TFTC 441

**Rob:** [00:00:00] All

**Marty:** right. We're live. Rob, we're we're here. We're talking. We're missing good content. That's right. Let's get right into it. We're, we're talking contentious, uh, potential Bitcoin protocol

**Rob:** changes here. Yeah, basically the future of Bitcoin. Um, it's interesting because, um, I, I've talked to, we were right before we hit recording, we were talking about covenants and drive chains.

And I've told Paul this directly at Tap Con last year. I was like, why don't you just launch it on Litecoin? It's precedent. It was already done for SegWit. Then you can already have people building tools where if there's a world where it ever got activated, people are hitting the ground running. 'cause an observation I have with Taproot is that we're two years post taproot launch and we're just, people are just starting to explore snore implementations of M P C and using tap scripts for more complicated like scripting structures.

And it's like the protocol change happened and it's like, you know, The, like Peter Will, and you know, Andrew Polster, like these elite level protocol developers [00:01:00] are so far out ahead that there's a huge gap between protocol developers and application level developers. And it took time to get actual application level developers in a place where they felt comfortable to build these more interested things.

Mm-hmm. So the question is then is like, you had two years that like, you know, could, could, if Taproot launched now as opposed to two years ago, would've really meaningfully had an impact on anything. And there, there are some people that got to it earlier, but my point being is that if you're trying to do a large sweeping change, like a drive chain, um, You're better off.

Like you, you wanna have the application ecosystem ready to actually use those tools. So launch a CNET with it, launch it on Litecoin, and then you can actually point and say, look at all of these things that are happening. And then people can make a decision if it wants to be brought into Bitcoin. And there's precedent with that.

SegWit was first activated on Litecoin. Mm-hmm. Right? Like we, like instead of like, you know, like actually using Litecoin as Bitcoin's testnet, it's like, okay, Litecoin bricks and all the incentives get wonky. Bitcoin's still fine, but you have something that's close enough in implementation to let people start building and tinkering with it.[00:02:00]

**Marty:** Yeah. And you're, I mean, you're saying tapper's two years in and hasn't had that much adoption. I mean, seg what's six years in and they're still. Laggards.

**Rob:** Yeah. To adopt that. Yeah. There's still a lot of, you know, there's a, one of them is on your shirt.

And then also I want to call out here as I was walking into the commons today, I got K Y C checked and Parker insisted I have to wear this blue check to be able to, uh, get on the podcast today. I didn't realize the Commons had a K Y C policy here. Uh, shout

**Marty:** out to B T C pins. Um, we have a box of blue checks to verify all members of the Bitcoin comments.

Fantastic. Um, B t c pins that make good pins. Yeah. I have the,

**Rob:** uh, blue, the faucet, so I have that and it's still sitting in the box 'cause I'm trying to find the right place to like display the pins. So until then, I keep it in the box. Are you uh, are you

**Marty:** mad at me for getting rid of my real blue

**Rob:** check? No, it's okay.

Um, it seems to me now that we have myself and Skylar, um, the design had it, Ty are now kind of like the, uh, you know, we're holding our own as kind of trying [00:03:00] to be the dignified bitcoiners with our blue checks. You know, you know, some bitcoiners are more equal than others and the blue checks just, you know, they're better people.

I'm just gonna say it. I mean, I do,

**Marty:** I do miss the reach. I'm not getting as many views these days. Oh yeah. Yeah. It's weird. It's everything. Bitcoin protocol developments like Twitter to X. Are they gonna be the everything app? It's, no, they're gonna go, it's a very chaotic

**Rob:** time. It was a very interesting juujitsu too, right?

Like from Elon positioning, because originally before Elon took over, the blue check was seen as this like cultural status symbol that, um, our cultural elite had access to, right? It was the journalists and there was a class of haves and have-nots. And then Elon came in and he democratized in the sense of you can pay for it and you can verify your identity.

Uh, and then, you know, then started layering in all of the K Y C and the payments information on top of that. And I was talking to Matt about this when I was at the park last time, and that was kind of like the ingenious of it. He was kind of like able to judo the cultural narrative and made it seem like getting a blue check was this act of altruism, rebellion.

And also like, like pushing back against those people that were [00:04:00] abusing their position of power for so long. Um, I, I ultimately viewed it as I use Twitter as a service and I enjoy consuming the content and I like, you know, I want to, I directionally support the system. I know there's, uh, what was it now?

Like the identity verification. Everything's coming down. We'll, we'll see how it all pans out. Yeah.

**Marty:** I was, before Elon even took over, I was paying three bucks a month for Twitter Blue. Mm-hmm. And it was, 'cause I'm a user for a decade. Yeah. And I get a lot of value. This podcast would not exist. Logan would not be sleeping in the corner.

**Rob:** I can't believe it. I got here and there's like a whole cott set up for him. He's just, he has a little camping set. You know, you get, you have a can of, like, you have a wall of canned beans for him and you, you, it, it looks like there's a cuff around his ankle and he's like a ball and chain. He's not allowed to leave the room.

Yeah.

**Marty:** No. Or he gets switched,

**Rob:** but, well, you already let car get away, right? You can't let the next one get away. No. But

**Marty:** like, Twitter's transition to X. Yeah. Like I've got a lot of value outta that platform for a [00:05:00] decade. Mm-hmm. Um, more than the decade. I joined in 2011, so like 12 years. Mm-hmm. The deprecation of tweet deck, really, like they destroyed that product.

It was a perfect product and need to know no updates. They did that and then, Elon posturing, like the Everything app. Like I don't want a WeChat in the us I don't think one platform should have all that power. Yeah. And then the new c e o, she's definitely just gonna start censoring people

**Rob:** again. Yeah, I saw that.

That was, um, things could be, what was it? I I, she had like a little like little catchy saying of something like, can be like legal, but like a problem basically. That there was some sort of awful but lawful. Awful but lawful. That was it. Yeah. And it was just like, oh, this literally could have been any of the previous Twitter people could have said that.

Yeah. Right.

**Marty:** Then you see there's like, it seems like they're picking favorites with the payouts. Some people are

**Rob:** getting, I saw like Laura Loomer had like 80 bucks or something. Yeah. And it's like you could have just not paid her, but to signal that you're getting so little, um, [00:06:00] and independent of your perspective of her, she definitely has a reach that would justify more.

And then I saw with Elon, removing, putting out, removing the block function. I think that's 'cause people block advertisers. I block

**Marty:** advertisers, I block advertiser. I've had to block blue Chew. It's like they're just like trying to put horny ads in front of me, like I'm married. Oh no, I've gotten those. Uh, I don't have an erectile dysfunction.

Like I'm just,

**Rob:** I'm just block, yeah. Blue chew and then like random mobile, like, like anime, like checks. And it's like, no, yeah. Not interested. Like just remove it. And the problem is, is that like if it comes up once in passing, you won't notice it. But like I, I used to work in digital, like online advertising and there's this concept of frequency capping.

And the idea is that there's a certain level of saturation you're gonna have and you're not gonna want to actually convert at a certain point. So like, Show the ad three times in 24 hours, or like, but like it'll just be 100% of my feed until I block it. And it's just like very basic like ad infrastructure that just makes it like a very poor user experience.

So I do blocking as well. Yeah, yeah. Yeah.

**Marty:** The um, and I think the payouts, if [00:07:00] they favor certain forms of like thread content and engagement hacking mm-hmm. People get paid out more for doing that type of stuff. Like creates this environment of self-censorship that, that really does not

**Rob:** appease me well.

And there's now like anti-patterns that emerge like that, where also people are just lifting other people's contents and screenshots and putting out there, because if they quote retweet, then someone else is gonna get the monetization. But if I like totally cut out the middle and I put it out as a, an image, then I get full of the credit.

Right. Yeah. So it degrades the, you're changing the game. Theory, incentives of using the social media platform where it used to be Twitter was a means to an end of like, you know, sign up for my newsletter, sign up for my sub stack, like subscribe to my YouTube channel, whatever it was, or my podcast. And now it's, you know, Twitter itself being the end has this very, uh, zero sum mentality when it comes to content distribution on the platform, which is just overall, like, it actually diminishes the, the quality of the experience.

Yeah.

**Marty:** And that's actually something we're working on, some [00:08:00] stuff at T F T C. Mm-hmm. Uh, don't wanna tease it too much, I just wanna get it out there at some point next month, so be on lookout for that. But that's something I've really been diving into and thinking about, um, very hard this summer particularly, is what is content distribution and the monetization look like.

Like, um, I guess I will tease it, but like mm-hmm. Zero Hedge is a really good model. Mm-hmm. Where, um, Tyler Durham writes content. They have a couple other writers that write under that pen name as well. So they have original content on the site and then they syndicate and back link to original content creators, which is good for distribution.

I don't know how they do it. They've pulled some of my shit and just put it up there. Mm-hmm. I'm like, oh, like it's cool to see the Bent on Zero Hedge. Right. They didn't ask me, they just scraped it. Mm-hmm. They link back, which for distribution purposes is good, but then obviously Zero Hedge has all those shitty ads.

Mm-hmm. They're [00:09:00] monetizing that. Yep. And obviously they have the premium, how they're monetizing as well, but like how do we replicate that model but allow the. Contributors that you're the content creators that you're syndicating to participate in that monetization as well. I do think Bitcoin plays a role in that.

**Rob:** I actually just had an idea sitting here, you could layer in value for value insofar as if I have a buddy and I refer like my referral link, you can get a percentage. Like if I refer someone to the bent with my link, it would like tie back to like my lightning pub key and then maybe whatever residual would kick through and like be part of that referral.

That's me just sitting here in real time. Like using the lightning prisms for like part of that like distribution and incentivizing people to share content. Right. And you're only, it's value aligned because if no one clicks the link and no one pays, then you don't get anything. But if like it, it's a way to like monetize this syndication system where if you're redistribute, like you can link that in there as a way to like have an alignment of outcome and incentives.

**Marty:** Yeah, and that's, so that's sort of. We're not going exactly down that road, but, um, fuck it. I'll just say

**Rob:** it out loud. I wasn't trying to bait you out. [00:10:00]

**Marty:** Something like that where we employ like a zero hedge model with the syndication to increase distribution for individual content creators of their own websites sub stacks, but then layering in value for value functionalities with lightning and then doing a rev split.

Nice. Oh, okay. Yeah. That comes in from those revenues on the

**Rob:** site. It makes sense. Yeah, right. I mean, uh, especially with, um, Twitter trying to insert itself as this central point trying to find other ways to route around that. Yeah. Makes sense.

**Marty:** Yeah. Yeah. And then like, that's the other thing too, like, um, just thinking about where we are in the cycle of content creation, distribution, and monetization.

Like, are people really happy with the CK model where they go and they subscribe to each individual creator and pay a monthly feed to each of them, right? Or would they rather. Get all that content aggregated somewhere else and then pay a little bit

**Rob:** per, sounds like an interesting way you can turn this into [00:11:00] with, um, Noster as well.

Yeah. You start like making your, this is the, my, my, my thing with Oster is I have an Noster account and I think that like most of the use cases up to this point of like a Twitter clone is like, I get it because it's a mental model. Other people can gr and they can start following and seeing like how you can take the experience and import it over here.

For me, like Nostri to be successful, it's gonna be like, that's gonna be a very minority use case. And one example I think offhand is like, um, wallet coordination. If you use Specter and I use Sparrow, we should be able to use Nostri as a way to coordinate output descriptors and PSB ts. So like I can request a signature from you and then you would get like a, that's something to pop out here, and then you could be able to coordinate and move all that stuff.

To me that's like, it's a perfect use case for Bitcoin and you can use this as a way to just like share this information. And Nostri is just like the dumb pipes that are just into smart clients, right? Like your wallet is the smart client. Your, your dumbest, your your, um, you know, those are smart clients with dumb servers that are just like spitting out information.

I think that's a really interesting way to start thinking about using noser and in this context [00:12:00] with like social content. Like you subscribe to this feed and then the server's just pushing out the content, but then your applications like doing the more fancy curation based on your likes and interests.

Yeah.

**Marty:** Yeah. Didn't Ben build something like that for the coordination

**Rob:** of Multisig? Did he Oh, I, I've been, um, I've been talking about it for a couple months, hoping someone would build it. So maybe he did actually he might've built

**Marty:** it. Um, I could be wrong though. He built some multisig coordination or maybe it was a coin

**Rob:** Joinin coordination thing.

Oh, it was Coin Joinin I think. Yeah. He was doing coin joinin. Yeah. Yeah, yeah, yeah. But, uh, I think this world of like, um, it's just a model of like, you should be able to use whatever user, like whatever wallet user interface you prefer. But if you're doing some sort of distributed custody, we should be able to just, you know, use this as a coordination for all of the backend stuff so I can have my user experience.

You have your user experience and everyone's happy. Yeah.

**Marty:** Um, I do wanna bring it back to the beginning of the conversation 'cause I do mm-hmm. Think it's very topical, number one. But it is important like to talk about [00:13:00] these protocol. Up upgrades. Mm-hmm. Changes, whatever you wanna call them mm-hmm. That are being discussed right now.

Whether it's drive chains, uh, op, c t v, op vault, uh, a p o,

**Rob:** um, it's checks sick from stack that's been floating around too. Yeah. C ss f s, which is, yeah. But yes, there's a lot of stuff floating around right now. So in

**Marty:** your mind with that list, everything floating around, what do you think is a top priority?

**Rob:** Uh, I mean, top priority is who has actual code, right? So that's what kind of the drive chain stuff really started getting like extra turned around this week. And, and the conversation was that Luke put out that pull request, but it's a partial pull request. It's not even like, you couldn't even take that code and click go live to my understanding, and actually have drive chains working.

So I think, um, Francis Paleo was saying this, that basically like if you want a fork and change bitcoin, Write your BIP eight, your user activated software client and get people to talk about it. 'cause until then, it's all just kind of hypothetical abstractions. People should be able to look at the code and see exactly, [00:14:00] okay, you wanna make a nut change, what exactly is the change?

And I think that's the first threshold. And and to my understanding right now, um, I think a p o and uh, uh, C T V are the two that actually have like code ready to like roll. I don't think it's formally rolled into a bit eight, like, like rease into the current version of Bitcoin and like forking it in.

But the code's sitting there and I think that's the actual serious place people should start with conversations. And that's actually like, I think the most, like whatever your independent opinions are for like drive chains around like game theory and changing of incentives and stuff, the code isn't ready to go.

So what are we talking about? Yeah, right. Like, like if I can't actually activate the drive, like there isn't, if the code doesn't exist and I can't play with it right now, then like you're way premature in talking about let's upgrade the entire protocol to do this. And I think to my understanding, that was part of.

Luke's role is that Paul contracted him to start writing this implementation. And this is secondhand from people we're talking about on Twitter space. Paul wanted Luke to get the initial code out there to get people to start talking about it. So that's the actual way if you actually wanna make a change.

Um, [00:15:00] I know I didn't really directly answer your question on like, what interests me, I think C T v op vault or the things that I immediately look to, um, A P o I know, and this is also, I guess is part of my biases being I call myself a proud layer one boomer. Like I just, I'm, I'm, I, I use Lightning, I have my own lightning node.

I play around with it. But like, I'm, I'm definitely more focused on a day-to-day basis on layer one, Bitcoin and C T V I just think has such massive and like op vault, like this idea of, um, making more intelligent custody solutions if it just drastically changes from a scaling perspective and being able to have ways you can have trusted, like, like, like, like trustless, like more like aggregating of U T X O.

So more people can like co-own A U T X O and for just like from a self sovereignty. Custody perspective, the idea that I can like commit this address to only go to a certain address or like Val, like those are the massive step functions. And like James ZR calls it proactive versus reactive security. All Bitcoin security today is you set up all of like your traps and your drawbridges and everything, and then you [00:16:00] hope no one gets in.

But if someone gets in, the money's gone. And Val is explicitly reactive. And I think that's a really powerful paradigm shift when it talks about custody, whether you're a business or you're an individual. And I think it, and that's why it's a great use case 'cause it serves everyone that uses Bitcoin.

**Marty:** Yeah. I mean, I think James' positioning of Op Vault as a potential upgrade that can make exchanges, ex exchange hacks a thing of the past is extremely powerful. Yeah.

**Rob:** Um, exchange hacks and $5 wrench tax. Yeah. Things that like, oh, okay. Um, you moved the money, but it sits here for two weeks. Like, it doesn't make it impossible for something to happen.

Um, but it definitely makes it signifi much signifi harder, significantly increases the cost. And additionally you can have, um, a, you can have a watch part watchtower service, so you can like have a op vault like transaction and let's say all of a sudden you try to spend your entire life savings out of your vault and you work with me as like a partner.

Even if you are getting like $5 wrench attack or something like, and you don't get a whole, like, I can pull the switch and just [00:17:00] like sweep it to your emergency cold storage. In that sense, you still have to figure out, okay, with op vault you have an address, you take it to like a staging area and you wait for the time lock and then you can send it to where you were trying to, or you can pull the emergency switch and go to like a different cold storage.

You still need to consider how you're gonna secure those funds. Right? Yeah. In that like emergency cold storage. But it does, it, it, it makes these things, um, infinitesimal risks as opposed to like very real visceral risks

**Marty:** that have existed throughout the 15 years of Bitcoin's existence so far. Yeah, absolutely.

Um, That gets to another point. It's like something that you've really been beating the drum, and I really like your framing around this subject, which is, it's maybe not rush into all this stuff. Maybe let's just play around with things. We have like mini script obviously you're building Yeah. A company around this primitive and, um, it hasn't been, uh, too well explored yet.

Obviously you guys, Liana mm-hmm. Are playing around with it. Others are beginning to play around with it. Yeah. And like in your mind, [00:18:00] like diving into that idea of, all right, let's play around with what we have and then see like if that's good enough, and then do we need this other stuff? Yeah. Make that decision down the line.

**Rob:** And, and for us, like, it's also from a enterprise risk perspective of running a company, um, I guess you, you could compare it to like Paul layer two labs where the entire premise of the company is this soft forecast to exist, right? You need to make an upgrade change. Um, while things like op vault, op C T V would make.

What we're offering at Anchor watch a better solution. We can't live in the world of like, uh, and all we need to do is just get a soft work into Bitcoin, right? Like that's way too much risk. So we're, we're in a much better position of just working within Minis script. And what's great about it is that it just uses the existing tools that Bitcoin has.

And it's, uh, something that I think is massively underexplored and the fact that Leonna, the Leonna team, like Kevin Antoine Eduard, like we're working on this for like a year and there was really no one else, I think, really. And, and the signing devices are finally starting to come online with it, which is another major step function.

'cause it was [00:19:00] working and ready to go, but then you had to use a hot, you'd use your computer, right? Didn't have hardware wallet support. So getting the hardware wallets and just, uh, this morning, uh, on my way over here, uh, the bit Box oh two just announced support for it. Okay. Right. So the bit, so we have the Bit box oh two, we have the ledger, we have the cold card, MK four on their Edge firmware.

And the Specter d i y

**Marty:** is this support. H w

I

**Rob:** at all? Uh, no. The Wizard Sardine guys are working on h w I specifically. Okay. Um, so, uh, how do I say this? Uh, so for the bit box, so what, the way we're integrating everything right now is like through the web app. So, uh, ledger has a JavaScript library you can plug in cold card's great.

Because it's just file upload. 'cause it just uses output descriptions. And PS BTS you just like drag drop file where they're using micro sty or plugging into the computer. Um, the Spectra, d i y uses QR codes, so we have that all fully rock and loaded and running. And the bit box O two guys have, uh, they wrote everything in Rust and then they have bindings into [00:20:00] JavaScript.

So it can all work in the web app. Okay. But I think the next step, and since the Wizard Sardine guys with Liana, it's a desktop wallet, they need to have the H W I interfacing, so they've been working on it from that side. Um, but ultimately, like, this is just where it gets really exciting now is like being able to do more advanced custody solutions that don't require a fork.

Making it accessible to the everyday user of Bitcoin to have things like time locks without worrying about like I have to make a custom wallet and script that's gonna be able to access this Bitcoin core. Just merged mini script support for signing and reading. Well, reading was back in January, but signing support was like last month.

So now even if you wanted to use Bitcoin core as your wallet, you could even just use it there. But you can also load it as a watch only wallet, which is great for if our servers go offline and they cease to exist, you can still port your wallet somewhere and be able to access it. Right. Um, so there's been a lot of movement this year and it gets really exciting just being able to have more advanced custody solutions and for like a regular user, the idea of like, I have a two or three multisig, but if the funds haven't moved in two years, it's a one of three multisig, [00:21:00] or it's a one, one of my three keys plus maybe like an emergency like friend for social recovery.

Right. I think the idea, um, for us as a business, we use it in the lens of multi-institutional custody, but as a sovereign individual, you could use it for social recovery too. You can have friends that you trust that only if a certain amount of time passes. You can be able to coordinate this stuff. And I think it just, it's sticking to the, like, making Bitcoin programmable money and many scripts makes Bitcoin easier to access that programmability.

And because of that, it makes Bitcoin better money. We can move beyond single sig and multi in like two of three, three of five, like multi sig and you can do much more advanced, um, constructions. And it's been really fun to be building on top of those tools. Yeah.

**Marty:** And so let's take a step back for anybody who's listening to this and it's like, what the hell are these guys?

I realize talking about jump right in. No, but I mean, I mean I love getting into the weeds like this, but I do think just for the appeasement of people who may be newer to these concepts, I think we do, like how does minis [00:22:00] script improve multisig? Mm-hmm. Is it even an improvement on multisig or is it something completely different?

Um, how are you guys implementing it into anchor watch? Mm-hmm. Um, Whether it's just pure custody or via your insurance products.

**Rob:** Yeah. So I'll even take one further step back. What's Bitcoin script right? Before we even talk about what many script is? So Bitcoin script is something that Satoshi invented with Bitcoin.

It's the actual language that locks your Bitcoin on chain. So when you see an address, um, you have a locking script that maps to that address. And the very simple one, let's even, let's put segue aside for a second. It's like a public key hash. You have your public key, you hash it, and then you encode it into an address.

And then when you go to spend, you present your public key and you present your signature and you verify you can unlock the funds. Um, this gets expanded upon in Multisig with op check multisig, which is, uh, this is an op code, right? We talk about this in Bitcoin for things. When you're doing an upgrade to Bitcoin and you're adding an op code, you're saying, I [00:23:00] want to add a new way to.

Use Bitcoin as program, like as a program function. Um, there's 256 op codes. Uh, about 110 of them are active Satoshi, right before he left the project, deactivate deactivated a bunch of them because one

**Marty:** of them created like a fatal loop

**Rob:** or something like that. Yeah, so I think like, like Opca was one of them, which I, I believe Opca, which is concatenating to strings actually allows recursion.

So it allowed like all these weird things. It also had op multiply divide. There were all these crazy things you could do. Um, my favorite op code that got deactivated very quickly was op ver for op version. So if you're running version 23 and I was running version 24 of Bitcoin, we would get different values, which is basically op hard fork because you, like our addresses would map differently.

It wouldn't make sense, right? So, um, Satoshi, when you put all these like op codes in there, um, definitely didn't see the externalities there. There was no idea of Nakamoto consensus yet what that even meant, right? So you very quickly start, when the system goes live, you realize, well wait a second. Like we need to have uniformity of information and that's.[00:24:00]

Part of the idea of soft works is that you have things that are backwards compatible. So Bitcoin script are all these crazy rules, right, that allow you to use Bitcoin, um, for different locking conditions. And what Minis script does, it says, okay, let's take like 20 of these, like the core building blocks and treat 'em like Lego bricks, where you can kind of do more interesting custody solutions.

Um, there's three main tools, um, security tools, let's call them that minis script leverages one, a Bitcoin signature, right? That's what we all use today. Um, then the next thing is a time lock. So a time lock. Um, we've talked about like time locks got added into Bitcoin. It was actually the last forks before SegWit.

There's two kinds of time locks. There is an absolute time lock and a relative time lock. An absolute time lock is, Hey, I'm gonna meet you at five o'clock tomorrow. Uh, relative time lock is, I'll meet you in eight hours. Right one's based on the relative time of what it is right now and one's based on a set fixed time in the future.

Additionally, There's two [00:25:00] ways you can do a time lock. You can either do a block height or you can actually do the timestamp. And this is something that, uh, so, uh, like the, as a con, like it is a fun thing to just think about. The only piece of external information that exists in Bitcoin is the timestamp the miners put into the block header.

Everything else within Bitcoin exists within the rules of Bitcoin. So you can use a time lock and you can actually say on July 1st, this happens. Mm-hmm. Right? Uh, or you can say at block height a million, but you can't, you can't do both. You have to only pick, you can only bring one clock to Bitcoin script.

Um, so you have to be able to say, it might gonna do a block height based thing or a calendar based thing. And then the final tool, so you have time locks, you have signatures. And then the last one is a hash lock, which we use enlightening for like hash time lock contracts. But additionally, like as a general mental model, instead of a signature, you have a.

You have like a, a pre-image, so you have like a password or something that allows you to do something. So that can allow you to do, it does not solve the Oracle [00:26:00] problem. But you could have Oracles put things on chain. So a very simple example of this is like we could have a bet where like we think the a Phillies are gonna win or lose, right?

So you bet the a Phillies are gonna win, I'm gonna bet the Phillies are gonna lose. And the way you would spend it would be like my signature plus the Oracle saying Phillies lose and then I could pull the money out. Yeah, right? So you have to have an Oracle somewhere and it doesn't solve any of that, but it allows you to do this stuff.

So Minis script takes these three security tools plus and an OR and you can start clicking things in together to do more interesting custody solutions. Uh, a practical example of what this looks like is one a key hierarchy, right? So talking about like, is this, it's different than plain multisig, right?

Because Multisig, the way most people construct it, I view it as democracy for your money. And I think as a sovereign individual, like as an individual use case, that makes sense. I have a two of three. If I get majority of my keys, I can spend my money. I'm the only stakeholder that may get more complicated in a corporate governance setting, right?

Maybe. And how we kind of think about this is the idea of a key hierarchy. So let's say for example, it's a two or three multisig, um, but Marty, it's your money and you just give me a key and you give Logan [00:27:00] A. Key. You're concerned though, if it's a regular two or three multi SIGs that Logan and I are gonna go run off with your money with a key hierarchy.

It could be your key must sign, plus either myself and Lo or Logan, right? So there's no way the two of us can run off with the money you have seniority 'cause it's your money, right? And this is the idea. You could start thinking about this in a corporate governance setting. Maybe you want to have a board of director sign off plus one of the executive team, right?

So this allows you to do this on chain governance for more complicated custody. Inevitably the follow-up question is cool. So my key must sign have to get hit by a bus. Well, that's where time lock comes in. You can say, um, after a certain amount of time, another spending path becomes available where your key's no longer required.

And this is where we are thinking about this with multi-institutional custody. It gets really interesting because maybe in a two of three where this one key is held by another company, you can actually have it be your two of three is the customer plus our two of three as a service, right? So we get to do risk distribution, not just from you versus another company, but within a [00:28:00] company you can distribute that risk.

So there isn't just one person with the key, and this is where it gets really exciting about more elaborative ways, and there's no one right way of doing it. It's very openly permissive and expressive and you can just, you know, do whatever you'd like. So that's a high level review of the tool set of what Minis script is and how it can allow you to do more interesting custody solutions.

Yeah,

**Marty:** and just building on that explanation, I guess you. Building out anchor watch and thinking about this, like how do you weigh the trade off of making something as simple as possible, like, how do you like mm-hmm. Sort of narrow it from making it just simple enough and not too complex.

**Rob:** Right? Yes. So, uh, I've been championing this idea of templates mm-hmm.

In that. Um, so we have a developer tool that allows you to make all these crazy custom scripts, and we have fun with that, just to kind of like make sure all of the, from a website interface standpoint, everything works and there's no unexpected issues. But for mass adoption, you [00:29:00] don't want to have someone walking in and just be like, I'm gonna make a custom vault today.

Because what's gonna happen is they'll time lock their money for a hundred years and be like, Hey, like what happened? And be like, I can't, there's no refunds. Like once the money gets confirmed on chain, I can't, I can't change the rules of how time locks work to get your money unlocked. Right? So the idea of a template though, I think is a great way to streamline this.

And the perfect example earlier I talked about was this idea of a two of three decaying multisig where maybe it's two of three, but if a year goes by and the money hasn't moved, you can have it, you can have, uh, one key be required, right? And that's the cool thing with like a relative time lock. It's like a dead man switch.

'cause the timer starts once funds get deposited on chain. So as long as you're alive and everything's well, and you keep moving the money around once a year, like you reset the time lock. But, um, if something were to happen, you're able to use that as a way to like emergency recover the money. So templates are really great because it streamlines one the, um, mental load of a user.

They just like, I'm using template A, it's a 2 0 3 K multisig, it streamlines the hardware wallets. They [00:30:00] don't have to show as much information if they know it's within this constrained template. And they also know they can protect users to make sure they're not setting up an arbitrary multisig that's locking their money for a hundred years.

Um, it streamlines the other wallets that can talk to each other to make sure that everyone like, oh, use template a cool, we know we like to visualize templates like this. And then every person can have their own take on how they visualize it. And then also for on chain, um, privacy, um, if more people are using the same kind of template, you kind of blend in a larger crowd.

If you, you can make a really crazy random like multisig, but when you go to spend, you have to reveal that and it's a very unique footprint. Right. So those, that's how we kind of think about it is using templates as a way to, uh, streamline the mental load so people can have safe confidence. Right. And also having people security audit those templates.

Right. So then you know that there isn't some weird unexpected bug that could possibly have an unintended spend consequence. Yeah,

**Marty:** no, it's very. Exciting is going back to like the op vault. Yeah. Example, like just that peace of mind knowing like, all right, I have fail safes. Yes. In okay, something messes up, somebody [00:31:00] dies, somebody loses a key.

Absolutely. Like this is gonna be massive. Mm-hmm. And then on top of that, like you can add value added services like insurance products. Yeah. And then what does that unlock for Bitcoiners companies like having that ability to insure funds?

**Rob:** Yeah. So this is, uh, on the insurance piece, it's really interesting.

So we, we founded the company in March of last year, and since then we've had Prime Trust, F T X, Celsius, voyage, all, all of these, like all of these companies have gone kaputt and Belly Up, right? And for us it was this baseline premise that as Bitcoin continues to mature as an asset, and if it continues, if it's on the trajectory, you and I both think of it being, um, Aral World's Reserve currency.

There's going to be a risk market that develops around it just like any other asset. There's, you can get insurance on your home, you get insurance on your car, how, um, you're gonna want to have insurance on your Bitcoin because unless you know, you're deep in the weeds and [00:32:00] even, even if you are like very deeply technical and you're able to construct and you feel comfortable with how your custody is at the end of the day, like you want to be able to go to sleep at night and know that everything's okay.

And the idea of insurance has been around for hundreds of years. Um, it's kind of what really kicked off like, um, the Amer America because that's how all of the ships got underwritten to actually do all of the exploring. 'cause until then, you would have a merchant who would put their entire life savings in the boat and if the boat sank, they'd be done.

Whereas with insurance, they'd be able to take risks and not totally get destroyed in the event that something wanted to go wrong. Right. So, um, the idea of. Having insurance for Bitcoin in a way for being able to provide custody, a, a sense of safety where if you choose to get exposure to Bitcoin, you're already accepting the volatility risk of the price.

The last thing you also wanna take on top of that is Keyman risk, where, what if I mess something up and I lose my money? And we've had a lot of conversations with people who maybe invest in Bitcoin companies or like [00:33:00] they, they hold G B T C, but they can't self custody because they, they can't from either their family office or the fiduciaries or trust, whatever it is.

They can't actually directly hold the, the coins themselves because they can't, they, they have to worry about this governance problem of you don't wanna have, like sailor is not sitting with a ledger in his desk at his house with all of the Bitcoin for MicroStrategy. Right? And it's a very suboptimal way of thinking about how Bitcoin should be ed.

And additionally, it emerges this anti-pattern where everyone keeps their money at the same three custodians, right? So being able to sufficiently distribute the risk of not all of the keys sitting at one place, but additionally having the keys. Um, sharded in a way with, with like leveraging minis script, but having this distribution of risk of where the keys are located brings more resilience to the network at large.

Because you don't have to have a so sole focal choke point. Like if you use a Coinbase or you use a bit of like the keys are sitting there. Yeah. And that's it. So, um, they, they, they both have insurance products, but the insurance coverage is an aggregate per incident limit. So if they hold [00:34:00] a lot, you know, they don't have dollar for dollar denomination for your.

Coins specifically, right? So this idea of being able to have you as the named insured on an insurance policy so you can feel confident that you have a, like, you have a recourse in the event, something were to go wrong and you're not standing in line for claims if something were to go wrong. Um, and it just allows people to take that wr, be able to take that leap and get exposure to Bitcoin and also be able to have this like distribution, uh, ability to go to sleep at night, right?

Being able to have that peace of mind. So that's kind of like our lens and our take on it. And Minis script was the really big unlock for being able to encode this governance in a sufficient way for enterprise amounts of money, right? Like talking about underwriting $10 million of Bitcoin in a vault, a two or three multi seg, right?

We can go back to before like maybe the customer run, like they could either collude or there's a crime incident that happens. But the idea, like for what we're building at Anchor watch, uh, we call it a wa our coordinator, we call it Trident, right? Like a multi-pronged security. Is that even like we don't store any keys on the platform.

[00:35:00] It's all hardware wallets. But even if something like, uh, if, if, if you've lost all of your keys, like someone came to your house and fired all wrench and like took your stuff, no funds have been lost yet. On the, on the same exact piece. If someone were to massively compromise our keys, your keys are still required to sign for the length of the policy.

And this is where it gets really interesting too, is leveraging these time locks where for as long as you're engaging in a service with us and we're providing value to you, and we are holding risk, we are a required signer at anchor watch. But if you don't wanna work with us anymore after the insurance policy expires, we can use a calendar time lock.

It goes back to just being your keys again, right? So it's having this fair alignment of incentives compared to using a custodian. You're like, oh custodian, I don't wanna work with you anymore, can get my money back. And you're, is the person on the other end a Prime Trust or an F T X or a Celsius, right?

Like this idea of being able to use Bitcoin as this programmable money to have this handoff of once the contract expires and you're not working with us anymore, it's actually easier for us. To let you just take your own money out. 'cause it's less operational overhead in our piece. You, you don't have to, [00:36:00] we don't have to like process a withdrawal for you.

It's your keys. Go spend them. Yeah. Yeah.

**Marty:** Instead to dive into this, like, to explain it more granularly. Sure. Like when the insurance policy's up via mini script, the sort of multisig setup decays and you don't need an anchor watch key to sign

**Rob:** to move the Bitcoin. That's exactly right. Yeah. So for the length of the policy, we are required to sign, but after the policy expires, it goes back to you.

Yeah. Yeah. And that's just, uh, and you could verify this yourself. This was a really big unlock when Bitcoin Court added this, is that you could load the wallet yourself if you wanted to. Right. You could go look, take the output descriptive, you could load it into core, verify the deposit addresses. Right.

And when I'm not trying to like hoodwink you into giving me money personally, you can independently verify this and you could hire your own experts if you wanted to, to go through and be like, okay. Yep. It does at, at this calendar date. It's just your keys and you can sign. And we also can contin have contingency plans where if you had a catastrophic event where your office and your home like all burned down, like there's a massive like natural disaster.

We can have [00:37:00] contingency situations where it's us plus a third party that can come in and help recover the funds for you as well and a, and like indemnify you and make sure you can get your Bitcoin back. Right. It allows this to, to have this way of not viewing custody on a binary, it's more of a spectrum.

And now you're adding time as a variable into the custody. Like is it right now or is it a year from now? And it, the coins don't have to move on chain. It's all just programmed into the script. Yeah.

**Marty:** And then diving deeper into like the policy construction, like what if somebody was to approach anchor watch, like, I need to ensure my Bitcoin.

Mm-hmm. What does that process look like?

**Rob:** Yeah, so, uh, we're gonna have the quote process live later this year. We're launching first with just getting the tech demo. Next week should be live out there for anyone to go in and start. Messing with their cold card, their spectra, d i y or their ledger to actually use this themselves and see what the user flow looks like and help us give feedback.

But specifically for insurance, it'd be underwriting just like it would be for any other insurance product, right? So, um, people have asked me it, this is a [00:38:00] K Y C product. If you're signing a financial contract, we can't do a financial contract with a pseudonym, uh, because if there was recourse, you can't go to court as a pseudonym, right?

So this is a regulated legal financial contract, and insurance is probably second most regulated industry behind banking. But you'd go through an underwriting process like you would for a home or a car, where we would understand, okay, this is how much Bitcoin you have, this is, you know, um, how it's currently cued.

Like you, you're gonna have key holders on your side, who are those key holders? Understanding that, kind of clicking it in, um, and assuming we go through underwriting, everything's approved, uh, we would, uh, walk you through, set up a vault. Deposit funds. Funds are there. And then you'd be able to log into your dashboard, be able to look at, see your funds are sitting there.

We also added additional functionality for like audit logs. So you can see anyone in the vault who's like, you can give someone view only access. So maybe you have a lawyer or someone you wanna have to be able to look at the funds, but they're not gonna hold the key themselves. They're not spending anything.

You can add them as a viewer, right. From the interfacing side, you can see who's proposed transactions. When [00:39:00] you do a spend, we can actually show you also who signed. Right? So on your side you have maybe three keys. You'd be like, oh, it's key two and three that signed for you. Right. And those are things that, um, anyone could do today if you have the information.

It's just, I was surprised that no one had really done that yet, where you can see specifically which key signs. So on the insurance side, we're trying to streamline as much as possible to be like a traditional insurance product where you go through underwriting, you sign everything up, and then we have the tech intersect with it to actually deposit and secure the funds.

And then you're off to the races. Mm-hmm. Pay your premium and then move on. Yeah.

**Marty:** What does this unlock, do you think? You obviously, the. Family offices, high net worth individuals. Mm-hmm. Gives them more comfort, but more broadly beyond that.

**Rob:** So for me, I think it actually provides peace of mind for anyone who wants Bitcoin exposure to understand that it's actually safe.

There's actually a big misunderstanding. Most people think that their funds are sitting at an exchange, that there's some sort of insurance, just like people think that dollars backed by gold and it's, you know, it's really not. They think the F T I C covers this stuff and it's not the case. [00:40:00] So for, for me, I, I view it as it removes the mental burden for getting exposure to Bitcoin because you don't have to worry about what if I get hacked and then additionally you have this, um, it, it also enforces better governance in the industry, right?

This idea of, um, this idea of insured duties, like when insurance started, um, in the fifteens and 16 hundreds, it was guilds of merchants, skilled merchants who understood the best practices in the industry, and they enforced that on anyone. Who was going to get insurance from them? It was, um, the Lex, it was in Latin, but the term was like the merchant manual, and it was like this big thick book and it had all of like, you know, if there's storms, if there's this, there's that.

And that's, we get to kind of push forward that governance and best practices to people who are using Bitcoin. So it removes a lot of the mental load of how do I secure my funds? Like, well, this is like for people who think that like self custody be complicated, we just said like, here's like the instructions.

Do it this way. And if you follow these two, like this is part of your insurance. And [00:41:00] it removes the mental load of actually getting insurance to be like, to getting, uh, exposure to Bitcoin and self custody. We kind of like provide as a curated experience that bundles in with the insurance. And if something were to go wrong, you're insured, right?

Yeah. So it just, it removes all of that mental friction and like all of the anxiety, um, for you and I who've been in this industry for like a decade, right? Like, um, The, these are things that are like, they become second, like it's the water we swim in. But for each incremental person who's looking to get adoption of Bitcoin, they're not gonna be as technically competent as you would I, and we want to be able to make it as easy as possible for 'em to say yes and get exposure.

And, and if you have a custodian or some sort of aggregator who's managing these services, you can have confidence that they're following best practices. Yeah. And it's not just, uh, Sam Bankman free, but the ledger in his desk moving funds around. That's

**Marty:** funny. You just said that and that makes me think like, is this current crop of Bitcoin or is going to be the most technically competent crop of Bitcoiners that ever exists?

Like will the UX around interacting with Bitcoin get to such a point that you don't even need to understand any of

**Rob:** [00:42:00] this? It's a really inter, having been building this wallet now for, uh, we, we started working on Trident, uh, in full swing in like January. It was around November. I was having a conversation from our Buddy Vic at Coin Kite about minis scripts specifically.

That really like turned the light bulb on for me. The real pain point is the ux because you have this really delicate walk you need to do where if you abstract details away, you then disempower users to understand what's going on. So it's a very tight line to walk. I think this, this current generation would be most technical because we kind of had to build the tools, right?

We had to understand this stuff at first principles. Um, now there as an aggregate class of users, I would say that's probably the case because I mean, when I first started getting into Bitcoin, it was paper wallets. So you had like, like the friction, like this is back in like 2013, I started going to the New York City Bit Devs meetup and like that was your best option.

Armory came out a couple years [00:43:00] later, right. And that was still like running air gap computers and everything. Hardware wallets got more proliferated, which made it much easier to understand this stuff. So to answer your question, yeah, I think just by the nature of like, we had to like build the stick to like make the spear, right?

Like we're like, we're cutting down fire. Like we're like cavemen. You have to kind of at first principles really grok this stuff. Um, so yeah. And that's, it's probably a good thing in so far as it not every, like we, I'm a big believer that Bitcoin is a tool. It, it's a means to an end. It's not the end itself.

And we, I think it's our job as the early adopters here to make it so that people can just live their lives and enjoy their, enjoy their work, enjoy their families, and enjoy life. And just know that the money problem solved, it works and it works, right? So like, it, it's on us to kind of shoulder that burden and make it easier from a user experience standpoint so that more people can just use Bitcoin as a tool to live a better life.

And then Bitcoin doesn't have to be their life to get too super deep in the technical weeds. 'cause that doesn't scale.

**Marty:** No, no. I [00:44:00] mean, that's one of the biggest knocks on Bitcoin. You talk to anybody trying to convince them, like, Hey, this is something you should probably be paying attention to. They're like, it's too technical.

Yep. Nobody's ever gonna use it. Yep. It's like a UX will improve.

**Rob:** The UX will improve. Yeah. And that's, um, yeah. It, it's, it, it's fun. But it it, it's hard. Like it is like having now and just to like talking about one of your earlier questions around was like, how are we building this? We use Bitcoin dev code.

Bitcoin Dev Kit, B d K, and shout out to Akos, Steve Meyers, thunder Biscuit, Daniella, like Matt now who joined the team, uh, with the recent Spiral grant. Like they, it's a very powerful Swiss Army knife that lets us do all this stuff. So the actual hard part is the ux. Like you have to be careful and thoughtful in how you're constructing your APIs and making sure you're not doing silly things and whatnot.

But the tools are coming outta the box and it works. And it's a really powerful primitive to do, like all of this Minis script stuff is just outta the box works. Um, it's built natively in Rust. So it's [00:45:00] built on top of Rust, Bitcoin and Rust Minis script, the built, uh, libraries that Andrew SRA maintains.

And it allows for you to, for us, it's actually like talking about this like abstracting things. I don't have to go and write Ellipta Curve cryptography and like, like we get to just sit on top, stand on the shoulders of Andrew SRA to be able to actually work on the application piece. So here I am talking about like, oh, you know, it's our burden to figure it out.

Like, Stand on the shoulder of giants like Andrew's the one who like wrote all of this code, like, and built all of these things so that I don't have to start at square zero, I can just start with the working tools to then make the user experience that I want to need from to service my customers. So yeah, like it's, it's a, it's been, it's been a really great experience.

And uh, also the foreign language bindings down the line, like adding a mobile app much easier. 'cause you can just take, I have all the instructions and just port it over to Kotlin or Swift and so you can just have an Android or iOS app outta the box. And that's like, I think it's largely the credit. You can look at what the Mutiny guys did.

They built it as the web, like the, you know, the progressive, the web app, the progress, the progressive web app. And then they just [00:46:00] like, oh, flip a switch. Okay, it's Android. 'cause they had all of the tools sitting there. So like, I'm not, I'm trivializing it a little bit, but like, they didn't have to re-architect their code all over again to make it work in a mobile app.

Yeah. And that's a really, it's just an incredible tool. I can't, can't thank them highly enough and like just sing their praises because it's a real superpower and that's why we're a very small team. Um, It's myself. We have one other full-time engineer and one person we're looking to bring on soon, but like it's, and we're able to build this entire experience.

Yeah. And like have high confidence that all the bitcoiny stuff works. It's pretty crazy.

**Marty:** Yeah. And it, I mean, it speaks to one of my largest frustrations in the space, which is not in the space, but like critics of Bitcoin. It's just their impatience. Like to, you gotta crawl before you walk, before you run, before you fly.

And you need all these foundational toolkits to be able to do all this. And it's getting to a point at the protocol layer, and I think even at the lightning layer where that tooling. To, to build on top of, to build the [00:47:00] application layers on top of the protocols is hitting a point of maturation where things are gonna get really exciting.

Absolutely. There's lightning

**Rob:** dev kit, right? Yeah. Like, and that's, it's just everything I just said about layer one bitcoin for B d K, there's also L d K for Lightning dev kit, and that's just, it's a massive force multiplier where, um, it allows people to experiment more freely. I think they can take more shots on goal because they don't have to start from scratch every time.

And it's a really, and um, Rodolfo's really big on this. It's like you just wanna have like, like have the gray beards, like a Steve Meyers just like maintaining the core tools and let everyone else go runoff so you're not building everything from scratch. It's a much more scalable approach and I think that's gets really exciting of having empowering more developers to build these applications that can actually service end customers.

And this is something where if three years ago I wanted to try and do this, Like there was initial reference, mini script code floating around. It would've been a huge hassle to try and like write wrappers for all this stuff, but now it just comes outta the box. Yeah. And that's where like, it is, like there's a bit of an inflection point in the developer ecosystem to make this stuff more [00:48:00] accessible, and I expect to see that compound and continue.

**Marty:** Are you saying like, all the developers aren't at

**Rob:** Ethereum anymore? I was actually at Pple lab yesterday and there was a bunch of guys that came over from Solana that are now building a lightning. Really? Yeah, I I was briefly chatting with them. Um, yeah, so apparently they, they, they were really big on Solana for payments and then they discovered lightning and now they're working on a pple lab and like building stuff.

Was

**Marty:** that, was one of those guys on Stacker news this week? Maybe? Um, there was a stacker news post where, uh, some guy was like, Solana, I got completely jaded by it and then found

**Rob:** lightning. And Sounds that, that sounds like I'm, yeah. What,

**Marty:** like what did you draw out of that conversation? Um,

**Rob:** it was very brief in passing, but just this understanding of, um, I think these bear markets where, you know, Bitcoin, you know, gets sick, but then everyone else dies.

Like in the sense that people can get this fleet, like, there's like this fleeting fomo sense of like, I'm building on bleeding [00:49:00] edge technology. And there is something to be said about the reliability of Bitcoin and that there is a foundational base here of real organic transactional value that's being built here.

Um, I think it, I think it's built like, it, it, it's, it's building cathedral brick, brick by brick. Yeah. And the fact that it continues to exist, um, there's definitely things to optimize. We're talking about upgrades before. I know. A p o is very big among the lightning proponents 'cause of ln symmetry and it streamlines a lot of things.

Um, makes lightning more scalable, makes lightning more scalable. It also enables other things, like I think people have found ways to construct, basically drive chains using a P O A P O. Right. Um, and that's just part of the, the value, the trade-off conversation of like the, the features that get added. Um, all this to say it, it's a really exciting time to be building and like, this is my first time in Bitcoin.

So I've been in Bitcoin since, like I mentioned earlier, 2013. This is my first time actually as a full-time career during a bear [00:50:00] market working on it. And I wake up every morning and just like full, just like sprint ahead and like so many things to do and the price is really like secondary, but also you just realize like there's so much to do, there's so much to be building.

Um, and I would encourage anyone who's listening, um, even if you're not super technical, you don't have to start out super technical. Just, um, find something that really interests you and start pushing forward. And that's what I was talking like with, um, Amer, our buddy American Hoddle. Um, I started talking about the manuscript stuff.

He's like, why has no one else done this? And then I was talking to Pete Rizzo, uh, in, uh, Miami, and he looked, he walked up me, I was showing him the demo. He was like, why are you the first one that's like doing all this stuff? I was like, no, there's like the wizard sardine guys. He is like, no, but like, but no one el.

Like why is no one talking about the manuscript and the scripting stuff? I was like, I don't know. He's like, you found an opportunity and started building on it, right? And now people are adding hardware, wild support and all this to say, don't assume that someone else is building what you think should be done.

You [00:51:00] need to get your hands dirty, get in there, scratch your own itch and like find these opportunities. Because now, like Minis Script's a totally fully open source tool. And what I'm really hoping for is, um, the work that, uh, I'm doing and the work that the Wizard Sardine guys are doing and streamlining this adoption.

The next incremental person who wants to build on this stuff. Has so many more things knocked down. Like you're gonna already have five hardware wallets out of the box. Whereas like in December last year, I was flashing custom firmware on my ledger to do any testing, but now it just works. Yeah. So like making it, like pushing these things down so someone else can just stand on my shoulders and do something that's super accessible and easy and making their own applications right, like that's the dream.

And just giving back and brick by brick building that cathedral and, and like, it's a really rewarding experience so far.

**Marty:** Yeah. I mean, you guys are crushing it. Like something like getting like templates standardized across hardware, wallets and Yes. Giving that to people to build on. Yeah. That could be massive.

**Rob:** No, I think it, I think it'd be incredible and providing a, a, a way for people to start suggesting and promoting their own templates and just getting things in there. Um, it's [00:52:00] really. Exciting 'cause like I think that it's just totally been overlooked. This idea of Bitcoin being used as programmable money and all of the great things manuscript does to standardize.

Not on the template side, but like it just abstracts away a lot of problems. Yeah. You don't have to worry about constructing custom witnesses to spend your money. Like it all just works. And that's a really powerful idea that you can draw something on a board, you get a string of text, you can, you can look at it and reason about what you want and you hit a button and it becomes Bitcoin script.

It's like a superpower.

**Marty:** Yeah. And I'm extremely happy that you guys, the Wizard Sardine team are building on this. 'cause it does validate, going back to like we're building cathedrals and. I get impatient with the people who are impatient with the, um, with the speed of development with Bitcoin. That's right.

You guys are validating what has been a long-term thesis for me, which is like, yes, you can go do robust scripting on Ethereum salon or whatever it be, but they're working on structurally on sound foundations. Mm-hmm. Where we're gonna try and do it right over here in Bitcoin. It's gonna take longer, [00:53:00] but the long term effects are gonna be profound in terms of absolutely.

How valuable the network is overall.

**Rob:** Yeah. Um, Andrew had this, uh, Andrew Cher had this point that, um, I. A lot of the things we tease Ethereum about of having this like intractable, complicated programming language actually could be applied to Bitcoin before minis script. 'cause like if you were like, by hand, I'm gonna do this, like, to write a Bitcoin custom contract script by hand is not an easy thing unless you're a wizard or a super testnet and someone who like lives for those little details.

Like, it's not something most people can just do outta the box. And what I call like manuscript is bowling with bumpers. If you, if you, if you, if you use manuscript, you're not gonna throw a gutter ball, you're not gonna have an impossible spend condition with your money. You may lose keys, but you're not gonna have a way where you brick your money the moment it gets deposited.

Mm-hmm. And that's, it solves that problem now. So you can actually, um, think about Bitcoin from more reasonable perspective and you can, you know, we, we, we can now actually laugh at like, oh, you had a bug in your solidity contract. Right. It's like, like, because before, like, it's like, okay, you try and do this custom by hand in Bitcoin, you could easily brick [00:54:00] yourself as well.

So it's really exciting For sure. Yeah. Let's talk edge

**Marty:** cases. Yeah. What I'm thinking, like with absolute time locks mm-hmm. Where you, where you hit like a date in the future. Yeah. What happens if 75% of the hash rate falls on the network and a block isn't produced mm-hmm. On that date? Mm-hmm. Like how does that affect insurance policies or anything like that?

So let's

**Rob:** talk about this. So the way, um, it's BIP one 13 is the, um, method in which it's called the meantime passed. So how the Bitcoin network keeps track of, um, network time is there's, there's a couple conditions. One, your node locally will reject any block that comes in that is further than two hours ahead of your local time on your node.

Right? And this is like an idea of a time warp attack, right? Like minor start colluding. Um, Shout out to Jameson. Lopp has a really great blog post. I tweeted it out a couple weeks ago. I'll have to go find it again. Um, but he, uh, had a really great blog post specifically around timestamps, uh, and how they're being [00:55:00] maintained in the network.

So, um, all this to say, so if you go two hours and forward in the future, your node will reject it. The bitcoin network though, requires that a minor, when they put forward a timestamp into a block header for it to be network valid has to be ahead of the median timestamp of the past 11 blocks. So you can actually look on men pull space and you start clicking through.

You'll see all of a sudden like, oh, this block was found at 7 0 1, and then the next block will be, oh, it was found at 6 59. 'cause time's fuzzy in that sense. And also the timestamp is something the miners will cycle through to get more guesses on like their hashing. Right? Um, so if you were to have miners where like 75% of the network stop.

So was your question, 75% of the hash rate this

**Marty:** blocks. So you have absolute Yeah.

**Rob:** You have a timestamp July 1st.

**Marty:** Yep. 2024. This policy's over. Mm-hmm. June 30th, 75% of the hash rate falls off the network and a block isn't produced for two

**Rob:** days. So that's actually an easier thing to [00:56:00] solve than the, uh, block height equivalent.

Okay. 'cause block height equivalent, if it's like, if let's say it's at block height, a million, you're doing something, it's like you've got 9 9 990 9,950 and the last 50 blocks take a really long time. There's no way around that, but the timestamp can leap forward. Okay. Right. And the timestamp again is integral part of Bitcoin security.

'cause it's, how the difficulty adjustment works is it actually takes that actual clock time and says, okay, you know, 2140 blocks happened. Well, how much time passed? And it uses this like time approximation to understand that, um, fortunately in that edge case, the money's not lost, the security hasn't been violated.

It just may take a longer to move it, to move it, which is definitely a much better, you know, condition. Right. So in that sense, that's why the timestamp point's actually fine. 'cause once enough blocks eek out, you know, you would be able to say, okay, the median time passed now is July 1st, so you can move the money.

Yeah, yeah,

**Marty:** yeah. And even in that case where policy's done [00:57:00] July 1st, a block isn't produced on July 1st. The next one's on July 2nd, you can then move those funds. Yeah. And you're still beholden to block production anyway if you, if you wanna move those funds out, so. Right. You're

**Rob:** still waiting for confirmed transaction anyway.

Yeah. And, and even, and, and, and like a, a crazy edge case like that, it's not like we would be like, well, well, It sucks to be, you wait for your mind. Like we could, uh, we could still sign and go to the higher level branch and still execute a signature for them, right? Mm-hmm. It would be only in a sense where if we went fully adversarial for whatever reason, you would be beholden to waiting for the time blocks to move the, the, the time lock to expire.

And this is a funny thing, like, um, so the, the language we use in Bitcoin from a UX perspective is interesting 'cause it's really not a time lock. Um, it's a time unlock because you don't, um, and the shout out to my, my co-founder Becca, who, uh, a really great asset she has is she did not get into Bitcoin until 2019.

So I'm like, like talking like a mile a minute, like all the things. She's like, that doesn't make sense, like time lock. And she's like, oh, so like after this amount of time you lock this and it's like no longer spent on, I was like, no, a new [00:58:00] path opens up. She's like, so it's a time unlock. Like, yeah, no, you're technically right.

Like, so if you have like, um, you have this like big complicated security layer and then a certain amount of time passes and then it's like you can move the money yourself. It's a time unlock because after a certain amount of time, time unlocks a new way to spend the money. Mm-hmm. But we call it time locks in Bitcoin.

Right? So like, there's like the, all this like language semantic things that like, um, for you're trying to communicate to a wider scale audience. You need to think about like the internal jargon we use versus what is actually something that maybe is more naturally intuitive for a

**Marty:** larger population. Yeah.

Yeah. The alternative like time lock, you're locking it up for time mm-hmm. In the future. So like the lock happens on the front end, right. But you can also flip that and be like, it's a time unlock on the

**Rob:** back end. Like that's exactly it, right? 'cause like this condition is locked until a certain amount of time passes.

But if you're thinking about it sequentially, you're like, okay, oh, so that first layer I no longer can spend from that layer. I was like, no, you can still spend from the first layer. She's like, okay, [00:59:00] well then nothing's getting locked. Then the future spend path is locked until a certain amount of time passes.

Um, and this is 'cause it's like going through like the initial reasoning. This is another UX thing, um, where you have to. Pick what layer you're spending from now. It's not just I spend the money, you need to say, okay, well are you spending from layer 1, 2, 3? 'cause you need to construct your P S B T, um, relative to that.

And so, and if you're using taproot, we were talking about earlier like taproot adoption, um, if you're using, um, the script path and you have like basically all these tap leaves of different ways you can spend the money, it's much better for privacy. 'cause instead of having this massive like script all in one block for a SegWit output that anybody can read, anyone can read you're little untap or you just have a little leaf.

So you just have exactly what you're spending to. But the thing is, is like, let's say you wanna spend from layer one, but then you decide later you're gonna spend from layer two. When you're signing things in taproot, you're committing to that little tap leaf. So you actually need to rekick off the signatures all over again.

Mm-hmm. Right. [01:00:00] Um, so, but this is part of the ux, like you have to say like, okay, how do you plan on spending this money? And we are like normalizing that in the UX flow. I. Um, to streamline it for them to be like, oh, you need device one, two, and three to sign, or if you want to do this layer, you have to wait for this much time to pass and you can sign it now.

But it's like a post-dated check. Yeah, right. But these are all things that were not any other wallet really hasn't had to worry about the UX around before. So that's been a lot of, that has been really doing a great job spearheading that and trying to make it as reasonably approachable and understandable as possible for something that's really complicated to the point where, but we're still empowering users to understand what's going on.

'cause you can just wave your hand and be like, oh, like come back in three weeks or whatever. And it's like, that's not really a, it's your money. It's not really a satisfying answer. So trying to balance that information overload and making sure users have like informed consent and knowledge of how their money's being held.

It's a very tight line to walk in a way where you don't have to have a, a nerd on staff to like reason it for you. Yeah.

**Marty:** Yeah. And that gets into another thing. It's not really an edge case. It's actually just like an inherent, [01:01:00] um, inherent, uh, Thing you have to deal with is the activity, like with minis script, once these things decay or like with your insurance policy, if you wanna re-up it, you do have to move.

Yes. Bitcoin. And is this sort of where the battle between minis script and M P C enters? Because what's the idea with M P C is that instead of having to move to Bitcoin and you could just change out keys. You

**Rob:** could rotate keys. Yeah. So, uh, the infamous, uh, team script versus M P C gang Twitter war. So, uh, Rendell's a good buddy.

So we, uh, I'll, I'll let everyone peek behind the curtain a little bit here. We were, we were mocking everyone, having stock to flow and price, um, fights. So, Him and I decided that we should have a, a, a fight, like an actual Twitter drama fight that was about nerdy things and with the goal that maybe everyone will learn a little bit about Bitcoin along the way.

Um, so, uh, the whole, so it's really interesting with M P C [01:02:00] and like, huge shout out to Jesse Posner. Um, working over at Square, um, working on this for Frost, right? Um, like round optimize, like, like threshold signatures using shore signatures. Um, is this idea that you have a single public key on chain? We're talking about Bitcoin script earlier.

So like, um, multisig, the way it works right now is like you do, um, three public keys device, 1, 2, 3 and then op check multisig, and then you provide your signatures. The way it works for Frost though, is you have one single public key on chain and what that actually is, what you're doing off chain, you have three devices that are coordinating signatures and it all aggregates to that one signature.

And this was a really great app upgrade with Snore. Um, a little context is, Snore signatures were around when Satoshi invented Bitcoin, but they had a patent on them. Mm-hmm. So he had to use E C D S A and when the patent expired, it was right on the time doing taproot, they upgraded and added a new signature mechanism.

So that's why taproot is like four, three different upgrades all rolled up into one. Um, but schnoor signatures make it really easy [01:03:00] mathematically to have security proofs to understand that you're able to aggregate these signatures in a much more streamlined way. So, um, this is a really interesting point with M P C, is that, let's say you, me and Logan again are in a two of three multisig and, um, you finally let cut the ball and chain free from Logan.

Logan runs outta the studio. He's gone forever. Now we have a two of three, right? But, uh, you and I need to move the funds on chain 'cause Logan's public key is sitting on chain. Right? So we need to move the money to a new vault, right? Which is talking about like, if you need to re-up your insurance policy, you need to re-up it too.

Because like the timestamps are hard coded on chain. You need to refresh the timestamps. Um, With N P C though, we would have one aggregated public key of you, me, Logan, and you and I could regenerate a third share and give it to someone else that comes in. Mm-hmm. And we don't have to move the money on chain.

And like, uh, I think someone who's been putting a lot of thought into this, and I think is thinking about it the right way, is Alex Leishman at River is this concept of, from an enterprise use case, you have people who want to know [01:04:00] that if I generate a deposit address and 10 years goes by, I can still put money into that address and I don't have to worry about like, oh, that address is bricked.

Yeah. Prime Trust ran into this problem. Exactly. Allegedly Prime Trust ran into this problem. Uh, so the idea though is that you can have, uh, an enterprise like Key and you can have these shards and you can over time rotate out the shards and you're able to actually transfer custody without having to actually move funds on chain.

And that's a really interesting, scalable approach too. Um, it gets really interesting for like, is that, does that make.

**Marty:** UT X is equivalent to like r stones at a certain, in a certain

**Rob:** way. Yeah. Yeah. 'cause you're able to move everything off chain, right? Yeah. So you can have company treasuries that actually rotate out custody without ever having to do an on chain transaction.

Yeah. Now there are, um, there are things you need to consider, right? This isn't a silver bullet. You need to worry about non generation. Um, so basically, um, an no is a number only used once. And the way this works in traditional Bitcoin today is there's a deterministic non scheme. So if you have a transaction, you know, you'll get the same no [01:05:00] every time.

And that's all of the harder wallets. You know, implement this to make sure that you're not, uh, gonna flick on yourself. Um, the problem is if you use a number, The S is not only used once, it's used multiple times, you can actually reverse infer the private key. Mm-hmm. So you degrade the security of you actually ruin the security.

Right? Like, so like if, if, if I get you to sign once, I'm like, oh, you know what? Oh, that, that, I didn't mean to sign that, sign this instead. And you use the same private key and you use the SS again, but you're signing to a different transaction. I can reverse engineer what your private key is. It's basically a math equation.

I can say like you, you hold things constant and you like, you know, equation, you cross out both sides, you get the private key. Um, so nons coordination is a really important element, um, when you're using M P C and additionally in this, like you and me, Logan example, like you and I need to destroy our old share because, um, you what in theory what would happen is, is like Logan could come back and be like, oh, hey Marty, you have your old share story.

Hey, let's take the money and run. Yeah. Right? Yeah. So like you have to make sure you're securely deleting your old share and you [01:06:00] have to make sure that you're not reusing nonsense. And

**Marty:** that's a big problem. 'cause how do you verify that you actually deleted

**Rob:** it? Yep, exactly. It, it becomes a complicated thing in that sense.

Um, From like, how do you prove a negative? Like how do you prove you deleted something? Um, so these are the things I think. What was the, was it Nick uh, working on the, that Frost Hardware wallet? I saw this on Twitter the other day. Nickla? Uh, yeah, ler was it? Yeah. Yeah. He was working on this like, it was like really cool, uh, like it almost looked like raspberry pie zero, but like you can click a bunch of things together and start generating shares.

Like people are gonna just like, uh, people are now starting to explore what, what this design space looks like. And that gets really exciting. Um, over time. Huge shout out to Bitcoin ec actually. Um, another version of uh, M P C is music. Music Two. So Frost is interesting 'cause it's a threshold, right? So it's a N of M Musig.

Um, it's just N of N, right? You have to have everyone present. Um, but Bitco did a field report, um, Brandon Cole, I think is his name. Uh, rearing code on Twitter. He did a field [01:07:00] report for Bitcoin opex latest newsletter where they were leveraging snore. And M P C for Musig too. For the Bitco product. So it was customer key plus Bitco key only looks like a single sig on chain.

And this is where it gets really cool too, is that when you're using M P C, it only looks like a single sig. You don't know that it's multiple signers. 'cause that's all done off chain. You do. And that's, that's, that's the trade off is you do this all off chain so it's smaller, more discreet, more private, but you have to then offload a bunch of things that you would do on chain, off chain.

Mm-hmm. And that's where the nons coordination and the shared generation, everything kind of comes into play. What they did though at uh, at Bitco is they worked with Sonke over at Blockstream Research and they were actually modifying, adding proprietary fields into the ps bts to do this, like this non generation handoff.

So they were just using ps, bts and actually using music too within the Bitco client. So that gets really interesting that people are starting to like, think of like fun ways to hack into A P S B T, the nons coordination. 'cause now you can actually just take the same standard payload of A P S B T, it has some extra data in there [01:08:00] and you can start doing the secure signing and everything.

And it makes it much more scalable and adoptable to have people leveraging

**Marty:** these tools. And you have that nons validation that the S generation is done the right way. Yeah. That would be

**Rob:** have degrade your security. Exactly. That would be, I think those, those tools are yet to be fully seen and fleshed out.

But that would be the idea that you could use the P S B T and you can kind of check and be like, Hey, have I looked at this nonsense before? Oh no I haven't. Cool. So now your software wallet becomes more important. 'cause maybe it's doing extra checks to make sure you have, you're not reusing nonsense.

And it was really cool, uh, what Bitco ISS doing is actually like the idea of the actual platonic ideal of the, the silly, uh, the very serious, very, very serious debate between team script and, uh, N P C game. If, uh, what they're doing is they, um, so Taproot has a key path and a script path. In ways you can spend the money.

So the key path is a single pub public key, but it's a musig aggregated key. So that is bit go plus the customer and it looks like a single sig In the event. One of those keys goes missing though. They have the script path and they have a [01:09:00] Merkel route and they have a Merkel tree with the tap leaves. And then your backups are, uh, the backup key plus bco or the backup key plus the customer if, if either BCO or the customer go missing.

And it's all contained in a single address. And that gets really interesting that you can have your default happy path. Maybe that just looks like a single sig and then in the event you need to go down some sort of contingency branch, it's all in there. And you're able to use both script, more advanced scripting conditions and M P C to aggregate all of these things down.

Um, it gets really exciting. And then leveraging PSB Ts to make it more interoperable, I think it makes it a lower threshold for say, hardware while it's start supporting this as well. Mm-hmm. Right. Because it's in a standard form factor, everyone can, you know, expect and understand to

**Marty:** use. Yeah. And so outside of the problems that could arise with the non generation mm-hmm.

Not being done correctly, but it seems like this P S P T hack that KO's working on could prevent that. Yeah. Why does N P C get a bad rap? Um, obviously fire blocks is leveraging it. Mm-hmm. [01:10:00] Is that implementation of N P C, um, which secures Bitcoin keys and shit, coining keys, would that be different than this M P C implementation you're describing?

**Rob:** Yes. That's a great observation. So M P C, um, it gets a bad rap, I think. Rightfully so. 'cause E C D S A M P C is a mess. Absolute mess. Mm-hmm. Um, there was actually just, um, like, you know, there was a bunch of like hacker conferences and a bunch of these implementations were actually broken. E C D S

**Marty:** A is, uh, yeah.

E C D S A. Like you just mentioned, like recent months, like there's some

**Rob:** vulnerabilities, there's been a bunch of breaks. Yeah, there's been a bunch of breaks in eec, ds a MPCs and the difference. And so one there, it gets a bad rap because it's from a custodian standpoint, like your fire blocks, they wanna have one security solution that can secure your Cardona, your Bitcoin, your like coin, your Dogecoin and everything, right?

Since it all uses E C D S A, it's a wrapper that can just do everything, right? So they use that from a streamlining user experience. I would say at the threat of, of security, right? Bitcoin [01:11:00] script natively has the ability to do things like multisig, that things like E and other coins do not. So what they're able to do with M P C is provided multisig like experience by using multi-party computing M P C and extra cryptography to unify the user experience.

And it's strictly worse from a security trade off perspective. Um, The difference here is leveraging taproot and snore signatures has a much cleaner mathematical way of actually aggregating these keys and doing this distribution. Like you said, there's, there's still the next-generation problem. They're still making sure if you're rotating out stakeholders, you're securely deleting old shares, but mathematically it's much cleaner.

And that's kind of like the really big thing is that, um, all of the very cynically people using E C D S A M P C just to kind of like hack in multisig to all these other coins at the risk of the security of the actual like system. Um, less fund loss this year, right? Yeah. Oh yeah. It's, it's a [01:12:00] real, it's a real serious problem.

And that's where like schwar signatures provide a better way of being able to offer this security. Um, and it'll still take time. There needs to be more tooling. I was actually talking to, Uh, Jesse Posner, uh, who's been working on Frost for a while. The next step level will be really cool, um, is getting a security proof that can actually wrap music and frost so you can have it.

Let's say us, you, me and Logan have a, a single sig as a MPC is a two of three. And then let's say there's another company that has a two of three, and then you have two R signature and their signature aggregated, and then Musig toing it. So it just looks like a single key so you can start collapsing everything that look like a single sig.

The security proof hasn't been done yet to show, um, Jesse was confident that it should be doable. But if you start bundling in these different M P C approaches, you can just make every single signature look like a single sig. A single sig. And what's cool is that you can actually use like tap scripts and like, have like different conditions and you only reveal the condition that you're gonna use [01:13:00] that makes it look like a single sig at the end of the day.

And that's where it gets like really exciting is just aggregating all these signatures, which is a better scaling solution because you're com taking up less space on chain. Um, it's more private. It's way more private. Um, you're not able to directly reason about like how this money's being secured. And then you're also gonna do all this like off chain custody swapping too, right?

Yeah. Like and this is like the next frontier and this, these are all things that don't require a fork. Like going back to like all of these tools are just out there. Yeah. And it just takes people to have the ambition to start like building on top of it. Well, that's what

**Marty:** like our last conversation in Nashville mm-hmm.

Really got me thinking. And then I sat down with Alex Thorn, he was asking me about like a P O C T V. Mm-hmm. Off vault drive chains. And I think you convinced me it's like, let's just play around with this and see how far we can go with minis script, frost music, whatever. Then if we get to the edges and we need more mm-hmm.

Then let's have those conversations. I think a p o in my mind, 'cause I do think lightning needs to be more scalable. Like in my mind, my list of priorities for all. [01:14:00] These up upgrades, that's number one. Mm-hmm. Because I do think if we can unlock scalability at the lightning layer, it's gonna be massive for adoption and usability.

Um, but when it comes to like robust scripting and vaults and covenants and all that, like, I think we should just play around with all this stuff you're describing

**Rob:** first. Totally. Yeah. And that's, um, and that's why I, I, I work in the field in which I have agency to affect change, right? Like, I don't wanna be defeatist if, if even I think like OB Vault is a great idea and it would actually be really complimentary to we're building an anchor watch.

I'm able to provide better security assurances and it's just better security from a reactive standpoint. Um, I have to work within things. I have the agency to change. And, and minis script is something that I can do, and I don't have to ask for permission, right? So I can just build the tools, I can build the user experiences.

I can provide a better service without being gated by things that are outside my power. And that's, and, and so that's, I, I, I try not to take a defeatist take on it, but it's just working within what I have the means to actually control. And, and then I can be laser focused on that. [01:15:00] Um, yeah. And that's, that's how I've been trying to track it and think of it and just building what I can and, uh, thinking about these hard problems and empowering users to leverage Bitcoin in interesting ways that don't require a fork.

And if those four conversations come, I'll review it when like, the code is ready to go and there's like a bibe client, and like when it's ready to actually start, like talking, um, actual details, activation and activation, everything. Yeah. Like, I won't be passive, but, um, until we, until someone puts forward those kind of things, I, I can't, I can't invest myself into it.

Yeah. Things will, things will

**Marty:** change like beyond that too, like I think, um, There's a bit of scar tissue from the taproot upgrade, particularly like with Ordinals. I think there was some unforeseen consequences of the combination of taproot and SegWit Yep. That led to ordinals that mm-hmm. Many people think is wasting space on chain.

Like I saw somebody say like, they're, they're, um, [01:16:00] their storage on their node ballooned from like 5.2 to 7.3 gigabytes this summer for the U T X O

**Rob:** set. Yeah. Yeah. No, it's, um, it's a, I can understand that people are reserved about making changes to Bitcoin because there's always on, you have just, like, you can't prove a negative, like you deleted, you can't prove the unknown unknowns.

Yeah. Right. So there's always gonna be an unknown unknown with any change that happens to Bitcoin. And as Bitcoin grows and. You get more sensitive to like what are the things that could structurally change? It's actually purely like happenstance that a p o wasn't already part of the sig hash flags.

Like there's usually an alternative universe where like almost everything's identical and Satoshi also added sig hash none, right? For a p o. Um, and you know, like there's like kind of this just echoes of like how Bitcoin and everything develops from them. The other option is you can actually, and you can do um, a Lightning network symmetry if you had C T V plus check sick from Stack and check Sick from Stack is an op code that's actually live in liquid network.

So there's [01:17:00] actually working written code. But like this is where now people start going into fights of, well I don't want a p o 'cause it gonna enable drive chain, so let's do it this way. And then like, it's like really, it gets really contentious and then it like, it becomes like a political lobbying thing.

'cause everyone wants their upgrade in, um, I am humble enough to understand Bitcoin to a place where I, I know more than most, but I do not fully understand the implications of these deep protocol level changes. That is something that is like, I will have an opinion when those times, when the times come, but like, I can't pretend that I have perfect knowledge of all this stuff that, you know, maybe 10 people in the world do.

Yeah.

**Marty:** And that's, I mean, from my perspective too, like whether it's on this show or rabbit hole recap, I mean leading up to taproot, like we were big cheerleaders and I think for good reason, I think tap route's a net positive, but totally did not understand the unknown unknowns. And I think the lesson I've taken from that is like, maybe I'm just more reserved in what I'm actually like championing.

Mm-hmm. From my perspective, because. [01:18:00] I can't fucking audit the code. Yeah. I don't know these edge cases. I can't do the cryptography. Mm-hmm. Like I do not know like what is good enough. Yeah. And going back to the point, like I think we should experiment with minis script, frost music, push that as far as we can.

Yeah. And then if we need more like, all right, let's have the conversation then.

**Rob:** Frost music was only possible because of Taproot was shore signatures, right? Yeah. And like the more, and using script lead and using tap leaves is another taproot upgrade. Like that idea of like, you have many, many spend conditions nested within one single address.

So like we did get a lot of value on lock and I'm ultimately of the position, um, it's funny, a lot of people think I'm like super pro ordinals. 'cause I did the, what Bitcoin did, like the week after, like I met, I got to meet Casey at Bitcoin Park. I think he's a really great guy. Like I'm of a level of agnosticism of like, Bitcoin is a permissionless system and like if people put in JPEGs really breaks your conception of how Bitcoin will ever survive as global money, then like I don't, I.

I think that's a serious position. Like people are just gonna do whatever they want to on chain. This is [01:19:00] echoes of what was happening with counterparty. Yeah. Like it's just gonna happen. And like I do think from a narrative perspective, it did change the perspective and how people maybe outside the core community you and I roll in of viewing Bitcoin as this asset to like put other protocols in chains like these BRC twenties and like not using Bitcoin as sound money, but as this like the network model of Bitcoin as a network and distributing things.

And ultimately like, it makes transactions more expensive and I think the miners are all happy that they're getting economic activities. So like you have to just kind of like live with like the, the, the terms and just move on.

**Marty:** Well that was like a short, like hash price right now is 6 cents. Mm-hmm. Um, fee revenue is nowhere near where it was in May,

**Rob:** April.

I'm checking the block lock men pulls are not clearing

**Marty:** again. Men pulls are not clearing. And then you have the chain state bloating by two

**Rob:** gigabytes over the summer. Yeah. The U T X O set and that's, yeah. Um, It's, uh, like, it's definitely not ideal. I would, you know, I think the, the bigger culprit, [01:20:00] I mean, removing the script size limit is something that definitely, it's shocking that someone didn't look through that and realize, wait a second, we're removing the script size limit.

So what does that mean for arbitrary data? All, all that said, like, it, I, I think it just ultimately, like Bitcoin, I think, I think Bitcoin's able to transcend and move beyond this. Like, I, I agree as well. Like, and like, like I get it, like it's, it's suboptimal, um, agree for how people view it, but it's not the end of the world.

No, not

**Marty:** this time around. But like, that's my thinking is like, all right, dodge the bullets. Yeah. Something like we, we keep doing these soft forks and upgrades and these unknown unknowns present themselves mm-hmm. Compound, um, this type of activity. Like that's, I guess that's where my thinking is coming from now.

It's like, all right, I sort of adopting like a Steve Barber. Maybe we should ossify because mm-hmm. Do we fuck ourselves up by doing this many times in the future? Like maybe we [01:21:00] can get away with it this time, but how many times can we get away with it before it degrades the ability to sufficiently distribute the

**Rob:** network?

I, I got this mental model from Jamon LOP of the idea that like, ossification is a natural end state. It's not a declared goal now. Like if Bitcoin were to never upgrade again, I'm, I live my life and I make assumptions and decisions for myself and anchor watch as a company. On that Bitcoin will not upgrade again.

That is my default state assumption. Ossification is here. That's, and that's just as a, as a pragmatic default in how I can kind of like, plan and strategize over my life. Right. I don't think that's necessarily, like I, I, I'd love op vault, like, like I'd love just a very simple, just like claw back ability.

Like if I have money sitting on chain, being able to like, have some means of being able to pull money back. Um, I know Upul and the latest upgrades looks closer to just a generalized C T V. Now, to my understanding, I haven't looked at the code myself, but, um, if I don't get that stuff, I will still be here working on Bitcoin and building things.

Right? Like it's not gonna be the [01:22:00] end of the world for me. So I dunno that that's how I try to view it.

**Marty:** Yeah. Yeah. These are heavy subjects though. Like, it does it weigh on. I mean, it, I'm sure it weighs, like it weighs, it's weighed on me, um, from the perspective of like, we have this platform, we're trying to educate people about Bitcoin.

With the taproot activation, maybe obviously did not know the full ramifications. Mm-hmm. With that, no. Um, script removing the script size, removing the script size, I cannot foresee that. So I'm trying to humble myself and be like, I, I, it's above

**Rob:** my pay grade. Yeah. Yeah. And I, I think, I think that that's the responsible take.

I also take too, like I said before, like there's certain things I just not understand the deep level pieces of it. Um, but I try not to still be, I still try to, as a good steward and participant in the Bitcoin ecosystem, try to understand this stuff so I can have some level of opinion. Because at some point a four client will come and it'll be, will you run [01:23:00] it or will you not run it?

Or will you run an actual rejection of it? Right. Will you like force a fork? Right. And you have to have some baseline level of understanding. 'cause you have to run a node, you've already opted into the game 'cause you have a node, so you have to make a decision. And not doing anything is a decision.

Mm-hmm. So, yeah. Uh, I mean, I'm. I'm still long-term bullish on Bitcoin. It's great to be here in Texas. I got to come to the Commons. I wore my un unchanged shirt today. All of my, uh, bantering about, uh, Bitcoin Park versus the Commons. I wanted to wear friendly colors, even with my little blue check pin here to, uh, make sure that I come in peace.

You

**Marty:** started some shit with that chart.

**Rob:** I know. Listen, it, it, I've had some really good breakfast tacos here. They're not as good as Lady Bird out in Nashville. Ah, they're gonna

**Marty:** start some shit. Austin inspired Lady Bird

**Rob:** tacos. Yes, they are. No, yeah. Um, I'm a proud member of Bitcoin Park. Um, I have to do my proper ribbing of the commons while I'm here.

I'm a member of Bitcoin Park too. Yeah, no, it's, it's a magical spot, man. It's, uh, I've been there six [01:24:00] times this year. Um, every month having someone, a different crew, people rolling in, getting to see different people. Me shamelessly harassing poor Steve Meyers about whatever latest bug I'm having in Bitcoin desk kit, because like a local help desk support.

Um, And great people. Yeah, it's been, it's, it's incredible spot. And I, I do love Austin. I mean I've been here the five times, well, four times probably in the past year. I was here for bitcoin plus, plus I was here for the south by Southwest takeover last year. Bit boom, last year, bit bit Bob boom this year.

Um, it's a great town and like I gotta swing by Pple lab, like people are building and people are working and um, you wouldn't even know it's a bear market man. Everyone's just heads down, grinding along and uh, it's a great time to be grinding along and building in that cathedral. Agreed.

**Marty:** And I wanna be clear, I'm still extremely bullish on Bitcoin too.

Um, I didn't want the conversation about os ossification to come off. Like I'm worried about the long term survivability of Bitcoin. I'm not. Um, but I do think [01:25:00] conversations like this are important to like Absolutely. Um, 'cause as the years go on, we're approaching 15 year anniversary of the white paper and eventually the protocol going live and more and more people are adopting it like the.

The, literally the value at stake is increasing. Mm-hmm. And these decisions come with way more weight. Like and Yeah. Which is also weird, like at the bitcoin core level, like people are a bit dejected and then mm-hmm. Burn. I've been seeing that. Yeah. So it's like, how do you weigh all these things?

**Rob:** Yeah. Um, it's this idea, I think like developers want to build things and see their things.

Like they want like to be motivated. Like, um, it's, it's the equivalent of like, in the sense of building the cathedral, do you wanna be building one of like the pirouettes, like, like one of like the towers? Or do you wanna be mopping the floor? Right. Yeah. Because like there's a lot of grunt work that needs to be done of just doing pull request review and writing unit tests, right?

Like things that aren't sex or [01:26:00] glamorous or aren't changes of Bitcoin. And you have to bring people in to want to like, help maintain that cathedral. And I think a. There's been a natural kind of model of patronage where people are like, hire developers that work on Bitcoin full-time. Right. I think that's a, and like you have Open SATs, you have spiral grants, you have the H R F grants.

Like there's a lot of things that are, like, there's a natural ecosystem that develops around it to help try and provide that maintenance. Um, and just trying to make sure everyone feels happy and motivated and they feel valued. Right. Yeah. I think that's another thing too. Just make, and like, um, you don't have to do anything special, but just like, like under gratitude and appreciation for the people that are just kind of like doing the grunt work that is not fun or glamorous at all.

**Marty:** Yeah. Let's give a shout out to Russy and Osky for all the hard. Unglamorous work he's done to separate the wallet in the node. Oh,

**Rob:** that's a huge undertaking. That massive, massive shout out for that. Absolutely. But that thing is like a, it's like trying to separate conjoined twins. Yeah. He's been working on it for like

**Marty:** seven years.

Right.

**Rob:** Yeah. And that's [01:27:00] a, it's one of those things that is just slow and study, but that's a really important thing for, because like we run multiple notes, like what we're building and like just, if I could just have the node and not have to worry about the wallet architecture, you can run, wallet, disable whatever too.

But like it's just housekeeping and infrastructure. Yeah.

**Marty:** Yeah. Um, beyond all these protocol developments and application developments, what are your thoughts on like Bitcoin as it stands in the overarching macroeconomic landscape right now? Like, do you think there's headwinds or tailwinds for Bitcoin?

**Rob:** Um, so this would be like putting on my macro think boy hat. Um, you're a good think boy. I'm, I'm a good think boy. I, I try to stay in my lane of like the nerdy think boy as opposed to the, the macro think, boy, I guess my, my take would be that, um, Interest rates are continuing to rise, which is probably the largest macro factor on, uh, risk assets at large.

If you put Bitcoin in that risk asset bucket, I would say, um, it's been fascinating watching the, like the housing market still not [01:28:00] capitulate on price, even though like someone who's like looking to buy a house and it's like 30 year mortgage rates are, you know, 7% and the prices haven't moved 'cause it's like no bid.

Yeah. Everyone's like has Airbnbs and they're renting things out or their people rent and or there's no actual liquidity. Right. It's like the market's like, just like Frozen and Austin here, it's like even worse. I can imagine. Um, but it's not sustainable. You, you've, uh, as the debt has to get rolled over.

Um, I was listening to, uh, Preston Fish's latest podcast and they were talking about like a lot of companies, like just locked in corporate debt, like five, 10 year corporate debt. At like 2% interest rate. Like, like one was like at the bottom. So even though rates have jumped, there's a huge lag on people that are looking to buy a house.

Mm-hmm. Right? Because if, like, if you're not moving the, the 30 year mortgage interest rate being 7% doesn't impact you. Right. And if you're, if you're Apple and you refinanced billions of dollars of debt at 2% interest, you're not affected. You're not really, you're not affected yet. Right. It's [01:29:00] when this stuff has to start rolling over.

And the people who've mismanaged this the most is the government. The government debt has been massively, like, they should have been raking, like doing mass refis when we're, when the covid slumps and like, you know, everyone's flooding to us dollars and demanding it. But shockingly, the US government mismanaged, shocking, shocking breaking news.

So like, I think you're gonna have natural pressures. Um, we have just as a more people are retiring, people are trying to like check out, um, live off their retirement savings. You're gonna have, um, I think overall the piper's gonna start getting, get paid when it comes to all of the entitlement spending.

The government has to keep on printing. Like we're just printing another $2 trillion or something this year. Mm-hmm. It's just like, oh, there's just another 2 trillion. Right. Yeah. Like things that were as deficit, not spending just deficit more than what we're actually collecting in taxpayer. And I think inevitably you're gonna have to, it's basically a game of chicken.

And while they can run [01:30:00] rates for a while longer and higher, short of insolvency and massive printing, they're gonna have to drop it. And that's where kind of like an opportunity where the release valve blows up in Bitcoin, you know, runs off to the

**Marty:** moon. Yeah, yeah, yeah. The rollover thing is something that most people are not prepared for.

No. Like the interest payments on the debt alone at some point next year are gonna balloon like above 1.5 trillion. Right.

**Rob:** And they're not gonna have the will in Congress to raise taxes to do it. And they're also not gonna It's election season. Yeah, it's election season. And they're not gonna have the will to reduce benefit payments.

Right. Yeah. Like, like, um, this is like one of the things that Trump did, um, that was polarizing at the time from political pundits, but from a political posturing was genius. Was just like, I'm not even gonna touch the third rail of like, entitlement spending. And that's where you have people like Paul Ryan who just kinda like flopped because it's like, shut up nerd.

No one wants to talk about reforming any of this stuff. We just wanna keep on living in the party. Well, that's what like,

**Marty:** People really don't [01:31:00] understand is yes, we're at $33 trillion in debt, but if you add in the entitlements, it's like 250 trillion. Yes.

**Rob:** It's, yeah. Quarter of a quadrillion dollars.

Unfunded liabilities. 'cause these things are commitments we've made to the American taxpayer, and the money has to come from somewhere. Yeah. And then the, this is where like there's a natural forcing function where eventually you're gonna have to have that devaluation of the dollar. Yeah. And you're gonna wanna be holding onto things that aren't dollars.

And that's where like, and that's where like the short to medium term, I try not to have any strong opinion on price action one way or another. Um, but the inevitable long-term outcome is a devaluing of the dollar. Yeah. It's the only way through there. Unless, uh, well, especially now that LK 99 turns out to be a, a hoax.

But I mean, genuinely like some sort of like room temp temperatures, like sup, like superconductors, like some sort of crazy step function in tech that like, like all of a sudden we have like, Orders of magnitude and gained productivity short of some sort of miracle Rabbit outta a hat like that. You're gonna have to devalue the dollar.

Like there's no way out of this. [01:32:00]

**Marty:** I guess you're not, you're not picking up what Spencer Schiff's putting down these days. What is,

**Rob:** what has he been talking about? Like mass

**Marty:** evaluation? Like, we're not gonna need money

**Rob:** anymore. Everything's Oh, ai, yeah. Oh, because large language models. Yeah. So I previously was a, I was a data scientist at I B M before, uh, started anchor watch.

And like, and I only say this to say that, um, the step functions and there is a compounding effect of like how much better it's getting. It's still massively oversold in the scope of what it's able to do. It's able to do narrow domains very deeply, but it's not gonna be massively disrupting every single capacity of everything.

And we live in a post abundance space, communism. Everyone has everything they ever want, like world, like it's still not gonna happen. Like there's still physical constraints in the real world that govern us all. Like, you still need oil, you still need energy. Like those things aren't going away. Yeah. You need energy to run the ai.

**Marty:** That's right. It's, I think that's something that people really don't understand intuitively.

**Rob:** I think that's gonna be really interesting. The idea of, um, data centers from competing [01:33:00] against hash rate versus, um, ai Yeah. Like, like actual training, crunching a models. Yeah. I think, um,

**Marty:** I mean, shout to Cruso, they were ahead of the game.

Mm-hmm. Many people were knocking them years ago for doing co-located ASIC mining and, uh, H pc mm-hmm. Seemed to be a very smart play on their part. And I think, I mean, from a minor's perspective, like it, it does make sense to diversify revenues. Mm-hmm. Um, to, um, right. Um, to areas outside of, uh, block production.

**Rob:** I imagine also because like everything's short of the last mile. And in this case, I mean, like literally the thing you plug into the wall is identical infrastructure. It's your, it's electrons at the end of the day, no matter what you have to worry about, probably like stability if you're doing like off-grid mining.

Yeah. And like you don't have internet, so you can't,

**Marty:** like uptime's more of a, a. Like a very high priority for AI versus Bitcoin, which is not as high of a priority. Right? You can be disrupted and not fuck up the Bitcoin network, but totally. When it comes to these models, you could fuck them

**Rob:** up. [01:34:00] Um, oh yeah, data reliability too.

Like, just like submitting your work shares is a much more straightforward thing compared to the two way in. Like you get a block template and you just start doing the mining versus like, this is the specific query and here are the parameters. Like it's a much heavier like data infrastructure you have to manage too.

And then you have to do all that network routing internally and all that stuff. Yeah, no, I could, I could see, while it's nice, there are that last mile of differences, a lot of operational differences

**Marty:** for sure. Yeah. Yeah. Um, so with this, all this in mind mm-hmm. Wrap up with this, like, do you feel urgency to build what you're building to get these tools into people's hands so that they're ready for a massive devaluation or, um, Uh, maybe even before that devaluation comes on the dollar side, Bitcoin's just better and people begin opting into it and yeah.

Manufacture a soft landing.

**Rob:** I mean, in the sense of like, the sense of like urgently trying to build the arc. Yeah. Right. Um, it's a very strong [01:35:00] motivating force. Uh, it's very, you know, from a sense of giving yourself a sense of purpose, it's very rewarding and very high charge to give you the endurance to push through because it's not like, it's been a lot of work to get this far and there's still a lot of work to do.

And if you're not doing what you love, and this is just like from what I'm doing, but as a journal concept, if you're not doing what you love, you're gonna have this inertia and friction that starts to compound and you're gonna start getting demoralized. But it takes a very strong conviction and high.

Passion to charge through that and push through the friction and that kind of sense of urgency is part of what, at least for me personally, is a motivating force of building better tools to make Bitcoin better money so that when the time comes, we're able to get more people on the life raft and like things like, you know, minis script on the tech side, um, and being able to enable this more advanced custody solutions.

Um, being able to have an insurance [01:36:00] financial wrap so you're able to actually have, um, you know, better confidence so that you have custodians and stakeholders who are holding money for third party or exhibiting better behaviors to protect customers. Right. Um, those are all things that are really motivating for me.

Yeah.

**Marty:** Yeah. Well, thank you

**Rob:** for doing what you do. Thank you. Thank you for doing what you do. You know, longtime listener, first time caller. You know, I've been, I've been listening

**Marty:** for, I can't believe it took us this long. We wanted to do it earlier this year, but it was gonna be remote and I was like, you know what, let's wait till

**Rob:** we're in person.

Yeah, no, absolutely. I, I've, uh, I've been listening to T F T C probably near the start, not like right at the start. I remember one of the early rabbit hole where recaps was like finally something I could start listening to. Right. But, uh, 'cause that, that's why I was like more active on Twitter, like starting to get more into the Bitcoin culture and seeing for sure.

Um, but yeah, that's, uh, great. And you're also a New York City bit devs alum, right? Yes. Yeah,

**Marty:** that's, I started going in January, 2015 right after, uh, The Hong Kong

**Rob:** agreement. I was December, [01:37:00] 2013, I went, I went through my old meetup emails. It was Socratic Meetup 13. Yeah, they're like a hundred and whatever it is now.

Oh,

**Marty:** I think 200 is actually coming up next

**Rob:** week. No kidding. This upcoming week. I'd love to go back. Shout out to the crew there.

**Marty:** Yeah. Shout out to Jay Max. Um, incredible guys. Yeah. Yeah. No, I moved to New York in September, 2014. My first bit devs was January, 2015. And I'll never forget, I have my notes too, in my journal.

Um, like Ruski was actually explaining SegWit for the first time to people. Wow. Um, I have it in my notes, like how seg works, like what is this thing? And, um, Yeah, it was pretty cool that that was my

**Rob:** first bit devs. I was at a bit the bit devs where Vitalik came through before Eef launched. Oh really? And he did a whole presentation on Eef.

Oh wow. Yeah. What was that like? It was really interesting 'cause he had a whole posse of like a dozen guys rolling with him because people would, every bit dev someone would do a presentation on something and I [01:38:00] had seen some conversation around e and Vitalik showed up and he had like a dozen guys with him.

It was like a whole crew that rolled, which was very different compared to other people. Like I'm a solo engineer working on a project. Right. Um, so that was interesting for sure. Um, but yeah, that, that's, that's really was like jumping in the deep end. 'cause I did not know anything about Bitcoin. I walked in there doing poll requests of c plus plus and I was like, I knew walking in that's really orange peeled me.

It was like walking in, I'm like, there's a lot of very, very smart people here. Mm-hmm. Working on a really hard problem and I don't understand anything that's going on here. And that call to adventure was really what pulled me in.

**Marty:** Yeah. No, I think New York bit devs for me allowed. Me to start this podcast in the newsletter.

I started going two years before any of this started. Mm-hmm. Like you, I've gone in there, I was like, I have no idea what these guys are talking about, but I know they're smart as shit. I, we got that gut feeling that they know what they're talking about. And over the years I'd show up and be osmosis.

**Rob:** It is osmosis.

**Marty:** So true. Slowly [01:39:00] but surely began to like get a better understanding. Again, nowhere near uh, the ability or capability to actually fully understand what's going on. But I think I do have a, a better grasp of how everything sort of interacts with each other from going Yes. To these bit thats meetups over the years for the last

**Rob:** eight years.

Mm-hmm. And you often get a lot 'cause people start debating and fighting in front like, like disagreeing. And then you're like, okay, now I get to see both sides of an argument. And you start to like piece these things as little like. You know, like puzzle pieces to get your fuller understanding. It's definitely, um, if you have a bit devs in your city and you wanna learn more, can't recommend it highly enough.

Yeah. I mean, it's the most

**Marty:** high leverage thing you can do to Yes. Understand this stuff that hopefully most people don't need to understand. But if you wanna be able to talk about it,

**Rob:** if you wanna jump in the deep end, you can. There's the Olympic pool for you. Yeah, absolutely. Well, Rob, it's great to have you in Austin.

It's great to be here. It's a good place to visit.

**Marty:** I'm pumped we were finally able to do this. I'm sure this won't be the last time. Absolutely not. Yeah. What, uh, [01:40:00] what's your parting note for the freaks

**Rob:** build the future you wanna see in the world?

**Marty:** It's a good parting note. Peace and love freaks.