EPISODE 652

[INTRODUCTION]

[0:00:00.3] JM: Cryptocurrency security is a concern to anyone who has a significant amount of money in the form of Bitcoin, Ethereum or other crypto assets. Most Bitcoin is held in either a Bitcoin wallet or a Bitcoin bank. Your Bitcoin holdings are recorded on a public ledger. You access these holdings by authenticating with your private key.

A Bitcoin wallet could be described more accurately as a Bitcoin key ring. Securing your Bitcoin wallet is about securing that private key, and just as there are many different ways to secure any individual piece of text, there are many ways to secure a Bitcoin private key.

A Bitcoin bank is a term that can be used to describe institutions such as Coinbase. Coinbase takes the technology of the Bitcoin wallet and wraps it in additional layers of security, identity and failover that we associate with the banks and large technology companies. By using a Bitcoin bank, you sacrifice the autonomy of managing your own private key. On the bright side, you don't have to manage your own private key, because private key management is annoying. But of course by giving up that private key management, you are giving up some autonomy. A Bitcoin bank gives you the downsides and the upsides of working with a centralized service provider.

Jameson Lopp is a cypherpunk and a cryptocurrency engineer at Casa. Jameson was previously on the show in another popular episode relating to cryptocurrencies. Casa, the company where he works, is a company that is building long-term cryptocurrency storage and secure key infrastructure.

In this episode we explore how Bitcoin wallets work, how to secure them, the common threats, the scams and the hacking attempts of Bitcoin and what he's working on at Casa.

I want to mention that I'm hiring for a new company that I'm starting and I can't talk about the product quite yet, but I just wanted to plug that before we get started with this episode. The product is not related to cryptocurrency at least right now, but I'm very excited about it and I'm looking for an engineer in the Bay Area with significant experience in React.js and either AWS or Google Cloud. You can email me at jeff@softwareengineeringdaily.com. You can also check out the job posting at softwareengineeringdaily.com/jobs.

[SPONSOR MESSAGE]

[0:02:39.0] JM: Azure Container Service simplifies the deployment, management and operations of Kubernetes. Eliminate the complicated planning and deployment of fully orchestrated containerized applications with Kubernetes. You can quickly provision clusters to be up and running in no time while simplifying your monitoring and cluster management through auto upgrades and a built-in operations console. Avoid being locked into any one vendor or resource. You can continue to work with the tools that you already know, such as Helm and move applications to any Kubernetes deployment.

Integrate with your choice of container registry, including Azure container registry. Also, quickly and efficiently scale to maximize your resource utilization without having to take your applications offline. Isolate your application from infrastructure failures and transparently scale the underlying infrastructure to meet growing demands, all while increasing the security, reliability and availability of critical business workloads with Azure.

To learn more about Azure Container Service and other Azure services as well as receive a free e-book by Brendan Burns, go to aka.ms/sedaily. Brendan Burns is the creator of Kubernetes and his e-book is about some of the distributed systems design lessons that he has learned building Kubernetes. That e-book is available at aka.ms/sedaily.

[INTERVIEW]

[0:04:14.5] JM: Jameson Lopp, you are a professional cypherpunk and an engineer at Casa, which is a platform aimed at cryptocurrency holders. Welcome back to Software Engineering Daily.

[0:04:25.7] JL: Great to be back.

[0:04:27.5] JM: I want to talk to you today about cryptocurrency security, specifically wallet security. Let's start with the discussion of wallets. What is a Bitcoin wallet and why does a Bitcoin holder need one?

[0:04:40.6] JL: Well, a wallet is not the best name thing. It's probably better to call one of these things a key ring, or a key management service. But basically what you're doing is you're creating software that helps you manage both the private keys that unlock your crypto assets, allow you to spend them, and allows you to manage other aspects of your actual money. So in Bitcoin, that basically means managing the unspent transaction outputs, which are the real "Bitcoin".

[0:05:14.4] JM: Those unspent transaction outputs, are they held in the wallet or are these publicly accessible? Let's just do a little bit of review on the interaction between a Bitcoin wallet and the public ledger.

[0:05:28.5] JL: Yeah. So the UTXOs are basically the database of currently available spendable Bitcoins that you get from parsing the blockchain itself and looking at the entire history of the blockchain. So the blockchain is just a series of inputs and outputs. Every transaction is spending some inputs and then it's creating new outputs. By following along the entire history from the very beginning, the Genesis block, we are able to delete the transaction outputs that get spent to create the new ones that the new transactions get created when they're creating the transaction and broadcasting out on to the network and then getting into the blockchain. Eventually we arrive at the current state.

So if you could actually think of transaction on the Bitcoin network as a state transition function, where you're consuming some transaction outputs and then creating new ones, and eventually we have the current state at the current tip of the blockchain.

[0:06:35.5] JM: When I initialize a Bitcoin wallet, what do I need to do?

[0:06:41.5] JL: Well, all you're really doing is creating those private keys. There're a lot of different ways to do that, but there is a standard now for what they call hierarchical deterministic wallets where you're really just creating this root master key pair and then you're deriving all of your public private keys from that master key pair. That is good for a number of reasons, but especially because it means that you only really need to back up that master key pair, and in fact there are other standards around that that allow you to just backup a 12 or 24-word seed phrase that is then used to derive the master key pair itself.

So when you create a new wallet, there's nothing in there except for some public and private keys, but of course there's not going to be any value in the wallet if you've never used that set of public and private keys before, because nothing will have been sent to those addresses.

[0:07:44.0] JM: So you do not need to scan the entire blockchain in that case and find all of the transactions that are associated with this wallet, because you know that it's unique.

[0:07:56.0] JL: Yeah, if this is the first time that you've ever used the wallet. Now if you are importing a seed phrase or a bunch of key pairs that are from a wallet that you use previously, then you will need to go back and do some sort of scanning so that you can pick up those unspent transaction outputs.

[0:08:12.7] JM: What you're describing there, if I'm already a Bitcoin user, I've got one wallet that I want to leave it home at all times and then maybe I’ve got another wallet that I can walk around with and use occasionally, and I want them to be copies of the same account structure. If I was setting up that new wallet that was a copy of the same address schema as the first wallet, what do I need to do in that case?

[0:08:42.8] JL: Well, in that case, what's going to happen is the wallet software is going to either, from the very beginning point in time, or in some cases you can tell it to only start from a certain date if you know when you first started using the wallet. But that wallet is then going to have to go out on to the network, or you could of course have it connect to your node. But it's going to have to connect to some full Bitcoin node somewhere out on the network and then start querying that node, and it'll basically walk through every block that has ever been put into the blockchain and it will send a query to the node saying, “Here is a sort of fuzzy filter, and I’m looking for any transactions that are related to any addresses that match this fuzzy filter. If anything matches, send it back to me and I’ll inspect those transactions more closely locally.”

So you can do this pretty quickly, because you can – This is actually called SPV, the simplified payment verification, which was actually described in the Satoshi whitepaper many years ago. By using the Merkel tree root that is in each block header, you can actually get a strong cryptographic proof from the node that specific transactions existed in specific blocks without having to download all of the transactions that ever happened.

Now, without getting too deep into the details, there are some privacy issues here. There are some potential censorship issues, but it works pretty well most of the time. Of course, there are a number of proposals out there to improve upon this and make it even more censorship resistant and more private.

[0:10:27.8] JM: Let's save the SPV versus full node discussion for a little bit later in the conversation.

[0:10:33.3] JL: Sure.

[0:10:33.8] JM: Focusing just on the wallets for now, what's the spec for hardware that I need? Can I just run this on my MacBook or on my phone? What are the requirements for secure Bitcoin wallet software?

[0:10:47.6] JL: Well, that is quite a broad question, and if you know anything about computer security, you know that nothing is really 100% secure. So what you really want to try to do is to minimize the attack surface of whatever wallet you're using. Of course, there's always going to be performance trade-offs and convenience trade-offs. So generally, the more secure your setup is, the less convenient it's going to be or possibly less performant.

So when it comes to running a wallet on your regular hardware, like a laptop, a desktop, a mobile phone, what have you, those are always going to have more potential attack vectors, because you're running a full-fledged operating system. There could be malware that gets on it. There’s just like a million different things that could go wrong and could result in you potentially losing your private keys to some attacker, or the attacker basically spoofing addresses, swapping them out when you're not looking and you accidentally end up sending money to an address that belongs to an attacker rather than your intended recipient.

So for the average user who has more than probably $1000 in crypto assets, I recommend going out and getting one of these hardware devices, whether it's a Ledger, Trezor, KeepKey, Coldcard, what have you, because those are going to give you basically the highest level of security that you can get while still having a pretty good user experience.

In fact, we’re building on that at my current company. Trying to merge the user experience you can get with like a mobile app wallet with the security that you can get with these hardware key management devices. Those devices, they’re generally more secure, because they’re custom-built hardware that does basically nothing except managing the private keys in a secure element and doing the transaction signing operations for various cryptocurrencies. So it's basically impossible to get malware and other bad things on to those devices, because they simply don't support other operations.

[0:13:01.7] JM: That is, unless there's some kind of supply chain interloper, one thing I saw it recently was that you have a store, the Casa store, where because you’re a dedicated security company, I think there's an argument to be made that it would be more secure to buy a Trezor wallet from your Casa store than from – I don’t know, eBay. You probably don't want to buy a Bitcoin wallet on eBay.

[0:13:30.2] JL: You probably don't want to buy one from a random person. Now, the types of attacks that we’re seeing when people buy a hardware wallet off of eBay or some other more peer-to-peer marketplace, it's not that those people are actually going and tampering with the hardware itself. It's usually much less sophisticated, where these people are buying a hardware device. They’re then opening it up and putting a wallet seed phrase on there that they know the seed phrase and then they're shipping it off to other people and basically giving them instructions telling them, “Oh, don’t reset the device. Just keep using the seed phrase. Here is your seed phrase.” Then of course they wait for someone to deposit money on it and then they steal it all.

Now, I'm not a hardware expert, but if you go on to like the Trezor and Ledger websites, you should be able to find more material where they actually have a number of tamper proof mechanisms built into the hardware itself that make it very, very difficult for someone to open up the hardware and tamper with it without the hardware itself noticing. It's like the firmware basically checks the integrity of the hardware every time the device turns on.

While, of course, anything is possible with enough resources, like I think if you go to some three letter agency that has like electron microscopes and all kinds of other equipment, they might be able to tamper with this type of stuff. But in general, you get a really, really high level of security that the device itself has not been tampered with.

[0:15:00.9] JM: This is the Bitcoin wallet that we have now thoroughly discussed. There's also a term that is commonly used, Bitcoin bank. I think this might be what you could describe Coinbase as. What is the stack for a Bitcoin bank? How does a Bitcoin bank account compared to a Bitcoin wallet?

[0:15:21.4] JL: Will, normally what we're talking about when we call something a bank, it's a large custodial service. And so they are managing Bitcoin and crypto assets for a large number of people. So that basically means they have to keep all of these private keys safe on behalf of others, and that means they're going to have much more sophisticated multilayer storage solutions.

When you're talking about Coinbase, for example, which last I heard, they probably are holding at least like 5% of all the Bitcoin is in existence. You can go on to their engineering blog, and they have a post from a year or two ago where they talk about some of the security mechanisms they use. That basically means that the vast majority of these private keys are going to be held off-line in a highly secure default where you have to have multiple humans that are going in at the same time to open up the vault and get into it, and it's basically this huge Faraday Cage with air-gapped computers on it. Whenever they want to send money from this cold storage into their hot wallets, then it's a very long convoluted process that has many, many checks and balances to ensure that their safe not only from hackers and external threats, but even from insiders who might be incentivized to try to steal the private keys and jet off to some non-extradition country.

[0:16:55.5] JM: In this description, you've outlined a difference between cold storage and hot storage, and you've given it some examples. I know cold storage and hot storage are extreme characterizations that there's actually a lot of granularity between what is cold and what is hot storage. Can you describe the types of accounts that would be classified as cold storage or hot storage and what falls in between?

[0:17:21.7] JL: Yeah. So generally when we say cold and hot, we’re basically saying it's connected to the internet or it's not connected to the internet. Obviously, when you disconnect the device from the internet, you are creating this moat or this air gap so that hackers cannot get to it. That's the safest you can possibly be from hackers, is just pull the plug.

Now when people think of cold storage, they usually think of a paper wallet. I actually don't recommend that the people use paper wallets unless they're extremely advanced, because there're so many things that can go wrong with them. But I generally say that a hardware key management device is cold storage, because the device itself, while you still plug it in to a computer or even a phone in some cases, the way that these devices are set up is that the private keys can never actually leave the device. Even though there is a cable connecting the device to another computer, the data that is transmitted between that cable is very limited and the keys never get transmitted off the device.

So the other side of things, of course, is a hot wallet, where you actually have these private keys on a machine that is either constantly connected to the internet or sometimes connected to the internet, but it's just a piece of software that is managing the private keys on a general-purpose computer. The problem that you have there is that even though a good wallet is going to keep those keys encrypted in a file on disk at rest, at some point in time you're going to have to access those private keys. You’re going to have to decrypt that blob of data in order to be able to sign a transaction with it.

Even if that's only for a matter of milliseconds, if there are some malware or something else sitting on the computer waiting for you to do that, then it can swipe your private keys and steal all of your crypto assets, and that's the primary problem that we run into with hot wallets, and that's why exchanges get hacked all the time, is because they have to be running hot wallets in order to be able to do automated withdrawals.

[SPONSOR MESSAGE]

[0:19:51.7] JM: Failure is unpredictable. You don't know when your system will break, but you know it will happen. Gremlin prepares for these outages. Gremlin provides resilience as a service using chaos engineering techniques pioneered at Netflix and Amazon. Prepare your team for disaster by proactively testing failure scenarios.

Max out CPU, blackhole or slow down network traffic to a dependency, terminate processes and hosts. Each of these shows how your system reacts allowing you to harden things before a production incident. Check out Gremlin and get a free demo by going to gremlin.com/sedaily. That's gremlin.com/sedaily to gear free demo of how Gremlin can help you prepare with resilience as a service.

[INTERVIEW CONTINUED]

[0:20:51.0] JM: Do you have prescriptive or proscriptive protocols for who should have what kinds of wallets? Because I assume somebody who’s completely unsophisticated with cryptocurrency, you would recommend one type of wallet set up for them versus somebody who is a security expert, and there's probably also the dimension of how much you are storing. What percentage of your net worth you’re storing. What the different combinations of wallets and configurations that you recommend for different types of people?

[0:21:24.1] JL: Yeah, I've written about this a little bit. In general, I kind of broke it down into like three different categories that probably require different levels of paranoia. So your very entry-level category is just spending money, hundred dollars, a couple of hundred dollars, basically, whatever level of cash that you might normally be walking around with in your pocket. That is an amount that would be fine to just keep on a regular hot wallet on your mobile phone or any other device, because it's probably not going to ruin your life if something happens and you lose that.

Now, the next level of storage when you start getting more intermediate level is more like a small investment. So if we’re talking about like a month salary or more, getting into the thousands of dollars range, then that's when it starts to make sense to invest 50 or $100 into one of these hardware devices, and that's going to give you the best security without having a huge investment of time or money.

But then the third level is when we start talking about like life changing amounts of money, like hundreds of thousands, or millions of dollars’ worth your crypto assets, and that's when you're probably going to want to devote more time and resources and money into a more complex and more redundant system, because you're going be worrying about not only loss due to hackers and external attackers, but even more commonly, most of the loss seems to happen just due to user ignorance or negligence. Not having sufficient level of redundancy and robustness against any type of natural disasters.

So that's really the type of level wallet that I've been working on this year with Casa, and we think that there's a pretty big niche for that where a lot of people started out with that first or second level, and then as these bubbles keep happening in cryptocurrency, they wake up one day and now they have a level of wealth that they never thought they would have to worry about managing before.

[0:23:39.3] JM: So what are some of the – I want to ask about the scams and the thefts and stuff, but maybe we should first cover the user level incompetency. What kinds of mistakes do people make? Particular, you already mentioned paper wallets, and obviously with the paper wallet you could just lose the paper wallet or spill water on it. You can have a computer hard drive where you've got your private keys stored somewhere and then you accidentally lose the computer. We’ve heard many stories about that. What are the common scenarios where people just make mistakes?

[0:24:10.5] JL: Yeah. I mean, I think it’s usually someone either not creating a backup in the first place, and they’re just running a hot wallet on a computer and then there's some sort of hardware failure, or they have one backup somewhere and something happens to that. So like we've even heard there was a really good story. I think it was a wired journalist or someone a year or so ago where he had a backup of his seed phrase, but it was just like written on a piece of paper in his desk, and apparently the maid came through and thought it was a scrap piece of paper and threw it out.

So it's usually just not having good IT practices and not having multiple off-site redundant backups. Then even if you do have good backup practices, then a lot of times people won't actually test them. So they might have some flaw in their backup and recovery mechanism where, sure, they have backups, but then when something happens and they go to try to recover it, they find that flaw and now it's too late.

So we're trying to think through all of these different possible failure scenarios, because I think most people just think about, "Oh! My house might burn down, or there might be a flood or something. So all I really need is one of those metal storage devices where I attach the seed into that." I think those are good against a lot of common threats, but I actually have a stress test blog post that I wrote recently where I show that there are a number of things that can go wrong that can even make those metal devices sufficiently unreadable even if the metal itself isn't completely destroyed.

Then even more recently, we've been hearing things of, for example, bank safety deposit boxes getting opened and thrown out without the owner necessarily even knowing what's going on. So I think there's also a lot of people who are just putting their single backup recovery phrase into a bank safety deposit box and not thinking that, "Oh! There are actually potential failure scenarios for that as well."

[0:26:23.4] JM: And the scams, the Bitcoing thefts scenarios, the tricks that people can wage against each other. We've seen so many of these over the years. What are the most common types of scams and Bitcoin thefts scenarios that you've seen?

[0:26:40.6] JL: Well, the most pervasive right, and I don't know how successful they are, but there sure are a lot of them on twitter with the various giveaway scams. I think that's the getting some of the more naïve folks to send their money off thinking that they're going to get more money back as a result.

There's also a lot of exit scams from seemingly legitimate businesses, and this is why having a long history and reputation is also pretty important. If you're going off and using some exchange or other service that's only existed for a few days or weeks, then you never know. They might just amass a lot of deposits and then disappear often to the ether.

But in general, you just have to go with your gut of, "If this sounds too good to be true, it probably is." There's just such a much higher reward for scammers in the crypto space, because these are bearer assets. So once you send them, there's no way to call them back. So I think that's why more and more scammers keep flooding into the space.

[0:27:45.6] JM: Okay, let's start to talk about how to build a more secure wallet and money management system since that's what you're focused on at Casa. So when Casa was getting started, what were the predominant mechanisms for storing cryptocurrency and what made you think that there were some gap and there were some set of remedies that you could provide that would be a sweet spot in terms of security?

[0:28:16.5] JL: Well, over the past few years, these hardware wallets have become more popular, but we were just hearing a lot of horror stories of people having millions and millions of dollars on this one single device that even though it's incredibly secure against various types of attacks against the device itself, just the fact that you have a single device creates, of course, a single point of failure. We kind of came to the conclusion that there is a bit of a usability flaw even with these high security devices, because if you buy one of them, the first thing that it's going to do this is it's going to display this 12 or 24-word recovery phrase to you and then it just says, “Keep this in a safe place.”

While that seems simple enough, it's actually a huge ask, I think, of average person to understand all of the ramifications of security and like good IT practices of keeping 12 words safe against all kinds of different possible loss scenarios, and loss of course doesn't necessarily mean attack and loss to some other person. It can just mean data loss that makes the thing unrecoverable.

So what we found when we started asking around, is that there were a lot of OG crypto folks out there who were just petrified to be responsible for storing their private keys. So a lot of them were just leaving them with custodians, because they have this thought process of, “Well, if I leave all my Bitcoin at Coinbase or some other exchange that's pretty reputable, then they might actually be more safe there, because there's whole teams of people that are devoted to the security of the cold storage that is being managed by these companies.” I think that's a pretty logical line of thinking for yourself that very well may be more secure and more robust against certain failure scenarios. But of course, it kind of goes against the whole ethos of the system, because now you're just creating more single points of failure where we’re now putting billions and billions of dollars into these Bitcoin banks and that is creating systemic risk.

So we wanted to try to kind of pushback against this centralization of this aspect of the ecosystem and make it easier for people to be their own banks and still be able to sleep at night without having to spend large portion of their life actually thinking and worrying about all of the stuff that's required to be a good bank.

[0:30:59.9] JM: To the point of centralization – Let's talk about centralization for a little bit. This is slightly off-topic, but I heard recently that Bitmain, which is the company that mines most of the Bitcoin in the world, I think they control at least enough hash power to have a 51% attack if they wanted to. Is that problematic? Is that a fundamentally problematic to the health of Bitcoin?

[0:31:28.4] JL: Yeah. I mean, it's hard to actually measure their level of hash power, because they have all of these other business connections. Now, they definitely build the vast majority of the machines with the hash power as to who controls the specific machines. It gets a bit murkier. But it's not good in the first place. I mean, it's not optimal. It would certainly be better if we had like four, five, six or more companies that are actually producing these ASICs and then distributing them more widely than they are distributed at the moment.

Now, the main thing when it comes to 51% attack is you kind of get into the game theory behind it, is that I'm not worried that Bitmain itself will try to do 51% attack the network, because they would be shooting themselves in the foot. They would cause such a massive loss of confidence in Bitcoin if that happened, that the price would plummet and however many billions of dollars’ worth of Bitcoins that Bitmain has, and of course their probably future revenue would be severely impacted.

Now, it is more concerning from the fact that, well, this is a single company and they could then become a target of nationstate, and some nationstate might come in and seize all of their operations and then say, “Okay. Well, we want to try to kill Bitcoin now. So were going to put a gun to your head and force you to 51% attack the network.” Of course, it's hard to kind of put a level of risk on what that scenario might actually be, but we don't want that to be possible if at all.

[0:33:09.5] JM: If that occurred, you probably run this scenario out in your head a couple of times. Would there just be a fork and Bitcoin would figure out how to deal with it?

[0:33:19.5] JL: Yeah, and this is kind of the fundamental strength of Bitcoin, is that while we have this this great machine consensus protocol that is automating the consensus of the current state of the network, if that fails, and it has failed a few times in the past, then you have a layer of consensus below that, which is the human consensus. So if machine consensus start screwing up, if the network ceases to operate, then all of the major players on the network and really anyone who's paying attention and cares enough is going to start conversing and saying, "This is bad. We need to fix it. What's the best way to fix it?"

So if, for example, there were some 51% attack that was ongoing and it looked like there was no reason to believe it was going to stop, then you would see people come together and say, "Okay, what protocol change needs to be made in order to stop this attack?" The extreme example, of course, would be a proof of work algorithm change, which would make all of those ASIC essentially worthless.

[0:34:30.8] JM: Thanks for describing that and going there with me. One reason I took that slight deviation is because there are some people who listen to the show that are still not completely convinced that Bitcoin is a thing worth paying attention to. So I like to occasionally revisit some fundamentals, particularly the kind of thing that you just described, which is essentially a really strong durability guarantee of the network, which makes it so beautiful. I hesitate to use the word indestructible, but it's hard to imagine something that will destroy it at this point. I mean, you've had the best security experts in the world try to think of a way to destroy this thing or to disrupt it forever, and I haven't heard one yet. So it's pretty strong durability guarantees.

[0:35:22.6] JL: Yeah. Well, I mean, it kind of goes back to the cypherpunk manifesto and some of the ideas around what they were doing. If you read that manifesto, I believe there is one section that says, "We believe that sufficiently, like widely distributed software cannot be stopped."

So this system, while it does have its points of centralization that could be used to attack, it’s fundamentally driven by all of the humans who are interested enough in maintaining and improving the system, and those people are so distributed around the world, and this is why I’ve been doing so much global travel over the past few years, is because they’re in jurisdictions that are very diverse and composed of individuals with wide diversity of perspectives.

So it's just the issue of like there's not enough people or attackers out there who can kick down all of the doors of all of the people who are helping to maintain this network. It's too distributed. It's like trying to attack a swarm.

[0:36:28.0] JM: I love it. By the way, I’m hearing some occasional like kind of the networky blips or recording blips. Is there like a fan or any kind of – Anything that could be causing some slight network disturbance on your end, or microphone disturbance?

[0:36:44.1] JL: I’ve got the fans turned off. Though, if anything, you never know what the VPN might be doing.

[0:36:49.5] JM: Coming back to the discussion of Bitcoin bank centralization, now that we have absolved ourselves of the question of Bitcoin centralization globally. You've described some fallibilities of the Bitcoin bank model as it exists in something like Coinbase, and Coinbase is a paragon of the community. I love Coinbase. I’ve done several shows about it. I have used Coinbase in the past. But we can agree that there is some centralization. It's a victim of its own success essentially.

You look at that and you see something, you see an opportunity, perhaps a more decentralized Coinbase model is what I'm hearing you kind of allude to. What's the solution there? What's the way to build a coin base like entity where you have security guarantees that are in some sense associated with the reputation of this large organization, but you don't have the failure scenarios inherent in a large organization?

[0:37:53.7] JL: Well, this is one of the reasons why I am so excited about the developments in the decentralized exchange space. So there are already a few decentralized exchanges out there like Bisk. But these are basically software that are creating their own peer-to-peer network and creating order books and allowing you to find other people that you trade with directly.

So this, once again, means that you're taking on a little more risk and responsibility yourself, because you're having to manage the private keys and run the software. But it means that we’re no longer creating these large honeypots with enormous amounts of value where an attacker only has to get in to one door in order to sweep up a lot of money and harm a lot of people.

So by further distributing that value around, and once again like creating more doors that attackers have to get through, then it's decreasing the systemic risk in the system. But of course right now, the software is a bit clunkier . It's not going to be as user-friendly and it's probably going to be a number of years before that type of software is able to compete on the usability front with something as centralize as Coinbase.

[0:39:15.7] JM: So does this relate to what you're building at Casa, or do you see this is a different question?

[0:39:20.8] JL: Well, with regard to exchanges, it's definitely different. Now, the thing is Coinbase is both an exchange and a wallet. So they're kind of doing multiple things. At Casa, we’re more focused on this secure store of value side, but there's definitely some overlap there, where we want people to be pulling their value out of third-party custodians who could make any number of mistakes or even be coerced by other larger entities that are more powerful and result in loss, but it's a multi-prong, I think, type of evolution that we see a lot of different teams working on a number of different projects in order to try to further decentralize the various aspects of the space.

[0:40:10.7] JM: So the problem that you are focused on specifically right now is long-term store value.

[0:40:16.7] JL: Correct.

[0:40:17.4] JM: Okay. Can you contrast how you're thinking about solving that problem with the solutions that we've already discussed so far?

[0:40:27.2] JL: Well, one of the big differences that if you want to take on the responsibility and be your own bank as it were in the crypto space, then right now you have a lot of education that you need to take on in order to do it correctly. What we're trying to do at Casa is to facilitate the technical side, but also provide a lot of support just on the human side where we are providing more of a boutique experience helping people set up and maintain the wallets themselves, but without us actually having control over more than one out of the five keys to their vault.

[0:41:14.1] JM: Okay. How far along are you in the development of the long-term storage software that you're building?

[0:41:22.8] JL: On the Bitcoin side, it is up and running and we've already onboarded a number of clients, and of course learning more as we do that every time we onboard something. We find little, small other thing that should probably be tweaked, and we're really focused on scaling up the onboarding and then scaling out towards supporting all of the other popular crypto assets that our clients are demanding to have the same level of security around.

[0:41:51.7] JM: What are some examples of design decisions and implementation decisions that you've tweaked over time with customer interactions?

[0:42:00.4] JL: Most of the is going to come down to figuring out like the simplest way to describe a series of actions that they need to go through. So we're trying to shove as much of the technical complexities under the hood as possible, but there are times when a customer might hit an edge case where you need to give them a warning, or give them a choice, some sort of decision to make.

So instead of if they have a wallet that's full of dust, for example, instead of saying something like, "Oh, you have too many UTXO's and you're trying to send a value of this, and it's not possible to compute." Figuring out what a more human readable message could be so that they have an easier decision to make. So giving them some options of saying like, "Well, if you want to send this level of value, you may need to wait this many hours in order for your transaction to complete," type of thing.

[0:43:04.8] JM: By the way, when you say a wallet full of dust, you're talking about fractions of Bitcoin that are so low that they're beyond denomination of anything that would be of value in the real world?

[0:43:18.5] JL: Yes. So you can get in this both technical and economic edge cases when you're dealing with wallets. Actually, I wrote an article I think two years ago called The Challenge of Unspent Transaction Output Selection, and it's just all of these edge cases that users can get into because they don't understand what's going on over the hood and they can basically fill up a wallet with a lot of UTXO's, that in certain situations, if the fee market goes up to a certain point, you actually have to build in some logic that we've been calling economically unspendable transaction outputs, where you then need to figure out how to kind of guide the user in the right direction to help clean up their wallet without having to expose them to all of the complexities of what's actually going on inside of the wallet.

[SPONSOR MESSAGE]

Get your free $100 credit at do.co/sedaily, and thanks to DigitalOcean for being a sponsor. The cofounder of DigitalOcean, Moisey Uretsky, was one of the first people I interviewed, and his interview was really inspirational for me. So I've always thought of DigitalOcean as a pretty inspirational company. So thank you, DigitalOcean.

[INTERVIEW CONTINUED]

[0:46:31.2] JM: So since you are building wallet management software, there are these trade-offs that you need to make between how easy you make it for somebody to transact with that money versus keeping it secure, because, for example, if you expose the user to some vulnerability through two factor authentication of a cellphone provider, that makes them vulnerable to a cellphone takeover attack. Then that might be more convenient than something that is a more stringent security protocol, such as perhaps Google authenticator. It's not a great example, because Google authenticator is just about as convenient as going through a cellphone-based transaction provider, but I think the thrust of my point stands. You've got these trade-offs between security and convenience that you've discussed a little bit earlier. Tell me where you're trying to play in that set of trade-offs, or what's what are some specific trade-offs in that security versus convenience that you've made.

[0:47:42.0] JL: Well, we're definitely prioritizing security, because if you fail on the security front, there is no going back. The general mantra that we have is the it's better for the user to lose access to their wallet for some period of time than it is for an attacker to gain access for even a few milliseconds.

So there certainly are situations where a user might trip over some security alert that causes their wallet to become unusable for a little while, or they might misplace some of their hardware devices and then require Casa assisted recovery, for example, and that process could take hours or days to actually go through.

But we think that the trade-offs there, when we're talking about vault type products that are potentially this person's life savings that usually you don't need to access your life savings on a very short notice. So that's an acceptable level of inconvenience.

[0:48:50.4] JM: I want to revisit the discussion of SPV's and full nodes. I'm not sure if it relates to product that you're building Casa. Does the decision to validate or build a wallet through an SPV versus a full node, does that impact your customers at all, or does that impact you, or do you think of this as just a completely disjoint concern?

[0:49:14.7] JL: It is all related. So one of our primary tenants, I guess, at Casa is to help maximize user sovereignty and safety. So far we've mostly been talking about safety, but the sovereignty aspect is important and that definitely comes in when we're talking about running a full node, validating that the money received is in fact abiding the rules of the network that you are agreeing to. It also comes down to trying to minimize the trust between the user and our own service.

So right now, by any number of measures, Casa itself is fairly centralized, but we're going to continue to work on pushing as much of the security and trust out to the edges so that the clients themselves are performing more of the validation and not relying upon any data that Casa servers are giving to them in response to a query. So that's more of a medium to long term vision, but it's definitely all related.

[0:50:26.8] JM: Speaking more generally for people who are managing their own wallets or they have different solutions for managing their currencies than Casa, how should they think about SPV's and full nodes? Why do you have some strong opinions about the costs of using SPV's?

[0:50:50.1] JL: So the trade-offs of using the simplified payment verification is that you are making an assumption that a blockchain with the most hash power is the correct blockchain, and a lot of people are fine with that assumption, and it works well in the vast majority of cases. But there are a ton of things that miners could do, for example, to start creating a blockchain that does really screwy things, but still has the most hash power.

So one of the reasons I'm not a fan of that, is because I don't think that we should be trusting the miners. They have a job, which is to basically timestamp transactions as part of the global consensus, but I think that the onus is on the rest of us to provide checks and balances and make sure that we’re not trusting them to be doing that job. We should be verifying all of the work that they're doing.

There's also some major privacy issues where I believe Matt Corallo and Jonas Nick have shown that the bloom filter mechanisms that get used by SPV, they were originally thought to be fairly private. But over the years, we’ve come to determine that they’re actually not. They’re terrible at privacy, and it's very easy for someone who's running nodes out on the network if they wanted to actually figure out which addresses belong to you by inspecting those bloom filters.

Once again, it comes down to this convenience. It's really easy to start up the wallet on your desktop or your mobile device and the SPV consumes very few resources on the client side and it's pretty fast to get synced with the network, but you are making these privacy and security in a way trade-offs. So that's why there are some improvement proposals out there for better client-side filtering, where believe it was Olaoluwa, roasbeef, has this mechanism that he has proposed, where the client would basically be downloading the data, but filtering it locally so that no one actually knows what data you're interested then, which should give you more privacy on that standpoint.

[0:53:18.2] JM: Let's talk more about Casa and building a business around cryptocurrency. I have a number of questions about security. So Casa has, I'm guessing – What? 10 or 15 engineers? How big is the company at this point?

[0:53:36.5] JL: Yeah. We’ve got around a dozen or so employees.

[0:53:39.2] JM: So that’s a big organization – I mean, it's a sizeable organization. It's not tremendously big. When you have your security product set up, your cryptocurrency provenance product set up, do you get it routinely audited by external security people? Do you get it audited by people who can help you understand that you’re secure against natural disasters, for example, the tail risk questions? How do you make sure that your cryptocurrency holding product is resilient beyond all of the tail scenarios?

[0:54:20.9] JL: Absolutely. So yeah, we get regular external third-party audits of our whole code base and infrastructure. The trickier thing though is when we’re talking about the robustness of like any given client’s wallet, is that because we are giving more sovereignty and more control to the user, we can't force them to follow best practices. We can certainly advise them and try to build features into the software itself to try to guide them in the right direction.

For example, when you create a wallet with Casa, it's going to create one key pair on your phone that gets secured by Apple’s, like secure element key ring encryption functionality, and then it will create one key pair that are kept off-line by Casa for disaster recovery, but then you're going to have three different hardware key management devices, so Trezors and Ledgers, that you have purchased and then initialize and set up. So it’s a three out of five MultiSix solution.

Now, obviously, the point here is that you want the wallet to be multi-sig, requiring multiple signatures in order to spend from the wallet. You want to be multi-device with preferably diversely of different devices to once again prevent single points of failure. Then one of the most important things for redundancy is you want it to be multi-location. You want these keys and devices to all be geographically spread out.

While we’re certainly going to tell this to our clients, we can't force them not to keep all of their hardware devices in a drawer in their desk at their office or at their house or something, and that's just like one of the trade-offs that comes with giving more control and more responsibility to the end-user.

[0:56:21.9] JM: Tell me about the product roadmap for Casa. Let's say you get this cryptocurrency holding problem solved to a great degree, where you’re just getting lots and lots of customer balances that are putting their money into long-term storage. What's the next product that you build and what are the guiding principles for the longer-term product development strategy?

[0:56:47.4] JL: Will, the extremely high level of you from Casa is that we want to be the best personal key system that is available for people. So right now, of course, that means crypto assets. But we believe that if the world keeps going in the direction that it is, where it becomes less about having centralized authentication and identity and more about having your own public-private key pairs that prove that you should be able to access certain things, that having robust key management solution is going to be important not only for your financial life, but for many other aspects of your daily life.

So we want to continue building out a secure but usable key management software. So obviously we’re going to be supporting any of the popular crypto assets that our clients want to support, but we think that long term it's going to go a lot further than that. I think the one way to make this more clear is if you actually know the history of Casa, and Casa, the guys who really started working on what became Casa were originally about a year and a half ago working on a block stack app called BedKin, and it was basically a decentralized Airbnb on the block stack platform. They had started working on this for a few months and eventually realized that there was no really good key management solution and they weren't sure how they were going to get people to use this app if they weren’t going to be able to easily secure and manage the keys to control access to the app itself.

So that's where they pivoted and they decided to go a layer deeper into the problem as it were, and then perhaps someday be able to pop out and start building and facilitating other things that are using this type of distributed infrastructure. But that is kind of the high level vision of – You could call it crypto anarchy if you will, building many, many different things on a more distributed platform that requires public-private key cryptography to use on a day-to-day basis.

[0:59:01.7] JM: There's a product called Keybase that we've done several different shows on, and I feel like Keybase was pretty prescient in realizing that key management is going to be something that consumers are going to have to deal with, and it's an open question as to what level of technical detail the consumer is going to want to get into. What you think of the Keybase solution? How does that compare to your ultimate vision of what Casa would provide with key management?

[0:59:31.3] JL: I do like Keybase, especially just from the way that they have that key tree, where you can authenticate new devices and new account and they're basically signed off by your existing keys to add them in. I think that that type of thing is great in terms of the flexibility of having sort of a digital cryptographic identity. I guess the only thing is I'm not sure that Keybase is supporting any hardware specific key managers. It seems to be all in the software right now. So still somewhat vulnerable from that standpoint.

[1:00:09.6] JM: Okay. Do you see yourself becoming something like a bank in some regard? Because if you have all these balances that customers are depositing with you, do you see that is something to be lent against?

[1:00:24.4] JL: I don't know that we would have that type of financial service, because we’re not custodial. so we don't actually have control of the asset. Now, there are a number of services out there, like Unchained Capital, or BlockFi, or SALT or what have you, where you can do these crypto backed loans, and I've of actually used them myself, and they work pretty well. But I don't think it would be possible for Casa do that, because we wouldn't have the ability to actually like freeze someone's money and prevent them from taking it away if they were trying to back some other loan or service with their assets. I don't think that Casa wants to be responsible for actually custodying any of these assets need. You get into a whole new level of like regulations and issues with the traditional financial industry when you start custodying assets. So that's the nice thing of spending three years working a BitGo and now working at Casa, is that while we are providing financial services, we are only really regulated from the sense that we are a software as a service company and it just gets rid of a lot of headaches.

[1:01:42.6] JM: And it might even make more sense for a company like that to be built on top of Casa. I would love if I'm using BlockFi, which by the way, I don't know anything about. That sounds like a company I should inspect more closely, and that other one you mentioned, I think Unchained Capital sounds interesting too, but those sound like companies that could use Casa. I mean, they probably don't want to have to build the security that you’re building.

[1:02:07.5] JL: Yup.

[1:02:08.7] JM: What other – I guess just to wrap up, what are the other platforms that you think could be built on top of a company like Casa? I mean, obviously, today it's more for individuals, but are there other services that you think people could build on top of Casa?

[1:02:25.0] JL: It’s tricky, because we really are more focused on individuals at least at this point in time. You can get more complicated if you start building like enterprise treasury management logic into the software. A better example of that is BitGo and the software that they have built, where there's a lot more permissioning and multiuser management around it.

It’s certainly possible for Casa to go into that direction, but for now we kind of figure there's already enough enterprise focused companies out there and not necessarily enough individual focused ones. So anything is possible, especially when you start talking about some of the more complex scripting operations that are going to get built into the Bitcoin protocol over the coming years.

We already have some ideas and stuff that we would like to implement around there to make the vaults themselves even more secure and robust. For now, I think we’re going to be busy enough just to trying to build user-friendly vault product. So where it goes from there, let's just say we have some ideas, but they won't be public for at least a few months.

[1:03:41.8] JM: Okay. Well, Jameson, thanks for coming back on the show and sharing your time. I really enjoyed talking to you.

[1:03:48.5] JL: Thanks for having me

[END OF INTERVIEW]

[1:03:53.1] JM: Cloud computing can get expensive. If you’re spending too much money on your cloud infrastructure, check out DoIt International. DoIt International helps startups optimize the cost of their workloads across Google Cloud and AWS so that the startups can spend more time building their new software and less time reducing their cost.

DoIt international helps clients optimize their costs, and if your cloud bill is over $10,000 per month, you can get a free cost optimization assessment by going to D-O-I-T-I-N-T-L.com/sedaily. That's a D-O-I-T-I-N-T-L.com/sedaily. This assessment will show you how you can save money on your cloud, and DoIt International is offering it to our listeners for free. They normally charge $5,000 for this assessment, but DoIt International is offering it free to listeners of the show with more than $10,000 in monthly spend. If you don't know whether or not you're spending $10,000, if your company is that big, there's a good chance you're spending $10,000. So maybe go ask somebody else in the finance department.

DoIt International is a company that's made up of experts in cloud engineering and optimization. They can help you run your infrastructure more efficiently by helping you use commitments, spot instances, rightsizing and unique purchasing techniques. This to me sounds extremely domain specific. So it makes sense to me from that perspective to hire a team of people who can help you figure out how to implement these techniques.

DoIt International can help you write more efficient code. They can help you build more efficient infrastructure. They also have their own custom software that they've written, which is a complete cost optimization platform for Google cloud, and that's available at reoptimize.io as a free service if you want check out what DoIT International is capable of building.

DoIt International art experts in cloud cost optimization, and if you're spending more than $10,000, you can get a free assessment by going to D-O-I-T-I-N-T-L.com/sedaily and see how much money you can save on your cloud deployment.

[END]