Laura Shin:

My guest today is Jeremy Welch, founder and CEO of Casa. Welcome, Jeremy.

Jeremy Welch:

Thanks for having me, Laura.

Laura Shin:

Let's start with the basics. What is Casa and what products and services does it offer?

Jeremy Welch:

Sure. Casa, we describe it a couple different ways, but current one is Casa is the best personal key system on the planet. That's a somewhat technical description, and you know we view that we're headed towards this world where a lot of wealth and data is going to be managed and controlled by private keys, public and private keys, by cryptography, and so what our system does is it enables you to manage those keys easily, and then we're building easier ways to manage all of this new data. That starts with Bitcoin and that starts with other cryptocurrencies, but we will get to other things.

A less technical description would be that we're building a kind of sovereignty as a service. We are trying to build more independent systems, and if you want to live a life that is more independent of some of the big data companies that gives you more control of your data of your wealth, then we will give you flat fee options on how to do that.

Laura Shin:

And let's talk about just high-level overview your main products, what are those?

Jeremy Welch:

Sure. So, the direct products that we have today, we have the Casa Node, which runs Bitcoin and Lightning, and we have Key Master, which is the key management application. The key management application today is running 3-of-5 multisig primarily, so it's a 10 thousand dollar a year service and software package, and we help our users manage a multisig scheme that's 3-of-5. There are five total keys. You have to have three of those keys in order to make a transaction, and the user controls the majority or the client controls the majority of those keys, so the client controls a total of four, we use Casa to hold one key, and that key is used as an emergency recovery, then we assist the client if they ever have an issue, if they ever have a technical issue, or they've lost a key, we can assist them in getting their keyset back up to speed, but again, this is targeted at these, what we call premium HODLers, people that have a lot of cryptocurrency, 500 thousand dollars or a million dollars plus, and they want an easy way to manage that themselves instead of storing it on an exchange or an outside provider, they want to self-custody app.

The Casa Node itself is a Bitcoin and Lightning Node, and that enables you to route and send the payments yourself based on your local device.

Laura Shin:

All right, so before we dive into the details on those products, let's fill in your backstory. **How did you come to found Casa?**

Jeremy Welch:

I founded Casa, this company goes back actually a couple years. I've been building companies for over a decade. I actually dropped out of Duke for a little while, and I joined these guys at Invite Media. We built the first demand-side platform. This was in the advertising technology space, and we sold that company into Google in about 2010, and so I got a really good view of what the entire internet at the time and kind of up to now has been based off of, which has largely been advertising technology and advertising systems, so you know did that company, we sold that in, I spent a year at Google, learned as much as I could, I went back to Duke where I studied political philosophy before dropping out and I went back to finish up, and when I went back to finish up, I had all these questions. I was in New York with that company and with Google around the time of the financial crisis, so I had all these big questions as to how the global capital system worked, and I'd went back to school and started digging into these questions, and that's around the time that I found Bitcoin, so the kind of first public thing I did, I did a lot of private study, and then the first public thing I did was we did a Duke Bitcoin conference there. Matt Corallo, who was a Bitcoin core contributor, a few other people that are now on the ecosystem, we were all at Duke, and we wanted to do something to get more people at Duke into that, but that was kind of the first public thing, and then, fast forward a few years later, when I was building another company, this company started getting pulled and shifted more and more towards this ecosystem and it really became Casa, so we actually started funnily enough as a home-sharing app, and I'd been in the ecosystem for a long time, I knew the space, I was technical, and the shift towards this broader kind of sovereignty as a service or more of a platform company instead of an application company happened because we tried to build an application first, so we were trying to build an Airbnb competitor actually with the Blockstack team, so we were going to build on Blockstack systems, and during that process of building an application in the space, we did an ICO, we were never going to ICO, you know we evaluated a lot of ways to do this, but we quickly found that some of the kind of core or I would say fundamental technologies are around personal key management, around personal node management. There were major problems there, and by solving some of those problems, we can enable not just ourselves to do well with an application but many other teams and companies, and so our long-term vision has always been about, you know started as trying to build a decentralized application and to counter some of these older systems that we'd seen in the ad tech ecosystem. We went below that and started building foundational technology, and then now, we're starting to give a much bigger vision with the Node and the Key Management in One, and 2019, for us, will be about a lot of building a coherent experience not just for ourselves, not just for our direct clients, but for other developers, other partners to be able to reach these customers and many others and simplifying their lives that they want to build more in this ecosystem.

Laura Shin:

Yeah. I'm a fan of Tim Ferris' and he talks about how one model of entrepreneurship is to what he calls scratch your own itch, and in your case, I feel like that is what happened, like you were trying to build at the application layer, and then realized, oh, which are some of the really basic things run, how to manage private keys are not easy to do, and so that's kind of like a more foundational problem that needs to be solved, and this is something I've been commenting on recently in episodes, **but one thing that's always puzzled me a little bit about some of the hardware devices is that they ask you to safely store your seed phrase, right?**

Jeremy Welch:

Your seed. Yeah, your seed phrase. You're right.

Laura Shin:

And I'm just like, oh my gosh, where would I store this without…because like I'm the kind of person where if you ask me to kind of organize documents or something, then if I kind of file them away, I will never know ever again where I put them, like I just will not remember how I organized…like I will not, and **so I just wondered if you could just sort of describe what you think are all the problems with how an individual might try to safely store their seed phrase?**

Jeremy Welch:

Yeah. I mean, you really hit the nail on the head. We talk a lot about how beneath that single statement of you know keep your seed phrase safe is an entire discipline, right, there's an entire company, there's an entire…you know you have to be an expert just to do that, and the brilliant thing, you know Alena, who joined the team, she was the CEO and founder of Trezor, one of the first hardware wallets, and the real problems that they were addressing tackling key management were actually against online threats. You didn't want to keep keys directly on your computer or any kind of hot connected device, and they succeeded in that, they succeeded in solving that kind of core set of problems, but along the way with the design of having some form of backup, they opened a new set of problems, and we are addressing this kind of new set of problems in the kind of broader ecosystem, and one way we do that with the multisig is we have what's called a seedless setup where we don't know the seed phrase. We've intentionally built the system so that we don't know the seed phrases, whenever we're setting up your keys, and you know you don't know the seed phrases, you don't record them, you don't write them down, you generate all the keys, and then we've made it really, really easy to swap in new devices, so what happens is if you know you lose the device or the device becomes compromised, you're attacked and the device is stolen, then you just swap out the new device into the keyset, and we've made that really easy. It's seamless, it's two or three taps, happens in a few minutes, and you know no command line, no copying/pasting, just very fast, and by making that easy and then wrapping a support service around it, again, we're trying to address this entire discipline that you have to learn. We do view this whole process, it is going to be a journey for most people.

Anybody that's used a Trezor, it's incredibly empowering the first time they try it and whenever the funds actually land on the device, and they're walking around like, wow, I mean, I could cross borders with this, I could go anywhere with this, and then, the scarier thing is, if I lose this, right, then it's just gone, so there are these kind of like scary things around it, but it's also incredibly empowering. It's like, you know I don't know if you think back to like the first time you drove a car, as a teenager, today, we totally take it for granted, but the first time you get behind the wheel and you're driving this big car and you go fast, it's a rush, right, and it's really empowering, and you know I think we're going to see similar things around this technology is as it gets easier and easier…and I describe cars a lot because if you think about what goes on behind a car, the pushbutton nature of just a Toyota Camry, you just push the button and it starts, and you just hit the gas and it goes, but behind that, there's an incredibly complex engine, you know it's over 10 thousand parts in a standard automotive engine, and it just works, and so I think that where we need to get to is even though we have these components like a Trezor or like a Ledger and we had these current experiences to where it's like, wait, okay, this one component, even though it's supposed to be simplified, this actually is creating more complexity, over time, we will get it to a pushbutton, just swap in keys, you know if you lose one you can just go buy one at a Best Buy or some other store, I mean, we want to get this world where it's just common nature to have lots of these key devices around and just much easier to use.

Laura Shin:

Yeah. That would be comforting to someone like because I am known for losing things constantly, and it's super annoying for me, even though it's my family who's always complaining about it, and I'm like, why do you guys care, it's me that like who's affected by this, but anyway, so I actually just want to unpack this multisig solution. You kind of briefly described it, but from a diagram I saw on your site, so as you mentioned before, you guys keep one key that’s kind of like an emergency backup, and then the other four…

Jeremy Welch:

Right.

Laura Shin:

Are accessible to the user themselves, so…

Jeremy Welch:

Right.

Laura Shin:

There’s one on their phone app, one that they would keep at home, one that maybe they put in a bank, and one that maybe they keep at work, **so like, for instance, in my case, where I don’t have another place where I work, where would you recommend that I put that fourth key?**

Jeremy Welch:

Sure. So, this changes, each person is different. Some people will store them, they have you know some remote properties, some people use a series of bank vaults, everything has tradeoffs, and we advise clients on what the mix of those tradeoffs are. Some people, they have a brother or a sister or some sort of sibling they’ll end up storing it with they trust and that they’re very close to and you know they maybe co-owned some other properties or something with and they do some already, they do some kind of combined financial work with, sometimes it’s another business partner, right, like so it’s not always just different locations, sometimes it’s different people.

The important thing about it is multisignature, multilocation, multidevice, so even spreading out across different types of devices actually protects you from what’s called a supply chain attack to where someone could gain access to one of these company supply chains and potentially cripple or cause problems with a single device provider, but you know the answer, again, kind of jumping back to that is that it really depends on the client. We do have these kind of core principles around how we approach clients, and the first one is sovereign customers, and what’s important about that statement is that the decisions, every client will be unique in a kind of age of a lot of companies in the kind of Silicon Valley way of just like scale rapidly and treat everyone the exact same, we are distinctly trying to go against that and treat every customer as unique as possible and think about really tailoring our security recommendations to each user’s life because everybody's different, and they're all going to have kind of different security situations, so you may have a very different security situation and the location where you'll put it, but we'll find something for anyone.

Laura Shin:

But how could you be certain that some individual users are not implementing it in a way that would leave them vulnerable, you know what I'm saying?

Jeremy Welch:

We can't. Yeah, it's a great question. I mean, we can't, and that's part of the point of building systems like this and part of the point, I think, of going down this road of Bitcoin generally is about personal responsibility, and again, I think we've been through an age where things were easier and everybody was treated the exact same, and we oversimplified things, in a sense, where now there's a lot more responsibility, the consequences are a lot heavier, and we make it very clear to our clients that if you lose three of those keys that you have, three of the four, then your funds are gone.

The funny thing is that you know as we describe that, you know that feels terrifying whenever you're seeing it on the screen and we've made it really easy to visualize you know if one key goes down, then the entire kind of shield drops, and then the one key that you've lost goes completely red, and it's this very visceral visual experience by design, right, but the funny thing is that as we think about you know if you have a total of 3-of-5, right, and you lose one key and then you lose a second key, then you're at the absolute edge, if you lose another key, then it's done, right, you've lost all your funds.

Laura Shin:

I would probably end up in that situation.

Jeremy Welch:

Well, the funny thing though about that is that that's actually the normal state of everybody that just has a Trezor or a Ledger. The normal state of everyone that just has a single device is this case to where if they lose that device or they lose that seed phrase, it's gone…

Laura Shin:

Yes. Right.

Jeremy Welch:

And so, we've built layers above that, and to simplify that, the chances that there's a natural disaster that affects your city and the other city that you have one and one of our customer support centers, and so you didn't have access to your keys is much, much, much lower than if you're house was just in a fire, and then your Trezor and a seed phrase got destroyed, right, and we're by distributing risks across, again, multisignature, multidevice, multilocation, we are minimizing it as much as possible, but still, you can never take away the personal responsibility element of that, and we've seen it as an empowering thing, we've seen people respond and excited about the fact, but it's definitely daunting, and it's not for everyone.

Laura Shin:

Yeah. Well, since you brought up fire, **I actually did have a question about a natural disaster-type of scenario because, as we know, recently, there was a fire that did wipe out a whole city, and there are times of, of course, when we've got things like hurricanes and other sorts of natural disaster, Tsunamis, that kind of thing, so in those situations where maybe I even have spread my different keys out to different locations, but potentially, I could end up in a situation where three or more of my keys have been lost, then what, are the funds just gone?**

Jeremy Welch:

Yes, the funds are gone, and that is why, again, in terms of spreading these out in multidevice, multilocation, it's really important that you're spreading them across multiple locations. Most of our clients do it across multiple cities. They will frequently leave the devices in a fireproof safe in any one of the locations that they're in. We don't know the exact locations of devices, that is up to the end client, but we've heard of bank vaults, we've heard of personal fireproof safes, we've heard a variety of things, and this echoes and this is similar to how people normally store their devices, but we've also seen cases…we're kind of hypersensitive to this, so we're constantly reminding clients to check their devices, and even when they're in cold storage, we do regular quarterly checks and just making sure.

So, there's one problem that a lot of people aren't even thinking about right now, which is Bit Rot, so if you take just an iPhone, and the error rate on an iPhone is such that Apple assumes that maybe it's 1 percent or 0.05 percent of iPhones that they manufacture are going to fail within a year or within a half-a-year just because of the error rates and manufacturing process, that becomes a lot more terrifying if it means that you're kind of managing personal funds, and you have devices and key devices that tie into your personal data, and even just checking, we have automated checks inside the system to where you can do these health checks of your devices regularly, but yeah, I would say it brings a much more kind of visceral, tangible knowledge or awareness of systems whenever you're using this.

Now, the reality is that the real world isn't actually that much different. I think what's happening is that, you know by design, we're bringing this kind of to the forefront and making it real easy to understand what the real risks are and what the real situation is, but the reality is that the world's not that much different, you know more car analogy, is if you're ever in a car accident, for awhile after being in a car accident, most people are jittery, like they're careful, and they're looking around, and they're realizing again like how fast cars are going, but then we get in these flows of being used to being in a car and no car accidents are happening, and our minds kind of just turn off to the real risks, where, again, we just see it as these are the risks that are around us always, it's just that we don't think of it that way, and we're making it a little bit more visceral, but we're also giving you more control and more safety checks to kind of protect you better.

Laura Shin:

Yeah, but I just wonder, I mean, like this is a lot of responsibility for an individual. **Whereas, if I use something like Xapo where they have the private keys in multiple geographies around the world, that's kind of a level of protection that I myself can't probably implement, right, so why would I choose to use the Casa method as opposed to entrusting a company that can do it better than I can?**

Jeremy Welch:

Sure. Sure. I mean, it just comes down to kind of personal belief and the statement, not your keys, not your Bitcoin, so a company like Xapo, great product, great company, we've heard nothing but good things, we know some people over there, but it's just a different kind of model. We can't personally, maybe if you're a friend of one of the founders or employees, you can go visit the facilities to make sure that those servers and the keys and everything else are there, you are inherently trusting that company and that they are running those and that they're not just kind of storing it on a server at someone's back office or in someone's house, right, you're entrusting that those things actually exist. To be honest, like it is a lot of marketing. It is mostly marketing, and they may actually have those bunkers and do serve a real purpose, but you're still trusting, there's still that element of trust, but we are trying to build the best possible system for you to self-manage and self-understand and have the full power, and this stuff, you know it may be tested sooner, it may be tested later. I think that we're in a time right now, which we're very lucky with the bear market, to where we're just able to build and build a lot of new features, and there's not as much of a rush, but whenever bull markets hit, everybody looks around, and the prices are shooting up, and everybody is like, oh my gosh, if this does actually kind of hit this hyperbitcoinization situation, even if they just go to 50k a coin, even back to just 20k a coin, like the calculations become very, very different. The amount of money on the books becomes very, very different, and the way people think about these systems becomes very, very different, and we're only, you know Mt. Gox, there's the famous video, I think of Roger saying, oh yeah, everything's fine, and Mt. Gox something like a week or two weeks before, it was just absolutely mayhem, and they realized they lost all the funds, so it is one of those things, where it's personal choice, it is some people are never going to want to fully manage this and fully take responsibility for it, but for those that do and those that want to go down this path, that want to grow stronger through it, and that want the absolute best protection, you know we're going to offer that.

Laura Shin:

So, let's talk about attacks as well, which we started to do. You mentioned earlier that if someone loses one of their keys, you guys can easily replace that, so in that case, the other four keys are still usable, you're just replacing the one that is lost, is that correct?

Jeremy Welch:

Right. So, the client, they can grab a Trezor or a Ledger, we work with both systems. They can grab any Trezor or Ledger from any manufacturer, it doesn't have to be us, it can be directly from the manufacturer, it can be from another store, it can be an extra one that they have laying around, they can use any device and pop it in and reset their key shield. We also offer, for our clients, we are authorized resellers for both Trezor and Ledger, and we hold extra devices in reserve. There have been cases to where there's supply chain shortages or you know other factors, it would end up taking a week to ship a device, and if you've lost the device and you want to get yours the next day, then that's a problem, so we hold extra devices for all of our clients, so overnight, no matter where they are in the world, if they need a device, you know we will ship it overnight shipping, fast as possible, most expensive, whatever it is to get them the device as soon as possible.

Laura Shin:

So, what if I'm a bad actor, as they say, and I will use my sound engineer, Chris, as an example, let's say, I go hold up Chris, hold him at gunpoint, and he's a Casa user, and I force him to report that he's lost one of his keys, so then you guys give him a new key, and so maybe what happens is maybe I'm the attacker and I have brought my own Trezor, and so Chris now has the key on his phone, the key at his house, and now, I have Chris report a key lost, maybe the key at work is lost, and then I say, Chris, have them send the new key to my Trezor, so now there's three keys at this one location where I'm holding him at gunpoint, so then can I force him to send out all of his Bitcoins that way?

Jeremy Welch:

No.

Laura Shin:

No. Okay.

Jeremy Welch:

So, you can swap in keys, but you can’t actually access funds because you have the funds have to transfer over, so we’ve simplified. The two steps that we’ve actually done, we actually did user research and noticed that any time someone lost or thought their device was compromised, we talked to some people that even just firmware updates that you know someone got scared that their device was malfunctioning, but what would frequently happen if someone would buy a new device, they would reset the seed on the new device, and then they would transfer funds from the old device to the new device or they would immediately transfer funds to a totally new, fresh device and fresh seed, right, so we’ve taken the kind of the middle step out, and so what happens is you rotate in a new key, you have a new key shield, and then you transfer the funds, you do a wallet sweep to that new key shield, to that new setup, and with that new setup, you still have to transfer the funds, so in order, if you were holding Chris at gunpoint, you would still have to travel with Chris to several other of his locations to actually transfer the funds and do a signature to get the funds onto the new key shield, but even then…

Laura Shin:

Even though he has two keys in his possession and I’ve now fashioned a third?

Jeremy Welch:

Correct.

Laura Shin:

Oh, okay.

Jeremy Welch:

Correct.

Laura Shin:

And wait, and so why, and I guess what I don’t understand…

Jeremy Welch:

Because…yeah.

Laura Shin:

Is that like…

Jeremy Welch:

Go ahead.

Laura Shin:

So, in this situation that I outlined where he's actually lost one of those…or sorry, **I forced him to report that he lost one of those keys, then how do you transfer the funds to the new device if supposedly that other device, you know we lost it?**

Jeremy Welch:

So, you're still having to sign with the existing keyset, so you're still having to sign even though you lost one key, you have four remaining keys.

Laura Shin:

Oh.

Jeremy Welch:

Right? And of those four remaining keys…

Laura Shin:

Well, I guess three in his possession and then the fourth is with you.

Jeremy Welch:

You have to still do a…Technically, only two if you're at a location to where he had two devices, so say he had his phone and he had a device and this was at his home and in his home safe or something, then of the old keyset, there's still only two keys there, so he's going to have to travel to another location to get another device and make another transfer, and it's that element of having to go multiple locations and interact with multiple parties that is the real security around all of this. That extra time for most attackers is not worth it, and in that extra time, we had the ability to use an even emergency lockout feature that just shuts down the account, locks out the account, so even as you're walking in the door, if Chris just tapped that, that locks his account down entirely.

Now, if you had all the devices, you could still get access to it, that doesn't enable Casa to do anything malicious because Chris still holds all the keys, it just slows down the process of executing your transfers because you're not doing it through the actual end interface, if that makes sense. Through the iPhone apps and the web apps, you would have to do it manually with a command line in a more technical way, so all of that just to summarize that, again, you know multidevice, multilocation, that model, that protocol is what's helping protect Chris. We are here as a service to help run that model and help keep those keys up to date, help provide service, help debug problems, but at all times, the end user is in full control, they have the full set of keys, Casa is never in a position to where we can touch, access end users funds, and an attacker would also have to go to these multiple locations you know to get anything.

Laura Shin:

And then, what if I get ahold of Chris' phone, and then I flag a couple of his keys lost and somehow can access one in a new location, then could I generate new keys for myself and then hack his Bitcoins?

Jeremy Welch:

So, repeat that, again.

Laura Shin:

So, if I get ahold of…

Jeremy Welch:

I mean, we can walk through this specific model.

Laura Shin:

So, if I get ahold of his phone…

Jeremy Welch:

Yes.

Laura Shin:

We were joking about SIMS swapping before the episode…

Jeremy Welch:

Sure.

Laura Shin:

So, what I'm talking about is like it's not SIM swapping, it's like if I literally just steal his phone, and then I get into his Casa app, **can I flag a couple of his keys lost and then issue myself new keys but claim that they're his, do you know what I'm saying, and then use those new keys to hack his Bitcoins?**

Jeremy Welch:

Yeah, the important thing is that with any of this key management, the end user is doing everything, so we, as a company, like we can provide…

Laura Shin:

Right, but that's what I'm saying.

Jeremy Welch:

We provide a simplified UI, and we provide some support service around it, but ultimately, the end user is doing everything, so what's important about that…

Laura Shin:

Right. Right. That's what I mean, so what if I'm the hacker…

Jeremy Welch:

Is that even if you…?

Laura Shin:

And I've stolen Chris' phone, and then I pretend that I'm Chris, and I'm doing all this stuff, but really, I'm going to end up having the funds?

Jeremy Welch:

You would still have to have Chris' permission. You'd still have to have Chris walk through all of the…

Laura Shin:

But how would you know?

Jeremy Welch:

What do you mean how would we know?

Laura Shin:

How would you know whether it was Chris or me giving the permission?

Jeremy Welch:

So, again, the general point here is that you would have to get Chris held at gunpoint, take him to multiple locations at gunpoint, across a pretty large period of time.

Laura Shin:

But I can't just…?

Jeremy Welch:

Just to be able to…

Laura Shin:

But I can't just say, hey, those…

Jeremy Welch:

Just to swap in one key. Yeah. Yeah.

Laura Shin:

But I can't just say, hey, those devices were lost?

Jeremy Welch:

Right. Correct. Just think of it like this, think of it like this, okay, there are two stages in a key transition or in a key shield update, okay. The first step is in flagging a key as lost or stolen or compromised, and then syncing a new keyset, okay.

Laura Shin:

Yes.

Jeremy Welch:

When you make that new keyset, that is a totally new set of addresses, a totally new set, and there are no funds on that new keyset.

Laura Shin:

Okay.

Jeremy Welch:

The second stage is that you actually have to transfer the funds from the old keyset to the new keyset, and to do that second stage of that transfer, even if you got some access to the UI and you tried to swap in some keys and you generated a new keyset, you still have to transfer funds from the old keyset to the new keyset, and when you're doing that, you're going to have to go through the process of going to multiple locations, potentially a bank, potentially offices, potentially other business partners or siblings or family members to get devices…

Laura Shin:

Right, so can't I open up a safety deposit box at my own bank and pretend that…do you know what I'm saying, like tell you that…

Jeremy Welch:

Yeah, but you're…so, what I think the disconnect here, Laura, is around it doesn't matter what you do…separate this out into the new keyset and the old keyset. You can do all you want as an attacker to generate a new keyset, but you still have to get Chris to transfer the funds from the old keyset, and transferring the funds from the old keyset is very hard. Transferring the funds from the old keyset is going to require you to go to multiple locations.

Laura Shin:

Okay, even though he's…

Jeremy Welch:

And certain parties…

Laura Shin:

Even though he's…

Jeremy Welch:

Yeah, even though the new keyset…

Laura Shin:

Even though he's reported…

Jeremy Welch:

Is created…yeah, it doesn't matter.

Laura Shin:

Those devices lost at those new locations?

Jeremy Welch:

Yeah, exactly, and so it's like…

Laura Shin:

So, it's like checking your IP or something like that when you do it?

Jeremy Welch:

Let's think of it like this, okay, think of it like literally opening a new bank account. Sure, you can go to a bank and you can use a false name and you can set up a new bank account, but that's not going to put funds inside that new bank account. Even if you used Chris' name and you set up that new bank account, you actually have to go to his old bank account, and somehow scam the…

Laura Shin:

Even if I've reported it lost?

Jeremy Welch:

Even if you've reported it lost, you still have to convince the old bank account, the old people, to transfer funds into the new compromised, fraud bank account, and again, the calculation here is that the level of complexity required for you to generate these new keys, new keyset, and go through and transfer all the old funds is extremely high, going across multiple locations, needing to know multiple pins over multiple days, multiple hours at a minimum, potentially multiple days and multiple geographical locations is extremely high…

Laura Shin:

Okay.

Jeremy Welch:

And the chances that no one would notice are very, very low, and also, keep in mind, that the instant that a key is compromised in the system, we know about it as a company, and we're calling to check on our clients, and if we don't hear back from a client and the key is compromised and there's something going on, then there are procedures, we have procedures with different clients for whether we would call authorities, whether we would call other family members, whether we would call you know what the kind of emergency process is.

Laura Shin:

Okay. We're going to keep discussing this in a moment, but first, a quick word from our fabulous sponsors.

CipherTrace:

Within months, cryptocurrency anti-money laundering regulations go global. Are you ready? Avoid stiff penalties or blacklisting by deploying effective anti-money laundering tools for exchanges and crypto businesses—the same tools used by regulators. Ciphertrace is securing the crypto economy. Face it, regulations can stall or kill a fast-moving crypto business. New financial action task force and european union cryptocurrency AML laws are coming soon. You could be hit with stiff fines or blacklisted—no matter where your servers are in the world. Prepare now. Deploy the same powerful CipherTrace tools used by regulators. protect your assets, streamline your compliance programs and keep your exchange or crypto business out of the regulators crosshairs. Learn how effective anti-money laundering tools help keep your crypto businesses safe and trusted. Learn more at www.ciphertrace.com/unchained. CipherTrace is securing the crypto economy.

Microsoft:

Getting your blockchain app off the whiteboard and into production can be a big undertaking. From connecting user interfaces to integrating disparate systems and data, blockchain app development can be time-intensive and costly. Well, the folks at Azure have you covered. With a few simple clicks, the Azure Blockchain Workbench can create a blockchain network for you, pre-integrated with the cloud services needed to build your app. And with their new Development Kit, users can extend their app to ingest messages from bots, edge devices, databases and more. It's free to download and gives you the tools you need to get your first app running in less than 30 minutes. To learn more about the Dev Kit and how to get started, visit (aka.ms/unchained) or by following them on Twitter @MSFTBlockchain

Tokensoft:

Issuing a digital security on the blockchain can be a significant undertaking, particularly to ensure compliance requirements are met. TokenSoft's trusted platform for digital security issuance provides security in a world of uncertainty by working with top legal and financial experts so that your digital assets are secure. TokenSoft leads the market in providing tools to support tax, banking and securities regulations for issuers of digital assets. We are honored to have supported the leading companies in 2018. To learn more about issuing digital securities successfully, visit tokensoft.io or follow them on Twitter @tokensoftinc.

Laura Shin:

Back to my conversation with Jeremey Welch of Casa. **So, when you say that like I as the attacker or anybody would you know if they need to kind of create new keys, and you say that you require them to go to different locations, how do you know they're in a different location?**

Jeremy Welch:

Again, that's the proof of a signature of a device, so that comes down to using actually a Trezor to sign a signature to execute a transaction on that Trezor, right, or Ledger.

Laura Shin:

But how do you know that they're doing it at a place that's from a different location, like how do you know that they're not just doing two different signatures both from the comfort of their own home?

Jeremy Welch:

Yeah, my point is that it doesn't matter. So, I think what you're suggesting is that how do we know that the attacker hasn't gotten access to these extra keys and like brought them back to the home and is doing these transfers at the home or something.

Laura Shin:

Yeah.

Jeremy Welch:

What I'm pointing out to you is it is a challenge just to get one of these keys, and if you're going to a bank safety deposit box to get one of these keys and the client looks under duress or you're not the client and you're trying to go get the device under the client's name…

Laura Shin:

Right. No, no, no, but the scenario I'm outlining is different. I'm saying I'm the attacker, and I report that one of those keys is lost.

Jeremy Welch:

Yes.

Laura Shin:

I get control of Chris' phone, and so to your mind, Casa thinks, okay, that device at the bank no longer works, and then I…

Jeremy Welch:

No. No, no, no, we don't. We don't. We don't. We don't.

Laura Shin:

Oh, okay.

Laura Shin:

That's what I'm pointing out to you is that we don't. Our system is not designed in a way that says that, again, I would split this. I'm trying to like create a simplified model on connecting this into the two different steps of like you can create all the new stuff you want, but you still have to go get access to the old stuff in order to make a transfer, and it's the protections that are in place around the old things that this attack would not work.

So, again, like just using a simplified case, okay, and using the existing financial system, which I think will hopefully clarify things a little bit more, you know you go attack Chris, you get some of his information, and you go open bank account at Bank of America, okay. It turns out Chris has been banking for a long time with HSBC, and you go open a new bank account in his name under Chris, you control it, but it's under his name, it's a fraudulent account, okay, when you open that bank account, it doesn't have any money in it.

Laura Shin:

Right.

Jeremy Welch:

Right? But it's a new bank account, and it's a fraudulent account, it's in his name, but it has no money in it.

Laura Shin:

Right.

Jeremy Welch:

The only value you're going to get is when you can convince Chris or can convince someone else to transfer funds into that fraudulent account.

Laura Shin:

Right. So, that's what I was saying, if I have control of his phone…

Jeremy Welch:

And what I'm saying is that…What I'm saying is that just by having control of his phone, that doesn't mean you have control of his keys, so it's like you would still have to, in the bank account example, you would still have to somehow defraud Chris to get him to send the money from his old HSBC account to this new account, and so in our case…

Laura Shin:

Right.

Jeremy Welch:

And our case is like the…

Laura Shin:

That’s my point about the gunpoint, couldn’t I just force him to say like, hey, report this one lost and then send the funds to this new…?

Jeremy Welch:

Yeah, but again, reporting a key as lost doesn’t send any funds. That never sends funds.

Laura Shin:

Right.

Jeremy Welch:

That would be a massive security…

Laura Shin:

Report that it’s lost, and then also get Casa to you know tell them, hey, this is your new device.

Jeremy Welch:

But again, that still doesn’t do anything, like that just reporting it as lost and even setting up a new device, that doesn’t send funds anywhere. What that does is that creates a new…that’s the equivalent…that’s the equivalent of creating a new bank account with no money in it. Yes.

Laura Shin:

And so, there’s no way that an attacker could force their target to get Casa to send funds to the new device?

Jeremy Welch:

Correct. Now, what they could do is they could hold Chris at gunpoint, and they can take him across multiple locations, and they could take Chris to…and Chris, you know wherever you are, I mean, you’re the example in this case, I hope you’re doing all right.

Laura Shin:

He’s here but silent.

Jeremy Welch:

Yeah, I hope you're doing okay, man. But what would still have to happen is Chris would have to be taken at gunpoint to his bank to get access to this key to the safety deposit box and to send a request, right.

Laura Shin:

But this is what I'm confused about.

Jeremy Welch:

Yeah.

Laura Shin:

So, like let's say that he's not held at gunpoint, let's say he's actually lost one of his keys, and it's not at the bank, let's say he's lost the one at the office, if he reports it lost, then how does he get funds onto his new device?

Jeremy Welch:

Because he still has access to other keys in the setup.

Laura Shin:

Right, so that's what I'm saying, that somebody can hold Chris up, and Chris now has the two keys, one on his phone and one at his home, he reports…

Jeremy Welch:

Okay, I see what you're saying. Okay. So, the disconnect here, okay, is that the total and the 3-of-5, it has to be 3-of-5 of the same keyset, so in the old case, right, Chris has a total of five keys, he's now reported one as lost, okay, you're attacking him and you're trying to swap in a new key, you've now reported one as lost, so in the old keyset, he now has four listed as working and one as compromised. New keyset is created, total of five keys, okay…

Laura Shin:

Oh, but I thought that you said that when…

Jeremy Welch:

You have two…

Laura Shin:

When one is compromised, that only one gets swapped in and the other will remain the same.

Jeremy Welch:

Well, that's correct. That's correct.

Laura Shin:

Oh, okay. So…

Jeremy Welch:

The other four remain the same.

Laura Shin:

But it's not five…

Jeremy Welch:

But it is treated…

Laura Shin:

It's not a new set then…

Jeremy Welch:

No, no, no. No, no, no, but…

Laura Shin:

It's just one new key?

Jeremy Welch:

No, no, no. It is a totally new set of addresses. That one new key, with the old four keys, creates a totally new keyset with a totally new set of addresses, so in that case, you now have two keysets, you have the old keyset and the old set of addresses, and you have the new keyset. Right?

Laura Shin:

Okay. So, wait, and just to understand, so old keyset has these five addresses, A, B, C, D, E.

Jeremy Welch:

Yes.

Laura Shin:

The new keyset, even though there's…

Jeremy Welch:

It uses some of the old keys…

Laura Shin:

Even though four of the keys remain the same, now the addresses are what is that F, G, H, I, J?

Jeremy Welch:

Exactly.

Laura Shin:

Something like that?

Jeremy Welch:

Or X, Y, Z.

Laura Shin:

Oh, okay.

Jeremy Welch:

Yeah. Yeah, and again…

Laura Shin:

Interesting.

Jeremy Welch:

That's where this new keyset is like a totally new bank account. It is totally fresh, totally fresh addresses, and so you still have to. The stage that you're missing is that you still would have to attack Chris and have him transfer funds from the old keyset to the new keyset from the old addresses, from the A, B, C, D addresses, to the new addresses for you know F, G, H, I.

Laura Shin:

Right.

Jeremy Welch:

And that transfer, that would still be very, very hard.

Laura Shin:

Right. Well, maybe I could do it.

Jeremy Welch:

Okay. Okay.

Laura Shin:

Wait, with Chris.

Jeremy Welch:

I know that was a lot of back and forth…

Laura Shin:

I'm sure Chris would give me his Bitcoins.

Jeremy Welch:

And I know that that was confusing. Yeah.

Laura Shin:

No, I'm just kidding.

Jeremy Welch:

I know that was a lot of back and forth and I know that was confusing, and this is complicated stuff. It took us a long time to map out this model, and the specific decision we made from a security perspective is that we wanted a more rapid response system and wrapping a lot of support around that to where we're you, basically, get two approaches to security. Either you're going to put yourself in a steel cage, cement cage, you're going to surround yourself with guns and everything is going to be secret and no one's ever going to know, and everything is like tightened down as much as possible.

There's an alternative security approach to where it's like a rapid response model to where it's your ability to rapidly respond very quickly, and we joke about this being like the terminator model to where you have this T1000 that keeps coming, in the terminator movie that keeps coming after him, and it doesn't matter if you shoot a gun into him or they throw something at him or they hit him with some sort of construction equipment, it doesn't matter, he keeps reforming himself quickly and coming and coming after them.

Laura Shin:

Right. Right.

Jeremy Welch:

And in a similar way, we're taking a model, the old model of using just a singular device, we're using a singular cold setup at Xapo or wherever with a singular bunker, what we're creating is this faster model to where you know, yes, you have a bank in New York and then you have a home in San Francisco, and you got a key at each of those, and you got a key at some other place, and you know what, yeah, the house in San Francisco might burn down, but then you quickly, rapidly readjust and shift to a new keyset in a new location, we're creating this more rapid response model, then each of those situations you're kind of hardened down and you got things in a fireproof safe, and you've got things protected, but it's that rapid response piece that's very, very different, and that's where the service is super important too.

Laura Shin:

Wait. So, I just thought of something else, because…

Jeremy Welch:

Sure. Okay.

Laura Shin:

So, what if I hold Chris at gunpoint either that or I get control of his phone, and then what if I report the two keys in the other locations lost, so now, I only have two keys in my possession because both the one at the bank and the one at my office have been lost, and all I have is the one on my phone and the one at home, then I call you guys or I make Chris call you and refashion the new keyset and also move the funds so that way he…

Jeremy Welch:

But, we can't. That last step…

Laura Shin:

But it's me…

Jeremy Welch:

That last step you just said of just moving the fund, that's the thing that can be done easily, and we can't control that. Maybe one approach to think of this…

Laura Shin:

But I could force Chris to do that?

Jeremy Welch:

You could.

Laura Shin:

That's what I'm asking.

Jeremy Welch:

You could attempt to.

Laura Shin:

Okay.

Jeremy Welch:

Yeah, you could attempt to force Chris to do that, and we've never proposed that we like totally lock everything out of the system or we totally prevent any attacks whatsoever, we create a scenario to where to attack you becomes much harder…

Laura Shin:

Yeah.

Jeremy Welch:

And the chances of someone detecting an attack increase rapidly because you've got your keys in multiple locations, you have a rapid response model, you have a big red button on your account that locks the account down and locks all access to just even generating or flagging keys as suspect, right, and sends alerts to us, and so you have all of these precautions, it makes it much harder to actually attack, and it slows down any attackers, and that's really important…

Laura Shin:

Yes, and I just want to add that I'm…

Jeremy Welch:

Is like slowing down…

Laura Shin:

Definitely not advocating that anybody do this. This was more like an intellectual exercise.

Jeremy Welch:

Yeah. I am not either. I am not either.

Laura Shin:

I had a question, which was so in the 3-of-5, so let's say that I want to make a transaction, is there a timeframe in which I have to have all the 3-of-5 keys you know participate to make that transaction?

Jeremy Welch:

No.

Laura Shin:

Like do they all have to…no?

Jeremy Welch:

No. So, you can separate them by multiple days. You can do it totally asynchronously.

Laura Shin:

Oh, okay.

Jeremy Welch:

So, you could do three- or four-days difference, but yeah.

Laura Shin:

And what if it's like a week or two weeks?

Jeremy Welch:

Sure.

Laura Shin:

Oh, okay.

Jeremy Welch:

It would still work. Now, holding that long and building a keyset, it would still work, and we've also talked about building features that timeout after a certain period. Right now, it's relatively open, but there's a lot, there's a lot that we're still building, and I think that even having time locks around accounts and around certain signatures is something that we'll build in eventually. I would just say that the important way to think about this, so we started actually with Glacier Protocol and looking at the security model around Glacier Protocol and totally offline paper copies and the maintenance around that, which was enormous. We looked at Jameson Lopp's setup, you know he had his own custom setup, and he would've spent a day or two per year just going through and rechecking everything.

Our end goal was to take these existing models, that existed, that you know we're not reinventing the wheel, we're taking these existing models of cold storage and making them easier to use. We're building better user interfaces and better customer support around that entire process, and yeah, some people are technical enough to kind of reimplement this stuff themselves, but the UI and the customer support and the speed at which we can react and help you is not going to be present in any kind of custom situation, and so our company, the positioning of our company is in building all these experiences. You can look at the Casa Node is the same way. People were building Lightning and Bitcoin Nodes before we made the Casa Node. What we did is we made it much easier to set up, we made it much easier to run, we simplified customer support and setup and you know if something goes wrong, and we spent, you know our engineers spend hours at times with clients to get them set up and get their Node running and get them custom port forwarding setups and custom router setups. It's that element of we're taking these complex technologies and complex processes that exist and then we're simplifying it down to something that's usable and then applying all the customer support, and we're going to do that in more areas.

Laura Shin:

Yeah, and something else I wanted to ask was about the 10 thousand dollar a year service, why do people have to apply for that?

Jeremy Welch:

You could probably pop up a forum and just have people pay it out, but it is something that the setup is pretty involved, you know we do initial consultation to make sure that people understand what they're getting into, and most people, the odd thing that we've seen is that for a lot of our clients when they do kind of ask all their questions and they finally realize you know what it actually is, the sale is very quick. It is very fast. You know, we've had people tell us they've been looking for…it's been surprising to that end, but there are a lot of people we talk to as well that you know they want it to do certain things that are totally automated, and they want it to do certain things that custodial systems do that a security system that is more in your control just won't be able to do, and so we are very careful with clients in terms of like we are very careful with their setup and the process, and they have to apply because it is a little bit more involved at that level.

Now, with the Casa Node, you can just buy it. You can buy it today, you know it ships out. We caught up. We were shocked at the demand, but we have pretty well caught up, and it usually ships out about two to three weeks after your purchasing, but that is a much more rapid onboarding process.

Laura Shin:

Okay. Yeah, I want to get to the Casa Node in a second, but first, I just want to ask also, so what are the factors on which you would reject somebody, who's applied for the 10 thousand dollar a year service?

Jeremy Welch:

So, first off, you know we only support individuals and small teams. We don't support large institutions. We're not designed as a solution. We've had people kind of approach us around institutional setups, and although we do advise, we definitely advise companies, and you know this specific setup and key master is built for small teams, individuals, families, family offices, right, like this nexus of smaller teams or smaller families or you know one individual with one family member or a lawyer or someone that they're using as a trusted kind of outside party, those are the dynamics on which this specific system is built. We do have people that come ask us that they have a large corporation or a fund and they have a 100 million dollars and they're looking to set up a system, and they want to make sure they have control, and they've heard about our design and our approach and our customer service, and they're excited about that, but we're just not the system that's built for that. There are other companies, Anchorage just came out about a week ago, Diogo, they're building a phenomenal product, and the Fidelity team is building. They've announced their product last fall. They're building a phenomenal product. I mean, we've seen other teams that are looking mostly at that institutional side, and we are not that, right, so we do have some filtering around making sure that we're addressing the right user.

As far as an individual, as long as the user is technical enough and sees…I wouldn't even say technical enough, it's as long as the user knows that this is not just a regular bank, like they are running their own infrastructure, they're managing their keys, they know the security implications, you know we do a kind of brief conversation around that, then we'll onboard them pretty quick after.

Laura Shin:

And why do you not have multisig support for Ether, why is there only single-key support for that?

Jeremy Welch:

Yeah, that's a great question. The approach with Ethereum, and we wrote a blogpost about this, Ethereum does have some multisig smart contracts. The logic around not supporting Ethereum is that we didn't think that the system was to a point to where we could be confident that funds would not be lost or if they were lost that they would not be recoverable whatsoever, and the specific example around this is around the Parity situation, and I'm not sure if you're familiar with what happened with Parity multisig?

Laura Shin:

Yeah, I am, but why don’t you fill it in for listeners, who maybe don’t know.

Jeremy Welch:

Sure. So, the Parity multisig situation wasn’t exactly a hack, it was a developer…I think it was a young developer, like a new developer on their team that was going through and testing some scripts and happened to accidentally delete a certain piece of code that was critical to some of their multisig wallets that was irrecoverable.

Laura Shin:

Yeah or so they say.

Jeremy Welch:

Yeah.’

Laura Shin:

They say it was an accident.

Jeremy Welch:

Well, there’s an open question. I mean, we know some of the Parity folks, and they’re great people and very smart, and this was kind of a shocking situation, but the more shocking thing to us is that you know we saw in the case of the DAO, we saw there was a fork and there was a reversal in the transactions. In the case of Parity, there wasn’t, right, and even though it was a total accident, even though you know it was totally unintentional, there was no reversal, so those funds are lost. I think it was over 100 million dollars just totally gone.

Laura Shin:

Yeah.

Jeremy Welch:

And in that case, we look at it from two ways. You have to have the actual system and code has to work well, has to be logically sound, has to be well tested, has to be vetted. You know, we think that Bitcoin is definitely to that level. we think that there are some other coins that are approaching that level, but Bitcoin’s by far leads beyond most anything else on the multisig side, but the other thing about Bitcoin is that there’s only one multisig solution. There are a couple details of implementation on how you set it up, but there's kind of one dominant way to do it, and the entire community uses that, and what comes out of that is if there were a break, if there were an issue with this implementation, there would be no choice but to either run a hard fork or do a soft fork or some other fix to make that fix.

In a case on Ethereum to where you have multiple smart contract implementations, you know Parity is the one that got hit in this scenario, there was no change, but there are several others, and you know what if you're the one that got hit with a bug and there's no guarantee that the underlying team would have the incentive or the core developers would have the incentive to fix this core issue that led to your hack, and so we just don't think that for our user's funds or you know recommending to our clients, we don't feel comfortable recommending multisig on Ethereum today because it's not consistent or it's not you know fully sound on both the logical level and on the community level.

So, you know there's been a movement to get some smart contracts formally verified and get a lot of outside tests and that's great, that would be this kind of first level around formally testing the code, making sure there are no bugs, making sure there are no holes, but again, I want to remind you that in the Parity case, a lot of that code was tested, a lot of it looked perfect, a lot of it looked great, yet it was still able to be deleted, and there was still an issue in them not wanting to do a reversal, so just because a smart contract is formally verified and fully sound doesn't mean there couldn't still be an issue like the Parity hack.

Laura Shin:

Yeah. So, we're running out of time, **but let's quickly talk about the Casa Node. So, as you mentioned earlier, it's both a Bitcoin Node and a Lightning Node, so why would someone want to run a Bitcoin Node when they can't earn money from running it?**

Jeremy Welch:

So, the Bitcoin Node itself, I mean, that is partially supporting the network. On the Lightning side, you can, you can earn money. It's around routing transactions. Now, the amount it's satoshi, so it's a much smaller total amount, but you know you can earn some, and today, a lot of running a Bitcoin Node and running a Lightning Node, it is a somewhat niche experience, it is a kind of early adopter experience that is changing. There are now games and applications around Lightning. We think 2019 is going to grow a lot on that side, and we've heard of even whole teams that have shifted their entire focus towards Lightning and Lightning applications that's not public yet, but I would just say that on the Bitcoin side, it's about securing the network.

In the case of SegWit2x and the move to do the fork and the NO2X movement, you know I like the impenetrable fortress of validation example, I think it's StopAndDecrypt that has this example, and Bitcoin running a node is about validating the broader network and validating the broader transactions, and even the miners are creating those transactions and creating the blocks of transactions, those still have to be accepted and validated by the broader community, so running a Bitcoin node, you are doing a kind of community service in validating the broader network and strengthening the broader network, and I think that that's going to become more and more apparent and more and more of a kind of personal thing for people and contributing to the network, but on top of that, I think you're actually going to get this day-to-day use case and much more just kind of pure applications use case around Lightning.

Laura Shin:

And so, do you imagine that eventually that Lightning will be kind of how people end up using their node more often because I don't really know…?

Jeremy Welch:

Well, that's how it is today.

Laura Shin:

If I…yeah, what would…

Jeremy Welch:

Yeah, the majority of it today is all that.

Laura Shin:

Yeah, what would people use their node for, I don't get?

Jeremy Welch:

Yeah, I would say 90 percent, 90 percent is Lightning, 95 percent. The way to think about the Casa Node is…

Laura Shin:

But where can they use that because there's not many places, right, where you can use Lightning?

Jeremy Welch:

No, there's a…so, first off, people, there's a…I forget exactly what the hashtag is, it's like #**Intrustnetwork** or something, there's a hashtag where people have started a chain. It's almost like a chain letter group, right, but they're sending Lightning transactions to each other just to create this chain of transactions, so there is this kind of like community experience surrounding engaging with your friends in the broader community and sending things around, so that's one. That's a very base level of I'm going to connect with my buddy, he's got one at his house, I've got one at his house, we're going to send transactions back and forth just for fun, just to be a part of the Lightning network, right, that's one.

Two is that there are these applications. There's Satoshi's Place to where you can go and you can draw on this page, and you pay for it in Lightning. There's like a spinner application. There's now a tipping application, tippin.me. You know, people are building more and more applications, and I think that you know where this goes is that we could see applications emerge to where you do go, you know instead of upvoting someone on a comment thread with just a single vote, you're actually upvoting them with a satoshi, right, you could see a Reddit being rebuilt not on top of some other coin, but on top of Lightning and on top of Bitcoin to where you're actually upvoting and being able to send satoshi's, as you know some mechanism, and I think Y'all actually is allowing some of this in terms of payments to just read articles today, so there are a variety of applications now. It's still a small set, we're still in early days of this whole network, but I think 2019 is going to see a lot there, and our end goal with the Casa Node is you know we describe Casa's kind of end implementation setup as a node in every home and a key manager in every pocket. We want to get to a world to where the internet is rebuilt around nodes and around validation and a more personal controlled data, and also around better key management, and you know those two things in combination, we can rebuild a lot of applications and services, and so this is just the beginning in terms of your Bitcoin and Lightning are most important, but we are envisioning a lot more applications and a lot more ways to use those devices now that they're in the home, and we'll be announcing, making a bunch more announcements throughout the rest of the year for that.

Laura Shin:

Yeah. **Well, that's what I was going to ask you because I guess, like right now, it sort of feels like you're targeting these small niches, right, the people that have half-a-million dollars or more of cryptocurrency, the people that want to transact in Lightning using their own node at this very small number of places, but it sounds like your vision is that in the future, this behavior will be more mainstream, is that what you're saying, that having your setup…?**

Jeremy Welch:

Yeah, 100 percent.

Laura Shin:

Oh, interesting.

Jeremy Welch:

100 percent, and I would liken it to, I mean, in the early days of the internet, you had 28.8 modems and dialups, and people weren't even dialing up through ISPs, they were just dialing to each other and dialing into message boards and sending messages around in the early days of the internet, and somehow we got to a Facebook and Google and you know this massive applications-based world where people write entire documents and watch videos and watch TV and all of this data is streaming over the same network, and a lot of it's advertising built, but the incentives around Bitcoin and Lightning and these other based systems, we can rebuild a lot of internet architecture and a lot of application architecture around these instead of around the advertising-based systems that we've seen before, and so that's where we see the market going, and again, it's still early days, we're not proposing that these devices built today are ready for the kind of common person, but the Casa Node is built, if you want to try Lightning and if you want to try these early technologies. It is built for average people to get, to plug into the wall, and to just get up and running, so we do have, we're working on a lot more, I can't share all of the details there, but what I will say is that we are turning Casa into a sovereign experience at every price level, and we want to make that easier and easier for people, so it's not just about Bitcoin and Lightning, it's about broader applications but about this ability to kind of opt out and to kind of take more control of your data and take more control of your kind of computing life more broadly, and so over 2019, we'll be launching a lot more around that with multiple price points and multiple support points and multiple products that kind of fit into this sovereign experience.

Laura Shin:

All right, well, we'll see if you guys are able to capitalize on this sort of sentiment that's going against the current model, the internet. I don't know, I could see it going either way. There's momentum against right now, but also there's a lot of…what's the word I'm looking for, the opposite of momentum, but…oh, inertia where people are just lazy and willing to sign away their privacy. All right, so I have so many more questions I didn't get to ask you, but I was going to ask you is it okay if I just email you a few and then maybe you could write them up, and I can publish them on the website?

Jeremy Welch:

Yeah. Sure.

Laura Shin:

It won't be a ton, but yeah, I'll just try to be selective because we didn't get to everything.

Jeremy Welch:

Yeah, no problem.

Laura Shin:

But in the meantime, where can people learn more about you and Casa?

Jeremy Welch:

Sure. So, you can go to keys.casa, is the primary website. If you want to buy a node right now, you go to store.casa, and you can buy the Lightning Node today. You can also apply, again, for the key management service. Keep your eyes peeled even in the next few weeks, we have a lot more coming and excited to announce. The team has been working insanely hard. We've got a little bit bigger team than most people realize, you know we've got Alena and Jameson Lopp and a few others, just the team is amazing, so we've been grinding away, and I'm excited to release some of our new stuff in 2019 and kind of see what the world thinks.

Laura Shin:

Yeah. Actually, one of the questions I'll ask you to put on the website is about your team because I do think they have interesting backgrounds. All right, well, thank you so much for coming on Unchained.

Jeremy Welch:

Of course. Thank you, Laura, for having me.

Laura Shin:

Thanks so much for joining us today. To learn more about Jeremy and Casa, checkout the show notes inside your podcast player. New episodes of Unchained come out every Tuesday. If you haven't already, rate, review, and subscribe on Apple podcasts. If you liked this episode, share it with your friends on Facebook, Twitter, or LinkedIn. If you're not yet subscribed to my weekly newsletter, go sign up right now on unchainedpodcast.com, and also, go check out my other podcast, Unconfirmed, if you haven't already. Unchained is produced by me, Laura Shin, with help from Raelene Gullapalli**,** Fractal Recording, Jennie Josephson, and Daniel Nuss. Thanks for listening.