building these payment pools, these, um, all kinds of cool things, but you know, the lightning world is very excited about building L2 and thus kind of is pushing increasingly for what is the minimum set of things we can change to get L2 and that's largely APO.

Um, and. And I'll piss off a bunch of the Lightning folks saying this because they all, I think, strongly disagree with me, so take what I say with a grain of salt, but I don't care very much about L2. Um, I, I don't think it solves the hard problem. We were just chatting about this. I don't think it solves the hard problem in Lightning.

The hard problem in Lightning is every time I make an update, and this is multiple times per payment, it's like four times for every payment you want to send or, um, or receive. [00:05:00] Yeah, yeah. You have to, like, take whatever data you're, uh, uh, information about this update and you have to write it to disk, you have to make sure, you know, if you're doing a live backup, you have to, like, write it to your, like, cloud backups engine, you have to, like, do whatever you have to do, but you have to make sure this hits disk and that, like, adds a bunch of latency, it adds a bunch of complexity, um, especially if you're talking about, like, a phone and you want it, you know, you don't want to trust that the phone's not going to catch fire or whatever, um, Hmm.

That is hard, and that's a lot of work. I mean, it's very solvable, but it is a lot of work. And APO, uh, and L2 specifically doesn't change that. You still have that property. It's just that that, that amount of data doesn't kind of keep growing, right? So like Lightning, the data you have every time you do one of these writes, you can't throw away the old stuff, you're just adding more stuff on top.

Um, and with APO, you, you replace the old data. You can throw away the old data, you just, every time you do one of these writes, it's pretty small, it's nice and compact. That's cool and that's great, but the [00:06:00] total amount of data just isn't that big in Lightning. Um, and as we move towards splicing, uh, if people start using splicing, every time you splice, you can throw away all your old data, that resets your state again anyway.

So, it, to my mind, like, you know, if you're a mobile phone, and you're just sending a few payments, Your data is never that big to begin with, because you're just sending a few, you know, routing payments. If you're routing payments, I mean, you're on a server that's online all the time, you can buy a terabyte SSD for 30 bucks.

Like, why are you worried about your data storage that's on the order of less than a gigabyte? You know, why, that shouldn't be a concern of yours. So it's not something I'm, to my mind, it doesn't solve a lot of the important problems in Lightning. Um, it's cool, it cleans up a lot of stuff, it simplifies stuff.

Um, but... It doesn't solve a lot of the heart problems. So,

**Marty:** yeah, well, he's saying that it really makes me think [00:07:00] back to the conversation I had with Rob Hamilton a few weeks ago, obviously he's working on mini script at anchor watch and a big part of that discussion we dove into. The perspective soft forks that people are talking about.

And then we really leaned into, okay, these things could be cool. Uh, we don't know how they're going to get merged. We don't know how we're going to come to consensus to, um, actually activate them and we really fell back on like, all right, let's just run with the assumption that none of this ever gets.

Merge. Not that none of it ever gets activated. Maybe we should be focusing on pushing the limits of what we have at our fingertips right now. It seems like with this particular subject, there's things that we can do without a p o to make the thing that make the process better, more efficient.

**Matt:** Um, yeah, I mean, I don't know.

I, I feel like we, we should assume we should get some of these things eventually because we do need [00:08:00] them for things other than lightning. Um, you know, I think I keep coming back to this like, you know, if we assume. That Bitcoin is truly going to go global in a big way that we, that we really need. You know, Bitcoin is all about like being able to transact without trusting someone, without trusting anyone specifically, but usually because you don't want to trust one in specific.

Um, and if the world we end up in is like you can only use Bitcoin custodially, obviously we've lost that value for a lot of use cases. Um, and so if we assume that like, all right, let's assume a country is going to implode tomorrow and Uh, they need to be able to onboard to Bitcoin and, uh, you know, they're, they're not going to move to a stable coin for whatever reason, uh, they're going to onboard to Bitcoin.

We can't have every. Individual have a UTXO, which is the current lightning model, right? That like, you know, everyone's going to have a UTXO. Maybe they're going to do [00:09:00] a few transactions to get the liquidity right for their channel with their LSP or whatever. Um, but they're going to have their own UTXO or maybe a UTXO between them and their party.

And there's, there's other things you can do. There's like these multi party channels with trees of transactions. They also. a lot of overhead, um, and they're not going to scale that far. And maybe you can get another few X on top of, uh, where we are. But at the end of the day, we really need to get to a world where multiple parties together share a UTXO on chain.

Um, and. So you can do that kind of one of two ways. You can do this kind of lightning multi channel world where you have like an end of end multi state grapes, like 10 people are going to share this UTXO and it's a 10 of 10 multi state and we do state updates like we do lightning and all 10 people have to be online at the same time in order to do an update or have to at least be able to exchange messages to do an update.

So obviously this doesn't scale. Like everyone has their phone. They're [00:10:00] not online all the time. We can't scale that to, you know, a thousand people because then you'll never be able to do an update. There's always somebody offline. There's always somebody who like won't respond for a month. Like that's not a solution.

Um, the other world, if we have covenants, we can build payment pools so we can build these multi party UTXO schemes. Now I don't want to be. To kind of like, this is the solution because there's not a lot of concrete solutions here. There's like, various proposals that are, um, There's more naive payment pools.

There's like, kind of the ARC thing, which doesn't scale very well either. Um, so, there's a lot of ideas in this space and there's a lot of excitement in this space. There's not... A lot of like, real concrete, Oh yeah, that's been worked out, Someone's really designed this all the way to the end, And it's clearly gonna work, And we should like, be deploying this now, We should be thinking about this now.

Um, but there's a lot of excitement in this space, And You kind of have to end up there in one way or another. [00:11:00] Um, so I do think we need some kind of fork to get us there. It is not clear to me which one, um, and we don't need it now. We've got a while. So we can get this right. We don't have to rush this. Um, and I don't think, but I don't think we should just be like, let's just focus on what we have now.

Let's just like build with Bitcoin as it exists and not worry about this in the future. I think we do need to get there. It's just we can take our time and get it right. Let's not try to like rush into this. Let's not, you know, be like, ah, we have to do, you know, APO today because we need L2. It fixes important problems in Lightning.

No, we can wait. Yeah,

**Marty:** it's interesting because. There's a couple factors you have to take in here. It's like, I agree, I think we can wait. And, I also agree, I don't think we should just say, like, this is never gonna happen. Let's just push the edges [00:12:00] to what we have now and see how far we can get. I think we should do that and have these conversations in parallel.

But then you have this overarching theme of burnout within the core project where it just gets really frustrating for the people that are pushing these ideas and they've been waiting a while already. Like how do you keep people engaged and

**Matt:** motivated? Yeah. Um, You know, I think Bitcoin Core is doing a lot better than it was, yeah, a few years ago.

Um, you know, there's this kind of this, this long, there's this kind of story of Bitcoin Core where it's like, you know, during the, the block size wars, there was a lot of intense focus, um, a lot of people trying to do a lot of really good work to like, you know, to show that, that Bitcoin Core, you know, is, is You know, moving forward, et cetera.

Um, there was a lot of pressure at that time that led to a lot of burnout kind of as soon as SegWit2x imploded. Um, basically, I mean, [00:13:00] maybe I shouldn't say this, but we were in the chain code office and like the announcement came through the Mike Belshi sent that famous email. It was like SegWit2x is dead.

We're not doing this, whatever. Uh, and we pull out the whiskey from the top shelf. Like it was, I don't know, 11 AM or something. And we were like, all right, we're just drinking today. It's all right. Um, and. And so, but I, but I think that really did, you know, I think at that point. People kind of stepped back and people said like, Okay, there's all these other projects I want to do in Bitcoin.

Some people wanted to do other projects outside of Bitcoin, but other projects people wanted to do in Bitcoin. You know, I spent time working on, uh, you know, I started working on Lightning stuff. Other people started working on other pieces around Bitcoin Core that aren't necessarily Bitcoin Core. And that sucked the wind out of Bitcoin Core all at once.

And at the same time, you had a bunch of people trying to get excited and like contribute to BitcoinCore and all the people who'd been doing it for a while stepped away. Um, and suddenly you just had a bunch of people who like didn't know the project super well, were kind [00:14:00] of new to the project, trying to contribute, you know, doing good work, but like didn't know the project very well and not a lot of mentors to help them out.

And so that, that caused a real issue in the culture for a while. Um, but that, that's largely fixing itself now. You know, those folks who were getting involved at that time now know the project really well and are still working on Bitcoin Core. Um, and so there, there is a lot more momentum. In the Bitcoin Core project to really ship new features to really, uh, get stuff done with a lot of people.

There's a lot more excitement in that project now. So I do think Bitcoin Core is a hell of a lot healthier than it was, you know, even two years ago. Yeah. Um, but to your point, you know, when, when Twitter is spending all its time talking about like, Oh, we gotta, we gotta get one of these soft forks activated.

I prefer this one. Screw you for liking that one. Whatever. Yeah. I mean, that, that does. You know, it drives a little bit of burnout, but also I think Bitcoin core folks are just going to ignore that because it's [00:15:00] like, you know, there's not all, there's not a strong technical. There's like some, there's some thinking that maybe we should do this, something in this vein, et cetera, et cetera.

But like which one? And like, there's not really, you know, there's some arguments being made here. There are technical arguments that like this one is better, that one's better, whatever, but there's not a lot of great. And, and to go back to the point about like, you know, we want to build these payment pools, but they're not really fully thought out and like fully designed.

So it was like, how, how should someone be thinking about designing? A soft fork to enable these things if these things aren't fully fleshed out and fully like scoped out. Um, and so there's, you know, there's kind of a like, well, it's, it's not, it's not there. It's not like there's not a good way to evaluate what we should or shouldn't do yet.

And I think that's still a ways away. Um, now to the credit of some of the folks working on these covenants design, there is a [00:16:00] lot. Of work going on to formalize how to think about different ones and, and, and compare them. Um, so that's making a lot of progress, but, you know, people on Twitter just screaming about, we gotta do this one, we gotta do that one.

It's just not, it just kind of gets ignored and it's certainly not helpful.

**Marty:** Yeah. Do you think ultimately what will lead to something getting activated is something similar to SegWit2x where you have this pressure? Maybe it's not like... I hope not. I mean... Maybe it's not people like threatening to...

Arbitrarily double the block size and do what they did back then, but maybe it's economically driven this time around where Bitcoin Garners significant attention and adoption and we sort of reached the limits the UTXO limit that you were describing That sort of forces like alright, we really got to figure this out

**Matt:** Maybe I mean I wouldn't assign a high likelihood of like a massive flood of users in that vein And you know, [00:17:00] maybe we should talk about that But I wouldn't assign a high likelihood of like massive flood of users suddenly getting on boarded and this causing, you know, massive, uh, fee spike in that way.

Um, as super likely in the next few years. Um, and I certainly hope we're not put in a position of trying to rush things. And, you know, I mean, if we don't have a good payment pools design. Then trying to rush a soft fork to ship payment pools isn't going to help anything because we don't have a good payment pool designed to like actually build on top of the soft fork.

Um, so I, I, yeah, I, I, I don't think we're likely to see that outcome. I think we probably have some time. We can get it right. And I think, you know, eventually there will be like Taproot. I mean, there wasn't a lot of pressure to rush Taproot. There wasn't a lot of, you know, there's, there's Demand for snore.

You can do multi state a lot easier. There's a lot of folks who wanted it, but didn't need it. You know, there's a lot of folks who were like, yeah, we can do our multi state way more [00:18:00] efficiently. You know, maybe we can do a more private lightning. We can do more private, other things. It's great, but it's not like existential to Bitcoin.

It's not like really important right now. So I think we've got. Time and I I think more likely we're gonna end up there. Yeah huge pressure.

**Marty:** We got time So with that in mind, I think you were alluding to it Like what is the state of Bitcoin overall in your perspective from the adoption perspective?

**Matt:** Yeah, kind of.

Um, yeah, I mean, it's a good question, you know, obviously Twitter is now There's a lot of, uh, It's a crap bucket. Yeah, I mean, social media in general. Um, but there's a lot of, there's a lot of narrative around, you know, has Bitcoin failed as a, mechanism of of exchange, medium of exchange, you know, whether that's payments or settlement, whatever it is, but kind of, you know, moving a lot of value back and forth.

Um, you know, has Bitcoin kind of [00:19:00] kind of fallen flat on that front and and lost the stable coins. And I think I mean, largely we have right. It is true that for

Bitcoin fundamentally is all about providing a currency and a value transfer mechanism and a value movement mechanism where you don't have to trust anyone else. That's the goal, that's the North Star, that's why people are, or at least I hope are, Building in Bitcoin, care about Bitcoin, et cetera. And there's a lot of factors to that.

There's like, yeah, I don't want to trust the fed because money printing and something, something, I'm too inflation. And then like, I, I worry about that there's, Oh, I, I don't trust my local banking sector because they're forcing me to use, you know, Argentine pesos. And these are inflating away or, you know, I don't trust my, my local banking sector because they are, you know, if you're.

The history of [00:20:00] redlining, you're a black American, you know, you're worried about banks, you know, charging you a, a high fee, you know, because you overdrafted right when you, you know, you're poor in America, you, you get whacked with a fee right when you can least afford it, and that sucks, you don't trust your banks for that reason.

Whatever the reason is, there's some reason you don't like the solutions available to you. Or there are just no solutions available to you, so you use Bitcoin, right? Um, and on some of those fronts, you know, stablecoins don't compete. Obviously, if you're, if you're thinking, I don't trust the Fed, stablecoin's not going to solve your problem.

Um, but if you're thinking, oh, I don't trust my Argentine pesos, then stablecoins

are a competitor there, right? Like USDC, USDT, whatever it is. Often USDT on Tron. Um, and... In that particular use case, Bitcoin is obviously not winning, right? Obviously people are preferring, uh, dollars for, for many reasons. They just prefer [00:21:00] dollars as a, as a much larger brand in most of the world, uh, in all of the world, probably.

And so I do think we. As Bitcoiners need to consider how to build better for those people, you know, if we think that Bitcoin has value for, you know, if we think that, uh, you know, in the long term, you know, are these stable coins sustainable, these centralized issued stable coins sustainable from a regulatory perspective, you know, are they sustainable from, uh, you know, just from a practical perspective in many ways.

Can you trust

**Marty:** Tron? Is Tron well maintained? Yeah.

**Matt:** Well, uh, yeah. I mean, I think most people using, uh, USDT on Tron aren't using it for very long, right? They, they, they have a USDT balance on, on Binance or some big centralized exchange. They move into Tron, they make a payment with it and they move. They have moved out.

Um, so people aren't trusting it for very long, which is great. It, it worked well for them. [00:22:00] Um, there's this kind of, there's this meme in crypto, right, where it's like the, the, the three parts of crypto. There's like the, the scientists and the engineers and they're all like trying to build, uh, you know, the best system they can and coming up with all these clever ideas.

And then there's like, there's the priests and it's like the Bitcoin versus Ethereum people. And they're all fighting for their chain to win. And then there's the Solana people also fighting for their chain for some reason. Um, And then there's like, the actual product market fit, and it's people just sending USDT on Tron, and that's the only, that's where the PMF is.

Um, and, and to some extent it's true, and, you know, I, obviously, a lot of the value of Bitcoin is also people not trusting the Fed and people not trusting the, the financial system and wanting this truly trustless money, and, and we cannot compromise on that front, but we should also be building things For other users and we should we should take our North Star and still build things for people who want dollar denomination, right?

So let's not go down the same path and just build, you know, [00:23:00] issued assets on Bitcoin. Not not to call anyone out. Let's not just create these centralized issued stable coins again, because What's the point? We're not going to beat Tron. I mean, it's basically a database. It works great for these fully trusted systems.

We don't need to, we shouldn't be trying to compete on that. Let's actually build something that follows our North Star of having, not having to trust anyone or certainly having to trust as few people as possible. Right? So let's build DLCs. Let's build, you know, if you want it. Stable us dollar value with the ability to pay over the Bitcoin rails, which I think is something, you know, if you're a Bitcoin, you hopefully think.

People will value, you know, you hopefully think that, that there's some value to the world in having the monetary rails be open and trustless and not having, you know, circle or, or tethering, you know, Bitfinex, um, having the ability to say no [00:24:00] and, and, and, Take your money, block your payment, whatever, based on, you know, whatever chain analysis happened to say today, um, if we think there's value to that, then we should be building that.

And we shouldn't be building just the same thing again. We should be building something better. You know, you can't build a stable coin without having some trust. And that has historically always taken the form of either issuer tether circle.

Um, and I think obviously given the two options. An oracle is a way better option, they're much lower regulatory overhead, you can more easily federate it, you can have a ton of different oracles and you, you trust, you know, some, some subset of them. Um, so, but let's build that, you know, there's like the 10.

10. 1 guys, there's, there's various other folks trying to build DLC based, you know, dollar denominated wallets in Bitcoin using lightning where you can just pay over lightning. That's awesome. Like that is as trust minimized as we can [00:25:00] get and you know, that's that's a more trust minimized stable coin than Almost anything that exists on ETH.

There's some that that try to do something similar They don't have a lot of usage and you know, you look at like Maker or whatever that they've died. They've all moved to USDC. USDC as their backing, or USDT and USDC as their backing, which, you know, what was the point? Why we haven't built a decentralized stablecoin?

Um, so, you know, let's focus on building these things, and then let's try to compete in the marketplace. Because it is true that Bitcoin is failing in some of these markets where we should have, have some value. And it is harder, you know, we are trying to hold ourselves to a higher bar. Then USDT on Tron, but let's, let's build to that bar.

**Marty:** Yeah. No, you mentioned the 10, 10, one guys. We were talking about them yesterday, I believe last week or the week before they, they launched, um, a CFD DLC, a contract for difference, right. [00:26:00] Um, and they're leveraging crypto garages. DLCs over Lightning spec, right? I

**Matt:** don't actually know offhand. I

**Marty:** probably should know.

Is it extension signatures?

**Matt:** Uh, um, You're thinking of, um,

Yeah, I know what you're talking about. They had

**Marty:** to use a hack because PTLCs don't exist yet.

**Matt:** Right, yeah. And that's also coming, um, in Lightning. People are working on it more now, um, now that Taproot and Lightning is starting to be a thing. Um, you know, again, one of those things in Lightning, Taproot in Lightning doesn't really add any value by itself, but it enables PTLCs in the future, which is, which will be really nice.

Um, but yeah, I, yeah, I mean, there's people building in that space and it's really awesome, but we should, we should have more, we should have more in that space and we should have competition in that space and actually give Stablecoin some real [00:27:00] competition. I

**Marty:** agree. But also would put forth like patience is important too because that's that's another thing I've been writing about a lot recently is I think This year particularly is really highlighted that the first five years of lightning development whether it be the robust competition at the implementation Um, layer, or, uh, sort of development of LDK, which you've been working on.

Um, like, it's taken time to get these different areas of the Lightning developer stack to a certain point where you can then go build these

**Matt:** things. And I would say it's still very early. You know, that stack's still fairly immature. There's still... You know, I think the history of lightning is one of, you know, people building, people getting excited, and just like, this stuff is hard.

And, you know, we're finally at a point where, like, lightning, as it [00:28:00] exists, is... Stable is, is working and it's a great demo of how you can build this kind of thing and get it stable for custodial stuff. You know, we're finally getting to a point where we're building out the features we need to make a good first class non custodial experience.

Um, you know, we need async payments based on bolt 12. We need bolt 12 for some privacy. Like we're finally at a point where we can start fixing all of these issues like. You know, recipient privacy, we need O12, like, uh, you know, good first class mobile experience, we need async payments, like, you know, we're fixing these major flaws that we've had and just haven't had time to fix because we've been too busy just, like, getting stuff actually working.

**Marty:** Yeah, so with that in mind, I mean, there's a lot of people in this office, actually only Ben Carman has been saying that, this is the year of LDK. So what is the state of LDK? Everybody that I talk to that is beginning, [00:29:00] I don't want to say everybody, but many people that I've been talking to that are beginning to build products on Lightning seem to think that LDK, due to the fact that it was built in Rust and is very modular, is sort of primitive to build their products on.

**Matt:** Why is this? Yeah, I mean, we're, we're kind of the only modular game in town, right? Uh, Claire is to some extent as well. Um, it is in, in, um, Scala. Uh, so it's a little harder to get running. They, they had to actually re-implement it largely to get it running on iOS. Uh, they re-implemented it in Kolin, and then the, they maintain the Scala one, which is, uh, Flexible as well, but not as flexible and not certainly not designed with like flexibility as the sole, sole North star.

Um, so if you want to do something super custom, we're kind of the only game in town, you know, if you're like, uh, an exchange and you just want to like integrate lightning support, there's, there's good. [00:30:00] Tools for you, you know, whether it's, uh, Claire, uh, CLN or LND, they're, they're pretty good, you know, use one of those probably they're, they're, they work great off the shelf.

If you want really tight integration, you want your own, you know, custom data storage, you want to, uh, do some extension, you know, you want to run in Wasm like the mutiny guys do, uh, you want to, you know, build, you know, remote signing support with like a multi. Uh, uh, multi, uh, what's the word I'm looking for?

Just many nodes in one machine. Uh, CLN is working on stuff around there for the Greenlight product as well, but also you can do that with LDK. Um, and you can do it a little lighter weight, I think, with LDK. Um, so there's just like a lot of these more interesting LND.

You can maybe do some of them with core lightning. You can maybe do some of them with a Claire, [00:31:00] but for the most part, you can only do them with L. E. K. So. We're really trying to enable more experimentation, more different ways of thinking about deploying a Lightning Node or many Lightning Nodes. Um, and, and we're really moving, moving good towards that.

And, so, you asked about the state of LDK. We have a lot of people doing really interesting and very different deployments all at once right now. And they're all very, you know, we have a number of folks building on LDK, uh, building. Very divergent types of nodes and right kind of all reaching this point.

Right now where they're kind of, you know, they've built something they're testing it. They're kicking the wheels on it They're finding, you know edge cases in LDK. So it's crazy right now We have a lot of stuff, you know Improvements for this use case improvements for that use case this that whatever Going on while also trying to execute on you know We put out a really aggressive roadmap at the beginning of the year just based on kind of what everyone's working on and what they [00:32:00] thought their timelines were and Uh, we're making good progress on it, it's a little delayed, but, uh, you know, so we have a ton of stuff we're working on shipping, so we shipped anchors, uh, we're working on bolt 12, we added watchtower support.

And then this coming release, we have like better async support in Rust. Um, we're gonna move towards async payments. We did, there's just so many different, oh, Taproot Channels 2 is coming. Um, so there's a ton of different things we're working on and also trying to improve the state of everything in LDK for all of the users building, you know, new and kind of innovative types of lightning nodes.

Um, so it's, it's a little nuts right now, a lot going on, um, but you know, I'm, I'm really happy with, with all the contributors. Uh, you know, we have a handful of folks who are downstream implementing stuff with LDK who are contributing back to LDK, which is really great. And the, the team working full time on LDK at Spiral as well as some folks who are on grants is great.

Um, so I'm really happy with where we are and the progress we're making, [00:33:00] but. Yeah, it's, there's a lot going on right now.

**Marty:** Digging into the contributor base, like is it, is it growing pretty rapidly or are you guys trying to keep it tight knit, so? No,

**Matt:** we want, we want as many contributors as we can. We really, really want to avoid the outcome that we've seen with some other Lightning Nodes, and I won't name names, where it, it really is a corporate open source project and it's hard to contribute outside.

We really, really want to avoid that. We want to... Uh, encourage as much contribution from externally as we can. Um, we have some folks externally to LDK. Uh, both other teams at Block using LDK as well as other teams outside of Block using LDK who are contributing, uh, stuff that they need. And we're really excited about that and we really try to...

Have as good a contributor experience as we can try to get peers reviewed very quickly from everyone And so we that is a key goal of the project to be a true open source project in the sense that like anyone can [00:34:00] Contribute and we we try to make that contributor experience as good as we can. Yeah,

**Marty:** that's important and lightning more broadly like to me it seems like again going back to I think We can bring this even back to the stablecoin conversation.

I think it's inarguable more people are using stablecoins globally than the lightning network for payments today. And again, I think that's just a timing issue. I think in the future we can get to that point where you have feature parity and user experience parity.

**Matt:** Yeah, we have to get, we need stable value.

People do want wallets that have stable value. But we'll get there, you know, DLCs. Uh, you know, I do wonder. We'll see, you know, the marketplace will decide, people will try different stablecoin approaches and Bitcoin, you know, I'm not a fan of the, like, issued asset stablecoins, because I think reintroducing trust in the system sucks, um, but the market will decide, and [00:35:00] I am looking forward to people trying different things, seeing what fee structures customers want, you know, compared to, you know, obviously, USDT on Tron is pretty cheap.

You know, it's a pretty centralized blockchain. It is really cheap to, to transact. Um, so yeah, I'm, I'm looking forward to seeing what comes out there and I think it's going to be great when we get

**Marty:** there. Yeah, but it does seem like this year, particularly the activity at the product level on the Lightning Network has been somewhat impressive.

It feels like five years in, we're finally getting to the point where... People are able to create experiences that work well, I think. The emergence of, the intersection of lightning and AI, particularly through the spring and summer, is something that I've been paying attention to. Yeah. You're grimacing

**Matt:** right now.

Yeah. I feel like the whole lightning and AI thing is like, it's a little bit, uh, no, no, no, we're cool. We're in on the hot new thing [00:36:00] now too. We're in

**Marty:** on it. You don't think it's uniquely suited to solve some of the problems there? No,

**Matt:** why not? Like, I mean, what is the problem? Like the problem is that people want to pay for AI, uh, output, like model run output.

Like, okay. But this is like every, this narrative has come around many times in Bitcoin, right? This, like, you know, you're going to have some API that you want to hit and you want to like. Pay micropayments to hit the API and small scale. The reality is no one's ever wanted to do this. Like really no one has ever wanted this.

Um, it sounds great in theory. Cause it's like, Oh yeah, you know, it is true. All of these API hits are like, you know, a fraction of a penny, whatever. We want to make these small API, cheap API hits. That's true. At the same time, uh, paying up front or totaling it and paying it on a credit card at the end of the month works pretty damn well.

Um, it's just not [00:37:00] really a problem. Amazon AWS has solved this really well. They're a massive business based almost entirely on racking up small charges across different APIs as you use them. Um, even open AI has a, has a, whatever monthly. Service fee for access to GPT 4 and some of their newer works. Um, what value is Bitcoin providing there?

Like, okay, we can add, we can do micropayments better. Okay. Is that a 10X better experience than like credit cards suck for many reasons, but, and lightning improves on that, but it's not specific to micropayments. I think,

**Marty:** yes, I agree with that. I think the one interesting sort of development there is the accessibility that it, that it enables, where

**Matt:** Fewer people have Lightning access than credit cards.

I wish it weren't true, but, [00:38:00] like, I don't, I don't think that it enables more accessibility than, than there was. Really? No, I mean, like, Lightning, Lightning is awesome, and Bitcoin is awesome. I've spent More than a decade working on it, but we're still not there in terms of adding Bitcoin adds more accessibility.

It doesn't really, except for some niches, where, you know, if you want to enable people in Iran to use your, your product, maybe you need Lightning, but also if you're an American company, you can't do that anyway. You've got to block them anyway. Um, you know, maybe you're, you're a European company and you're allowed to have Iranian customers.

Um, But you can't charge them with a visa or, you know, bank transfers are annoying. I don't know, like, there are, there are niches where it might make sense, but it's not like you can easily get Bitcoin and Erron anyway, right? So, there are niches where it makes sense, you know, I'm optimistic [00:39:00] about the long run Bitcoin being more broadly available, I mean, we see it built into financial services today, I mean, what's the, like, You know, you can pay.

I get, I don't, I don't know that that PayPal Does PayPal do on chain deposits? Can you deposit into a PayPal account? I think you may be able to, but okay, let's, let's assume you can. I mean, let's, the only way you can pay directly from a cash up account to a PayPal account, right? Like, that's cool. And like as more places integrate it and have that as an option, as a first class option, then Bitcoin becomes more broadly available, becomes accessible, and then we can start having these conversations, but we're not there yet.

Um, the reality is, You know, cross border finances, financial systems suck for many reasons, but... You know, Bitcoin, where they suck so much that Bitcoin really adds value, is still relatively small niches. And if you're someone like OpenAI or someone like AWS, whatever, that's such a small percentage of your customer base that you [00:40:00] don't care.

It's almost not worth adding that option to your checkout flow. Yeah.

**Marty:** Alright, so with that in mind. What do you think, outside of like contracts for difference and mimicking stablecoins on Lightning, what do you think, from a product perspective, should be prioritized right now?

**Matt:** Yeah, I mean, I think that, yeah, that's a big part of it.

You know, certainly, I mean, I'm not That's not to say we shouldn't build things like, you know, it's L402, the, the Lightning Labs design for, uh, just paying for APIs with the Lightning. Like, we should build those. Those are cool. We should, we should have these options available in the marketplace. Um, we shouldn't anticipate that they get adopted broadly.

Um, again, in some certain niches they might, and in those niches, That's where we start to [00:41:00] demonstrate value, right? Like you have to first find niches where like it makes sense and it adds value. And then people see it. People, people want to access that service. People use it. People see how great it is, how, how easy to use it is.

And then they start to think like, okay, maybe I, maybe I do this, have this in my service, even though it might not be as required for my customers. I mean, like, uh, Snowden had a great. Nostra post, uh, whatever, a week ago, two weeks ago, it was kind of like, look, people have, people still think Bitcoin sucks, still think Bitcoin, uh, is.

These slow 10 minute confirmations where you send a transaction, it goes into the void and you don't know what happened for an hour, 10 minutes, whatever it is. Um, and they haven't used Lightning and they haven't updated their priors for what Bitcoin looks like. And so having that more visible to people, having that be exposed to people more will make people start thinking more about how to integrate Lightning, how to use it in their domains.

And so, you know, that's why we work [00:42:00] on, work on LDK is to provide a toolkit for people to. Integrate lightning in whatever way they might come up with, because we're not going to come up with, you know, this great idea for how to integrate lightning and build this great lightning user experience. We're not a user experience team.

We're not a UI team. You know, people like Mutiny are going to go build a progressive web app and see if that resonates in the market. People are going to go build, um, you know, pseudo custodial lightning where like the No, the client side has a key and they like, uh, run some little signer Damon on their end and then can just hit the API and like, not worry as much about lightning and kind of the green light model.

But people are building it with healthy gay too. Um, You know, we want other people to come up with some of those ideas and build those things out. 'cause that's not where we're gonna do it, uh, where we're gonna kind of shine as a team, but we can provide the tooling for people to be able to do [00:43:00] it. Um, so it didn't quite answer your question, but, you know, broadly , what do you want, Matt?

What do you want to see? Don't talk about the tools. Um, talk about the end products. Yeah. I mean, but yeah, I think, I think US dollar denominated Bitcoin transacting. Uh, is a huge one just in terms of like being able to truly compete in a marketplace where I think Bitcoin should be adding value. Um, you know, people have been posting about how Bitcoin has lost, um, but hasn't, to your point, you know, patience.

It hasn't really started competing in those marketplaces. And we, we should. Start moving towards that direction. Um, similarly, you know, I, I just want to, I want to see better and user tooling. You know, there, there are some great lightning wallets out there. There's Phoenix. There's no, I don't know if moon is actually rebooted since they had some issues with their, their non lightning design.

And, and I know they were working on. [00:44:00] Switching to Lightning, basically. Um, you know, there are great user experiences for it, but I want to see them more broadly available, you know, uh, moving towards getting Lightning in exchanges. You know, Coinbase announced yesterday, uh, that they were actually going to add Lightning.

They announced a while ago that they were thinking about it, and now, now they are going to do it. Um, you know, getting Lightning to a point where we've worked out all the kinks, so that It is always a great user experience, not just usually a great user experience. Um, part of that is the long tail of wallets that suck.

Um, you know, there's a lot of great Lightning wallets out there and then there's a handful that have integrated Lightning and still struggle with, you know, payment reliability isn't always great depending on, you know, your node. There's a lot of documentation out there that says like, oh, you want to use Lightning.

First install LND and then like, become a routing node and like, now you can use Lightning. That is bullshit. No one, that, that causes so many problems. People do that, they're like, oh, I installed [00:45:00] LND, I opened a channel, and then I tried to pay myself from CashApp and it doesn't work. Why doesn't it work?

Well, you have no inbound liquidity. How do I get inbound liquidity? I don't know. Like, that is not something for normal people to do, and we need to update the way we're telling people to integrate with Lightning so that they're not doing that. But that also means building better tooling. So that means we need...

You know, we have people are moving that towards that direction in the mobile front where it's like, you know, it's great experience. You don't have to think about channels. You have an L. S. P. They pay you etcetera. Um, but we also need that on the merchant side on the like, I want to run a Web store and I want to integrate Bitcoin.

I want to integrate all four or two, whatever it is. We need that to be a one click install where it has baked in LSP that's going to deal with your inbound liquidity and maybe you're going to pay for it but there's a marketplace of them, you can choose who you want to use. Um, it's not like you're trusting them, you're just, you know, relying on their liquidity.

Um, we need that to [00:46:00] be a one click install and it is very far from that today.

**Marty:** Let's dive into that, the emergence of LSPs over the last few years. There was robust competition, like you just mentioned.

**Matt:** There is increasingly, it's not easy to switch right now, they're all custom APIs, so there's some work to define an LSP spec.

So just a standard specification for how an LSP should interact with its client. Um, and that should enable much more robust competition. Um, and so I'm really looking forward to that becoming available, being integrated and a few LSPs and having clients for it that people can just use off the shelf and ideally having, you know, servers that people can just deploy to be an LSP off the shelf if they want to do a bunch of management of liquidity and inbound and outbound liquidity and actually, you know, be that kind of routing node.

Um, and so, you know, we have seen a handful of these big routing nodes be like, okay, I'm now in LSP2, you can pay me to get a channel. Um, but it's this very bespoke, like, user [00:47:00] custom API, and you'd have to integrate with just this LSP, and it's like Bob's routing node to LSP service. And maybe they have a great routing node, but like, it's Bob.

Like, who knows if Bob's gonna decide that he's bored and not do this anymore. I don't know. Um, but having a spec for it, uh, And having that integrated in Lightning Clients that people can just take and run is going to be big, you know, we, like, I've interacted with some credit cards are great, but sometimes they're a pain and sometimes I want to buy a server from someone in Lithuania and my credit card decides it's fraud and just makes it a hassle, so I prefer to use Lightning, um, but I've interacted with some folks who just like have installed BTC Pay Server and one click, okay, I added Lightning.

And it just like spawns a core lightning or an L and D node and doesn't do anything. And then I've interacted with them and they're like. Why are your payments failing? I'm like, well, you have no inbound liquidity. And they're like, what is liquidity? What is, I don't know what the fuck you're talking about.

I just run BTC pay server and like [00:48:00] everything else just works on this lightning thing doesn't just work. Um, so we need, we need better support for that. You know, BTC pay servers working on, uh, they're going to do a mobile client now. Um, so they're going to rethink how BTC pay server works, especially on the lightning front.

So they're going to, uh, start playing with LDK on a mobile. Uh, client side, um, and hopefully we'll also have LSP support. I think that's one of their goals. Um, so that'll, that'll clean that up a lot. Um, but yeah, I mean, this, this needs to exist across the whole lightning stack. Well, many people

**Marty:** will point to LSPs and say, Hey, this is a massive centralization risk in the long run.

Do you agree

**Matt:** with that? Yeah. I mean, it, it kind of is, um, but that's why you define a spec and that's why you create a marketplace for it, right? Um, it is the case that. You know, Bob's LSP service, a handful of them exist, you know, a bunch of these larger routing nodes that are just run by one guy, or, you know, not even a team, probably don't even have 24 7 [00:49:00] coverage, you know, it's just one guy, um, do have LSP services now, and they will open a channel to you for a fee, and they do have good routing performance, because they are, you know, run a big routing node, um, and I think that Is also going to be the future of this.

It's not just, well, you know, you're going to use C equals blocks like professional, um, you know, for profit. Routing node that that exists as a whole team within block with however many engineers on it. You know, it's not just gonna be that it will still, you know, we need this spec so that it's not just always tightly integrated, right?

Where you, you know, someone builds a mobile Bitcoin wallet and they use their own LSP and it's bespoke and custom and something, something, you know, there will be a true marketplace for it. And that I think that will cut down on the centralization pressure of it. Um, it is true that there's, there's valid centralization concerns there.

Um, but if we don't build it, no one's going to use lightning because the user experience [00:50:00] sucks ass. So, you know, I don't know what your alternative is. I agree.

**Marty:** That's. You need that robust marketplace for it. And with the spec, like what is the state of that? Is it

**Matt:** just early stage? It's still early. Um, what

**Marty:** needs to be specked?

Like what, what would the spec define? Yeah, just all

**Matt:** the, the, how you get a channel, how you, you know, obviously a big focus is kind of the zero conf channel use case, right? Where like. Um, you know, you want to, especially on the mobile side, where you, you're a mobile phone, you know, you, that, that first payment user experience is really critical, like the first time someone installs your app and receives a payment, like your, you know, their friend is like, look how awesome this lightning thing is, install this app, I'm going to send you a payment, well, if that first payment requires that transaction to confirm on chain, um, And then the payment, and then all the later payments are instant, but that first one sucked, well, you know, that user's gonna get turned off and not think that Bitcoin [00:51:00] is just still this shitty, like, ten minute thing.

So zero comp's obviously a big part of it, um, and that does introduce some trust. Now you're, you're restricted from just, Picking a random LSP, you kind of have to pick somebody you sort of trust, at least for that first payment. Um, and you can, you can do better things in the UX. You can display it pending, yadda yadda.

But, in any case, um, So, it, it So that's been a focus of it. You know, there's some folks working on it. Breeze folks working on it. There's some of the C Equals folks working on it. Uh, one of the folks from the LDK team works on it some. Uh, there's a handful of folks working on building that. But it's really just all about just defining the messages, right?

Like, most of the LSPs are just an API. You hit it, you say like, hey, I want a channel. Here's my, here's my node. Here's how to, here's how to get the channel to me. Gives you a price. You pay it. You get the channel. Um, you also want to want to support zero comps. You want to be able to say like, Hey, if I receive a payment, how do I, what's the fee going to be?

All that kind of stuff. [00:52:00] Um, so it it's early stages. There's It's kind of two versions of it. There's kind of v1 and then v2. And v1, uh, is defined. People are working on implementing it. Uh, there's some early implementations that people can play around with, I think. Um, v2 is a little further off. It's much more complicated.

Solves some of the problems in v1, but isn't, like, you know, a massive, uh, win. But it is more complicated. It's going to be a while before v2 gets implemented. But v1's there. Starting to be there. Uh, there's starting to be implementations. People can start to play with it. Yeah, it's gonna take time. It is gonna take, these things take time.

That's what I'm getting out of this. Yeah,

**Marty:** it's uh, it's weird because there is this

impatience that exists out there, particularly from, and I don't know if it's disingenuous impatience or just pure ignorant impatience from people in crypto or like, ah, look, it's failed. It's always been crazy to me to think, number one, [00:53:00] Bitcoin, people point at the volatility, um, and they've, Basically, shit on Bitcoin for years being like, oh, it's a terrible store of value.

Look at the volatility. And similarly with Lightning, like launch five years ago, like, oh, it doesn't work. It's like this stuff takes time to build. Like it just doesn't magically appear.

**Matt:** Lightning is, people underestimate how complicated Lightning is and how hard it is to get some of these things right.

You know, I think by comparison, like you think about like a pseudo centralized blockchain is pretty easy thing to do, you know, an issued stable coin. You know, there's a lot of work that goes in. I'm not saying, like, it's trivial to build a circle overnight, but a lot of that work is just regulatory, um, and it's not really, uh, a huge amount of technical work like lightning is, um, and especially, like, building DLCs on top of lightning, and you build lightning, get that stable, and then build DLCs on top.

That's a ton of work. Um, that's a crazy amount of work. [00:54:00] Um, so, um, So yeah, I mean, Patience is the name of the game. There's a lot of people in broader crypto who are like, Yeah, look, Lightning has failed in the marketplace, we've already won because these stable coins are just so much better. And it's like, yeah, that is, you know, a concern of mine that like, you know, these things are going to become more entrenched and, and Trustless options are not going to win in the marketplace because they're harder to build, the UX isn't always going to be as good, um, and they came to the game later.

So it is a concern, but, you know, the game's not over, like, the number of people in the world who use USDC and Stablecoin is still very small. Even the number of people in the world, like, the number of USDC or Tether directly is very tiny. You know, we're talking about, you know, some people settle. Their cash trading people still get us dollar cash.

Some people settle the back into those cash trades using USDC. Um, but the normal people are still just doing cash. Um, so there's, there's a lot of [00:55:00] room there to still compete. These things aren't entrenched yet, but we need to execute.

**Marty:** And do you think the entrance of companies like LightSpark, you mentioned Coinbase earlier, you think them getting into lightning and providing some intellectual capital helps with that at all?

Do you think it can muddy the waters if they're sort of coming in like... I'm new to lightning and I'm here to fix it. Um,

**Matt:** I don't, we haven't seen that behavior very much, which is good. We haven't seen the kind of, we've seen a lot of I'm new to Bitcoin and I'm here to fix it, but we haven't seen a lot of I'm new to lightning and I'm here to fix it.

I think people get in and look at it and are like, wow, this is complicated. All right. Um, so we haven't seen that much of that and that's, that's fine. I think it is definitely. I think Lightspark, Coinbase, getting into it, these things, these things are great and we should be excited that Lightning is becoming available because at the end of the day, that's, that is where a lot of the consumers are, you know, people use USDT on Tron, not [00:56:00] necessarily by having a Tron wallet by like going on Binance and clicking withdraw USDT on Tron, because that's the like faster and cheaper withdrawal option of the five options that are listed on Binance, right?

Like, it's not like they're like, Oh, using this all the time. And so having lightning integrated in these places, I think is going to be a big boom, right? So having a lightning withdraw option on Coinbase, having a lightning withdraw option from some of Lightspark's future partners, right? Where Lightspark can add, can provide this integration easier for companies.

I think that's big, and we really need to encourage that, and that needs to exist. is partially what enables these like DLC wallets to, to function, right? If you are You know, you have whatever, 10. 10. 1 is an example, or you know, there's a bunch of people working on building these things, too. Uh, you, you have that app.

How do you get money in? You know, you need an exchange that supports sending lightning, so you need to be able to go on Binance, send [00:57:00] money. You know, in your pesos or whatever to Binance, click buy, you know, buy Bitcoin and then click withdraw in lightning and then have it come to your 10, 10, one wallet.

And that, that does conversion back to dollars for you. Um, that is a big deal. So we need that to exist. That's a core part of lightning being able to exist. And like Binance now supports lightning. That's huge. Um, we really can't underestimate how big that is. Um, so I'm, I'm really excited about. That, but just as a, this is a requirement to get to where we need to be on non custodial lightning.

Not as a, like, this is going to solve our problem for us. At

**Marty:** the very least, it just brings more liquidity to the network as well.

**Matt:** Potentially, I mean, I don't know how much these guys are going to run routing nodes. It was like, you know, I know CashApp has nodes that don't route, right? Their compliance team said, no, you shouldn't be routing.

Um, [00:58:00] sucks, but it's fair. Um, you know, so I don't know how much these nodes like we don't talk about centralization, just like having, uh, Coinbase and others run big fat nodes that everyone routes through is not a great outcome either. You know, we do need these, these plug net style nodes, but of course we need ones that, that have sufficient liquidity and are really, really.

You know, to some extent, actively maintaining it, not just like the, the folks who just start a node and are like, why can't I use my node? It doesn't have enough liquidity, but I don't understand that. Yeah. Um, so, so I, I'm not a huge fan of that part of it. I'm just a huge fan of, of it enabling people to have a lightning withdraw option wherever they already buy Bitcoin.

Yeah,

**Marty:** that makes sense. Yeah, it's, um, I'm really excited. I've been using, I use lightning every day. It's, uh, That's like the one thing that frustrates me the most like nobody uses it I use a [00:59:00] literally potentially every minute of every day if I post enough podcasts via podcasting 2. 0 There's people streaming sets to my to my node that I've been paying a lot more Lightning invoices myself.

Like it does feel like it's happening.

**Matt:** So it really, I mean, you know, it, it works great when it worked bid pay still has is integrated in a number of places. And as long as, as long as the merchants not in Europe where you have to KYC yourself separately to bid pay and upload your ID to pay, which is nuts.

Um, and as long as you're not your IP address doesn't come up as New York, lightning is an option. Uh, and it works great. You know, when there's, you want to buy on a new egg or whatever. You know, you want to buy stuff. Lightning is an option and it works great. And there are a lot of, again, you know, credit cards usually work even better.

Um, but where credit cards. You know, credit cards are sometimes a pain. You want to pay a merchant in a foreign country, it's going to flag as [01:00:00] fraud. You know, you got to type in this whole thing. Like the UX of lightning is actually genuinely better than a credit card. Um, you know, you don't get the like fraud protection, whatever.

Um, so it's not necessarily always competitive, but the UX is great. Like really genuinely great. Um, And so I'm really happy with, with where things are going and where things have gotten to.

**Marty:** Yeah. And so that's the technical aspect of it and you touched on it a little bit, the regulatory landscape. What are your thoughts on that?

Are you? Yeah. Fuck New York. Are you worried about anything on the horizon

**Matt:** here in the US or? Fuck Ben Lasky. Fuck the financial action. Are we allowed to say that? I don't know. Yeah. Yeah. We can say that. Sorry.

**Marty:** Sorry Wolf. Um.

**Matt:** Yeah. But, uh, but yeah, I mean, I think. I mean, the travel rule. Travel rules concerning.

Especially, you know, where Europe's going. Was it AML5?

**Marty:** Or AMLD5? What did they just launch?

**Matt:** Yeah, um, Yeah, the standard AML. Their new AML [01:01:00] regulation. They also have their separate cryptocurrency regulation. Europe likes to be a leader in regulation, which is nuts to, I think, most of us Americans. But... Yeah, there's stuff, we'll see where the AML stuff lands, um, definitely concerning, um, with people's just ability to withdraw from exchanges to their non custodial wallets.

That is something that, that is currently allowed, um, but potentially is going to create some real big hoops to jump through. It already is on some exchanges, you have to like, sign a message to say, you have to like, a sign message to say like, yes, this is my address, um, to withdraw. Uh, And so, I mean, to some extent that the travel rule is going to, because the travel rule fundamentally says that you have to include this information.

If the transaction is going to another regulated financial provider, um, that means if the transaction [01:02:00] is going to someone's noncustodial wallet, travel rule does not apply. So the travel rule to a large extent, trying to enforce it is really just going to push everyone to withdraw to noncustodial, um, which is maybe great.

Um, as long as the hops that it creates. For people to do that isn't too high, you know. I don't know if anyone's ever bothered to read Kraken's Terms of Service, but forever the Terms of Service has said that if you withdraw, it must go to your non custodial wallet. You are not allowed to withdraw from Kraken to another exchange because of the travel rule.

It says that in the Terms of Service. You're not allowed to do it. Now, I mean, that's not sufficient. The question is, what hoops are, in the future, people going to have to jump to to prove that this is their non custodial wallet? Um, and you know, maybe lightning. Maybe they'll just allow it because it, it, the invoice looks different in one way or another.

I don't know. Um, but yeah, I mean, what are those hoops? But it's concern. It's not, it's not the biggest concern. You know, I also worry about, [01:03:00] uh, Just you know, there's now this chain analysis case. I was gonna bring that

**Marty:** up. You got it pretty heated on Twitter Oh,

**Matt:** well, not the case. You go. Oh, there's a separate.

Yeah, it's a separate question

**Marty:** The chain analysis case is Brian Bishop an expert on Bitcoin

**Matt:** yeah, well, I mean a usual legal Legal wrangling saying like fuck your fuck your expert. He's not an expert But I mean broadly in that case You know, they're really relying on chain analysis heuristics to throw somebody in prison on a criminal matter.

I mean, it's not even a civil matter.

**Marty:** The Tornado

**Matt:** Cash, right? That's separate, and I think the Tornado Cash... Oh, we were talking about BitFrog. Right. BitFog, yeah. The Tornado Cash case, I mean, I think it is relatively clearer that... North Korea put some money in tornado cash. There are other issues with that case.

I'm like, is tornado cash a business where the tornado [01:04:00] cash case they're arguing? Basically, tornado cash is a business and as a business, it has to, it has to act as an MSB. It should have been registered as an MSB and thus it has to comply with bank secrecy act and all the usual MSB AML KYC requirements.

Um, yep. That is concerning from a like, you know, is this a business point of view? And they, they, the prosecution really muddled the argument around like, well, but it is obviously that arguments muddled just because like they raised money from VCs, they operated as a for profit with this token that made money.

Not a fan of where the prosecution went there, but, but at least it's a more muddied case. Um, the BitFog case, you know, they're really relying on chain analysis as heuristics to throw someone in prison. Like, chain analysis heuristics are, you know, I mean, they're not bad at what they do, but they're still heuristics.

They're not a [01:05:00] concrete... Trail of evidence, like, like we've seen for some of these other cases where the, the, the indictment and the arguments the prosecution raises are really, look, we see this address which was the hack or the stolen money, it went to this address, it fanned out like this, it fanned back in like this, and we can like draw a nice graph that is fairly compelling about what happened.

In this case it's, well, chain analysis is saying that the heuristics say that this guy was to blame. So it's like... Uh, what, what, that's not an argument. Yeah. 'cause what

**Marty:** he went from Mount Gox to buy the d n Ss to buy the domain name. Mm-hmm. . And then they used like the change from that purchase, I think, to try to,

**Matt:** right.

And they're like, the heuristic is like that. This is the change. And like, you know, un unclear. Um, but yeah. So anyway, um, we'll see where that case goes. [01:06:00] You know, I think a lot of these. You know privacy in Bitcoin and blockchain is going to be a constant battle and you know what does um, you know, I think obviously I think I made the point you mentioned that the chain analysis paper that Vitalik co wrote with some chain analysis folks and some other folks basically arguing that like we should build Uh, Tornado Cash, where, uh, you, when you withdraw, you also prove to people that you weren't on some blacklist, like some chain analysis list of bad stolen money addresses, you prove that you weren't on that list, the money you put in wasn't on that list, um, which, you know, obviously relying more on these, like, centralized gatekeepers of chain analysis is for profit, whatever, is, like, so shitty, um, and really antithetical to, to cryptocurrency, I think, broadly, um, but, You know, where do we get the privacy?

You know, how do we, how do we get privacy in a future [01:07:00] where, you know, tornado cash and like, if you use a privacy creation. System like you, you go use tornado cash, you go use a mixer or whatever. That's immediately demonized. It's like, why are you hiding your money? Um, that's a concern. And then, and then there's kind of the, you know, my view has always been that we should get privacy as a side effect of building better technologies, right?

Like lightning where, you know, fundamentally having everything on a blockchain is public and like, you can do these heuristics and whatever. Um, but. So that that's where the privacy loss comes from. But if we do anything that's just designed to have a better payment experiences, instant payments, you know, uh, more scalable payments, fundamentally in order to scale, we have to move off of a blockchain and by moving off of a blockchain, we create more privacy.

Like that's just kind of fundamental to building better systems [01:08:00] on cryptocurrencies. Um, and so. So, you know, what does that look like regulatorily when we build systems that are better, that happen to be more private, you know, we weren't, Lightning wasn't designed with a goal exclusively of being private, you know, that's something we've, we've tried to build things into Lightning that do improve privacy, but that wasn't necessarily the singular goal.

The singular goal was like, how do we get Instant, cheap, fast payment, instant and cheap payments in Bitcoin. Um, that was the goal and that also had a side effect to privacy. So what does that look like regulatorily? Do regulators question that? Do regulators say no? Um, you know, so far that hasn't, to my knowledge, been something that's been raised aggressively.

And obviously New York has... Uh, basically banned anyone from doing any regulated financial institution from doing Lightning. Uh, if you're a merchant, you can probably accept Lightning, you can use Lightning in New York. But if you're, if you're a [01:09:00] financial institution, you can't touch it. It's not clear that that's, fucking, NYDFS doesn't have to tell us why they think that.

You know, they don't have to tell anyone that, like, no, you can't do this. They just have to say, like, Uh, you have to ask us if you can do that and we'll never respond. Uh, so they haven't really like said why, um, but some folks, Lasky, uh, like to talk about lightning nodes or somehow should be, routing nodes should be MSPs.

And so that's not a privacy question. That's not like a, Oh, we don't like it because it's more private. That's a like, we don't like it because there's, there's nodes that you're routing through that aren't. Really intermediaries, but they're still routing through them. Um, and we want to regulate those. Um, so Yeah, so there's a lot to worry about on the on the regulation front.

I don't panic about it. I don't Think that [01:10:00] Obviously there are a number of regulators who want to completely kill Bitcoin who want to completely kill everything cryptocurrency yada yada I don't think we are At huge risk of going that direction in the United States, um, Europe, I thought was at more risk of going that direction, but so far really hasn't.

The regulations they've passed have been, I would not say good. I do not, you know, I would prefer them to have been very different, but they are not of the we need to completely ban cryptocurrency from Europe kind of thing that a lot of MPs and a lot of European legislatures, uh, legislators had Spoken about wanting to do.

Um, so yeah, I don't, I don't think we're at, we're at huge risk of that and that's good. Um, but other countries. Much more so but you know Countries are in competition for this industry to some extent and that [01:11:00] that is good and that Regulators and legislators have seen that and do you think in that mindset to some extent some of them do at least

**Marty:** yeah And I think that's being acutely acutely highlighted in the mining industry You're seeing crazy competition at the nation state level to Appease miners to come in.

Well,

**Matt:** And use energy. Except for the current, uh, current U. S. regime. We're, uh, talking about creating an excise tax for mining. Yeah, that's bad. Um, But I saw Well, that's the, that's the, like, people who don't understand the electricity industry who are No. We need clean energy, and also we're gonna build it with solar and wind.

And blot out the sun. Right. Yeah. And then, and then we're gonna, and then we're gonna somehow turn off the net gas plants because we have enough solar and wind and batteries maybe, but don't worry, electricity will only go up in price by a hundred X or something like, it's just, yeah, I mean, it's a real failure of [01:12:00] understanding of, of like the environmental movements.

Do we live in an idiocracy?

**Marty:** We,

**Matt:** we just may. Certainly the, uh, the, I mean, it's the, the, the problem is the history of environmentalism, right? The history of environmentalism, most of these old environmental groups, you look at the green parties in Europe, most of them were founded as anti nuclear parties.

They're not, anti global warming, anti climate change parties, they're anti nuclear parties. And so they're, that's their first goal, and they're like, oh yeah, climate change, we should like build solar and wind, something, something. But like, we shouldn't build nuclear because that, that's bad, and we were founded to fight that.

Meanwhile, like, If you want to turn off the gas, that's your option. Yeah. That's the only option. That's

**Marty:** funny. The episode we, um, posted yesterday was Ryan McLeod who works at the Canadian nuclear laboratories, and we dove deep into the. The nuclear [01:13:00] conversation and it's crazy how it is

**Matt:** that whole conversation is a mess.

Yeah, it's all

**Marty:** right there In any case we can have cheap abundant clean energy.

**Matt:** We could we really could but we don't want to because Politics politics. I'm

**Marty:** so tired. Yeah, I tweeted this out yesterday. It's I think national politics is The biggest intellectual time suck. I think this gets highlighted, especially during election season.

It's like the amount of time that people spend talking about

**Matt:** the amount of time that people spend arguing about it without being informed is frightening. Like people who just don't, who argue about who they like more. Without really diving into what their policy positions are, it's frightening, um, and that's, I mean, that's just the reality of a democracy, I guess, but, but yeah, I mean, it's a massive time suck, but at the same time, you gotta fight it some, you know, we, we have to, we have to have [01:14:00] Bitcoiners in Washington, or we, Get regulated away or or people pass regulations that don't make any sense and make lightning nodes MSBs or what have you?

Or miners MSBs even worse So it's important, but you're right spend the amount of time people spend on it is is why it's

**Marty:** Nauseating with that being said that's been another positive trend Bitcoin lobby Has

**Matt:** gotten off the ground, gotten off

**Marty:** the ground, got more

**Matt:** organized. Yeah. Yeah, totally. And you know, historically we've, we've just relied on like a broader cryptocurrency lobby, which was fine when we were a really small industry.

But also the problem is the issues we care about are fundamentally different than most of the rest of crypto, you know, cryptocurrency and bitcoin really are two totally different communities and worlds. You know that, you know, I think most of the cryptocurrency people still love bitcoin, still buy bitcoin.

They're working on something other [01:15:00] than money and payments, and they care about regulation around securities laws, around issuing share, you know, public issuance of shares and their, their, their protocols and their tokens and whatever. And we don't care about that. And so they spend, you know, the cryptocurrency lobby broadly spends almost all its time on that.

Meanwhile. You know, we're sitting here like, well, we care about, you know, MSB regulation and onerous AML KYC that causes substantial damage to the economy, substantial tailwinds on the economy, um, without much benefit. Headwinds. Sorry, headwinds. Um, you can tell it's early in heaven. Coffee hasn't fully kicked in yet.

Um, what are you drinking there? What is that? Oh, I just put more water in my coffee. I've got coffee back. I thought it was like cider. No, it's coffee backwash. Um, the, the. [01:16:00] So, so, you know, we, we care about something different. So we really do need our own lobbyists. We really do need our own, our own folks.

And it, it's great to see that we're finally getting there and we're finally, you know, getting, getting folks who, who care about Bitcoin and who are gonna argue the Bitcoin position. And, you know, we're not gonna, not to take away from, like, securities regulation in the U. S. is also bullshit. In many ways, but that's not something we're as worried about as the Bitcoin community, um, and as people who want to use Bitcoin.

**Marty:** Yeah, like KYC, AML, privacy, energy. Right. I think energy is going to be one of the most

**Matt:** important. Right. Well, and that's, that's an important thing for humanity generally, you know, having, having abundant, abundant clean energy is like really important for humanity to, to, to, you know, have a good experience, you know, people to be able to live good, good lives for, You know, have, have good, uh, whatever you want to call it, you know, have lead good lives.

Well,

**Marty:** and it's going back to AI, not really [01:17:00] directly connecting it to Bitcoin with this line of thought, but I actually think that's a massive benefit when you consider the amount of energy intensity that comes with that industry and all the money behind that. We may get an ally on the energy

**Matt:** policy front.

Yeah, possibly. I mean, we'll see how much they're willing to go super interruptible, right? So the Bitcoin. Energy policy argument is really focused around like, look, we can turn off when the grid when it's not sunny and when it's not windy. Um, and we can. Fund more solar and more wind on the days when it is Sunday and more windy by buying any excess power.

Um, the ML training folks, you know, they might be willing to go interoperable. Theoretically, their problem is fairly, you know, they can turn the machines off and start up. You know, where they left off tomorrow, um, but whether they will is less clear, whether that market will really bear that cost, um, and whether those companies [01:18:00] are just willing to say, like, look, no, we, we want to have this model trained and we want to do it quickly so that our engineers can, can get feedback rather than taking a few days off from training just because it got, got cloudy.

I don't know. We'll see. And I think that does, to some extent, determine whether they become a true ally or whether they just, you know, find cheap. Power that they can fund. Um, here's how it happens.

**Marty:** You co locate the ASICs and the GPUs and I think that's what these AI companies are gonna need to figure out or come to realize is if they want to go get these Massive power contracts.

They're gonna have to have that caret of demand response and to do that If they want to keep training their models, they're going to have to have ASICs that can be interruptible alongside.

**Matt:** Yeah, I mean it does, it does, demand response does help those conversations. The other thing that helps those conversations is jobs.

And data centers have a hell of a lot more [01:19:00] jobs than mining. Most electricity is provided by some form of government. Private public partnership and when you show up and you say like yeah We're gonna have all these people working in the data center and it's gonna boost the local economy That also helps those conversations a lot in a way that Bitcoin miners really don't you know?

We really Bitcoin miners are like, yeah, we built it this farm. We're trying to be super cheap Uh, you know, we might have somebody who's gonna fix some ASICs and we might have a security guard, but our contribution to the local economy is really the build out. You know, a bunch of people doing construction during the build out phase.

Um, and a handful of jobs, but not a hell of a lot. Yeah. And so that, that does change those conversations and that, that makes the demand response part much more important. Whereas for like a... a more traditional data center, you might not. And you see this all the time, you know, Google and all these folks, they'll like build a data center, and then they'll talk about how they have also an engineering office in the corner of the data center, and they're also building an office there, and then actually they only hire like three people there.

But they told the [01:20:00] local government they were going to hire 50, um, when they got the contract. It is different. We'll see where they end up going, um, and we'll see how much, how much that ends up being a good ally for us, um, in Congress, but, you know, the, the other issue is it's also very easy for them to say, yeah, fuck those Bitcoin people they're doing, like, un We want the energy.

You know, bad, bad things with their proof of work and it's useless computation, but our computation is really useful and thus we should, we should be exempted and you should just kick those Bitcoin people out, we want the energy. We'll see, you know. I wouldn't get too excited about it

**Marty:** yet. Hey, AI guys, we can work together on this.

We can figure this out. Let's brainstorm. But I do want to bring this back to lightning and scaling Bitcoin because I do think it's an important conversation to have. Like, would you agree or [01:21:00] disagree with the statement that lightning is not the panacea of scaling Bitcoin on a second layer?

**Matt:** It's a really critical first step.

I mean, yeah, it doesn't, uh, yeah, I mean, the popular narrative now on Twitter is like, Lightning is stupid, and like, you know, you, you end up with so many on chain transactions, and the LSP, uh, liquidity allocation problem is unsolvable, and that, that leads to a ton of splicing, and, uh, you know, Lightning is just, just useless.

That's, that's naive, but also the flip side of like, you know, lightning is going to be great. You're going to like open your app. Once it's going to open a channel with the LSP and you're never going to touch the chain again is just as stupid, right? The reality is somewhere in the middle, right? So, uh, the LSP, like LSP liquidity allocation is hard.

You know, you have some bucket of money, which channels do you put how much money in? Based on how likely it is that they're going to receive a payment in the future. That's a hard problem. Um, if you get it very wrong, [01:22:00] you will do. One on chain transaction. If you get it maximally wrong, you'll do one on chain transaction per lightning transaction.

Um, and that sucks, but it's no worse than on chain was to begin with. Um, there's maybe a little extra overhead and multi secure there, but with tap root, maybe not. Maybe it's all the same. So it's like, okay, you haven't done worse. Um, and if you get it slightly less wrong, You get, let's say, a compression ratio of 1.

1 transactions to on chain transaction. If you get it very not wrong, maybe you get a compression ratio of 10x or 100x. Maybe you have a lot of liquidity and you, uh, have a ton of people making a ton of small payments. Now you're talking about, you know, a much better compression ratio. You know, we should talk about this as a function of compression ratios.

And it's going to be good. You know, there, there is a lot of compression to be had there. Uh, there's a lot of, uh, you know, you get all these nice UX benefits. You get these instant transactions. Some of them require zero conf trusting the L. S. P. But, you know, in many cases, not, [01:23:00] um, so The narrative of like, well, lightning is stupid because you can't solve this problem is dumb.

It just means that the compression ratio is not infinite. The compression ratio is some fixed number, and this brings us a long way towards scaling Bitcoin better. Um, Bitcoin, it doesn't... I mean, define panacea. You know, you asked, is lightning a panacea to scaling Bitcoin? It doesn't fully solve the problem, but nothing does.

Everything that we can possibly think of to start building today, uh, improves the state of things, but does not have an infinite compression ratio, um, and always has certain trust drawbacks here or there. And so, the question is... You know, like how far is lightning? What is that compression ratio going to be in practice and and how much do we need?

How many people are actually going to be using lightning on a day to day basis in the next 5, 10, 25 years? And what do we need from it? To [01:24:00] support those people and what other solutions might we come up with that might support it better or worse might add on top of lightning. Lightning might be a nice multiple on top of lightning.

Um, you know, whatever it is. So I, I reject the premise of the question. Well,

**Marty:** the, the, what I was trying to get at there is this idea that lightning may end up being the connective tissue between many different second layer implementations, whether it's Fetiments,

**Matt:** Liquid. Yeah, and that's, that's definitely going to be a part of it.

Um, you know, I hope we don't end up in a world where everyone using Bitcoin chooses to just trust a multisig federation of one form or another. Um, I think that would be kind of a bad outcome for Bitcoin. Um, and lightning lightning will certainly be a part of that connective tissue just because it gives us this instant transaction primitive.

You know, those, those types of use cases don't really care as much about the on chain footprint. They care about this instant transaction property. And so lightning is great for that. And payment [01:25:00] channels will always be used for that, I think. Um, but You're right. Like, you know, some people will opt to use these other systems and lightning might sit in between.

The reality is we don't have enough Bitcoin demand right now for this to be a big issue in terms of a scalability bottleneck. Um, it does allow them to offer better competitive fees, which may draw some more users in. And so maybe, um, You know, maybe that will also succeed in the market. You know, I'm very excited to see that competition in the marketplace for users.

I think the hard part is of course, how do you communicate to users? What this trust model is, how do you, how do you know, it's very important. That we, builders in Bitcoin, people building applications for users in Bitcoin, accurately communicate to the user who they're trusting, why, and for how much. Um, and that's hard, that's a really hard UX element to build in a way [01:26:00] that is accurate, but also not overly frightening to the user.

Um, and where the user actually looks at it and understands it and thinks about it. Um, which is generally hard. I mean, some UX people like to say pretend your user is drunk, I like to say pretend your user has five other things going on in their life and they don't care that much about the thing you care about.

Um, so it's hard and I think that's, that's going to be the hard part is accurately communicating these trust model differences and that's something that we as a Bitcoin community need to hold ourselves in high regard and hold, hold as something we need to work on and accomplish. Um, but, uh, But I am excited to see these other trust models in the marketplace competing for Bitcoin users, competing for, for just users of financial services, and offering financial services in a different way.

Um, using Bitcoin with, with Lightning as the connective tissue, to your point, uh, that will definitely be a part of it. But I do think some people will use Lightning, you know, if we do [01:27:00] a good job of communicating these trust model differences, some people will use Lightning. Um, because some people will look at Fetiment, uh, you know, Fetiment's gonna have some, some interesting regulatory questions in the Western world.

Uh, out, you know, I think they're, they're kind of targeting outside of the Western world to some extent. They're targeting this kind of like small community node thing. Um, That's going to work great where it works, and I think in many cases that's, like, I don't, I don't know, who is my community that I'm going to stand up a Fetiment node with?

**Marty:** Maybe the people you did the New York

**Matt:** City Mesh with. Maybe. There are worlds where this makes sense, but like, that's a lot of mental overhead as well, is my point. And that is going to be a drag on... Their usage in some parts of the world and some parts where there is maybe lower regulatory overhead.

Maybe that that mental overhead can be avoided with just, you know, trusting a basically custodian or a group of custodians more like the liquid model. Um, so that. You know, that's gonna work in some places, not in others. I think in [01:28:00] others, lightning will still exist. Non custodial lightning is gonna be a thing.

You know, all these people saying non custodial lightning is dead because turns out liquidity is hard and something something. I don't know, a ton of people use fucking Phoenix. Like Phoenix is great, the user experience is great, a ton of people use it. You can't tell me Lightning is dead when a ton of people are using it.

And, you know, I think that that user experience, in spite of the fees they charge, and people will try different models for the fees, see what works in the marketplace, part of why LDK exists is so that, you know, it's a lower overhead to build a Lightning wallet out, build out different features that might, uh, compete differently in the marketplace.

Um, and... We'll see what resonates, but I think there will always be people using it and non custodial lightning is going to continue to be better. We're solving the user experience pain points of it, um, that people point to and say, like, ah, lightning is dead because you can't receive offline payments reliably and lightning is dead on mobile because, [01:29:00] uh, you know, the fees are so these things are are being worked on, they're being improved upon, um, and we will continue to see people adopt that as a solution, even as there's more competition from other solutions.

Yeah,

**Marty:** which made me think of another thing, like how do you even define lightning success outside of like UX, UI, usability, considering the fact that unless you're directly sort of connected to particular nodes, you don't actually know what the overall activity on the network is, which is like a pretty cool thing, but also like...

If you're trying to pump lightning is this thing that has a lot of utility and a lot of use.

**Matt:** It's harder to do. Yeah. I mean, you, you can, you can get proxies and, and you know, I. I don't know what the numbers look like, but I wish folks like River and Cash App and, uh, you know, Phoenix would publish a little more numbers.

I think River does actually do a good job. They do a [01:30:00] regular ish, I don't know, yearly, quarterly, or just whenever they feel like it, uh, report on lightning stats. And they, you know, their lightning stats look good. Like, people are using it. People are using the lightning stuff from River. Um, and, you know, I've heard informally that Phoenix is doing well.

The, the... Claire, the Async guys are doing well. Um, you know, but, but yeah, I mean, you kind of have to ask them if you want to know how much people are using Lightning, how much people are paying with Lightning. Um, but I think the answer is, yeah, people are using it and it's not just custodial. You know, people, uh, have these charts of like where deposits are going.

A lot of it goes to Wallet of Satoshi or whatever, but people also use Phoenix. Um, and. You know, we'll see what the future of the regulatory question is around Wallet of Satoshi, um, what that, what that looks like in, in five years, um, but, you know, there are, there are absolutely people who use non custodial lightning, and it Even on mobile and it does work and it's continuing to get better [01:31:00] on.

We're going to make it a lot better in the next few years. Um, so yeah, I mean it's hard to define lightning, but yeah, the people who point to various parts of it as broken, the reality is people are using lightning and numbers. It's up and to the right. And even though more people are using Wallet of Satoshi than other Lightning, people are using Lightning.

And if you're going to tell me that like, you know, Fetimint is a solution to, you know, people are going to move from Lightning to Fetimint because Lightning has gotten too centralized and then people are just using Wallet of Satoshi, well, Fetimint's also a custodial model. It's a federated custodial model and you know, maybe some people will use it in like a kind of community sense and that's great and that's awesome and that, that, that will be a part of it.

Also, you know, community nodes don't, don't scale to the world. They scale to some communities, um, and for everyone else, there's, there's non custodialite.

**Marty:** And to wrap up, so you can get back to work, you're [01:32:00] here to work. PTLCs, we mentioned it earlier. Seems like that would be a massive unlock for privacy.

Yeah. For PLCs, for all this stuff. Right. How do we transition? Are we gonna have to close all of our channels?

**Matt:** No, yeah, yeah. Uh, you're going to have to have taproot channels. Um, and that will require an on chain transaction for your channel. You don't have to close. You might just have to splice. Maybe you'll want to splice money in anyway.

So you'll upgrade to taproot when you do that. Um, and PTLCs are going to be a big unlock for privacy. Um, you know, again, this is one of those things where it like, it substantially improves the privacy of Lightning, but it's not going to change the UX. Depending on how we do it, it might even slow down payments, which kind of sucks.

Um, so, we'll, yeah. All I'm gonna say is I'm not in like a massive rush to ship it. Um, [01:33:00] you know, it, I'm much more excited about it from a DLC perspective. People are already building DLCs without it. I haven't looked deeply into how they're doing it. Uh, so maybe I shouldn't. They're doing

**Marty:** Cryptogarages soon.

Yeah. I think it's extension signatures. I always get it wrong though. Adapter signatures? Adapter

**Matt:** signatures. Adapter signatures are... Or a Schnorr thing. I don't know. They, they might well just be doing taproot outputs within the Lightning Channel. I haven't looked into it. So they might actually be doing kind of pseudo DLC thing, er, pseudo PTLC thing anyway.

Um, they might have built PTLCs on non taproot Lightning Channels as like a second output thing. Um, I don't know how they're doing it, but uh, point being, in, in Lightning itself, uh, outside of the DLC thing, it's, it's nice. We'll, we'll do it. We should do it, but it's not. You know, it's not solving a major UX burden as it exists right now.

Um, and there are other lower hanging fruits for privacy, right? Bolt 12 is a huge privacy unlock in Lightning. And so, like, pushing that forward is, I think, [01:34:00] much more important than, uh, pushing forward the, uh, PTLC thing. Um, as much as PTLCs are important, Bull 12 much more so. Um, and other, you know, probing and other questions around monitoring payments flowing within the Lightning Network via active attacks.

Um, are also very concerning, and I think maybe even arguably more concerning than, than the just like payment hash correlation attacks that PTLCs solve. So, you know, there's a lot of issues with privacy in Lightning. PTLC solves one of many, um, and it, it is a lot of work to solve one of many, versus some of the other ones maybe we can solve easier.

Um, so it's not, not super high on my priority list. Um, maybe for the DLC folks much more so, cause I, I do think DLCs are really important. To enabling more people to build different lightning experiences that much better compete in the marketplace, especially against stable coins. [01:35:00] So, um, maybe we'll work on it from that point of view, but...

People in Bitcoin like to get excited about really technically hard things, when there are lower hanging fruits sometimes that we should just work on first. Um, you know, lightning is still early, there's still so many problems in lightning that we just need to solve. Let's get Bolt 12. Bolt 12 would be big L D K shipping.

Very initial Bolt 12 support for people. Hopefully this month. Knock on wood. Um, you heard it here first, soon tm, soon Tmm. Um, but Core Lightning also has experimental Bolt 12 support at Claire also shipping it. I think they're working on shipping it in Phoenix soon. Tm. Um, so yeah, you know, if you haven't.

Started thinking about how you're going to integrate it. It's time to start playing with it. Um, it does exist. Uh, it's not for L and D. Um, but there's some folks working on [01:36:00] building that, which will also hopefully be soon TM, uh, kind of sidecar Damon that you can run next to your L and D that'll give it full bolt 12 support.

Um, they have to ship blinded paths, which I think they're going to do in a, in a version or two. Um, but also soon TM to be able to add bolt 12 support to your L and D. Um, but if you're using something other than L and D. Um, Or even in general, it's time to start playing with it, it's time to start looking at it, because the code exists and you can actually run it now.

It's not just fictitious in the future something something. Um, you can start integrating it. Uh, I wouldn't say it's the most stable thing in the world. It's not gonna, you know, um, it's not the best privacy yet. There's still kind of early versions. But it is a version that you can start integrating, start playing with.

And by the time you're ready to ship. It will be much more stable. It will in fact improve payment reliability over bolt 11. Um, so yeah,

**Marty:** it's good to hear. It's great to have you in town.

**Matt:** Yeah. Thanks for having me on.

**Marty:** Great having you in the commons. You drag Jeff into the commons for the first [01:37:00] time in a while.

It's great to see him here. Yeah. And, uh, you guys are doing great work.

**Matt:** Thank you. Thank you. I'm very excited. I'm excited about the future of lightning.

**Marty:** I'm as well. Um, so historically on this show, when it's just me and you. You're given probabilities of Bitcoin success in the future. It started at 5%. You bumped it, you bumped it up to 40 percent at one point.

Where are you now?

**Matt:** It's a great question. Um, yeah, I mean, I think we still have a lot of room. Did I really say 40? You said, I think, pretty sure you said 40.

**Marty:** I don't know. I'm going to have to 5 to 40. You were very bullish.

**Matt:** Uh, yeah, that is very bullish for me. I would say 20. Oh, phew, 20. I think we need to do a better job competing in the marketplace against other cryptocurrency projects, and I don't mean that in the sense, a lot of crypto people like to [01:38:00] talk about, and we've, we've hit on it for the last hour, but, you know, a lot of crypto people like to talk about, like, crypto's killing Bitcoin and, like, Bitcoiners just need to learn from crypto, and I, that's the wrong lesson to take because, you know, Cryptocurrency broadly tends to not have this trustless goal as the North Star and tends to just kind of build what they think is going to work best in the marketplace, um, even if it requires trusting circle or tether or what have you, and that's not something we should be doing.

You know, there's no oversimplification. Obviously, cryptocurrency people I broadly also do want to build more trustless solutions, but the thing that gets built first is the trustful one, and that just gets adoption, and like, the trustless one often never does. Um, Uh, or gets less adoption, certainly not in the kind of consumer marketplace.

And I think the consumer marketplace is where Bitcoin needs to compete because Bitcoin isn't a DEX platform. It's not, you know, a token trading platform. It's not a, [01:39:00] it's not a, uh, investment platform for, uh, various tokenized assets. I mean, the, the big thing in cryptocurrency now, again, is this, this, we're just going to take.

You know, shares of regular old companies or investment contracts for regular old companies and put it on chain again to get, get liquidity there. Like that's cool. I mean, it's not, it's not something that Bitcoin cares about or competes on, you know, whatever they can, they can do that. Um, there's some regulatory arbitrage games.

Maybe they're going to provide value there to, to some of these companies. Cool. Um, but not relevant for Bitcoin and. You know, Bitcoin is not competing in that space. We're competing in the payments and money space. And to a large extent, competing in that space does mean competing for consumer eyeballs.

It's not just, you know, just saying we're just going to compete on the money space and we're going to out compete U. S. dollar. Maybe, maybe we will. But that's a... [01:40:00] Long tail outcome. That's a long ways away. It's not like going to happen next year. It's not going to happen in the next 10 years. It's a long ways out in the short term.

In the medium term, we have to compete for consumer eyeballs, and it is true that we're not doing a good job there. However, it's also true that there's a lot of Bitcoin companies who are working on fixing that because the problem is felt acutely. by some Bitcoiners, and the problem is pointed out often naively by many non Bitcoiners.

And so I'm excited about where that's going. I'm cautiously optimistic, but I also know that that is a big marketplace that is hard to compete in. And I want to set Bitcoin up to make sure that we have the most comp, you know, we don't just want to have one app that has TLC wallet, whatever. We want to have many potential solutions for people built by different people in local communities who can tailor it to what is needed in that community.

Um, [01:41:00] And, you know, that's why we build LDK. That's why I'm excited about where Bitcoin is going. But we need more of that to compete much better. I would agree. I would agree. And that is a hard problem. And so I'm not gonna say that we're definitely gonna win. I'm gonna, I'm gonna put us at a low probability of winning, in fact, because I think our fees are gonna be higher and people do care.

**Marty:** We're gonna win, um, but, but Matt's bearish, so. Always bearish. Yeah, you gotta be. We need that stick in the mud. Go write some code. I've

**Matt:** been a, been a stick in the mud for 30 years, so. You're in your 30s now? Yeah. Wow. We're all getting old, man. We're all getting

**Marty:** old. Alright, this has been fun. Thank you.

We'll do it again at some point. Yeah. Alright, peace and love, freaks. Takee!