Introduction

Patrick: **[00:02:45] My guest today is Nick Neuman, CEO and co-founder of Casa. Casa helps Bitcoin investors and owners keep their digital assets safe from loss or theft by providing managed self custody services. In our discussion, we cover the history of asset custody, from ancient temples to decentralized ledgers, look at the mechanics of how private keys work, and explore why people are better off holding the keys themselves. We then dive deep into the future of digital wallets as gateways into our virtual lives, what's interesting about identity authentication more broadly, and whether these innovations may lead to unintended consequences. Please enjoy this great conversation with Nick Neuman.**

The History of Asset Custody

Patrick: **[00:03:23] So Nick, I think an interesting place to begin this discussion, where the theme will be private keys and custody of assets, and crypto maybe even more specifically, but generally those two big concepts, is with a history. I'd love you to just teach me and the audience as much as you can about at the history of how humans have owned and custodied different kinds of money. Because I think we're all in this fishbowl of, I have a Wells Fargo account or whatever. We've all grown up with one very specific version of this, but history can teach us a lot of lessons. Give us an opening history lesson here, and then we'll dive into all the aspects of Casa and what you're building.**

Nick: [00:03:57] Banking and money and where you store money has been this evolution over all of human history, basically, because you can go back thousands of years to a temple called the White Temple, which was this Uruk temple, which is located in the Middle East, modern day Middle East, and back then people didn't really have money. They just had belongings, which were things like livestock and grain. They were mostly farmers, and they wanted a place that they could put their valuables, their livestock, their grain, where they didn't have to worry about theft. And so one of the very first banks was actually this temple that let you put your livestock and grain in the temple. It was guarded by temple guards, but they also believed that the gods would protect their belongings. And so that was one of the very first banks that we know of. And then if you fast forward to about the 17th century or so, our money then at that point was mostly in the form of metal coins. So it was gold. Gold, silver, bronze, all these different denominations, and people were generally storing this themselves. So they were holding it in their house in a treasure chest. That day's form of self custody, you could call it.

But there's a real problem with this because of the nature of the metal coins themselves. So the metal coins, the gold was heavy, so it was very difficult to move it around. If you wanted to go to the market, you had to actually bring along a certain weight of gold and it had to get weighed by merchants. And it was just a pain to use. It wasn't very divisible. So to make it more divisible, you had to carry more coins. That increased that inconvenience problem. So what ended up happening was people said they didn't like having this in their house. It was kind of a theft problem. But they also really didn't like moving it and trying to use it for spending. So they went to this one group that was really good at storing gold, which were the goldsmiths. And so the goldsmiths were already holding a bunch of gold in their shops, and then their shops would have these vaults and they were making gold coins. Well, these goldsmiths said, okay, I'll hold your gold coins, and I'll give you this paper receipt that says you own this much gold with me. And so that was really the start of how paper money started to evolve today. And so people would actually, instead of taking their gold coins to the market, they'd take that paper receipt to the market and do that, hand that over to a merchant and then the merchant can go later, pay that with something else or go to a goldsmith later, et cetera.

Then a little bit later, fast forward a little bit, the Bank of Amsterdam was created as one of the first international banks and the big innovation that they had was internal transfers. So instead of having to even take your paper slip to go and give it to somebody and make sure that, hey, my goldsmith is reputable, he's not getting rid of my gold, you can trust me, the Bank of Amsterdam was so big that it had so many merchants as its customers, it actually just allowed them to do internal transfers on its books. That was a huge jump in terms of convenience for people using money. Initially, people were really keeping their money themselves and storing it themselves. But the reason that this banking system and deposit banking has evolved as we know it today is because people wanted the convenience factor. They wanted that capability to really easily use, transfer, and store their money. You fast forward another few hundred years, and that was the seed that has evolved into today's banking system.

Private Key Primer

Patrick: [00:07:55] It's an incredible history. A lot there that I didn't know. If we think of convenience as the lens through which to understand the job being done here, obviously we want security, but also ease of use. Those seem to be the two big things, from the temple guards and the gods through to the crossing within the Bank of Amsterdam, it seems pretty reliably that with your money, people are always going to want safety and convenience.

With those two things as a lens, I'd love you to now do something kind of similar for this concept of private keys. And anyone that's in the crypto world will probably know what this is. I'd love to just understand what the concept is in the first place. Why are we going back in time to something that might allow for a different kind of self custody and the potential unlock that private keys represents from a technology standpoint? But first, just tell us what they are. Teach us about literally the mechanics of how they came to be and how they're used.

Nick: [00:08:47] Sure. So maybe we could start with comparing Bitcoin to the current banking system. And the only comparison point I'll make here is that the current banking system feels very digital, but under the hood, it's still based on a very physical system. We've now built up some of these apps like Venmo and the Chase Bank app, name your banking app, where you can access your money digitally, but under the hood, the rails are still not really caught up to the digital native economy that we have today. So Bitcoin, on the other hand, is a natively digital currency. And so what's really interesting about this to me is that that convenience factor of being digital is really built in to Bitcoin from the start. The ledger's 24/7. It's instant settlement. There's some of these things that don't exist for banks. Exactly.

And so what enables this are really the foundation of the whole Bitcoin network is private keys. A private key, you can think of a good metaphor as a safety deposit box in the real world. So let's say you put some cash into a safety deposit box. Then you've got a key to that deposit box. In order to prove that you own that cash, or to use that cash, you have to take your key, unlock the box, and then you can take your cash out. A private key on Bitcoin works very similarly.

So your Bitcoin is stored on the Bitcoin blockchain by the ledger that everybody has. And then your key is what allows you to say, I own this Bitcoin, and it allows you to unlock the Bitcoin and send it to somebody else or to prove that you own it. So what a key actually is, is just a piece of data. A private key is a piece of data that has been cryptographically generated, and it basically in its raw form looks like a very long number. And so it can be used to protect any type of data by encrypting it. But what Satoshi, the founders of Bitcoin, realized, was that this could be used to protect and prove ownership over the data that is Bitcoin, the digital money that is Bitcoin. And so that key proves you own this Bitcoin, and it's kind of like your password to your Bitcoin. But there's something that is different about a private key from a normal password. So private keys have what I call the three Us. They are unique, they are unguessable, and they are un-forgeable. So unique.

This means basically, because that key was cryptographically generated and is so long, it is provable that you are the only person in the world who owns that key unless you give it to somebody else as well. So you have to willingly give it to somebody. Second is they're unguessable. Unguessable means because it's so long, a network of supercomputers would take millions of years to guess that key. And then the third is that they're un-forgeable. So what this means with regards to the Bitcoin network is that if I have a private key, you can't go to the rest of the Bitcoin network and fake your way through owning my key. These three things combine into this magical property of private keys that makes them an incredibly good form of authentication digitally. And that solves that huge problem of proving how much money you own to the rest of the Bitcoin ledger.

Patrick: **[00:12:21] Just a clarifying question there. So sometimes I think maybe I'm getting too in the weeds on the details here, but let's say I own one Bitcoin. I want to understand, so everyone understands out there, how is that one Bitcoin recorded in the Bitcoin ledger? And literally, what does stored mean? What is a wallet in this basic sense? And when I go to use my key, how am I literally using it? What software am I interacting with? Am I in a web browser? Where do I put**

that long string of characters? What does that do? The literal mechanics of it would be helpful.

Nick: [00:12:53] A lot of people think that your wallet actually holds your Bitcoin, and it doesn't. Your Bitcoin is just a output on a ledger that is known by every single node on the Bitcoin network. And so that says, somebody sent you X amount of Bitcoin and that's recorded, like in an accounting ledger, and then that is known by everybody. And that's the public key. So I could say there's one Bitcoin in this associated with this public key. Exactly. And the way that public and private keys work together is that they're connected in a way that you can know a public key, which is that public facing version of saying, I have this much Bitcoin, without knowing the private key. Without revealing that private key, I can show you that, yes, I own this public key. And that means that I own that Bitcoin. And so that's how it looks to the broader network, and your wallet actually just holds the private keys and the references to the public keys. And so when you're going to spend Bitcoin, as an example, you're taking your wallet, which is essentially saying to the network I am proving I own this private key and this public key. And I want to send this Bitcoin to this person.

So what that could look like is it could be a mobile app, like Casa's got a mobile app that you can do that with. It could be a web app. It could be a web browser extension, like a MetaMask or something like that. It comes in all these different forms of software, but all of the software, essentially the real purpose is for it to secure those keys and make them usable with the broader network.

Patrick: **[00:14:33] I've got one Bitcoin. I can prove that because I have the private key. And I want to send it to you. Then all I'm really doing is signing in quote unquote with my private key and addressing my Bitcoin to your public key and hitting send. Obviously, I'm simplifying here, but that's the basic concept. And then from that point forward, your private key governs that Bitcoin. And that's kind of the whole story.**

Nick: [00:14:56] And when you're hitting send, what's happening is every Bitcoin node on the network is checking that transaction, along with the Bitcoin miners as well. And so they're all saying, thousands of people are all saying, yes, I verify that you used to own this Bitcoin and now you've sent it to Nick. That's one of the magical things about Bitcoin, is you don't have to necessarily trust your bank or one central party not to mess this up because you've got thousands of people double checking each other on all of this.

Patrick: **[00:15:27] What's the next evolution, sticking with our points of safety and convenience, when thinking about private keys? So I get the unlock that comes from Bitcoin and crypto being digitally native and all the cool stuff that unlocks, the always on, the programmability, that seems kind of self-evident, but it seems like we're introducing something less convenient and maybe even potentially less safe. Because I don't hear a lot of friends getting their Bank of**

America account hacked or losing money, maybe hacked, but not losing money from Bank of America. So how do you think about private keys in a very simple way through the lenses of both convenience and safety, given that those are two things we've established are key to consumers and their money?

Nick: [00:16:10] Let's actually take a sec to dive in on that Bank of America example that you just gave, because it is correct that a lot of people do pretty regularly have their digital bank accounts hacked. And the reason they don't lose money is because let's actually take a credit card, for example, let's say your credit card gets hacked or stolen and somebody goes and spends a bunch of money on there. You're going to see that, and you're going to go and call your bank, and they're going to reverse all of those transactions. With Bitcoin, there's no reversing a transaction. Because of the way the network works, it's based on cryptography, it's a trustless network, there's no reversing. When you're looking at some of these businesses, a Coinbase, like an exchange, that are actually building the old banking system on top of Bitcoin, they will hold your keys for you. And all you've got to do is log in and tell them what to do with your Bitcoin. That's actually more of a vulnerability in the new world than it was on the legacy banking system. If you're leaving your keys with somebody else, you're not holding it yourself. That's v1.5 of banking.

It's almost skeuomorphic. Skeuomorphic was when the iPhone first came out, they had mobile apps that were designed to look like the physical world versions of their legacy predecessors, but they figured out once they actually let that go and left it behind, they were able to unlock a whole lot more use cases and really get to v2.0. So when you are using the native technology of Bitcoin and getting to that v2.0, you unlock more that you can participate in, with the network as a whole, but you also make yourself a lot safer. Back to an example, let's say somebody's letting Coinbase hold their keys. That makes the point of failure, your account login. So instead of it being the point of failure being the key itself, the point of failure is your login to your account. And we've actually seen over the last few weeks, a few different articles come out where thousands of people have had their coin base accounts hacked and had money stolen from those accounts. And because those transactions are irreversible, there's no getting that back. And you're just SOL. So what people have to realize is that with this new crypto economy and the new ecosystem, you're going to be a lot safer by holding the keys yourself, as long as you're doing that in the right way and with the right types of tools.

Patrick: **[00:18:49] So let's address, I think the most common objection that I've heard to this self custody concept, I'll call it peace of mind. So let's just stick with Bitcoin, obviously this applies to other stuff too, but you've got this crazy long string of characters and looks pretty hard to memorize. Maybe I get hit in the head or something and now I can't remember my thing, or it's on a piece of paper and the thing burns. All these stupid examples of, if you lose the key, for whatever reason, you forget it, you lose it, whatever, like you said, you're SOL. So how do we start to introduce the combination of private key self custody with more piece**

of mind so that if I screw something up, it's really convenient for me to not lose control of the wealth that I've built.

Nick: [00:19:30] You are exactly right, that this is the problem, when you are holding your own keys. You make one mistake and suddenly you've lost all your money and let's be real, people can barely keep track of their Facebook password, so how are they keep track of this private key, right? I mean, 4 million of the total 21 million Bitcoin has been lost. So that's 20% of Bitcoin's total supply. It's nuts. This is a really big problem. It's this trade off of with great power that comes with being your own bank and having that empowerment and permissionless capability to interact with the network comes the great responsibility of protecting that key. So this comes down to a few different things, but the biggest one is picking the right tools that help you manage your keys in a safe way, where you don't have to worry about losing a key and making a mistake resulting in you losing all of your money. And so my company, Casa, we realized this three years ago, this was going to be a huge problem. And we realized that something needed to be done that would give people more peace of mind in securing their own keys so that they can have that power and it's much easier to protect it.

So an example technology, which is what we've built on, but we can just talk about it more generally, is one that lets you actually have multiple keys protecting one pool of Bitcoin. And so what this means is you've got, in a traditional wallet, you've got one key, you lose that key, everything's gone. With this multi key setup, let's say you've got three keys and you only need two of them to actually spend your Bitcoin. This means you can lose one of those keys and still be able to access your Bitcoin without having to worry about loss or anything like that. Different setups like this can be built and abstracted a way to make it really simple for customers to use, to where they get that peace of mind, but they're still holding their keys. And it leaves them that room for being a human and making a mistake without losing all your money.

Patrick: **[00:21:39] So do you think that the way this ultimately feels is no different than having a Coinbase account or a Bank Of America account? What does it feel like? I want to really stress this, the idea of whether or not consumers will adopt this. Just even everything you just said, multiple keys, it's mounting intimidating in some sense. It sounds like a lot to manage and Coinbase seems like they've got a lot of money and they'll take care of me. I'm just kind of playing the fool here, but help me understand like what it will feel like to have your cake and eat it too, if this way of self custodying works, make it convenient and secure.**

Nick: [00:22:14] There's a few different approaches here, but what it comes down to is making something that feels very natural and very so simple for somebody to understand from a user experience side of things. But if you build that correctly to where the software is helping you do everything you need to do, and you've got a team of support people that are helping you do what you need to do here to get set up, that can really go a long way in terms of making people feel comfortable with this. It does sound complicated at first at. Casa, for example, what we hear over and over again is our customers will sign up, they'll say, "I was a little nervous about this. I've kept my Bitcoin on Coinbase, but I knew that I shouldn't do that anymore. Because it's grown to a significant value here. That's why I came to you guys."

They'll get set up and they'll say two things, "That was 10 times easier than I thought it would be." And, "I feel 10 times better about the security of my Bitcoin than I thought I would. It just feels like this weight has been lifted off my shoulders." And what's interesting is for some people there's even a little light bulb that goes off, which is this feeling where they're like, "Wow, I'm really my own bank. This is crazy. I am the only person that has control over my money now." And so there's this little bit of a cultural movement behind this, which helps people to really get this feeling like they're participating in something bigger. When it boils down to it, yes, taking your own security into your hands is going to take slightly more work than sticking it in Coinbase and just forgetting about it. But it's going to also be incredibly rewarding and that reward combined with a great user experience that makes it approachable is really the things that will help pull people through to the end.

Vision Questing

Patrick: [00:24:10] I'd love to talk about some vision questing of the future of all this. So I always just say for the sake of argument that this works because the UI, UX, whatever customer experience continues to get better, it just feels the same as what we're used to, a Bank Of America, a Coinbase account, whatever. And let's also assume that there's a bunch of blockchains and there's NFTs and there's all this stuff and I own all this stuff and I sell custody at all and I'm a walking bank and I feel secure and no one's holding a gun to my head or I guess it's the $5 wrench, is the classic example. And I don't feel like I'm going to lose my stuff and I'm the point of failure, I've got a partner, maybe it's Casa, maybe it's something else. Why is that a better or interesting state of the world relative to how we hold all of our stuff today?

So right now I've got a Schwab account. I've got a Bank Of America account. I've got all this stuff, I've got some stocks, I've got some bonds, actually I don't many bonds, but I've got some stocks, I've got some cash, I've got whatever, across a couple different places. And I've got some crypto. Why is this other version of the future of asset custody so interesting to you? What kinds of things do you think if we leave the skeuomorphic era of just trying to copy the bank experience, the centralized bank experience, why is this exciting? I want to understand this feature because if it is different and better, we should be interested in it as consumers.

Nick: [00:25:26] There's a lot of different answers to this question. But one that I've really been thinking about lately is that that world that you were just painting there of how you hold all of your different assets is very US centric. There's a lot of places around the world that don't have financial systems that are built up to this level. And if you back up to thinking about when America was founded, it was founded at a time when it was, relative to the rest of the world, one of the most open, it was the land of equal opportunities system, with allowing people to participate from a capitalist perspective, right?

Well, when you take that permissionless aspect of building a financial system like Bitcoin and you make it so anybody around the world can plug into it with zero permission and zero gatekeepers. That to me says that there will be an incredible amount of innovation that can be unlocked by simply enabling more and more of the world to participate in a financial system together where they couldn't do that before. And so that's something that is a little bit more of a vague answer to what you were just asking me, but it's something that if you look back historically and just look at all of the innovation that has come out of the US, because of our more open permissionless and accepting financial system and capitalist ecosystem that applying to people everywhere around the world is super interesting to me. And then I think that's one thing that if we do this right, we will see come out of this.

Patrick: [00:27:04] Might the first manifestation of that be what we're seeing with decentralized finance with DeFi. It seems to be moving at the speed of light. It's still very captive, meaning it's all within crypto. It doesn't seem to have a ton of crossover into non crypto world. Maybe it never needs to, but is that the right early green shoot to look at, just look how fast we're rebuilding core financial functions there, lending or whatever it might be, staking options, derivatives, so on. Is that probably the best early example of what you mean?

Nick: [00:27:36] When you look at what's going on in the crypto ecosystem with all of these different decentralized financial building blocks being built, what's really interesting is to see that these things are happening from completely different teams. And they're getting built on top of each other because it's all built on this open and permissionless network, because of that open and permissionless, it enables that innovation to just move much faster. And when you look at it today, you can take a skeptical view of it, which is, "Okay. A lot of these DeFi projects are less decentralized than they like to pretend they are." They look like toys. It's only within the crypto ecosystem today, but there's got to be some phase of that. Everything big starts out looking like a toy, as we experiment and learn and start to build things that can go beyond just speculation within the crypto ecosystem, bring branch out into providing real world value for a broad array of people. I think that it's going to be done in a much more efficient and innovative way that brings it at a mass scale, just simply because of the fact that anybody in the world who is smart and wants to build something can plug in and do it.

Patrick: [00:28:57] One thing that I don't know what level I am now in this whole ecosystem, I've certainly been interested in it for a long time. I'm just curious to see as an observer and as a holder of some of this stuff, is that the number of even base layer stuff, Ethereum, Solan, others seems to be proliferating. And then

that's probably healthy. They serve different functions. They're good at different things, just like any set of businesses or something, the specialization can be interesting.

And let's just imagine that I'm going to hold 10 different things, five years or whatever it is. One thing that seems certain is that I'm going to not want to have 10 different companies that I have to engage in to custody all that stuff. I'm probably going to want to trust one. So I'm curious how you think about this and this gets a little bit more into your specific business than the broader stuff we've talked about, but traditionally Casa has been a Bitcoin company. How do you think about how you need to adapt in the future to make sure that if convenience is the governing concept here across all of this, that you're convenient for people might want to hold a whole bunch of different stuff?

Nick: [00:29:55] Yeah. So I think that there's a few different nuances to this question. So the reason we've been Bitcoin only historically, is that we are highly focused as a startup and as a small team on having as much impact as we can in one narrow focused niche and Bitcoin, out of all the cryptocurrencies has clearly proven that it has product market fit in its niche, which is, this is the most decentralized non sovereign form of money store of value. And that's something that is being recognized around the world, governments are adopting it. The story of Bitcoin has been built and Bitcoin has won that money narrative. So that's where we said, "Okay, this is very clear here. So let us focus on this." When you look at a lot of the other layer one chains right now, one of the things that I view these as similar to, are startups. They are all trying to solve these problems and they haven't necessarily proven that they are going to be the one to solve this problem.

There's things that they're working out over time that if they do this right, they could be highly successful. And in that scenario, it makes sense for somebody like us to say, "If we reevaluate our stance and potentially move into supporting something like that, if there's real value and a real solution being provided there." But you can look at some of these once a day like Ethereum and I think what's really interesting about Ethereum is it's clear that there's a lot of volume and value being transacted through the network. So much so that it's running into these problems where Ethereum is almost breaking. You've got people who are paying thousands of dollars to mint an NFT in the hopes that they could get one of these and it'll be worth more value in the future. In the end, that's not something that can achieve mass adoption. There needs to be things where you're thinking about, "Okay, how do we get these NFTs up to layer two of Ethereum or something so that more people can participate in this." You don't have to be an ultra high net worth Ethereum whale to participate it in this. And I think as we start to see some of those things get solved, some of this gets more interesting.

The Future of Personal Authentication

Patrick: **[00:32:16] I certainly understand the logic through Casa's lens. I'm always thinking about that Frank Slootman from Snowflake idea of, narrow the focus,**

increase the quality, is almost always good advice, especially early on in the business' life. If you take your Casa hat off and just put on your speculative hat or your interested party hat, how do you think about the future of wallets and their importance in just how consumers operate online? Do you think that we're going to show up places, quote, unquote, plug in our wallet in the same way that we would log in with the password and that's going to dictate how we engage with the digital world? And if so, what will that look like and feel like? I'm just really interested future of digital wallets, generally speaking and curious for your take.

Nick: [00:32:56] If you think back to the three use of private keys and what they do, what I mentioned was that they make private keys in incredibly good form of authentication. It is basically an unbreakable form of authentication. Now compare that to a username and password. Usernames and passwords are stolen all the time from people. People are reusing username and passwords and you hack a company and get a bunch of password dumps and suddenly you can go try that in a bunch of other places and get into a bunch of accounts. So what's different about a private key is that when you are actually authenticating with a private key, you're never revealing that key to whoever you are authenticating with, but at the same time, it is 100% provable without a doubt that you are who you say you are. And so private keys will become our identities online, get rid of username and passwords, you're going to share your public key with a random web app or website.

And then anytime you want to log in, it's going to ask you for a signature from your private key, just saying, "Hey, is this you? Do you own this public key?" You're going to prove it, and then that will be your login. So what's great about this is if you have the right tech that actually abstracts away the private key from the user, it's even easier than using a username and password, because with usernames and passwords today, they've got to remember their password, they've got it written down on a sticky note on their computer or something like that, and in this scenario, let's say Casa was your wallet that had your private key where you're logging in here. You get a notification on Casa. It says, "Do you want to log into this website?" You face ID, yes, and it sends a signature from your private key to the website and automatically logs you in. I think that things like this will get very interesting with making the internet experience and proving who you are online much, much easier.

Patrick: **[00:34:56] Largely as a result of meeting you and getting interested in this area, I've tried to talk to some companies just in the world of passwords and authentication and all this stuff. One of the most interesting ... I'm sure I'll have the founders on at some point is a company called Stytch, which creates password-free user authentication flows. It's an API company. You can build their flow into anything. Their point, I think they're very convincing, that usernames and passwords are kind of ridiculous. They're really easy, they have all sorts of problems with them, and that if you're to recover, let's say, a password, something more reliable is used, your phone, something that is easier to authenticate that to your email, et cetera.**

Walk us through all the ways that this happens today that are interesting to you. We probably need to mention hardware wallets as a component here. What is a hardware wallet, is a fingerprint, is a retinal scan, is a face scan? What do you think the relevant true methods of authentication are that are interesting to you as a company to work with to make this process both seamless and also easy to back up, so to speak?

Nick: [00:35:56] I think that the three basic forms of authentication are something you know, a password, right? Something you have. So that could be like a hardware or something, or something you are, and that's like your face ID. Any form of authentication is going to be one of these things or some combination of these things. What you can start to do is think about layering these things together, depending on the importance of the situation that you're in. So let's say you're just logging in to something like a random website that doesn't really matter to you. Maybe it just makes sense for that to be only one of those authentication methods, and it's something that's super quick and easy to do.

Then maybe you're doing something separate, which is you are signing a mortgage document online, and they're not in-person to sign it so that you're not proving that it's you with your ID. So they're trusting that you are who you say you are. Maybe for that, you want them to require you to have something you know, something you have, like a little key from a hardware device or your phone, and something you are, like a face scan. I think what we'll see is people get creative in terms of ... If we're going to get better than username and password authentication, we're going to get creative with the different types of authentications that we are asking people to do, depending on the severity of the situation. That, I think, is where we're going with all of this over the future as our identity becomes increasingly digital.

Self Custody Solutions

Patrick: **[00:37:38] So the one category that we can click a little bit deeper into is something you have, your face, your thumb. Those are kind of self-explanatory. Something you know, a password, that's self-explanatory. Can you talk us through what a hardware wallet is or a device, what are some names of them, and literally how they work? I think this has been mostly for what we might call OGs in crypto or something, people that have a ton of crypto that are really intense about security, and they literally have a physical device. For those that don't know out there, what are those physical devices, and how do they work?**

Nick: [00:38:09] A hardware wallet essentially looks like a USB stick, and it's a special purpose device that is built only to hold private keys and then to use those private keys to sign, meaning approve, signatures on the blockchain, on all the different types of blockchains. So focusing on Bitcoin specifically, let's say you've got a few different types of hardware wallets, might be a ledger, a Trezor, a cold card. You've got a key on one of these devices, and instead of going and approving a Bitcoin transaction from your mobile phone or from maybe a software wallet on your desktop, you're actually plugging in this device and using it to approve that transaction, because it's where the key is held. The benefit that this gives you is that you don't ever have to worry about this key being on an online connected device, where maybe if you get a virus or some sort of malware, it could steal that key from you.

Patrick: [00:39:10] So literally, I plug it into a USB. It gets auto-read by the software. Is that how it works?

Nick: [00:39:15] You plug it in to your computer, as an example. What the software will do is say, "Hey, I've got this transaction that you have built on my interface. I want to send five Bitcoin to Coinbase," or wherever you're sending it. Then the software is going to package up that transaction cryptographically, send it to the hardware wallet, and say, "Please approve this." Then on your hardware wallet, you'll actually look at the little device, the USB stick, and it'll have a screen on it. It'll say, "Do you want to approve this transaction? Here's the details. You're sending this much Bitcoin to this address," et cetera. Because that's a totally self-contained special purpose device, you actually can trust that it's giving you the right information. You want to double-check all the information on there, and then you hit a button that says, "Yes, I approve this transaction." That just gives you that additional layer of security for people who are storing larger amounts of Bitcoin.

Patrick: [00:40:16] So if I was the most hardcore user of Casa, what does that look like? How many different ways do I have of authenticating something? Let's just take the most extreme scenario. I've got $1 billion of Bitcoin, and it's stored with Casa. I want to send it all at once to somebody else. How would that process work? What would I need to do for that to happen?

Nick: [00:40:36] Our highest level of security that we offer is a three of five key set. What that means is you've got five total keys and you need three of those keys to actually approve moving Bitcoin. So in that setup, you have one key on your phone, you've got three keys on hardware wallets, and one key is held by Casa. So those three hardware wallets, what you're doing is people are going and distributing those into different locations. This means one could be in your house. One could be at your office. One could be in a bank safety deposit box. But this protects you against a couple of different things. So it protects you against somebody breaking into your house and trying to steal your one hardware wallet or your phone and get all your Bitcoin, and then it also protects you against things like natural disasters. So if your house floods, you don't have to worry about losing all your Bitcoin, because most of your keys are in other places.

So the people that are at our highest security tier here, what they're doing is in the Casa mobile app, they're saying, "Hey, I want to send this much Bitcoin to this address." Then they're going to get a notification from Casa that says, "Okay, approve this from your phone. Yes, I approve. Now go get one of your hardware wallets and approve it from that hardware wallet as well." So then maybe they've got one at home, or maybe they're traveling to their office. They're plugging it in to their computer, and they're going through the process of approving it. We try to make this as simple as possible for people where we are just walking them through every single step along the way. All they've got to do is get in the rollercoaster ride and sit on the track while it's running them through the process. But the big benefit is that you've got multiple sign-offs on moving this money, and you don't have to worry about losing one of these keys, meaning you've lost all your Bitcoin. You don't have to worry about somebody stealing one key and getting all of your Bitcoin. So it makes you really like a high-security Swiss bank, essentially, but it's all digital and it's all you are handling it yourself and have full control.

Patrick: [00:42:44] What about the very light end of the transaction? Is it basically like I have it on my phone, you have one? What's the simplest, most convenient ... Let's say I have a quarter of a Bitcoin or not much, move it around a lot, and have the lowest friction experience. Is that relevant for you guys, or if I'm doing that, should I just be a Coinbase or something?

Nick: [00:43:01] This is definitely relevant for us, because Casa's mission is to make private keys as easy as possible for anybody in the world to use, no matter how much Bitcoin they have. On the very free end, simple, convenient, free mobile wallet end is our single key product, which is just one private key held on your phone. All this means is it's like using Venmo. You've got some Bitcoin sitting at this public address, which this key points to, and if you want to send 10 bucks of Bitcoin to somebody else, you just pull up your phone, face ID to verify, and it goes. The thing that's different that we've done is a lot of wallets, if you're to have this, you're going to sign up, and the first thing they're going to do is say, "Okay, go write down this 24-word private key on a piece of paper and put that in a safe place," which for me means my sock drawer. Stick it in the sock drawer and hope it never disappears. We don't make you do that. So when you sign up, it feels like you're using Coinbase or Venmo. Super simple. What we're doing in the background is actually backing up that key for you.

So we will encrypt that key with a key from Casa's server and then upload that encrypted private key, which only you have access to, to something like iCloud or Google Drive. This means if you lose your phone, all you've got to do is come back, download the Casa app, log in with your Casa username and password, log in with your iCloud username and password, and it magically brings that key back and decrypts it and stores it on your phone. But it protects you in case let's say somebody gets access to your iCloud account. That key means nothing to them, because it's been encrypted. So we've tried to make this very simple for people in a way that they don't have to think about it. It feels like using your bank app. But you're using Bitcoin, and you're holding the key in a way that you are in full control.

Patrick: [00:44:51] Do you have a sense today for I guess how many crypto holders there are and what percent do self-custody? Seems like probably it's a minority, but is there any way to know this number? It seems like a really hard data point to collect.

Nick: [00:45:04] Yeah, it's really difficult to figure this out exactly, but there's been some ways that we've triangulated it from a few different sources. So in 2020, University of Cambridge did one of their regular every few year survey reports where they survey all of the exchanges and crypto business providers in the industry and ask them a bunch of questions. One of them is always, "How many separate user accounts do you have?" Then Cambridge does this thing where they try to pull out the non-unique user accounts. Essentially, long story short, they said, "100 million people is our estimate of the number of people around the world in Q3 of 2020 that own cryptocurrency." Then if you look at sources like Chainalysis, so what Chainalysis does is they actually monitor a lot of the different crypto networks for fraud and money laundering and these kinds of things. So they have a lot of tech that gives them insight into different wallets in the ecosystem, and they know a lot of the custodian wallets, like Coinbase. So they can see how much is there.

So in 2019, they estimated that about 40% of all existing Bitcoin ... So take out the 4 million that's lost. They estimated about 40% of all existing Bitcoin is held in self-custody wallets. That's been a number that over time has decreased, because the original Bitcoiners, it was all self-custody. Coinbase did not exist. But then as some of these exchanges and stuff have come in and that's where people buy their Bitcoin, that number has decreased in terms of the number of people self-custodying. So this is where for Casa, the mission gets urgent, because we want to help build this world where people actually are using their private keys and have that ownership, because we view it as a better world. It's on us to make sure that we can reverse that trend. We're starting to see that, more and more customers coming in that are saying, "I've never self-custodied before. I've always wanted to, but I was too scared to do it. Now you guys are around, and I feel comfortable with this." So we're starting to make a dent here, but it's going to take more than Casa. It's going to take a lot of our ecosystem really pushing on making it easier, simpler, safer for people to use private keys.

Patrick: **[00:47:31] What is the craziest security setup around Bitcoin that you've ever heard of?**

Nick: [00:47:36] The funny thing is that the craziest setups are probably ones people never talk about, because they've spent so much time setting it up perfectly that they don't want to break it. We hear stories of people that will take their seed phrase and split it onto multiple different pieces of metal and bury those different pieces of metal in different locations on their properties, around the country, or something like that. So it's meant to give them all this redundancy and help them recover their keys if they ever lose them. The interesting thing about it is the more complex you get, you can actually get less and less secure once you pass a certain point. We call it the treasure map setup. You're building this treasure map that you've got to follow in order to recover your keys. You end up shooting yourself in the foot. You're trying to get too cute with it, basically, and you end up messing up. Then you forget one piece of your treasure map, and suddenly you can't access your Bitcoin anymore. So Jameson Lopp, who's the co-founder, CTO of Casa, always says, "Simplicity is security." So keep your setup as simple as you can for the right level of security that you need.

Patrick: [00:48:48] Maybe a picture five years from now in what I'll call the success case, both for Casa and for the ecosystem. If in five years, this has gone sort of the good version in your mind of how it could go, what does that look like, how does it feel, and why is it better?

Nick: [00:49:02] I think what it looks like is people around the world are able to hold Bitcoin, hold cryptocurrency, and participate in financial networks that they never had access to before. We're starting to see this with some of the things in South America. I think some of the things with remittances over the Bitcoin Lightning Network that are significantly cheaper than using something like Western Union, that's a really interesting use case around this that's starting to get built up. So people around the world have more real ownership over their money. They don't have to worry about corrupt regimes taking money from them. They know they are really the ones who have this ownership. So that's the first part, is really that feeling, safety and security and ownership of what matters most to you. The second is that I think you start to see some of that composability that we were talking about earlier around these financial networks unlock a ton of innovation around the world, and we'll start to see more types of products being built that even today,

I can't even pretend to be like, "This thing is going to happen." You're starting to see some of it in DeFi with people being able to lend to each other automatically in a way that they don't even have to know who the end user is. It just opens up these pieces of the financial system in a way that they've never been open before. What happens when you start doing that with all of the rest of the digital world? You start having things like ... As an example, I was a big World of Warcraft nerd when I was a kid, the ability to go after that one great sword or something that everybody wants, and then instead of just having it in the game, you can turn around and bring it to other ecosystems because it's an NFT or something like that, and it's tied to your private key. So you can go and plug it in in other ecosystems to show it off or to sell it or whatever you want to do. I think that all of this composability and permissionlessness just unlocks new things that we never really expected to be able to do before. That is a cool world, to me, especially as more and more of our life becomes this digital life, where we're interacting with each other online and we are living online in many ways.

Patrick: [00:51:26] We spend a lot of our time talking about the broader picture here and some on Casa too. But at the end of the day, Casa is a business. You're trying to build a business here. How do you think about the biggest stumbling blocks or competitive frontiers on which you have to operate and battle against others trying to solve the same problem for people? Like what are the challenges that stand in the way of Casa becoming a huge business and sort of a default way that people store their money?

Nick: [00:51:53] I think it would be making these story and telling the why correctly. So that's why I come and do things like this, to help people understand why this matters and why you shouldn't just say, "Yeah, I'm going to keep my Bitcoin on an exchange and just leave it there, because whatever." By helping people understand the why, you get people to care and that's what helps human behavior actually change. And then building the right utility and use cases so that people actually want to do this. In the end, if this evolves into just this self-contained speculative industry where all people are doing is essentially trading back and forth a bunch of otherwise worthless tokens, I think we've failed as an entire industry. This isn't on just Casa, but it's part of what we have to do is give people access and value in the right ways that it actually makes a difference in their life. And that it's not just something where it's a speculative game that in the end doesn't really do much beyond the people who enjoy participating in speculative games. Those are the three main things that I think about when I think about what Casa really has to accomplish.

Other Important Crypto Building Blocks

Patrick: [00:53:06] As we start to wind down the conversation, what other aspects of the crypto ecosystem you think are the most important building blocks? So if I think of Casa as the security layer, self-custody and security layer of this new form of money or exchange of value, what are the other big areas that matter, do you think, and how do you think they all interrelate? I'm just curious, like if you had to build the taxonomy of maybe layer one blockchains is another, and the security of those is a second, like what are the third, fourth and fifth?

Nick: [00:53:37] So I think I would be a little more abstract even than talking about layer one, other layer one blockchains. But what I would say is you've got the base foundation for everything, which is that secure custody. It's how are you holding the private keys. And then you've got, generally on top of that, the networks, which those keys are interacting with. But then you start to get into things like how do you scale those networks? Because inherently, decentralized networks are hard to scale. There need to be creative solutions like, for example, the Lightning Network on Bitcoin, or there's some layer two networks that are just popping up, like Optimism on Ethereum. That scalability layer is very similar to how the internet scaled and it's important. And it's a really important building block of making this thing work at a massive adoption level. And then the last thing would be the application layer. So what are people actually doing that they value with these crypto ecosystems in their life. Whether that's playing games, whether that's participating in art, like NFTs, whether that's participating in financial systems, DeFi, or even just as simple as sending money over the Lightning Network in a remittance fashion.

There's all these different types of applications, almost many of them that you could see in Web 2.0 world can be rebuilt in Web 3.0. I don't think every one will be, but I think that a good chunk of them will be. Making sure that that's really valuable for people and usable by the average person, not just these hardcore crypto OGs, I think is that last layer that's really important there. If we get those right, I think you get to mass adoption around the world of this new technology. But there's a lot that needs to be done there. And we've seen a ton of growth over the last few years towards this goal, but it's a long goal because you are rebuilding and replacing systems that have been in place for hundreds of years in some cases. And so it's not going to happen overnight.

Patrick: [00:55:48] Is there anything that we haven't covered that matters to you that is really important?

Nick: [00:55:54] We have covered a lot of the things that I think are most important to this story of Bitcoin, the story of this industry in general. The thing that I just keep coming back to is the feeling that people get. It's really hard to communicate this, but except for if you're on the call with the customer, helping them do this, and you're seeing them in real time have this reaction. But the feeling that people get when they realize that they have become their own bank and they feel very safe but they feel really good and excited about it is incredible. And it's just one of those things that it's really hard for people outside of Casa who aren't doing these calls and aren't actually working with customers one-on-one to see. And so it's really easy to dismiss that as this isn't something that really people care about. When you're on the call, when you're there working one-on-one with a customer and you see that light up in their eyes, that is cool. It's one of the things that most keeps us going. It helps us know, okay, we're on the right track. We're not just shouting into the void here. People care about this and we can help many more people understand and care about this as well.

Patrick: [00:57:13] One closing question on security just to sort of invert everything we've talked. We've talked more about convenience than about security maybe, or somewhat of a balance. Are there any ways in which you think the current system is more secure than the system that we're moving to? Meaning like is there any form of attack? Someone coming to my house with a gun or something, putting it in my head and making me walk around to my office and get all these hardware wallets, and maybe that couldn't happen with Bank of America or something. Is there anything like that that has you interested as like, "Oh, this is still a way that the old way is still better and we're going to have to evolve and at least match or surpass it?"

Nick: [00:57:48] There might be, but it all depends on how you actually have things set up for yourself around the new system and with your private keys, which you mentioned of somebody breaking into your house and trying to actually just force you to send your Bitcoin to them. If you've got it on a hardware wallet in your house, you're probably going to do that. And so that is definitely less secured than the old system where maybe you send them the money and then call your bank the next day or something to reverse the transaction. Something like that. If you've got the right setup, the new system is, in every way that I can think of, better. Because if you've got your keys distributed to different locations, or maybe you're relying on multiple parties, we've actually got people who will have a family member in a different location holding one of their keys, that kind of thing, it just becomes incredibly difficult for somebody to do that, like that $5 wrench attack. Thieves in general are going to be looking for much lower-hanging fruit.

If you zoom out to make this comparison point to the old system, what you're getting with private keys and the new system is that bulletproof authentication. So if you think about like sending a wire, for example, let's say you're wiring money for a sizable amount of money through the old banking system.

Patrick: [00:59:10] Yeah. I've got a token. Now I know it.

Nick: [00:59:12] You got a little token or they're going to be calling you and check in, "Hey, did you really mean to do this?" And I was talking to somebody the other day who said they literally sent the wire online and then had to do two different phone calls to approve that wire. Well, why do you have to do that? It's because the form of authentication is imperfect. But with a private key, it is a perfect form of authentication. It just makes the system from its foundation much more secure. And you're not having to band-aid these things on top of it to add security to an inherently insecure system. That's where we really get into the meat of it. Where honestly, there is not much that we can't fix or build in the new system that makes the whole thing more secure than the old system.

Patrick: [00:59:57] Have you ever considered like a badge equivalent, the same reason that someone puts like a Sonitrol sign in their lawn or something, like a digital badge that verifies that someone uses Casa? Maybe even it's Casa 5 and is that worth your time to mess with me because I can verify and you can check that Casa is indeed the way I secure my thing? Have you ever thought about something like that?

Nick: [01:00:17] Yes, definitely. We've thought about this, joked about it a little bit. Some of our clients have asked us, "Hey, can you send me an ADT sign that says I use Casa?" One of our clients made a custom one of these signs.

Patrick: [01:00:29] I love it.

Nick: [01:00:30] And put it out front of their house that says, "I use Distributed Casa Multisig for my keys." We might make the physical version of this at some point as almost like a little Easter egg fun kind of toy. But if you think about it actually, it has some real value because you are essentially just saying to potential thieves, "I am a much harder target than you want to mess with." And that's the reason why people put the ADT sign out front of their house. So yeah, I think it's a really interesting thing that we probably, instead of just joking about it, we should just go make it and give it to the people.

Patrick: [01:01:09] Look, I've been wondering, like what's the beware of dog equivalent here. Like if our identity is increasingly one identity that we poured around to us so we don't have a different Twitter profile than Facebook profile, et cetera, et cetera, if it's like one centralized thing that we own. Wouldn't it be cool to have things associated with that that are provable, that tell someone not to mess with us? Like that seems like a really cool, interesting, fun closing concept.

Nick, this has been so much fun. I think this topic is kind of mind-bending and cool and filled with history and interesting potential for the future. I know we got to wind down here. My traditional closing question for everyone is to ask what is the kindest thing that anyone's ever done for you?

Nick: [01:01:44] It's funny because I've been listening to your podcast for years. And every time you ask this question, I'm like, "Man, so many people in my life have done nice things for me. How would I answer this question?"

Patrick: **[01:01:55] And here we are.**

Nick: [01:01:56] And here we are. I actually have to think about how I want to answer it. I'll answer it like this. I've had a lot of people do a lot of nice things for me in my life, and I don't think I could pick the one king of it all. But one thing that stood out to me was the fact that I actually started my career in finance. I did investment banking and then moved into private equity. And I was on this track to make a lot of money, frankly. But I really didn't like the job and it was pretty soul-sucking for me. I wanted to be building something instead. And when my wife married me, I was in finance on this track to make us a lot of money. And when I wanted to quit, I talked to her about it and she was super supportive of me taking literally a 50% pay cut to go work a random job at a start-up in operations, just because I wanted to be building something.

And that obviously started me on the train that got me to being CEO and co-founder of Casa and building something that can have real impact around the world. Her initial support of me and giving me that push to do something that I was really passionate about, even though it affected both of us financially and was a little bit of a risk from a perspective of is this even going to be a solid job was huge. That changed the course of our life together.

Patrick: **[01:03:17] Fantastic. I love it. Such an interesting, neat conversation. Thanks so much for your time, Nick.**

Nick: [01:03:21] Thank you.