Fox Rothschild Podcast

The Presumption of Innocence

Episode 78: Decrypting Crypto: How It Works and How It's Watched

Featuring Matt Adams of Fox Rothschild and Jonathan Schmalfeld

The views expressed in this podcast are those of the participants and should not be considered the views of Fox Rothschild LLP or its attorneys. This podcast is for informational purposes only, is not legal advice, and does not create an attorney-client relationship.

Matt: Welcome back to "The Presumption of Innocence," a podcast brought to you by the White-Collar Criminal Defense and Regulatory Compliance Practice at Fox Rothschild.

Well, unless you've been living under a rock in recent years, you've heard of digital currency. In common parlance, it's generally called crypto, but that's a vast oversimplification of a fairly complex digital form of money, and a new one at that. And the digital infrastructure that surrounds it, using cryptography and distributed networks instead of banks or central government authorities to record, verify and transfer value.

My guest today is Jonathan Scmalfeld, a former big-firm lawyer that worked with a whole spectrum of digital assets in private practice, who now serves as the Director of Policy for The Digital Chamber, the oldest and largest digital asset advocacy group in the United States. Instead of doing it in courtrooms, he's taken his expertise in digital currencies to the halls of Congress and other stakeholders to educate and inform digital currency policy in our country.

In a nutshell, he is now doing for digital asset stakeholders what the traditional Chamber of Commerce has done for the corner stores and other mom-and-pops of Main Street, USA, well before we knew what crypto was. Since its founding in 2014, as digital currencies began to appear on the scene, The Digital Chamber has become a leader in promoting the acceptance and use of digital currencies.

Jonathan, welcome to "The Presumption of Innocence."

Jonathan: Thank you very much for having me.

The views expressed in this podcast are those of the participants and should not be considered the views of Fox Rothschild LLP or its attorneys. This podcast is for informational purposes only, is not legal advice, and does not create an attorney-client relationship.

Matt: Well Jonathan, the terms "crypto" or "digital currency" have alone been known to evoke fear, anxiety and sometimes great trepidation. Also a little bit of a healthy dose of skepticism as well, and I will put myself out there in this forum publicly by saying that I'm one of those skeptics.

But give us a primer on the necessary terminology and mechanics of how digital assets work starting from scratch. And in chatting with you offline, I heard a great story about a member of Congress asking you to do pretty much the very same thing. And it's your story to tell, but share that with our audience because it's funny.

Jonathan: Yeah, yeah. So a large part of my job is dealing with people that are either unfamiliar with digital assets or that have some familiarity but are very skeptical about it, um, which is fair. It's, digital assets have only been around-- what we're talking about here in digital assets that are done through blockchain technology-- have only been around since the Bitcoin Whitepaper, in early 2008, somewhere around there.

But we are constantly educating and trying to make sure people understand that. People think crypto, they think bitcoin is the first thing they think of, lots of times, they think crime. I think this is only being used by criminals, or this isn't, uh, actually supported by anything. This is like magic beans, almost. And so--

Matt: Wait, it's not?

Jonathan: It isn't. There actually is real technology and real value behind it. But yeah, so, lots of times we deal with those types of things. We try and make sure, try and make it less intimidating. So, recently we had a member of Congress come to Digital Chamber, staff for this member of Congress came to us and said, hey, we need a, I know we've been in like 30-plus hearings over the years that have touched on digital assets in one way, shape or another, but he still just, this, this member still needs just a basic understanding of it. So can you guys put together just a short two-pager, three-pager, right at like the 10th grade level so that this member has a better understanding with all the legislation that he's being asked to weigh in on digital assets.

And so we put that together. Talked about how digital assets work. Gave it over to the staff and the staff came back to us and said, hey, really appreciate that. That was great. Awesome. Um, there was perfectly at 10th grade level. But can you actually do this at the fifth grade level and give us another one?

So it's, we, when we have these conversations, sometimes people get it on the first, just like, here it is, this makes total sense to me, clicks right away. That wasn't me. Uh, I mean, when I first started buying and selling crypto back in 2014, I had a basic understanding of it, but it was, it was purely speculative.

I didn't, I didn't really, really know much about technology or anything like that. And then you start talking about how the tech works, what it's used for, kind of, what it can create as far as efficiencies and settlement finality and all these other huge benefits that come with this blockchain-enabled technologies.

That could be the fifth conversation, could be the first, could be the second. But that's, it takes a while for some people to understand kind of, all right, what is crypto generally? What do you mean when you mean crypto?

Matt: So what does it mean?

Jonathan: Yeah, so the easiest way to probably explain it is that crypto enables true digital ownership of digital goods. So we haven't had, as a society, a true bearer good that's been digital, ever. When you buy your book on Kindle, you don't own it. You have a license to use that. When you send somebody funds from your bank account, you're not actually sending it. The bank is sending it. You don't have a bearer asset. You can't say, Hey, I would like to send, like me, send you $5. I can't do that in an online --.

Matt: Add a couple zeros before you do that, okay?

Jonathan: You get $5, you get $5. You don't have that way of doing these, these intermediary-less transactions in a digital world. Crypto enables that. So,

Matt: So are you saying, are you saying that the, the crypto is the digital equivalent of handing me a $5 bill?

Jonathan: Crypto enables the digital equivalent of handing you a $5 bill.

Matt: Okay.

Jonathan: So when I, when I'm thinking, like, when I send you a file of a song. Like say I want to send you a, like, here's this, here's this great song, I'll attach it as a MP3 in an email kind of thing. That's actually creating a copy of that music and that's covered by Copyright Act and all these other things. And you don't have, you know, there's this thing called first sale doctrine, what's allowed, what's not allowed. There's a whole like, different realm that goes on there. But when I'm talking about just purely financial products, what crypto enables is, I can have my, idea of a mattress full of cash or a bag of cash under my mattress that I can actually send in an online system using blockchain technology because it's enabled through cryptographic proofs. So it's a long way of saying that we have this form of encryption that makes sure that I can send you something and you can receive it, and there's not a double spend issue. You don't have to worry that I sent the same thing to three

different people and three different people have ownership over that. It's only one thing, can only be spent one time, and that's enabled through this, like, cryptographic proofs.

Matt: So you can, unlike a bank where you would potentially overdraw your account by wiring out too many funds, that by the time it catches up and settles those transactions you may be in an overdraw situation, this is a, a true-to-life, like handing somebody a gold bar.

Jonathan: Exactly. Exactly. So it makes it technologically impossible to overdraft. I cannot send the same thing to multiple people. And it does it without an intermediary. So I don't need a bank to say, hey, you've overdrafted. The tech stops me from being able to spend something that I do not actually own.

Matt: Alright, so let's go into that tech a little bit. Let's define some of those terms before we jump into the meat of the conversation, which is, is really where we want to go, about crypto-based criminal activity. Let's start with the cryptography. Talk to us a little bit about what that is.

Jonathan: So, cryptography is just a form of encryption. Same way that emails are encrypted, chats are encrypted. It is just a form of encryption that goes back to, World War II, encryption of messages at the troops. So, um, the way that the cryptography works in most crypto assets is, there is something called a public key and a private key. So your public key, you can think of like your public bank address, like this is something that everyone knows. They can send you something to this address.

Matt: Wire instructions.

Jonathan: Correct. You can consider them wire instructions. So, the private key, you can think of the password. So the only people that can access the funds within a certain digital wallet-- and digital wallet is just a term for a place that stores keys for cryptographic-- but the only people who can access the, anyone can send anything they want to that digital wallet, assuming it's on a compatible network. Think of it like iPhone, Android kind of compatibility. I can't send certain assets on Bitcoin network, but I can send others on Ethereum network. There's different networks and different compatibilities, different kind of software.

Um, but the idea is then in all these is that there's this public address that people can send --as long as it's a compatible asset-- they can send anything to that one. But the only people can send from that wallet are the ones who have the private key, or the password to it. And then for all these sending transactions, you have to sign off on the transaction as the holder of the private key saying, I intend to send one Bitcoin on this day to this person, kind of thing.

Matt: And then the ownership is recorded in the blockchain, right? So talk to us a little bit, technologically speaking, what the blockchain is as it relates to digital assets.

Jonathan: Correct. So the blockchain is this, it's exactly what the word means: block and chain. So it's a chain of transactions that goes and, and labels each time that a asset on that network has been sent. And a block is a group of transactions that happened in a period of time, say the 15 seconds for, uh, that we're talking right now. But these 15 seconds. So there would be one block that's produced. There would be 30 different transactions within that. And that gets recorded onto a chain as a link in that chain. And the chain just keeps on adding to the end of it. So, it's addendum-only ledger technology. You can't go back and change anything that happened earlier in the ledger. You could see everything that happened earlier in the ledger through history.

That's why like the, one of the big misconceptions is that blockchains are great for crime. It's actually the absolute worst thing that you can use, that a criminal would use, unless they're one of two things: dumb or don't care about people finding out who they are, kind of thing. Like, uh, North Korea, they, they understand that people are gonna know, this is North Korea, we don't have extradition, so we don't care about it kind of thing.

Because what a blockchain does is it takes a permanent ledger of all these transactions through history and makes it public. So if you're a cartel member, the last thing you want is a permanent, immutable record of all your criminal activity that is publicly available that all they need to do is figure out who owns the wallet that was doing this-- which is pretty easy to do with modern technology, because you have to off-ramp eventually. You can't go into a grocery store and buy a loaf of bread with a thumb drive with bitcoin on it. You have to touch the traditional financial rails in some way, shape or form. Creating that permanent record of those transactions that, unlike a small bank, records don't get lost. Bitcoin doesn't go outta business. It's never down. Like, so it creates this constant chain of activity of, I can tell from the first bitcoin ever created where that bitcoin has ever been. I can tell everyone who's owned it. I can see, I can see what day it was transferred, how it was transferred, who was transferred to, all on this like public network. So you get this public benefit.

And that's, the security of the blockchain comes from two things, the cryptographic proofs that underlie it, and the fact that it is so public that whenever there is a exploit, a breach, something wrong with the technology, it's caught very quickly by members of the public. So you can see when something is happening in real time, fully audible. And it's immutable, so it can't be changed later on. No one can erase a history later on. Which is one of its huge benefits and one of its drawbacks.

Matt: All right, so let's go one step further then. What are these distributed networks where the blockchain currency is accepted and transacted?

Jonathan: So, what started with bitcoin, which is really just a way to send peer-to-peer currency, has evolved into what we call blockchain technology And some people call it Web3. So Web 1 you can think of as the, when you had an AOL disc that you get your internet on, and you could go to five different websites that were static and the only people could contribute to those websites were the

owners of the website. So, pre-social media, kind of web. That's Web 1, is what we consider. Web 2 is what we would say, social media.

Matt: This one?

Jonathan: What is that? Is that an AOL disc? Do you actually have an AOL disc?

Matt: Is that, is that, is that, is that what you're referring to as Web 1?

Jonathan: The, like, I'm, I'm referring to it as like Netscape.com.

Matt: Oh, I love that. That old modem sound from when I was in sixth grade.

Jonathan: Oh no, I couldn't hear the modem. But yes, yes, that is exactly what Web 1 was.

Uh, but so then Web 2 came along, which is social media. Which is content was being provided by users, but the content's not owned by the users. Um, it's licensed. You get a license to use Facebook or any of these social media, YouTube, whatever it is. The old saying of, if you're not paying for the product, you are the product situation. Where you get a license, you, you issue a license to others to also publish your data, but you don't truly own it. The Facebook, you do whatever. If you upload a picture, it doesn't matter how many times you post that 15 USC copy-paste that you see your grandma post that says, I prohibit Facebook from using this, kind of thing.

Matt: Right.

Jonathan: Like, I need to break it to you, Facebook can use anything that you post on there.

Matt: So it's a way of owner ownership in the cyber-verse.

Jonathan: Correct. So that's what Web3, what the Web3 technology does is it creates ownership. So instead of websites being totally done, instead of the tech infrastructure we're using being subsidized by the provider essentially, and then you get the benefit of their services but they're paying the web cost, server cost.

What you do on crypto technology is you pay a small fraction of a fraction of a cent transaction fee whenever you interact with these networks. And you get true ownership of whatever you do. So if I create a picture that I record on the blockchain, I pay that blockchain a small transaction fee, and now they store that data for me on behalf of the blockchain for that, like that small picture. So, essentially set up--

Matt: And those networks, those networks, if I'm not mistaken, are multinational.

Jonathan: Correct, correct. There is no national restriction. It's, it's, as open web, as open web can be.

Matt: And at, and at a certain point, can you cash out and then exchange for the bullion currency of whatever particular government that you, you want?

Jonathan: Correct. So, like I said, you still can't buy a loaf of bread with a hard drive. So you have to be able to, like, transfer these assets into your fiat currency of choice. So a way that's done is through exchanges. Binance, Coinbase, Kraken, Crypto.com: These are places that will take your digital assets, exchange them for fiat currency, which then you can send to your bank account and use it that way. There's also providers, like Visa is providing a way that you can use your cryptocurrency and then they will take care of the, the conversion from crypto to cash, and then you can use a Visa card that is, plugged into your account through your crypto. But they do all the, there, there has to be a transaction between your cryptocurrency and whatever the store you're using this at, that function out.

So that's where kind of the lots of, where you see like AML KYC is done is often at the exchange level. Same way that you don't, when you hand someone cash on the street or something like that, if I, go by and give cash McDonald's, McDonald's doesn't see my ID. But when McDonald's put that cash into the bank account, that's when people know like who the person is that's putting things in, kind of thing. So that's where kind of, that, that gating function is often at, is at that exchange level, where people can convert their digital assets to a fiat currency.

Matt: Well, let's go to the logical conclusion of this discussion of the mechanics of crypto or digital assets and, and talk a little bit about how it's emerged as an investment vehicle as well. How does that work?

Jonathan: So, there's two types of, I would say two primary, there's a million different types of investment areas within the digital-asset ecosystem. But there's two primarily that you're thinking, that you would typically think of. The first one is the bitcoin store value, kind of, there is a guaranteed rarity within it. There is network security within it. So it's a way for you to store your value. Which is, that was the --and store and send --value without intermediaries. The Bitcoin network is actually the first block of Bitcoin. Recorded within, it was a critique of England bailing out its banks. So there was a saying like, hey, we can't always necessarily know we can trust these, uh, financial institutions, so we want another way for people to be able to store their digital values. That's, that's the Bitcoin network. And that's uh, that's pretty substantial.

What you're seeing now, a lot more of it is people that want to tokenize their products. And when I say tokenize, what it is is you're creating a digital representation of a good or service that can be corded on a blockchain. And then you can use that tokenization for faster ease of transferability and settlement. So like, my big, like why crypto, like my moment, what made me understand crypto, was

that if you want to send $1 million from New York to London, it is faster to get $1 million in cash, put it in a duffel bag, take that duffel bag to JFK, fly it to Heathrow, then take that duffel bag of cash to a bank in London to actually have that transaction be finalized. The amount of time it takes to take cash out of a car, fly from New York to London and go from the airport to a London bank was faster than the electronic transfer between those two banks. Like there's just, it takes a long time for digital settlement to happen on a, on a traditional rail. 'Cause you have multiple parties, parts, counterparty risk, everything has to be settled.

Matt: So, so a traditional rail being like a fed wire.

Jonathan: Correct. But what digital assets allow for is settlement finality. Like I said, there's cryptographic proofs that prevents you from sending things multiple times. You don't need a, you don't need a bank protecting the overdraft or a bank to say yes, they actually had the account and now you can transfer this other account. Like the, the technology stops that. So for example, the CFTC recently approved the use of tokenized deposits, bank deposits or tokenized products as collateral to support margin positions. And one of the benefits of that is instant settlement. So if I need to liquidate a position, I can actually instantly get that collateral. I don't have to wait for any settlement time. I don't have to wait for anything to clear. I can instantly get that collateral and redeploy it. So that, we don't have that t-plus-three or t-plus-one or weekend closing or anything else like that. You can take these assets that people are already transferring and do it in a way that there's finality nearly instantaneously. Which in financial markets is a huge boon and it allows people to efficiently deploy capital better, manage risk better. There's no kind of delay in any of these things. So it, it's, it's a massive upgrade to how the current system works when it comes to settlement finality, network security and, just efficiency of that. And also without the added intermediary costs that come with those transactions.

Matt: So it's the, it's the digital bag of cash with assurances that the cash is delivered to the tended recipient and not diverted in some way. And on top of that, it tracks who the recipients of the bag of cash are.

Jonathan: Correct. You can send, or anything can be tokenized. You can tokenize a bar of gold. Say there's a bar of gold in a vault that you want to transfer. You can put that on a blockchain and then transfer that 17 different times without the bar of gold ever leaving the vault, without there being a risk of fraud that that's been transferred or something else like that.

And then whenever the person who holds that to that warehouse receipt essentially of this tokenized bar of gold, they can go to that vault and say, hey, I'd like my physical bar of gold now. So they can get that immediately. And there's no risk, unlike a warehouse receipt in traditional, like, formats, that there's two people coming forward and saying, that's my bar of gold. Like, you know, that's the only

one because there's an immutable record of when it was created, who it was created by and when it was redeemed, in that situation. So it's just a huge, huge benefit on, on that as well.

Matt: Would you agree with me that what you have just described to people that are used to dealing in fiat currencies is complicated, confusing and a little scary?

Jonathan: 100%. So what, what blockchain tech takes, is it takes two things that people are pretty hesitant to interact with-- computer science and complex finances-- and it combines them into one topic. So even computer scientists are like, well, I don't understand all the financial aspects of this blockchain tech thing. And even people that are very financially literate say, well, I don't understand all the, the computer science aspect of how this blockchain tech works. So it's takes two very intimidating, uh, kind of, ideas, two subjects that are intimidating to a lot of people, and combines them into one. Which obviously is going to be a, a large, like, learning curve for anybody to, understand both those things sufficiently to really understand the value of blockchain technology.

But that was the same way that internet was back in the day. So I mean, it's saying like how email, you don't necessarily have to understand how email works. It works, you can use it. You don't necessarily understand how, like all the technological background of like the internet and how, like what HTTP code is or what a get-request is or anything else like that. You just know when I type in www.facebook.com, Facebook comes up. And that's what blockchain tech is increasingly becoming. We're abstracting away all the scary parts of it and making it so it's much more user-friendly, so you don't even necessarily understand the reason that this is costing less, and the reason this is faster, the reason it's better is 'cause it's using blockchain tech. You just know like, oh yeah, that was, that was awesome. That was quick.

Matt: My grandma, my grandmother posted on Facebook and sent email well towards her hundredth birthday. She passed away at 100. But was on her iPad, sending emails and going on Facebook up until her 99-and-a-half birthday. So I get that the technology ultimately will maybe become like that. But you'd agree it's not there now.

Jonathan: Uh, I, I would say there's some things there, there now. Uh, there are some applications that, like my parents have a Coinbase account or a Kraken account or exchange account. They can buy and sell. They get that, if I wanna send my parents like a portion of a Bitcoin or something like that, they can receive it. They can take it, they can, they can understand. Like they don't see that as anything more than a website. They don't understand how anything, how it, how it all functions necessarily. But they can interact with it. And I think that's increasingly going to be.

But no, I would agree with you that a vast majority of the consumer applications are not there. Prime example: prediction markets. I am sure you heard the Polymarket odds of a presidential election or so-and-so election or anything else like that. The way that all these prediction markets run is with

crypto as the background. That's how they know how many buy and sell positions there are on either of these two products, is that they use crypto rails on that.

So like you can go on, uh, Kalshi right now and I don't think Kalshi is super hard to navigate or use as a standard person. You would have no idea that crypto is what's powering, or that blockchain tech is what's powering all that in the background without that understanding. But that's what it is, that's being powered by blockchain tech.

Matt: We've spent a little time now dissecting the "what is crypto, what is a digital asset?" Let's move into the enforcement trends associated with those digital assets. 'Cause after all, we're podcast about white-collar criminal law, which is financial crime heavy. Not exclusively financial crime, but predominantly financial crime. And if this is the financial instrument of the future, the enforcement trends of the future may very well come down to this particular type of digital asset. So, what are some of the enforcement trends that you are seeing with crypto or digital assets right now?

Jonathan: So there's probably two primary areas that are being litigated right now. Um, one is how money transmitter or money services business laws apply to digital asset transactions. And the other is how, like, fraud or computer fraud and abuse kind of issues deal with that.

So on, on the money transmitter side, there is a discussion currently going on, there's cases being litigated right now, on privacy-preserving technologies on these blockchains. So, like I said, a blockchain is public. Anyone can see every transaction has ever happened on a blockchain. The wallet address, the person who owns a particular wallet address, the person who owns that routing number, it isn't necessarily public, but it can be made public through various technologies. So there are, there are tracing firms that do that. And anytime one of these, these wallets interacts with a centralized entity-- a exchange of some sort, you're sending something of some sort-- there's a way you can trace that to a individual. So obviously, there's huge risk with that.

So we, there's something called wrench attacks, which is based on, it's saying that you you can be as secure as you want to with your digital goods, but if someone shows up and threatens to beat you over the head with a wrench, they can take those digital goods from you. They can take that password from you. So if you're somebody who has a $100 million of bitcoin, you might not necessarily want the world to know every single transaction you do with that $100 million or where that $100 million is stored. So people have built these privacy-preserving technologies. Mixers is one way. It's essentially a way you can throw a bunch of people's money all into, uh, what you would think of mixer, you'd all get mixed together, and then you can cryptographically prove which one is yours, but no one else can tell what it is.

That obviously has huge concerns, from financial regulators. So, we have KYC, we have the Bank Secrecy Act. We understand that there are times when you wanna be able to know who is sending

things to what and things like that. And the technologies that can obfuscate that is a potential danger.

So, these technologies, though, they don't ever take control of people's funds. So it's still peer to peer. You're still interacting with either another human being or just purely interacting with software. The software, the person who deployed that software, if somebody said, gun to your head, stop that software from working, give it to me instead, that the government says subpoena here, we know someone's going to use your software, you have to stop them from doing it, you can't do it on this software. It's not possible. It's technologically impossible on some of these things. So the question arises, if you create this privacy-preserving technology, are you a money services business? You're helping people handle their funds, but you aren't personally handling it. You don't ever touch it, you never have custody or control like every other money services business. So is that subject to, are you a financial services business? Do you have --

Matt: Like a trust, trust company in a way?

Jonathan: Exactly. It's a, all right, yes, you can transfer cash in a Chevy, but you don't have to register every single Chevy as a money transmitter, right?

And so it's, it's those things where that we're dealing with those questions, and that's what there's, there's market structures, the, uh, the legislation's going on in Congress right now that deals with some of these issues. But in the meantime, we're trying to apply laws that have been designed for non-bearer instruments when there's always going to be an intermediary, like, to apply something that doesn't necessarily need an intermediary.

We haven't had intermediary-less financial products since bearer bonds in the, what, sixties, seventies, somewhere in there. Cash is the only other example. But even cash, you have the, you have the limits on bank secrecy and you have third-party doctrine and all the things that come along with that.

But, these are new technologies that these old laws that are designed to regulate intermediaries are trying to address how do we regulate something that is intermediary-less? And who do you put those regulations on when we can't go to a bank and say, all right, you're the one with KYC obligations like we would with a cash transaction.

Matt: In your view, as an advocate of digital assets, why has crypto enforcement been sort of a pressure point for law enforcement and regulators?

Jonathan: I, I think it probably is twofold. One is just a lack of understanding of how the technology fundamentally works, which isn't the fault of the financial regulators, especially the federal government. Within the federal government, there is a government's ethics accountability ruling that

says that if you regulate crypto in any way, shape or form, you can't own crypto. So if I work at Treasury regulating stable coins, I can't own bitcoin or I can't own ethereum. Even though I don't, nothing I do regulates those particular digital assets, I can't own any digital assets. Now think about that from, if you said, hey, if you work at the SEC, you can't ever own stock. You can't, you can't, like, it doesn't matter, like not just the ones you regulate. You can't, you can't have used Fidelity before. You can't use a brokerage fund before. Like, it, so you have these people that are put in this hard position of trying to regulate something that they're not allowed to actually play around with, test, do themselves, understand like, here is my pain point, here is my risk, like here's where I found an issue with. So there's that issue. And it just goes back to like the initial use, the primary use of bitcoin in lots of its early days was Silk Road. Like it was a, it was used for crime in its early days.

Again, this is before people realized--

Matt: And on this very podcast we had the author of the book on the Silk Road. We talked all about it.

Jonathan: That's, yeah. So if you, you go back to that and that's just before people realize, oh, this is actually creating a permanent, immutable record to all these transactions and things like that, that, uh, when I was in private practice, we would have people come to us and say, hey, my sister died. She had this wallet. I transferred these funds to my, I found this, this digital wallet with funds on it. I sent it to her Kraken account and now I have the DOJ doing an asset seizure on it because it was used on Silk Road at some point. It was used, uh, it was something like that. So, people didn't realize how much of a record they were creating of their criminology at that early age, but that was what it was used for a lot.

And it still is used for like ransomware. Again, it's not because criminals think that like I'm getting away with it, that I'm being secretive about it. We know that ransomware actors, they're in Russia, they're in China, they're in North Korea, like we understand where they're at. But it's just, it's easy to transfer a bitcoin than it is a bar of gold or is other, any other kind of bearer-asset kind of thing.

So you do see that issue as well, of that it's using ransomware, it had a history, uh, being used in its early days in crime. So there's still that kind of, that idea that really that's used for criminal when really the latest report from the leading forensics firm in digital assets says, I think it's like less than 1% of all digital assets have touched any kind of criminality whatsoever at this point.

Matt: Are the traditional bricks-and-mortar, anti-money laundering, counter-terrorism financing regimes that exist in our country sufficient to police this new frontier of digital assets? Or is it high time that our legislators get their act together and put together a comprehensive set of reforms that bring our anti-money laundering laws and our counter-terrorism regimes up to this technology?

Because in my opinion, there seems to be a lag. Or can, can the direct analogy be made and, and there's just a seamless application of these laws to this new digital asset world?

Jonathan: There definitely needs to be new regulations and new laws as well. I, I don't think anyone would debate that, industry or otherwise.

You see that with market structure. So, back in the spring, House of Representatives passed what we call the Clarity Act that was this comprehensive framework for saying, if you are a developer of this software, here's where it's free speech and here's where it's money services business. Here is where you're publishing just open source code-- which is protected by the First Amendment-- and then here's where you run in, you have to register with Treasury. Or here's how we have to do this. And, and here's the parties that are responsible for this. Again, we're dealing with a, a system that has been reliant on third-party doctrine for the longest time.

So where are the on-ramps and off-ramps? Where are the choke points? We can't expect in a software that anybody can create a digital wallet without needing to have KYC, and there's no way you can make the technology require a KYC AML for every single one of these wallets you can spin up. Where are the choke points and where can we regulate to make sure that any assets they use in illicit finance, when they touch traditional rails, when they're trying to be used in everyday use, where are those choke points? So like exchanges are a big area, but that would be regulated on this. Same thing with like spot marketplaces, things like that. So that's what Market Clarity does at it, at its core, is create these, these rules of the road of when digital assets are sold as securities or commodities. Who has KYC AML obligations on top of it? What rights do people as software developers have in this technology and what rights do they not have with this technology? That's what's currently being discussed by Congress. Like I said, the House passed a Clarity Act. It's currently in the Senate right now being considered.

The Senate Agriculture Committee just passed their half, which deals with commodities portions of the industry. And now being on to Senate Banking to pass their half of the bill, which deals with these banking AML KYC, um, and securities aspect, of, of the digital assets. And in the meantime, regulators are moving forward, we saw actions from the OCC, from FDIC prudential regulators. FinCEN has put out guidance. FinCEN's guidance go back to 2016. They have guidance going to convertible virtual currency and how that works. You have SEC and the CFTC just had a joint meeting the other day, talking about their plans for Project Crypto. So legislation's definitely needed, and that's what Digital Chamber is strongly advocating for and what we're working with Congress for.

But in the meantime, the regulators are starting to move forward and say, hey, the past like three or four years, we tried to square-peg-round-hole this. It hasn't worked. The things we're trying to do are not working. So why don't we make a round hole for this round peg and make the regulations actually apply to how the technology works instead of saying, hey, we have everything that's been

relying on intermediaries, let's just force them to intermediate something, let's just make them use intermediaries-- which takes the core use case of the technology away, so it just turns things offshore, people just go offshore, they use VPNs, they just go around it --as opposed to, how can we actually regulate this in a way that's enforceable and that is actually lasting and doesn't hamper constitutional rights like free speech, publishing a code, things like that?

Matt: From the law enforcement side of the crypto or digital currency space, what are a couple of the more high-profile digital currency enforcement cases out there right now?

Jonathan: So one of 'em is dealing with mixer services, like I said. There's a service called Tornado Cash. And Tornado Cash was a service where people could send their, uh, certain digital assets within this mixing service, and then the, the software would, would run in the background and be able to obfuscate the origins of, of that digital asset. So, the developer of that, Roman Storm, was recently convicted of failing to register as a money services business. That is being appealed right now, as well. So, and that goes to the control aspect of it. So, even when he was in jail, even when the software has been sanctioned by OFAC, even when they did everything they could to stop it, it was still running in the background. Like I said, this is immutable, permanently running software. As long as there's somebody somewhere with a computer that is validating transactions on their software that could be located anywhere in the world, that software will continue to run. So you could continue to use the software regardless of it's being sanctioned, regardless of its website, being the front end, the way you access it, being taken down. That can't stop you from being able to access it. This is still running in the background because it's noncustodial software, it's just permanently out there. It's open source. Anyone can use it. You cannot take it down like a webpage.

So, that is one case that's currently being litigated. And that goes to whether custody or control is necessary to be qualified as a money services business, or whether just publishing neutral software and others using it for both legitimate and potentially criminality purposes, if that's something you can hold developers responsible for. So that's one, that's one key area that I think there's going to be a lot of debate on. And there's, there's multiple visions within market structure that goes directly towards what kind of liability a developer should have for their software being abused by third parties.

Matt: Does crypto, in your opinion, attract what I would refer to as an outsized law enforcement response because of the techy, spooky, futuristic nature of what's happening with digital assets?

Jonathan: I don't know if I would say outsized. Uh, I would definitely say outsized when it, when it comes to the total market cap of cryptocurrency and the amount of focus that law enforcement puts on cryptocurrency as opposed to physical cash and things like that. Just because the crypto market is still a $4 trillion market. Like, it's, it's relatively small in the grand scheme of things. I think that, uh, gold, the other day, the market cap of gold, did like a swing of half the total market cap of all crypto,

with like a 10% swing in the price of gold. Like that, like it's, so we're still talking about a fairly small market document talking about the grand scheme of financial markets.

So in that sense, yes, it does get outsized, I would say, law enforcement attention. But also it's a new technology that I think law enforcement understands is going to be increasingly used in traditional financial markets. It's not just a bunch of geeky computer scientists sitting in their mom's basement sending bitcoin back and forth and buying each other pizza with it.

Like it's, it's actually--

Matt: It's mainstream now.

Jonathan: Exactly. So, law enforcement understands they need to understand it. They need to have tracing technologies for it in the same way that they understood, they had to understand how like banks work when the wire transfer happened, when you weren't just sending everything in trucks.

So--

Matt: Do they, do they right now? Do they have that understanding that allows them to effectively conduct traditional law enforcement, anti-money laundering-type work while not throwing the baby out with the proverbial bath water and de-legitimizing the entire use of digital assets?

Jonathan: I think they're trying. I, I think that they are. And I think there are a lot of third-party resources within the crypto industry that are also helping with that. Like internally as an industry, we develop very, sophisticated tracing technologies so you can trace digital assets, not only from all when they've sent, but also when they, when they go across chains, when you use these mixing technologies. Like these mixed technologies are not foolproof. Like you can unwind lots of these transactions with the correct amount of technological know-how. You can find things through clustering of wallets and understand like, all right, well we can say with a 75% of certainty-- or 80% or 90% certainty --that these seven different routing addresses are all controlled by the same person. And that makes it easy to figure out who that person is if you know they're all the same person, controls all of 'em kind of thing. So they definitely are there. There is a, I, I work closely in private practice with the dark web task force, a group of members of FBI, IRS, DOJ, that were dealing with things on dark web, whether that's ransomware. Or pig butchering is a form of like where you get --

Matt: Tell our audience what that is. That's a very descriptive term.

Jonathan: So I, I, I always hated using it when I was talking to a client that was a victim of it. But what pig butchering is, it's where somebody will --usually, it's like a LinkedIn and social media, something like that-- will contact individuals, say hey, my uncle does crypto investments for you, or my uncle's crypto investment, he has a 10% return or 25% return this year. Want me to like, hook you

up with him and like, you guys can trade through him or trade through this exchange or things like that? It's all fugazi. There is no exchange. There is no uncle. It's a way to get people to send them digital assets. And then there's some complex social engineering that goes on in the background and people think, hey, I've already gotten a 10% return and I sent them a thousand dollars. Now I'll send 'em $10,000 and they can gimme a 20% return. And I'll send them $100,000 and they gave me a 50% return.

Matt: I've represented some of these folks.

Jonathan: Yeah. And then when they try and cash out, they'll do one final-- usually that's the, that's the worst part is they'll do like one final kick of being like, oh, well, because this is an offshore exchange, you have to actually send us another $50,000 to pay your taxes on all these gains we made for you. That never, actually, there's no, there's no, that money's long gone. It was gone as soon as you sent it kind of thing. But just like, it's social engineering scheme to get people to send them larger and larger amounts of money until they're completely drained. But that's what we call pig butchering.

Matt: Like the grandparents scheme, where they say, you have to show up at the CVS with a bag of cash, or your grandchild is gonna not get outta jail or something.

Jonathan: It's the old, it's the old, like, like we had the Kenyan prince scheme back in the day. We had the CVS. We still see like people being like, a CEO emailing you like, hey, I need these like 17 Amazon gift cards right away. Like, like it, it's those kind of, those, wherever there's money involved, there will be bad actors that are trying to separate good actors from that money. So that's no different in crypto than it is in everything else.

But, we are seeing that the DOJ just, they just caught somebody in Cambodia that had billions of dollars of these pig butcherings. Like we are getting more and more sophisticated, it just, it takes a while. There's this new technology that people are dealing with and there are, it's hit or miss when you're dealing with people at DOJ there could be someone with the FBI that you're dealing with that day that has a very sophisticated knowledge, they worked on Silk Road cases going back in the day. They understand, they've been working on this for 10 years. And then you'll get somebody that's never dealt with it before and you have to like kind of teach them along the way as the attorney working with them on behalf of a victim and, like, talk them through these things.

And the same thing when you're, when you're dealing with prosecutors or uh, U.S. Attorneys, there are some that are very sophisticated and understand the technology very well. And then there's some that, they just got handed a case that happens to deal with this technology and now they're trying to figure it out.

Matt: Well, we're rounding out this discussion about enforcement, right. What are some of these jurisdictional hurdles for enforcing this global currency that doesn't have a particular nation's flag attached to it? It's not the, "In God We Trust" dollar bill with the, you know, e pluribus unum and, and, and, and all that stuff that we have on the dollar bill. It is pretty much the Wild West. It's prevalent throughout the world. There's no central bank having regulatory control over it. What jurisdictional hurdles are we going to have to get around? Or is this going to take a global regulatory scheme?

Jonathan: So, uh, there's definitely regulation, especially when it comes to the use of this software that is always running regardless, and all it needs is one computer that's validating these transactions somewhere in the world, doing the validating function behind it that's running this software. So we saw that with, there's a case called the Mango Markets case, which was Avi Eisenberg, was the name of the individual. He found a way to exploit this marketplace, in a way that he made off with quite a bit of funds by, just this, I could go through the whole tech stack behind it, but all you really need to know is that there's a person that used this autonomous software. He was in Puerto Rico at the, in front of his computer at the time that was using it. And they prosecuted him in the Southern District of New York on the basis that, one of the softwares that he was using, they had servers that was running on it based in New York. So they tried to bring a jurisdiction, they tried to claim jurisdiction based on that. That actually got thrown out by the judge as that you do not have jurisdiction over this person that is trading this from Puerto Rico on this software that can be used anywhere just because there have to be one server that contributed to this software in the Southern District of New York.

Matt: The old international shoe, minimum contact.

Jonathan: Exactly. Minimum contacts, all of that. So yes, there's going to be a lot of jurisdictional challenges because this is a, thing that there is no gating function. There is no, you can't, it's not like worldwide web or ISP providers or things like that. You can put some kind of gating function on who can access what from where kind of thing.

So it's gonna depend on where the actor's located it or where the victim's located. And you build out jurisdictions, just like we have on the internet forever kind of thing. Like there's been scams that have happened across international lines using internet technology using VPNs that might obscure like where the person was accessing this technology from. But we figure out, we do our jurisdiction in the same way we do anything like it's, again, victim located, where the harm is felt or where the crime is committed by the individual. So I think there is going to be jurisdictional challenges, but it's mostly in the form of trying to assert jurisdiction because we wanna regulate it, not necessarily because that's where jurisdiction is correct. Which I think is where people are running into issues now.

Matt: Right, right. Makes sense. From my perspective as a defense lawyer, digital asset enforcement or crypto enforcement is one of those dangerous areas, right? Because there, in my view, is a substantial risk that the presumption of innocence that is afforded to every single criminal defendant could almost be shifted onto the defendant in the sense of having to prove, just due to the sheer complexity of these digital assets, that what they were doing was right and, and not illegal, not wrong. And I think that is the scariest proposition is the, almost the idea that jury nullification could be ripe in these particular cases where somebody, just by virtue of the way that they're conducting business, is left to prove the legitimacy of that business because it's this spooky technology.

And the case in point is, is is sort of the old, you know, paying in cash. You're allowed to pay in cash. The question is whether you properly withhold taxes from that cash, if you're, you know, doing payroll or something like that. But it, it's, it's very clear on a dollar bill that it's for all debts, public and private. But there was always the connotation that if you decided to pay somebody in a bag of cash-- and law enforcement loves to play into the stereotype that those that deal in cash are somehow engaged in illegality, even if those individuals are up-to-date on all their taxes, they pay every cent of their taxes. That's just the way that they could transact business for one reason or another. Is this currency faced with that same stereotype, the same presumption that would impact a defendant facing charges criminal, fundamental right to have the government prove that what they're doing beyond a reasonable doubt is wrong?

Jonathan: I, I think undoubtedly. In the criminal cases that we have seen, that has definitely played out. So going back to the Mango Markets case that I was talking about before, a jury actually convicted Avi of fraud in that case, that what he did was fraudulent, even though he didn't lie to any human being. He didn't, he didn't do the typical fraud case where you are saying a misstatement, or he didn't use someone else's password, so didn't touch Computer Fraud Abuse Act. There wasn't anything like, he wasn't saying like, hey, I'm actually 15 when really I'm 34. Like, there wasn't any of that situation. What he did is he used the software in a way that maybe wasn't anticipated, but was perfectly within that software's application. So he got charged with fraud. The jury saw, hey, here's this person that did something that we feel is wrong, that we feel is kind of shady. There's people, there was counterparties who got hurt, other users of software got hurt. He didn't defraud any of those users of software, but they had put their money into the software just like anybody else did. So money had to come somewhere. But he didn't commit fraud against any of 'em. He didn't tell any of 'em to put 'em in, put their money in there or do anything like that. So, uh, he got convicted of fraud, but the judge actually overturned that conviction on saying like, hey, this actually doesn't meet the legal requirements of fraud. There wasn't any of that, there wasn't, he didn't lie to anybody.

Matt: Intentional misrepresentation or omission inducing reliance.

Jonathan: Correct.

Matt: The basics of fraud.

Jonathan: He didn't do any of those. He didn't intentionally misrepresent. He still got convicted on commodities manipulation, which is a part of how he was able to exploit software, but it wasn't fraud kind of thing.

And we're seeing it now, there's this, there's this trial called the MEV Brother trial, which actually went to a mistrial. The jury couldn't reach a verdict on that. There was actually reports that there were jurors brought to tears trying to understand how this technology worked.

Like there was, like, they were trying to reach the right conclusion so hard, but they were probably, there were people brought to tears trying to figure out how does this even work and ended up being a mistrial. And so --

Matt: Thank god for appellate review where judges and experts can present the appropriate facts that maybe the jury can't grasp.

Jonathan: Yeah. And I mean, but that was also like, maybe Avi just got lucky that he had a judge that was able to think critically about that while another person could have the exact same situation happen to them, and it's a judge that just doesn't wanna take the time to understand how the technology actually works to really understand the nuances of it.

And maybe he would've been convicted for that and he would have to wait for appellate review of that and then hope the Court of Appeal judges took it a little more seriously or had a better understanding of it. And then if that doesn't work, hope that it's a Supreme Court issue that they could understand it.

But again, me explaining as a, both in private practice and then in my advocacy role now, me explaining how this technology works as whether there's lawyer or advocate or anything like that, they're still humans you're explaining it to. A judge is still a human you're trying to explain it to. So the, the jury is still, they have their internal or external biases that come along with kind of the crypto early days and what the human news about crypto and things like that. That these take a level of understanding of how the technology core functions to know where that fits within the elements that I think that you're gonna run into a situation, both with juries and judges, that see that proposition of trying to understand technology, how it works to reach the right conclusion, as too hard. And in the absence of that, do not rely, do not accept the instructions that they are to presume that you have this presumption of innocence and just see somebody with, who made a lot of money in crypto doing it in a way that they don't understand, but maybe that feels wrong to them. And they're just going to, they're going to, like, make an equitable ruling based on that, maybe not based on the actual law and applying the facts to the law.

Matt: We're talking with Jonathan Schmalfeld. He's the Director of Policy for The Digital Chamber, the oldest and largest digital asset advocacy group in the United States. Jonathan, in our waning moments together today, I, I want you to take out your crystal ball-- this is one of my favorite, lines of questioning on the program-- and I want you to predict what type of digital asset enforcement trends we'll be seeing five and 10 and 15 years from now.

What, what's on the horizon? What does the future of enforcement look like in this space?

Jonathan: So, I, I think for the next, at least five years, definitely, we're going to have to have a reckoning with privacy-preserving technologies as applied to digital assets and where that fits within Bank Secrecy Act/AML/ intermediary-reliant situations that we dealt with, and that there isn't that third-party doctrine. So we're gonna have to deal with when there isn't a third-party doctrine, what rights do you have to privacy and what rights do you have within your own uses of these technologies to privacy when there is not an intermediary here.

And same thing, how much can you do to protect your privacy legitimately? And then when is becoming, when is using these privacy-preserving technologies, something that we will deem to be illegal because there's enough use of criminality that we're going to apply that law there?

So I think that is a main thing, is where privacy comes and what extended privacy you have. If there isn't a third-party doctrine to rely on.

Matt: You know what, my mind immediately went to when you started talking about that was the crime of structuring. Structuring transactions. And in the opioid crisis, one of the ways that these pill mills were targeted is not because of medical necessity. It's very difficult to make a case of a doctor prescribing against medical necessity, because a physician goes to medical school, they have an enhanced expertise and who are we to challenge that? But structuring transactions became a huge tool in the Department of Justice's toolkit. And all that really means is that you have a high level of cash and you break it down into individual deposits into your bank to evade the compulsory reporting requirements of a deposit greater than $10,000. So, what you would see is criminal cases being made out of medical facilities having deposits of $9,999, and then the next day having one for $9,052, and then the next day, when in reality they made that, $20-30,000 in one day and they broke it out over the course of days. And I, I had a case where I represented a medical practice that the primary piece of evidence was the, the breakdown. They, they kept a spreadsheet of their daily revenues and then how they were going to go ahead and structure it.

And what I'm hearing you say is that it's gonna take us developing a regime that understands the way that, the nefarious ways that crypto and digital assets are being masked in order to first devise the laws that we can then use to police this stuff when it's used nefariously.

Jonathan: Exactly, 100%. Like, and how do we take--

Matt: You can't just say, blanketly say to everyone that decides to use crypto or a form of digital asset, that because they're doing it that way it must be illegal. 'Cause that's absurd.

Jonathan: Exactly, and I mean it, it's how do we take the BSA in its 1970s, both numbers of both amounts and what it applies to, and apply it to 21st century technologies like, like cryptographically proof technology. And how do we do that in a way that doesn't tread on people's constitutional rights, their First Amendment right to create the technology, their Fourth Amendment rights to be free of search and seizures.

Like how do we, how do we create this in a way that we, we really do affect the illicit actors, but we don't, make the same mistakes we did with the BSA where there are 99.99999% of sufficient activity reports that go nowhere.

Matt: Right.

Jonathan: And it doesn't really, it's no longer a flag for anything because the, when the BSA was decided as constitutional, that was the equivalent of $90,000 in today's dollars, but still $10,000.

Matt: Yeah. You can't buy a car without a, a SAR being

Jonathan: Exactly.

Matt: In, in today's environment.

Jonathan: Exactly.

Matt: In a quick, in a quick lightning round, what are a couple or three digital currency myths that you would like to see killed?

Jonathan: So, the first one is that it's primary use-- or that even a major use of-- digital assets is for crime.

Like I said, less than a fraction of 1% of all digital assets in modern technology are used in criminal activity. And a vast majority of that are, are not from, uh, what we think of like the cartels or somebody or gangs or anything else like that. It's usually in like a ransomware hack where if crypto didn't exist there would be the same ransomware. They'd just make 'em ship gold somewhere. They would, the same thing would happen. So, um, there is--

Matt: or the proverbial duffel bag of cash that I've been talking about the whole time.

Jonathan: Yeah, the ransom. Yeah, exactly. Ransom existed precrypto, it will exist probably like without crypto, like what people use for the transfer. So I, that's a one, that's a primary myth. I would say.

The, the second is that use of this technology, in a way that you do use privacy-preserving tech or you do take advantage, like you have good opsec, operational security, is any indication of criminality as opposed to just good sound safe practice. I don't have every single in my bank account, like whenever I use my credit card, I don't want the world to see every single thing I bought with a credit card. Same way, and I don't want everyone to see everything I did with my ethereum or with my USDC or anything like that.

That's not saying that I'm doing anything illegal with it or nefarious with it. It's saying that I'm using a immutable, public ledger so I'd like to obfuscate some of the things I do on this immutable, public ledger. I wanna give a political donation, if I want to send money to Ukraine, if I am a battered spouse who would like to use this money in a way. Like those are, those are, there's plenty of legitimate reasons for privacy and the idea that privacy is some kind of an indication of nefarious act I, I think, is something that we as Americans need to get farther away from and go back to our roots of our, our forefathers understood that privacy is an essential human right that should be protected, and that there should be some kind of warrant, reasonable suspicion or anything like that to invade that otherwise presumed right that people acting privately is just using their human rights. So that'd be the two main things, I would say.

Matt: I can't even get into my online banking app on my phone without it taking a facial recognition picture of me to make sure it's who I say it is.

Jonathan: And getting your 17 breach notifications you get later on with your 17 cents that you get because you're creating all these honeypots of people's facial recognition and their fingerprints and their social security numbers and driver's license.

And especially with AI nowadays, like you can, you can take a video of somebody that looks just like them and pull all these like online KYC AML systems. So I think that there is that cryptographic technology has developed really good alternatives to this, something called zero knowledge proofs is one area that they can use this. So, there is ways that we can-- especially in a world of AI-- still meet all those values of preventing criminality, preventing illicit finance, but in a way that doesn't invade people's privacy and doesn't create these honey pots of data that we've just come to accept as Americans that now my Social Security number like being out on the web is just assumed.

And I'll just, I'll get my 17 cents from whoever it was that got breached with that, and then that'll just be there forever and I'll just have credit monitoring forever kind of thing. So like there, there's better ways to go about this in the 21st century that I think blockchain technology enables. And it's just a

matter of getting that accepted by both regulators and everyday Americans that think that there aren't alternatives to the way the current system is. And that the current system isn't necessarily functioning the way it was designed to. So how do we fix that while still embracing the new technology?

Matt: Well, Jonathan, it's certainly been an eye-opening discussion today. I can't thank you enough for joining us. How, how do interested parties get involved in The Digital Chamber?

Jonathan: Yeah. So, you can anytime email me jschmalfeld@digitalchamber.org.

I am always happy to talk to anybody about digital assets. We also, if you're a company that is either involved digital assets or is a company that's looking to be involved in digital assets, you see where the future's going and you'd like to be involved in that, you can reach out to us. We're always happy to talk to people, whether it's for membership or whether there's any kind of concerns.

We work at both the state and federal level. And so our goal is to make sure that, at The Digital Chamber, that the technology is still useful in the United States and that we become the crypto capital of the world and we don't drive this technology offshore. 'Cause that's what will happen if we create a regulatory regime that tries to ban or tries to stop the technology in a international system.

So let's find a way to work through, let's find a way to address the concerns of real risk and let's find it in a way that works the technology so that developers can be in the U.S., so that we can be the financial leaders like we have been throughout the 21st century. So if you're a company that's looking to use the technology, if your company are using the technology, you are a law firm that's looking to do advocacy in the technology, reach out to me. I'm always happy to talk. always happy to work on any kind of advocacy efforts. And uh, it was very nice. Thank you very much for having me, and really looking forward to continuing this conversation in Congress, at the state level and at the administrative agency level.

Matt: Terrific.

Jonathan, thanks so much. I'm your host, Matt, Adam, that's all the time we have for this episode of "The Presumption of Innocence." Until next time, we'll see then. Take care.