Episode 1,513: Crypto and a World of Individual Sovereignty

Guest: Jameson Lopp

WOODS: All right, I'd like to start with your background. I have a lot of libertarians who are guests on the show, and everybody's got some interesting story about how he came to those ideas, but people who also have interesting Bitcoin stories. How did they tumble down into this world and become so fascinated by it and, in some cases, devote themselves to it? So I'd like to know a little bit of the making of Jameson Lopp.

LOPP: Absolutely. I happened to be at the perfect intersection of the libertarian philosophy and the ultra-nerdy computer scientist. This was seven or eight years ago. I was just working for an online marketing company, doing lots of data crunching, and this Bitcoin thing started popping up in the news. And as most people tend to do, I dismissed it as something that was going to get hacked, and everyone was going to lose their money.

But after it kept coming back time and time again, eventually I looked into it. And I realized, both from the computer science perspective, that it was actually solving a very interesting problem that I had never even thought about before. And as I started thinking about money in general, which I think most people never really do, they'd simply use it as it is given to them, I also realized that money is this concept that shouldn't really be owned or controlled by any entity in particular, because it is a mutual agreement amongst everyone who uses it. So the idea of money as an open collaborative project was also very appealing to me. I found it was just a fascinating experiment, and that's really where I started falling down the rabbit hole. And I've been doing it full-time since 2015 now, and I'm still constantly trying to educate myself and basically stay on top of the latest developments.

WOODS: You sent me some notes, because although we've spoken before, we don't know each other well, so I have some notes about your background and some topics that interest you. And in the introductory portion, you talk about getting SWATed and going dark. What in heaven's name does that mean?

LOPP: [laughing] That was an unfortunate experience that was the culmination of me becoming, I guess you could say, semi-famous on the crypto part of Twitter, where I was talking about Bitcoin for years and years, and apparently I just got the right tone and was able to amass a pretty decent audience on Twitter. And eventually, you get a large-enough audience, you probably are going to say something that upsets somebody. And I managed to attract the attention of someone who wanted to screw with me. And basically, they filed a

false call to the police in my jurisdiction and got the SWAT team to come out, locked down my whole neighborhood, and basically gave me a lot of grief.

And eventually, they were trying to extort me and do other stuff, but that basically resulted in me taking a look at my own security and thinking about how we've actually created an exploitable system with law enforcement, where now, due to advancements in privacy technology, anyone with a modicum of technical sophistication can place an anonymous phone call that can't really be traced by law enforcement. And because if you say the right words to law enforcement, they are basically obligated to send out large forces to investigate and make sure that a claim is true or false. It's very easy to get tens if not hundreds of thousands of dollars' worth of taxpayer resources deployed against almost any arbitrary target.

And that's essentially what happened to me, is some random guy made a five-minute phone call and pretended to be me and said that I had hurt a lot of people, and that resulted in my entire neighborhood getting locked down and caused a lot of grief for me — which then led me down a journey that lasted almost an entire year of me essentially burning down my entire life, starting over anew with a privacy perspective, and basically trying to live a privacy-oriented life, where it's not possible for someone to find my address in order to place a call to law enforcement to deploy resources and attack me with almost no risk to themselves.

And it's been a fascinating journey. I've written about it a lot, and it has really become a way of life for me. But it's also resulted in me beginning to understand exactly how difficult it is to actually retain your privacy this in day and age, and it's basically a nightmare scenario, that it costs innumerable hours of effort and cost me tens of thousands of dollars to actually pull off.

WOODS: That is unbelievable. I knew nothing about this. Wow. Now, if you weren't already thinking a certain way about how society works, I would think an episode like that would get the old noodle in action.

LOPP: Absolutely. And the privacy thing, privacy and security are both very difficult topics to talk to people about, because most people don't notice a direct impact on their lives. A lot of these things are fairly innocuous, and people have gotten used to it. I mean, you can look around and see a lot of people are walking around, and they're essentially carrying surveillance devices in their pockets, and they're placing other surveillance devices in their homes. And we don't call them surveillance devices; we call them personal assistants or Alexa or Google Home or whatever. And it requires a very different mindset to even look at the world in this different perspective and actually think, you know, what are the tradeoffs that I'm making in return for these conveniences.

WOODS: In a minute, I want to get into the big picture about what are the problems that something like Bitcoin sets out to solve, and then there really is a follow-up question of: there are, in some ways, problems with the solution, in that maybe it needs to be more user friendly. We'll get into all that. But I want to actually ask, if you wouldn't mind, to take just a minute to comment on your pinned tweet. You have a beautiful Twitter handle. It's just @Lopp. It's beautiful. Four letters. Perfect. And your pinned tweet says, "Bitcoin isn't a get-rich-quick scheme. It's a don't-get-poor-slowly scheme." Can you explain that?

LOPP: Yeah, this was kind of a pushback to some things that a lot of the early Bitcoin adopters get, where, yes, Bitcoin has appreciated in value enormously over the past ten years, but the reason why I got into it initially was not because I thought, hey, this thing is going to go 1000x from where it is right now. It was rather, I know that if I keep my money in US dollars or some other bank-controlled currency, that over the long run, it is only going to decrease in value. That is basically a known factor.

WOODS: Yeah.

LOPP: Now, Bitcoin creates a whole bunch of new set of rules, and those rules are not changeable on a whim by some random people who meet every so often behind closed doors. And while Bitcoin never has and never will have any sort of fiscal policy to try to maintain a specific value, we do know that the emission schedule of Bitcoin is set and is practically impossible for that to ever be changed. It is technically possible, but the likelihood that consensus to change it is basically zero. And so I figured to myself, well, at the very least, it sounds like an interesting hedge to keep some small portion of my portfolio in it, because it's just a little bit more trustworthy than these other systems that are controlled by people that are pulling levers willy-nilly on a whim.

WOODS: All right, now let's dig more deeply into the big picture of Bitcoin. I want you to describe what is the problem Bitcoin is seeking to solve, because sometimes I've seen Bitcoin critics say Bitcoin is a solution in search of a problem. It's a solution nobody's asking for a problem nobody cares about. But that can't be right. So what is the problem that Bitcoin solves?

LOPP: Well, the problem is actually outlined very elegantly in the white paper. And it can sound daunting to tell someone to go read a white paper, because a lot of academic white paper papers are incredibly complicated. But if you read the Bitcoin white paper, it's eight or nine pages. Sure, it has some technical bits, but it's also explained in fairly readable English in plain terms. So it is something that I think anyone who's interested in Bitcoin should start out with, and I have several resources on my website to help you understand that, some annotated versions and whatnot.

But in the white paper, Satoshi specifically said that the problem is that current systems require a level of trust in third parties to essentially help you intermediate payments across distances. And so whenever you're requiring some third party to intermediate the exchange of value or the exchange of data or really the exchange of almost anything, that third party, they may be trustworthy now, they may be trustworthy for a long time, but they can arbitrarily decide to start screwing around with you and make your life much more difficult.

And we've seen plenty of examples of that. And in fact ,just in the past few years, we're starting to see more and more examples of things like de-platforming or examples of various payment processor companies and banks refusing certain people to even be able to use their platforms, because they're doing something that is considered politically incorrect or gray market area, not necessarily even illegal, but just something that that company doesn't want associated with them.

And so, if we want to be able to have truly sound money and to be able to economically interact freely, then we can't have even the slightest ability for some random third party to say no. And that's essentially what Bitcoin does, is it creates a system where you follow the

rules of the system, and you don't have to follow arbitrary rules that are set by any other third party, because you are then transacting directly with whoever else you want to on the system.

And the original use case that was really proven with Bitcoin was, of course, the dark net markets. This was the first truly free market on the internet where people could buy and sell grey market or black market goods, and there was no way for any payment processor or other authority to freeze or to reverse those payments. And that was only the beginning. We've seen many other use cases arise over the years, even things, for example, like sex industry workers, who in many jurisdictions are acting completely legally, but they end up getting de-banked because the banks don't want to deal with them. Or of course, legal drug industry in many states has problems with banking, because the banks are dealing with federal regulations. And even though it may be legal for them to do business in a given state, the bank tends to apply those rules across the entire country.

So the fancy word is censorship resistance. It is the ability to economically interact without fear of someone censoring whatever that interaction is.

WOODS: Yeah. Yeah, yeah, and you know, interestingly, at the time that — well, I guess it pops up every now and again. There'll be these phases where Facebook or Twitter will go and purge a whole bunch of people, and then everybody gets upset, and they pledge they're going to start their own platform, but the problem is even if you start your own platform, payment processors even can come after you if they so choose. And some people have said, well, if you just use cryptocurrency, this solves your problem. But then the problem is the question of adoption. I mean, how many of my followers are going to adopt cryptocurrency. But nobody denies that that solves that problem. It's just a matter of: we haven't gotten enough people doing it.

LOPP: Yes, and the other interesting thing about Bitcoin is that, while I can project what I find to be valuable in the system, if you ask ten other people, you might get ten other opinions. And so I try to avoid being the authority on anything, because there are a lot of different approaches to the system, and you will find that a lot of people, especially even early adopters like myself, I didn't get into it, like I said, because I was having my own payments getting blocked by any payment processors. I originally got into it because I just found the economic rules to be more understandable, and I felt like over the long run, that would be more beneficial than a system that is going to be manipulated in ways that I can't really predict.

WOODS: Right, right, right. I mean, that would be why I would be interested in Bitcoin. That's primarily what motivates me. But I thought, well, look, whatever it is that gets people's attention to get them to look at crypto, I'm fine with that. As long as it gets them interested, that's good enough for me.

Now, you've described one of the problems we're facing as basically summarized as follows. We have a situation where government controls our money, tech controls our data, and you say the solution: cryptography allows us to control both. I'd like you to unpack that for us.

LOPP: This is where a lot of the ideas that, for anyone who has read *The Sovereign Individual*, that book was actually quite prescient in that they understood how the communication age was going to change the balance of power, dynamics in general. And the amazing thing about

cryptography, which is not really a new thing — I mean, people have been using various techniques to hide data from being intercepted for thousands of years — but especially in the communications age, with the public/private-key cryptography has become very easy to use, and everyone who's listening to this is using public/private-key cryptography every day, whenever you're using the internet, whenever you're using the banking system. Pretty much any technological platform is using it at some level. The amazing thing about it is that it completely changes the cost of attack, and you are now able to defend your data by expending milliseconds of computation time. And when you do that, you're creating a problem that then would take potentially thousands, if not millions, of years of computation time to unwind or to break through.

And when we use the term asymmetric warfare in the context of the digital age and cryptography, this is basically what we're talking about, is the ability to defend your digital life at a very low cost to yourself, and to be confident that you are secure because you know, mathematically, that the costs for someone to attack you would be thousands or millions of times greater than the cost that you have spent defending yourself. And that is when the game really starts to change.

WOODS: Well, I like that you more or less concede elsewhere that, now that we've kind of got a handle on the solution, there is still a bit of a problem with that solution in that, look, my grandmother, who's deceased now, she was a smart lady, but she probably wouldn't have adopted Bitcoin. And it's not just because she didn't see the merits in it; it's also that there are aspects of Bitcoin that are not that user friendly. And I know this might seem silly to a lot of Bitcoin aficionados, because you're so deep in that world, you can't imagine that there'd be people who don't get it. But it's not the easiest thing in the world to get started with. I mean, maybe it is, but I remember I even asked somebody what videos should people watch about Bitcoin or what should they read? And he couldn't even give me a straight answer to that. And sometimes when I hear people talk about it, it's all like engineering gobbledygook language. And I keep thinking: what Bitcoin needs is a good marketer. Like we have all the tech people, but tech people are not good salesmen, and I think we need people who just, they get it, they understand it, and they can explain it for the layman. What's a way of dealing with this and making it as — how can we make it easier for people, basically is what I'm getting at.

LOPP: Yeah, this is something where, when I first got into Bitcoin, I focused a lot of my efforts on marketing and evangelism and trying to convince people that there was value that they simply didn't see. Over the years, my perspective has changed a bit. And while I still talk about Bitcoin all the time, I no longer go up to people or friends or family and try to convince them that they need to be using it, even though I do believe it would improve their life over the long run. Instead, what I've focused on full time for almost five years now is building technology that lowers the bar for being able to use Bitcoin in what I believe is the way that it was meant to be used.

And when I say that, I mean, the "be your own bank" scenario. The "you can be your own bank" meme has been around for almost as long as Bitcoin, but the ability to actually do that has always had a very high cost of education, a high cost of time, of actually executing a lot of complicated technical steps. And it is the reason why I switched from working at BitGo, which was an enterprise Bitcoin wallet, to working at Casa a couple of years ago, where we focus on personal sovereignty solution.

It's because this usability problem is something that I have struggled with myself, and so I know that everyone else in the space also struggles with it, where we are essentially talking about boring IT data practices. When you realize that a Bitcoin is actually just a private key, which is just a bit of random data, and now all of a sudden, this little bit of randomly generated data unlocks potentially a lot of wealth, then you have to put in a lot of effort to make sure that that bit of random data is not accessed by anyone that you don't want to access it, because if a hacker or some attacker gets in there, then your money's all gone and there is no authority in the system that can return it to you. You also have to deal with even more boring loss issues of, you know, what if there's an environmental disaster. These are the type of things that traditional banks have dealt with for centuries, is creating robust storage that won't just burn down or get flooded or destroy everything.

And then there's also the sort of redundant backup issue of you need to be making sure that you're consistently managing your data and taking backups every so often, just in case something does happen. And that's something that I think almost nobody does, even highly technical people like myself. It's just something you don't want to spend any time doing, because you feel like it's probably not going to pay off. But it is ultimately a form of insurance against certain disaster scenarios.

And then finally, a thing that we've started thinking about more as Bitcoin matures, as the Bitcoin user base is aging, is of course, inheritance problems and the inheritance issues sort of overarching all of these other things, where you have to make sure that only the people you expect are able to access it, but then you don't want them to be able to collude against you and take it from you while you're still alive. And then there's also jurisdictional issues, with state law to deal with.

So there are many layers of complexity that can easily turn people off to wanting to deal with all of this, and at the moment, I would say, due to the relatively early nature of Bitcoin, the people who are thinking about these problems the most are the ones who have been at it the longest and probably have the most to lose. And so that's what we've been focused on at Casa, is dealing with people who have potentially millions of dollars. And when you have that level of wealth in this new-fangled system, you're going to be willing to spend a bit more to make sure that you have a secure setup because you want that peace of mind.

And what we're hoping and what I'm fairly optimistic that we've been making good progress on for the past few years is that we're essentially experimenting with the best practices and techniques and building software that pushes a lot of those best practices under the hood, so that instead of having to spend hours, days, weeks educating yourself on how to do everything right, all you have to do is just follow the software, and you click on things that it tells you to click on, follow the instructions of what the software tells you, so that we're able to lower that bar to the point that the software will then be able to be reused and redistributed by people who have a lot less to lose.

And by continuing to lower that bar, we can eventually get to the point where this technology is actually mainstream-user friendly. And if you look at sort of the way that the internet and technology has evolved over the past few decades, I would argue that a similar type of thing happened where, if you were using the internet in the early '90s, you remember it was a very different and more onerous experience to actually set up and navigate your way around. But over the decades, the software improved, the hardware improved. And now, you can give a toddler a smartphone, and they can start picking up on it fairly intuitively. And that's

basically what I want us to get to with Bitcoin, is to get to the point where it's just intuitive and you don't have to have a PhD in computer science to feel like you can use it safely.

WOODS: I have, right in one of the tabs on my computer this very moment, a presentation you gave with somebody else called "Constructing Crypto Castles," and I was intrigued by that castle metaphor. What does that mean?

LOPP: Well, because we're trying to help people be their own banks, we're trying to figure out a way to best present this concept so that people understand the difference between just leaving all of your Bitcoin with a trusted third party like an exchange or some other custodian versus bringing it in house, controlling it yourself, defending it yourself. And I think of a lot of these professional custodian services more as bunkers, and in fact, some of them are literally in bunkers, like Xapo famously had a bunker I think in Switzerland or something. It was a decommissioned military bunker that they put a lot of their private keys into. And it is possible to get a very high level of security by just locking away those keys so that they're basically inaccessible.

But if we want to get to a point where your digital wealth is both secure and usable when you actually need it, then we need to get away from this bunker idea and into more of a castle idea, because a castle is a place that someone lives. It is an entire ecosystem, but it is essentially a home and it's comfortable, and it's where you can protect yourself and your family and your wealth and still be able to go about your life. And so once we started looking at how castles are constructed, we actually found a lot of parallels between how you might set up a physical castle versus how you might set up a digital castle to protect your private keys.

WOODS: All right, I want to talk about Casa, which is your current project, and see how it kind of relates to this castle metaphor, the building blocks of the castle, and what role Casa plays in all this — and by the way, who would be a natural client of yours. Who would be the sort of person that your services would appeal to? Give me the whole picture.

LOPP: Sure. I mean, we are looking for anyone who wants to self-custody their own funds, but who either doesn't have the time or doesn't feel like they have the level of sophistication to do it themselves. That basically means that they want to be their own bank, but they need some guidance. The ultimate way to be your own bank, of course, is going to be to do everything yourself, but it's very onerous to do that. And even people who have millions of dollars' worth of Bitcoin often find that they have more important things that they want to deal with on a daily basis.

So, at Casa, we've actually created a number of different tiers, all the way from free tier, to $20-a-month, all the way up to what we call our diamond-level tier that's around $400 a month. And these all have different levels of service, different levels of security with the setup that we make available to you. But essentially what we're doing at Casa is building his personal sovereignty suite of services and products.

And the first thing that we built was the key master application. And this is an Android and iOS app, and essentially what it does is it allows you to easily manage and visualize your vault. And we're not fundamentally creating any new building blocks of software or protocol-type usage with this application. Rather, what we've done is gone out and looked at the different pieces of security functionality that are available in Bitcoin and put them together

in a way that hasn't really been done before. And essentially, the way that we started out was trying to build the most secure, but also most user-friendly Bitcoin storage solution that we could think of.

At the time, the most secure storage solution that was out there was something called the Glacier Protocol, which is this open source guide that is probably 100 pages long, and it requires doing all types of things like buying air gapped computers that never touch the internet, and scanning QR codes, and manually constructing transactions offline. It's essentially the extreme of how you might go about building your own Bitcoin vault. And while we felt like that was very secure, the tradeoff is that it was so unusable that even some of the people who wrote the Glacier Protocol are not using it themselves [laughing].

WOODS: Oh.

LOPP: And we actually ended up employing one of the people who wrote the Glacier Protocol, and he's been helping us with a number of other things, including our wealth security protocol, which is available to download from our website, and we're also working on the inheritance planning protocol.

But to get back to the actual key master vault, some of the building blocks that we put together that kind of go along with this castle metaphor is that we're using multi-signature aspects of the technology, essentially to create what you might think of as the walls of this key shield that you actually can visualize in the application. Because instead of having a single private key or a single set of private keys that are all together, instead, you create five sets of private keys and then geographically disperse them so that a physical attacker is not going to be able to access them and would, in fact, have to A) know where they all are, and B) travel to these different access-controlled locations, basically making a very, very high bar for anyone to physically attack them and get those keys.

We're also using hardware devices that are available on the retail market, such as Trezor, Ledger, Coldcard, what have you. And those hardware devices are what the private keys are actually kept on and secured by. And you can kind of think of those as almost a portcullis or a gate-type mechanism, where the private keys, even if a physical attacker managed to get to the device, they wouldn't be able to get into it unless they actually know the pin to unlock the device to be able to access those keys.

And then the key master app itself is almost like a gate tower or a watch tower or some sort of lookout management mechanism, where you can see everything that's going on, you can actively monitor the state of these devices, and you can even remove the devices and swap them out fairly flexibly as needed.

And all together, this creates a security model that, in my opinion ,is actually better than most physical banks. Because you can, in fact, use banks for one or two of these key devices. The really neat thing about using multiple keys in a system like this is that you can use a variety of different security setups for each key. But in general, the security of all the keys together is actually additive. So when you have a strong security model on one key and then a slightly different but also strong security model on another key, when you look at the entire system as a whole, you're actually adding all of this security together to get a level of security that I think hasn't really been possible before, at least for physical assets, and probably even for traditional digital assets.

But as you're using this key master app, we're taking away a lot of the nitty-gritty, IT, boring data management stuff, and actually building health checks into the app. We're building the ability for you to, if a device gets lost, stolen, whatever, just buy a new one off the shelf, plug it in, and we actually walk you through a key rotation mechanism, which under the hood is a very complicated thing, but if you're using our app, all you're doing is clicking through it and following the instructions and it just takes a matter of minutes to actually follow.

So this level of security is something that I think everyone in the Bitcoin space wants to have, and it's just not been feasible with such a user-friendly level before now. And so that a lot of the feedback that we've gotten from the people who we've brought on board, some of whom were using trusted third-party custodians, some of whom were using their own setups — but the feedback in general is that this has given them a peace of mind that they've never really had before.

And I think that that is probably one of the most glowing recommendations that we can get in this space, because at a technical level, we've already talked about how if you lose your keys or they get taken by someone, your money is gone forever, but at a technical level, whenever you're constructing a transaction in Bitcoin, whenever you're doing any sort of operation with the protocol, it's a potentially catastrophic operation. If you screw something up, it's actually possible to send your money off into the ether where no one can ever get it. It's possible for you to essentially lock up your money accidentally in a way that you can never get it. There's so many things that can go wrong that I think peace of mind and reliability are incredibly important in this ecosystem.

WOODS: Can you, as we close, take the stuff you've said in this episode today and encapsulate in, let's say, a one-minute elevator pitch to grab people's attention: why this all matters and why, frankly, what you're doing at Casa matters to them?

LOPP: Yeah, so this is pushback that I get often, is why do we need these "be your own bank" solutions, because there are already plenty of regulated and trustworthy custodians out there. We can just let them and their expert team of security engineers worry about all of those problems. Well, the most important reason, I think for a personal perspective, is because there are still things that can go wrong with that trusted third party. If you take any of the logic in adversarial thinking to the extreme, then the ultimate adversary is probably going to be a nation state. So you have to ask yourself, well, do I want to put all of my money in what is basically a bank, but is really more of a tech company, but they're still vulnerable to nation-state attacks, because it's the single point of failure?

Now, at a higher level and not just personal thinking, the reason why I think that this is important for the entire ecosystem is that if we all just put our money back into a new form of bank — which at this point is exchanges and other tech companies that are dealing with security and custody — well, we're just reintroducing systemic risk into the system. And we're centralizing the risk and creating a smaller number of points of failure, which, like I said, could fail due to nation-state attacks, they could fail due to internal attacks or issues within these own companies. But putting more value in a smaller number of places just means there are more things that can go wrong, that can affect a large number of people. And anyone who's familiar with Bitcoin is well aware of what happened with Mt. Gox and BitFenix and dozens of other exchanges, in which large amounts of value were centralized, and we want to avoid that from happening.

WOODS: How can people find out more about you in particular and Casa in general?

LOPP: As for myself, I have a ton of educational resources on my website at Lopp.net. You can also get there by going to Bitcoin.page, if that's easier to remember. And Casa is easy to find. Our domain is Keys.casa.

WOODS: Got it. Okay, I'm going to link to both of these on the show notes page, TomWoods.com/1513, and what I'm also going to link to for anybody who missed it was the debate you did on this program with Roger Ver about Bitcoin and Bitcoin Cash. Boy, that generated a lot of heat on social media —

LOPP: [laughing]

WOODS: — so maybe we can revive a bit of that. But the nice thing about that, by the way, was that, in my circles, I find myself involved in some very contentious debates on various topics, but it is so interesting, given that that's a topic that — you know, it's a very niche kind of topic to be debating, and yet I saw such viciousness by people on both sides of that. It surprised me that that's such an issue with generate that kind of heat. But the nice thing was, you really kept it just to the facts and the arguments, and we had a really good exchange of ideas. It was a nice break from what had been very bad blood, I think, around, so you were a really good model for everybody in that. So I'll link to that episode also at TomWoods.com/1513. Well, best of luck with what you're doing. It's very important, and we're all very excited to hear about it.

LOPP: Thanks.