FTC Decrypting Cryptocurrency Scams Workshop
June 25, 2018
Transcript

JASON ADLER: Good afternoon, everyone and welcome to the Federal Trade Commission's Decrypting Cryptocurrency Scams workshop. I'm Jason Adler. I'm the assistant director of the FDC's Midwest regional office here in Chicago. I want to thank you all for being here. And I want to thank DePaul University for hosting us. Before we get started, I just have a few housekeeping details to tick off. First, please set your mobile phones to silent. If you use them during the workshop, for example to comment about the workshop on social media, please be respectful of the others here.

If you do comment on social media, feel free to use #cryptoscamsftc as a hashtag. We'll be live tweeting this event using that hashtag as well. Webcasting the event today, and it may be photographed or otherwise recorded, by participating you're agreeing that your image and anything you say may be posted at ftc.gov and on our social media sites. At the end of each panel, if we do have time, we'll try to answer audience questions. We have question cards out in the hall. Feel free to write down a question. Raise your hand and someone will collect it.

And if we have time at the end of the panel, we'll ask them. We're also accepting questions on Twitter. So you can tweet a question to the FTC, so @FTC using hashtag #cryptoscamsftc. Finally, if you're here for CLE, please be sure and find Dan at the check in table. Your attendance certificates will be available [INAUDIBLE]. And now to start off our program, it's my pleasure to introduce Andrew Smith, the director of the FTC's Bureau of Consumer [INAUDIBLE].

[APPLAUSE]

ANDREW SMITH: Thank you, Jason. So good afternoon. Welcome to the FTC's workshop on decrypting cryptocurrency scams. I'm Andrew Smith, the Director of the Bureau of Consumer Protection at the FTC. And I'd like to begin by thanking our hosts here at DePaul University. And I'm particularly happy that we can bring this event to Chicago, which has become a hub for innovation in financial technologies, including blockchain, which is the technology behind cryptocurrency [INAUDIBLE].

I'd also like to thank the extremely impressive roster of panelists we'll be hearing from today, as well as our audience, including those watching on webcast and participating on Twitter. So today we're bringing together a law enforcement industry, researchers, and consumer advocates to talk about scams that are capitalizing on consumer interest in cryptocurrency and the ways that we can work together to fight this fraud.

First, let's start with the basics. What are cryptocurrencies? Mirriam-Webster, which added a word to its dictionary just this past March, defines cryptocurrency as any form of currency that only exists digitally. Cryptocurrencies typically aren't created by a government or a central bank, though they can usually be exchanged for US dollars or other government-backed currencies. And rely upon cryptography to prevent counterfeiting.

Some cryptocurrencies, like Bitcoin, have been in use for years. Others are being created every day. By latest count, there are now over 1,600 cryptocurrencies with a market value of over $290 billion. With the rise of cryptocurrencies, we've seen many signs, from public sources to law enforcement actions brought by us and many of the other participants today, that scammers are using the lure of cryptocurrencies to rip off consumers. We've all seen media reports where cyber criminals target hospitals, schools, businesses, holding data hostage and demanding payment in Bitcoin.

Indeed, one source estimates that in just the first two months of 2018, consumers have lost $542 million just from known cryptocurrency scams. If the losses continue on that trend, consumers will lose more than $3 billion by the end of 2018. But as we say at the FTC, this ain't our first rodeo. And we do say that, don't we, [INAUDIBLE].

So, scammers using novel technologies to defraud consumers, this is nothing new, be it fishing or tech support scams, or bots that pose as real people. Over the past few years, the FTC has taken a close look at emerging financial technologies, including cryptocurrencies that have the potential to dramatically alter many of our financial transactions. And it's clear, like just about everything else in life, that there are consumer benefits as well as risks associated with cryptocurrencies.

Just last year we held a forum at Berkeley to talk about the consumer implications of blockchain technology, and heard about its potential benefits, such as enabling faster, cheaper, more efficient payments. Our focus on scams today shouldn't detract from the many pro-consumer innovations that blockchain-based technologies can bring. But our view is that by attacking and mitigating scams, we can remove impediments to technology innovators who play by the rules.

To help frame our discussion, let me tell you about some of the FTC's cryptocurrency-related actions. We've pursued deceptive mining machine marketers. We've pursued crypto jackers. And we've pursued fraudulent cryptocurrency investment schemes. Back in 2014, the FTC sued a company called Butterfly Labs that we said was deceptively marketing Bitcoin mining machines. As in so many other cases, the company was touting a chance to make money quickly and easily, for an upfront fee.

But, we alleged, Butterfly Labs often didn't deliver the mining machines or shipped them so late that the then obsolete technology left consumers unable to profitably mine Bitcoins. We ultimately reached a settlement that included strong conduct provisions, as well as monetary relief. In 2015, the FTC settled a case with a developer marketing an app called Prized, that supposedly allowed its users to earn prizes by completing tasks like playing games and taking surveys.

In fact, we alleged, the app actually contained malware that used the computing power of consumer devices to mine cryptocurrencies for the developer, without the consumer's knowledge. This practice is now widely known as cryptojacking. And a few months ago we sued for individuals whom we alleged promoted deceptive cryptocurrency schemes, a few of which were what we call chain referral schemes.

According to our complaint, the defendants promised big rewards for a small initial payment of Bitcoin or light coin, as long as participants could recruit more members. In fact, despite a continuous chain of recruits, most participants would fail even to recoup their initial investment. This case is currently pending in the federal district court in Florida.

We've also taken steps to educate consumers about cryptocurrencies. Just a few weeks ago, we put out tips for consumers to look out for and take steps to avoid cryptojacking. We also have produced consumer education pieces, all of which you can find at consumer.ftc.gov that discuss the risks of investing in cryptocurrency, which not unlike other investment opportunities, cannot guarantee a return on investment.

The FTC is not alone in being concerned about cryptocurrency scams. Other enforcement agencies, including the SEC, the CFTC, and state agencies have brought actions and engage in outreach to try to prevent harm to consumers and to investors. And consumer groups, legitimate industry participants, and researchers have raised some concerns about cryptocurrency scams as well. So here's a preview of what's to come today.

Our first panel will provide some background on consumer uses of cryptocurrency. What is a cryptocurrency? How can consumers use it? And what makes it unique? For consumers thinking of buying a cryptocurrency, what information is out there? What information is missing? The second panel will dig into the types of scams that we've seen. Here, we'll be looking at some independent research into cryptocurrency frauds that has been conducted, including by some of our panelists, as well as the results of new law enforcement investigations.

We'll also discuss the challenges in detecting scams and what consumers can do to protect themselves and identify potential scams. The third panel will discuss effective approaches to fight scams. We'll hear more about the different roles that state-- that federal and state law enforcement play, challenges in enforcement, and effective coordination and complaint gathering.

We'll also discuss effective ways to reach out to consumers to protect them from fraud while encouraging innovation. I look forward to a robust discussion that helps further our common goal of understanding and effectively combating cryptocurrency scams. As we often emphasize at the FTC, consumer protection and innovation go hand in hand. [INAUDIBLE] consumer protection laws and regulations apply even as technology changes. Vigilant enforcement protects consumers from financial harm, ensures a level playing field for legitimate industry participants, and promotes consumer trust and confidence in the marketplace.

We will continue to be active in enforcing our laws to protect consumers as technology continues to evolve. I'm looking forward to hearing what our distinguished panelists have to say on these topics. And I want to thank everyone for participating. I again want to thank DePaul University for providing this terrific space for today's forum. And thank you to the FTC staff who put this together, including Elizabeth Kwok, Jason Adler, Dwayne Possa, Jason Moon, Sam Levine, Bruce Jennings, Amy [INAUDIBLE], Nathan [INAUDIBLE], Brittany [INAUDIBLE], Susie McGee, and Nathan [INAUDIBLE].

Now I would like to turn the stage over to our first panel. Thank you very much.

[APPLAUSE]

JASON ADLER: For those of you who have just arrived, I'm Jason Adler. I'm the assistant director of the FTC's office here in Chicago. With me today are Rumi Morales, Christina Tetrault, and Peter Van Valkenburgh. They each have extensive bios, but to keep us on time, I'm going to briefly introduce them and then refer you to the bios out on the check-in table for more information. So Rumi Morales, to my left, is on the advisory board for the chamber of digital commerce. And she previously was the head of CME ventures, a subsidiary of CME group that invests in early-stage technologies. Christina Tetrault is a senior staff attorney on Consumer Union's financial services program team. And she specializes in banking, payments, and financial technology.

And finally on the end here is Peter Van Valkenburgh. He's the director of research at Coin Center, a cryptocurrency research and advocacy group. So with that, let's jump in. And I'd like to start, really, at the most basic level. So Peter, I'm going to hand this one to you. What is a cryptocurrency?

PETER VAN VALKENBURGH: Sure. So the first cryptocurrency to exist was Bitcoin. Paper released in 2008, a network that went live in 2009 in January, and it's been functioning ever since as a way of having peer to peer electronic cash for the internet. The 2008 white paper described Bitcoin as peer to peer electronic cash for the internet. And that's its design goal. And that's generally what people see that technology as doing.

You have money. You want to pay somebody else. In the real world, it's fairly straightforward. You can have cash so you take your $20 bill out of your wallet and you hand it to somebody else. They have it. You don't anymore. This doesn't work well online because online we don't have that kind of scarcity that paper bills or pieces of valuable metal have. Online, a file, like an MP3, can be copied endlessly. So if I was to email everyone on the panel an MP3 file and say, this is actually a $10 bill, I've paid you $10. They'd say, no you haven't. You probably just copied the same MP3 file four times, or five times, or six times. You've turned $10 into $50. You've counterfeited.

So that's just something that's true about the way digital files are. They're replicable. They are not scarce. So having digital money that worked like cash was a hard computer science problem. And Bitcoin was the first network or cryptocurrency, if you will, that solved that problem, that made it possible for me to show somebody online that I've given something up and they now have it without relying on a bank or other intermediary in the middle to keep track of who's given something up and who now has it.

Now, with that as the background of what is a cryptocurrency, I want to just go over a couple of other things. So terms here, this is an organic emergent technology with people building it all over the world. There's no standard setting body that has any real authority, at least not yet, over the emergence of the technology. So the terms are messy because they're just common usage in

something that's very new. And different people have different vernacular that they choose to use to describe it.

So blockchain technology is a broad set of technologies that are inspired by, frankly, Bitcoin's emergence and what that technology made possible. But it extends to things beyond cryptocurrency. It extends to things that are open networks, like Bitcoin, and things that are closed or permission networks, like a consortium that's working on a blockchain, like say amongst six or seven, or 50 or 60 different banks.

So you might have heard R3, a blockchain technology company. The blockchain itself, not blockchain technology, but the narrower term, is specifically originally the word was created to describe the ledger of transactions between all Bitcoin network participants. So if I sent a Bitcoin to Jason, that transaction is going to end up on the blockchain. That's how we know that I've given it up and now Jason has it. That's how you solve that scarcity issue with respect to digital goods.

Other terms, coin, token, cryptocurrency, initial coin offering, initial token offering, these terms, coin, token, cryptocurrency, they are used interchangeably. And there is no fundamental difference, technologically, in general, between something that might be called a token and something that might be called a cryptocurrency, necessarily. And they're used arbitrarily. So just because something calls itself a cryptocurrency, calls itself the token, doesn't mean that they're necessarily different from a technological standpoint.

And then last thing I want to say is, what do all of these technologies seek to do? So beyond Bitcoin, we now have several cryptocurrencies and several tokens, which as I said, are functionally equivalent to cryptocurrencies. What's the general purpose of all this? Is it just craziness? The general purpose is to decentralize, in most cases. And what I mean by decentralization is this, you have a company online that does something like money transmission, and that's PayPal.

Bitcoin, or a currency that is focused on payments, seeks to take Paypal, which is a company that we trust to perform a function, online money transmission, and turn it into a network of computers that are running the same software. And then that network of computers running the same software does what PayPal did. And there's three things, essentially, that PayPal does, just to give an illustrative example, they open accounts for people and they authenticate transactions to make sure that someone else isn't pretending to spend my money on PayPal.

They keep a record of who sent money to who. And they have a management team that makes sure that those first two functions, authentication and record-keeping, are being performed with fidelity by the employees of the company. Now, without a company, there's no employees to perform those functions and there's no management to make sure those functions are being performed well. So what you have instead is computers around the world doing all those functions in a routinized fashion because they're running the same software.

And you don't have management making sure the computers are doing that faithfully because every computer is independently incentivized, or the operator of that computer, is independently

incentivized to perform faithfully because they're able to claim some sort of reward from the protocol. And that is referred to, often, as mining. If you faithfully do the authentication work and the record keeping, blockchain keeping work, you can give yourselves new bitcoins. Or you can get bitcoins from any fees that are attached to transactions.

And so that's, basically, what these systems do. But they're not all focused on payments. So just like you could decentralize PayPal and have a blockchain keep the record, and have cryptography for the authentication, and have incentives for management, you could also do centralize any other web company, in theory. You could decentralize Amazon, their S3 product, which is a Cloud storage project.

And now instead of Amazon providing you with cloud storage as a customer, you have a network of computers around the world running the same software, providing the cloud storage. And then the last way to differentiate between the various cryptocurrencies that have emerged is that they have different focuses and they have different aspirations, or real life accomplishments, in achieving basically four different things that maybe Bitcoin doesn't do well or could do better, privacy, flexibility, scale, and maybe a tie-in to the provision of a digital good or service.

So by privacy, I mean these transactions in the blockchain are all public. So if you knew my Bitcoin address or the series of addresses I use, you could see my salary, if I was actually getting my salary paid in Bitcoin. If we were going to run a global economic system like this, it would be vastly more public and more transparent than what we currently have. So there is a desire amongst cryptocurrency developers and technologists to find ways to retain some level of privacy as we move forward into a world that's increasingly using these things as currency.

Flexibility. So, there's more than just a peer to peer transfer. We have financial derivatives. We have contracts or payments that are triggered by external events. What we could code a lot of that into the automation and put it in the blockchain, smart contracting is what this is called. So if it rains in Peoria and Reuters reports it, my $50 automatically goes to the farmer who was doing swaps based on weather or things like that. Ethereum is probably the most known cryptocurrency that's focused on this flexibility or putting those contracting language, in addition to the payment language, into the blockchain.

Scale, Bitcoin handles about seven transactions per second on a good day now. Really, it's more like two. And that's globally, across all persons sending money to other persons on the network. And that's because everything has to go in the blockchain and then every computer has to independently verify the blockchain. So this is a hard problem and there's several different cryptocurrencies that are trying to solve that, in addition to Bitcoin's core developers. And then finally the tie-in to a digital good.

Some tokens or cryptocurrencies are really primarily used for payments. But the network is designed to do something else, like I was saying, to decentralize Amazon, for example. So you'd go to this peer to peer network to get cloud storage, which is measured in gigabytes, but you'd pay for it using a native cryptocurrency to that Cloud Storage network, which could be File coin or Saya coin, or Storage, which are some of the examples of companies that are doing-- or communities and companies that are doing this.

So that's a rough overview. This is a lot, I know.

JASON ADLER: That's helpful. One of the key points you hit on there was decentralization. So the very nature of cryptocurrency is that it is decentralized, which means that there is no third party intermediary governing it. And obviously that has consumer implications. So I definitely want to come back to that. But just to give us more of a basic understanding of how consumers interact with cryptocurrency-- and I'll turn this to Rumi first, and others feel free to join in-- how can I get cryptocurrency? How can I use it?

So for example, can I walk into a bank and withdraw a cryptocurrency? Can I buy a loaf of bread with cryptocurrency at a corner store? Can I buy a loaf of bread online with a cryptocurrency?

RUMI MORALES: Sure. The answer varies depending on the merchant, right? I think there are-- I think Overstock.com being one of the first, or the most well-recognized of the first companies to accept Bitcoin as a method of payment, or for transactions. There are Bitcoin ATMs. There are a number of them, actually, even here in Chicago where you could actually get Bitcoin through an ATM machine.

But I think it's not necessarily helpful just to think about it in terms of analogies that we have today. Because people are obviously using digital assets for things that are not normal consumer usages. And for example, for those who are familiar with Mt. Gox, we all know about the Mt. Gox hack, right? Mt. Gox being an early Bitcoin exchange. Mt. Gox, actually standing for magic the gathering the online exchange, was actually a place for gaming cards.

And I think about this because I've got two young kids, for example. But as you think about the increase in gaming, right, and the importance of virtual currencies, in that aspect it's being used frequently today. So this is things that it's not just about the corner store and buying bread. You know, this is about doing payments online through gaming and gambling, so on and so forth.

And then you can increasingly, as this technology continues to develop, assume-- and now this is going to get back in the weeds again. But I really appreciate, Peter, everything that you said. And you'll notice that Peter barely talked about this as a currency, focused much more on its technological aspects. But as we get further in the evolution of this technology, for people to use any type of digital asset as any type of representation of value, one example that I love to give is about Facebook.

Right now you use Facebook and you put your pictures on there and you put your stories on there, and you get compensated zero for this, right? And there are many people who say, well, wait a minute. This is my intellectual property. Shouldn't I get compensated for that? And there are certainly Facebook-like companies that are being launched now where you do get compensated for your IP through a digital asset or a token, or cryptocurrency, whatever you would like to call it. The same goes even for Google.

You know, if time is money, think of how much time you spend simply on Google searching for things. You should be compensated for that time. This would be another usage that people are developing right now for cryptocurrencies and being able to pay and accept money based on that.

So this is going a little bit further out, but guys, this is where it's going. So it's not just about finding analogs for today, but in future industries that are going to be created.

JASON ADLER: So you mentioned that there is this distinction between whether cryptocurrency should be seen as a currency versus seen for it's technological value, and I'm curious to drill into, can consumers understand that distinction? If consumer are looking to acquire cryptocurrency, are they treating it as a payment mechanism, or more of an investment, or something else entirely? And I'll open this to the panel.

CHRISTINA TETRAULT: So I would say that that's the crux of the issue right here, is are we talking about a financial asset or are we talking about a technology? And it used to be pretty clearly that $1 was $1 and the Visa network was the Visa network. And we see this blurring of the lines here with the advent of these cryptocurrencies. I think there is another layer to that, which is if we're talking about a financial asset, what type of financial asset are we talking about. Are we talking about money?

Are we talking about a security? Or are we talking about a commodity? If you think about it as money, the Consumer Financial Protection Bureau has a consumer advisory that's written from that perspective. If you're thinking about it as a security, the Securities and Exchange Commission has given a not very clear line about what-- and we can disagree about that, but about is it security? Is it not a security? And kind of where that is.

And then the Commodities Futures Trading Commission has a different opinion about when these assets are commodities. And I think to the question about whether or not there's consumer confusion is, I think it really depends, one, on the sophistication of the consumer. But there's also a question about how is this asset being acquired. And I think that can provide a lens into how to appropriately view what it is that's happening and what level of consumer disclosure needs to be there and that sort of thing.

So for example, if it's acquired by mining, which Peter has discussed what mining is, probably pretty high awareness on the part of a consumer, right? You have to be very sophisticated to buy a mining rig, hook it up-- I mean, unless your phone is hijacked, which is a whole other thing that was referenced earlier. But that's a separate issue. But if we're talking about people who are affirmatively mining to generate coins or value, I mean, sort of generally, because again, there's the question about what even the terminology is.

And then you've got one question. If we're talking about storage of these assets, so if you're acquiring them through an exchange and the exchange is holding your value for you, you have a whole separate set of risks. And that is a question about whether or not you're aware, say, of hacking or some of the other things that can happen. Like if you lose your key to your wallet, what remedies do you have? And then we have the question around transacting.

So if this is money and you're using it to buy something at a store, and you had paid with, say, your credit card, you would have a whole panoply of protections that apply when you use a credit card. If you're transacting with the distributed, decentralized network, and that isn't always the case when you are transacting at a merchant, but if you are, that transaction, as Peter has said,

is irreversible. And then the question is, are consumers aware that you don't have those same sort of chargeback rates and some of the other questions.

So I think it's really hard to answer because this is one where regulators don't have a common definition where there isn't necessarily even a common terminology to talk about it. And I think, also, over clouding this whole thing is a lot of the hype and a lot of, perhaps, you know, a lot of fear of missing out by not engaging with this technology, even in its very early days where that may not necessarily be advisable.

RUMI MORALES: Yeah, it's one of those things where, at least for me, it looks like a duck and quacks like a duck, but it's not a duck. Right? And I also think that maybe marketing is a funny part to it. I mean, it's called Bitcoin. So people think it's a coin. It is a currency. And I don't feel like, for example with Ethereum, and Ethereum, or ether, is the second largest digital asset out there by market cap. People think of Ethereum somehow vaguely like not as much of a currency as Bitcoin. It has something more about programs. It has smart contracts.

But it's as much of a currency as Bitcoin is. I don't know, though, to your point, like do consumers understand that differentiation? Is it a payment mechanism or is it a technology in and of itself? I doubt it because the other factor, obviously, is these are traded on exchanges. Exchanges, again, in air quotes because it's not any regulated exchange. But because it acts so much like a duck, people assume that it is. And that's the grey area that you all have to navigate.

JASON ADLER: Can you say a little more about what an exchange is, and how that plays a role, and how consumers can get cryptocurrency?

RUMI MORALES: Do you want to take that one?

PETER VAN VALKENBURGH: Sure. So in the early days of Bitcoin, the only way to get Bitcoin would have either be to find somebody else in the world who has it and say, hey, I'll give you $5, you give me a Bitcoin. Might have act-- for a time, it was just $5 per Bitcoin. Or to mine it yourself, which as Christina said, is a technologically sophisticated activity. Your average person is not going to do this.

Once these technologies gained a little bit more attention, after the first few years of their use primarily by people on the internet who find these technological problems fascinating and want to solve them, once it got more attention, you saw a number of businesses start up where they create an order book. They create accounts for buyers and sellers. And they smooth out the process of finding somebody who will sell you cryptocurrency for dollars, or for other currency pairs.

Now, that wasn't always a smooth process. As Rumi said, one of the first exchanges was Mt. Gox that gained a lot of widespread use. Mt. Gox was created by some guys who wanted to start a magic the gathering card exchange on the internet. And they built all the infrastructure to do payments and markets for these Magic the Gathering playing cards. And then they got into Bitcoin and said, oh, well we could just use the same infrastructure we just built for our website to allow people to trade Bitcoin.

Now, at that point, Bitcoin was worth very little. You're talking about like $1 or $5, maybe even less when Mt. Gox first started. I actually don't know for sure. And their security with respect to how they were holding people's Bitcoin for them, because they were holding it for them-- it's not peer to peer at that point if you're working with an exchange, because the exchange is kind of like a middleman to help you find someone to buy and sell the Bitcoin-- their security for the Bitcoin that they're holding was concomitant with a low Bitcoin price, or maybe with a Magic the Gathering card type security model.

And during Mt. Gox's rising popularity, the price of Bitcoin started skyrocketing because demand went up and there's only so many bitcoins and supply is constrained. Their security did not rise concomitantly with the rise in the value of the assets they were securing for their customers. They were still rather amateurish. And they either got hacked or there might have been an inside job. There's still ongoing debate about what exactly happened. And there's legal actions and things like this.

So that was the beginning. It sounds like a bad beginning, right? They were the first major exchange. But today, the story is very, very different. There are several exchanges, many of which are here in the US, and compliant with the US laws that apply. And these are things like anti-money laundering law, and in some cases, state money transmission licensing law for prudential and consumer protection purposes. You may have heard of the bit license in New York, which a number of these exchanges have gotten, which is another consumer protective prudential regulation.

And the Uniform Law commission has worked on a model state law for licensing these exchanges, which hopefully will be passed into law in several states. And I would imagine we'd see exchanges complying with that as well. There are still some rogue exchanges primarily based overseas that do not comply with laws, whether for anti-money laundering purposes or consumer protection purposes. But the story is very different than where we were with the days of Mt. Gox where there was basically no compliance.

And the cybersecurity story has gotten better, although you'll consistently see headlines about Bitcoin thefts from exchanges, and that's because it's very hard to secure bitcoins and do it effectively. So if you're holding a lot for your customers, you better have a very thorough plan as to how you store them. And there are things you can do, cold storage and multi sig are terms that you'll hear. And we can talk about them in a different format than this brief panel.

But the major exchanges, in general, I think have gone far beyond what you saw in the early days of exchanges. And you actually have a fair degree of protection and good cybersecurity practices at those, especially US-based and regulated exchanges. So what does it look like to a consumer to put some sort of meat on the bones, it looks a lot like online banking, or maybe like a Charles Schwab account, where you're able to buy and sell this thing that has a fluctuating price.

And you connect your bank account to it. You do ACH transfer or Swift transfer to move money, dollar money into your coin base, or Zappo account, which are some of the exchanges, and then you can trade. And it could be a brokerage service where they will go out and buy Bitcoin, or they have Bitcoin and sell it to you at what they think is a fair market price. And frankly, I think,

usually they are fair market prices for the more liquid cryptocurrencies because the prices are so widely reported.

Or it could actually be an exchange where you are matched with a seller, if you're a buyer, or vise versa if you're a seller. And there's an order book and it looks rather like E-trade or something like that.

AUDIENCE: [INAUDIBLE] drug cartels get all their [INAUDIBLE]. Because that was a big part of it also.

PETER VAN VALKENBURGH: So I don't know about drug cartels. But there were online drug markets, like the Silk Road, where people were buying drugs from people who were willing to sell them for Bitcoin. And so in those cases, you had people who were selling on these online drug markets rather than on the corner, using Bitcoin, which is a peer to peer electronic cash instead of dollar bills.

And in those cases, we've roundly seen a lot of those online drug markets shut down thanks to law enforcement investigation that has benefited from the transparency of the Bitcoin blockchain. Because all of those transactions, though they don't have human names on them, they have basically like account numbers but they're Bitcoin addresses, they're all there. So you see this address paid this address. And this address took a little cut of it. That's the dealer. That's the guy running the drug market.

And this was rather unimpeachable evidence against folks like Ross Ulbrich, who was the one who started the Silk Road. And so you do see that kind of illicit use. But yeah.

JASON ADLER: And I'm sorry, I should have mentioned this at the beginning of the panel. We're going to take questions on notecards. So if you need a notecard, just raise your hand. Someone will come around and give it to you. And if we have time at the end, we'll get through as many as we can.

So Christina, do you--

[INTERPOSING VOICES]

CHRISTINA TETRAULT: I just wanted to-- I think Peter's done a great job of describing these on and off ramps. And one of the things that I wanted to underscore about what he said is that there is varying oversight state to state of these off ramps. And so as yet, there isn't sort of one way that states are approaching. So for example, consumer disclosures might vary from state to state depending on where the acquirer is located.

And one of the sort of neato things that I would like to mention is anyone who's familiar with the Cash app, which is where sort of person to person, it started off as sort of person to person payment app, but you can actually acquire Bitcoin on that. So the friction to get some of these assets has diminished significantly. And I think that's a really important thing to think about while we think about what are the risks to consumers and whether there is appropriate disclosure.

You know, what is the environment in which these transactions are happening? And that can help frame, sort of, the appropriate ways that we may need to think about, what does it look like to make sure that there's appropriate consumer protection.

PETER VAN VALKENBURGH: Robin Hood, the app-based stock trading application, which is fairly popular, is also gradually unrolling cryptocurrency buying and selling on their app as well, which is interesting because Square is more of a payments. And they're making it possible for their users to access or by Bitcoin. And Robin Hood is more of an investment portfolio management app, and they're also. So we've got convergence from varying areas of Fin tech and consumer applications.

JASON ADLER: And I think-- so Christina, you mentioned the various on ramps. And I think that's obviously a helpful factor for thinking about how consumers are interacting with cryptocurrency and what they might need to know before acquiring it. The other that we mentioned earlier, and Rumi, you mentioned this, is just really what are you buying it for? Are you thinking of this as a payment mechanism?

Are you thinking of it as a duck, to use your analogy? And I want to touch on that a little bit. What are the reasons? What is inherent to a currency that is making it not take off as a payment method right now, something that I can just use at any store around the country to buy a loaf of bread or whatever else.

RUMI MORALES: I have thought about this a lot. I wish there was a good answer. I'm sure you two probably have a better answer than I do. Because if you go to Starbucks right now, you want to buy your coffee. You take out your phone. It has an app, the Starbucks app, you zap it. You get your coffee. It's easy, right?

So if somebody says, well, you can do, you know, peer to peer payments in Bitcoin. But they'll be like, no, but I just got my coffee. So for the consumer, I think, it's been hard to understand, well, you know, why Bitcoin is somehow easier or better. If simply all you want to do is buy a coffee. At the same time, what makes it hard is the cryptocurrency community is still so clubby, right? And just listen to the way we're talking.

I'm sure some of you are like, what in the world. You know, it's hard to kind of enter. It's easy to feel like, I don't know what these crazy people are talking about. I can get my Starbucks coffee just fine. I don't need this anymore, right? So I almost feel like there is kind of like almost a marketing push that the community needs to do for everyone else to really be able to explain what the benefits are, why something like, you know, tokenized economies in the future will actually be very empowering to the individual.

But it's going to be very hard while you just see people having wars on Reddit and Twitter about what the best crypto is right now and how to get in the latest ICO. It seems stupid. So I get that. But I mean, for me, again, for my own aha moment when I fell in love with this stuff and I realized there was no way back, at least for me, was a story that the Wall Street Journal had written several years ago about a guy who was a crypto enthusiast in New York watching the TV of a protest in the Ukraine.

And on the television screen he saw, you know, a picture of the guy in the Ukraine with a QR code and it says BTC, or a B with the two lines through it, which is the symbol for Bitcoin. So the guy in New York watching this TV recognized that, oh, that guy probably has a Bitcoin wallet. He did, too, right? He's an early enthusiast. So what he did is he freeze framed his TV. He took out his phone. And he just zapped Bitcoin through the TV screen. And that guy in the Ukraine got his money for his revolution.

That, to me, is the power of the technology. And we-- let's take that let's imagine, or re-imagine, future financial services or any other type of services, not in between people but between devices who choose to pay and transact with each other in the future. So again, it'll take a while, I think, for the beauty of the technology story to work its way through. And until that time, people are going to be using their Starbucks app to pay for their coffee.

PETER VAN VALKENBURGH: Yeah, I mean we're still in the early days of this as a technology. You can think about how difficult the internet was to use in 1994. And the small number of clubby dorks who were like, yeah, I really want the New York Times to start using the internet to send me my paper instead of the paper. And then everyone else would say, well, we have papers. This is fine. What are you talking about?

I don't want to have to type in a command line, you know, entry in order to get the latest story. But ultimately, the efficiencies of that technology of the internet, which really is the original sort of peer to peer networking, is the peer to peer networking technology. It is a world where you remove a lot of trusted central parties and you allow greater communication person to person. Ultimately the inefficiencies of that novelty, they fall away. And then the beauty of that system emerges.

So I think we're a ways away, just like in '94 with the internet we were a ways away. But there are real-- there is real value here in having a mode of exchange or a mode of establishing trust between two parties that doesn't go through someone in the middle. And that's especially important even today in countries that don't have the benefits of a functioning financial system, that don't have the credit card in order to get the coffee at the cafe.

And so you do actually see some uptick in cryptocurrency use in countries like Venezuela, where the national currency is being hyper-inflated into worthlessness. And families, if they have somebody in the family who is technologically sophisticated, think that they find a way to actually hold on to some wealth by moving it into something that is not dependent on the trust in their government or something like that.

But that's a very narrow use case and not the type of user that we're talking about today when we're talking about generally mainstream US consumers.

CHRISTINA TETRAULT: I would just add that on a lot of the enthusiasm that you see, so we've talked a lot about the confusion in terms of terminology. We've talked about the different approaches that regulators have taken. But I think one of the things that we're not talking about that I would like to name is some of the immense hype that is around is. Is there really was this

huge leap forward in computing-- it solved an immense computing problem, as Peter has outlined.

But you don't necessarily have the consumer understanding of what exactly that means. And again, we've talked about this difference, financial assets versus technology. But I would overlay that with the environment in which, financially, many Americans exist. And there was a report from the Federal Reserve that said 40% of Americans can't handle a $400 expense. So you see this asset that, until December, when you're looking at Bitcoin, it basically was like this with a bunch of troughs.

So let's be clear about the volatility. But I mean, it went from-- I started looking at this five years ago and it was a couple hundred bucks. You know, it was trading close to $20,000 per coin at the end of the year. If you look at the precariousness of most Americans financial situations, and you see some stories out there of kids who moved in their basements and bought Lamborghinis, it might seem really, really appealing to jump in here. And I think against the backdrop of all the confusion of the regulatory uncertainty, and the true sort of promise that we've talked about here, you end up with this environment where it can be very dangerous for consumers because there may be, as is documented by someone the scams that have already been shut down, people in this environment who are playing on that.

And I think that's a really critical element of thinking about what it is that we're talking about, and what the environment is, the larger environment, the larger financial services environment that we live in. Because also, you know, the Bitcoin paper was published while the financial crisis was going on. So again, this is the backdrop. And I think that's an important element to think about when you think about why some people may be jumping in, say, for their retirement money and they want to put in a virtual currency, which may be fine if you're 25, but probably not so good if you're 65.

And you know, again, it's about the appropriate level of caution, I think, at this time.

JASON ADLER: Yeah. So let's go down the hype and the excitement a little bit. A lot of that surrounds investments, investment opportunities that relate to cryptocurrency or that involve cryptocurrency. One of them that's been really big recently is initial coin offerings. Can we talk a little bit about what an initial coin offering is and what are the other investment opportunities that involve cryptocurrency.

PETER VAN VALKENBURGH: So in short an initial coin offering is a bunch of guys and girls, usually guys, frankly, get together and say, oh hey, you like Bitcoin. We could make some changes to the core code. It would work, as I said, I had my possible improvements, privacy, flexibility, scale, tie into other digital goods that are delivered by decentralized network, we could do those things better than Bitcoin's doing them. And we'd like to raise money to write the software that eventually will be a new running network like Bitcoin out there that's decentralized. But today, it's just me and my friends making promises that we're going to write that software and that it's going to work when actually implemented by that running network out there in the world, people running it on computers.

So Christina's right, Bitcoin is a risky investment. And we don't usually comment about price. We don't try and push people to think about investing in these things because of that risk. I think nobody should ever buy any more cryptocurrency-- put any more money in cryptocurrency than they're completely willing to lose, a tiny amount, if you want to participate at all. And that's a message that needs to be repeated and repeated because we see consumers seeing some people get rich and they think, well, I'll just bet the farm on it. And it's terrible.

But to the extent cryptocurrencies are volatile and risky investments, these initial coin offerings, where you're handing your money to a software developer who's just promising a future decentralized network, hasn't actually built it, that's even more risky. Satoshi Nakamoto, whoever he, she, or they were, that was the name on the 2008 Bitcoin white paper, they didn't raise money to develop that software. They did it on their own dime and they released the software open source to the world, and then people started running it on their computers.

And then eventually Bitcoin had some value. So they didn't take any money up front. They didn't create that kind of information asymmetry. They didn't create those kinds of incentives where like, oh, well I've already got the money. Why should I continue working on this thing? They built it. It worked. And then it achieved some level of value. These ICOs, you're just often buying promises that someone will build it and you're handing them a lot of money with not many guarantees that they'll do what they do.

So buyer beware.

JASON ADLER: So why would an ICO be any more risky for a consumer to invest in than a stock IPO?

PETER VAN VALKENBURGH: So stocks give you actual legal rights. And assuming that they've done their registration, which anyone who's doing an IPO in the US with the SEC, they'll also have to make disclosures in a very regularized fashion. Here is what your rights are. Here's what you're going to get when you invest in this thing. And it might be a rights to profits or revenue streams. It might also include things like the privilege to vote as a shareholder to determine how management will actually run this company to hopefully make it profitable in the future.

Now with an ICO, as I said, somebody has said we're going to build a better Bitcoin or it's going to do something differently than Bitcoin, but it will be a decentralized token, like Bitcoin, and you'll get the token. That's what you're going to get. And I guess that's a kind of right, although some will even disclaim that. Some will say, no, you're just donating to a foundation whose mission is to make this decentralized token enter the world. And maybe, if that works, you'll get a token. So your rights are far-- they're not spelled out well. They're spelled out poorly. And you're really reliant, then, on the good nature of that developer.

Now, I want to be clear, because I probably sound very negative on ICOs, which might surprise some of you if you thought I was some sort of industry pumper or something like that. Coin Center is a nonprofit that just wants good information about the technology. So I'm not that person. But I will also say, just to clear the air, there are some compliant or more compliant

token sales out there. In the US, these are people who have said, I think maybe this thing is actually a security. So I'm going to try and comply with securities laws.

Now, we haven't seen anyone do an actual S1 and register their token as a security. But we have seen people say, look, this promise of future tokens is effectively an investment contract, which is a type of security. And I'm going to register this investment contract-- or I'm not going to register this investment contract, but I'm going to do a reg defiling with the SEC and sell it under Rule 506(c) only to accredited investors, because that would then be a way of complying with securities laws and it would also be a level of consumer protection because that means you're only selling to people who have over $1 million net worth and/or can prove an income of $200,000 for the last two years.

These are the people who could afford a $400 emergency purchase. So they're less vulnerable. And so there are those who want to sell tokens who are doing it in a way that I think is more responsible. I don't mean to say that all token sales are bad. But in general, token sales are risky business.

RUMI MORALES: Another question for the ICO, is well, where's the o? Right? Where is the exchange upon which these tokens could be traded. I mean, for those familiar with Coin base, for example, Coin base only has, what, six of the major cryptocurrencies at this point being traded, out of the 3,000, 4,000 plus digital assets that are out there. So not only if you'd be buying into an ICO do you have to understand that the technology that the developers are purporting to achieve as an improvement on what exists today, but where is it going to be traded?

How are you going to get liquidity? If you want to get your money back, can you? So there's another like outsourced level of trust that you almost have to have. And I find it so ironic because this is all supposed to be about the lack of-- you don't need trust anymore, right? It's amazing how centralized all of this still is.

CHRISTINA TETRAULT: So Christina, can you comment more on, if a consumer is about to invest more in-- or considering investing in an ICO, considering investing in another cryptocurrency-related endeavour, or even just acquiring cryptocurrency on an exchange, what sort of things should the consumer know? What kind of information would they want to know before they go ahead?

CHRISTINA TETRAULT: Sure, so there are any number of resources. So anything I'm going to say right now is certainly not the final word. But I would suggest that consumers, just overall, is pump the brakes. I mean, that absolutely is sort of my fundamental message here. You know, there are a lot of really cool things that the technology can do. And obviously there are these wild financial stories about these assets, or whatever you want to call them.

But you know, again, in the environment in which we exist where so many of us are financially fragile, a huge dose of caution, I think, is necessary. So the CFPB has a great consumer advisory that sort of lays out some of the risks about volatility and transaction costs may not be clear and some other things that I think is a terrific resource. And then I think doing your due diligence.

And in this environment, it's very difficult. So that's why that wasn't my first thing. But I would really suggest to pump the brakes. Do your homework.

JASON ADLER: Other comments to the panelists on things you want to think about before investing in a cryptocurrency?

PETER VAN VALKENBURGH: I mean, if you, yourself, are not capable of explaining to somebody such that they understand what the token is supposed to do, you shouldn't buy the token. Because sometimes you'll read these white papers and it's just not even clear what this thing is designed to actually achieve. And the bottom line is, when there's a lot of hype and excitement and people seeing other people get rich, there's a lot of just outright fraud.

So apart from that maybe good natured bunch of folks who truly do want to build a better Bitcoin and are taking money upfront to develop the software to do it, apart from them, there's bad natured folks who think, well, it's easy to make that promise. And with money flowing all around, all I need to do is string together the right series of words, like blockchain, DLT, decentralized, distributed--

RUMI MORALES: Or you get Dennis Rodman to wear your Potcoin shirt in North Korea.

PETER VAN VALKENBURGH: Sometimes stunts.

RUMI MORALES: The marketing stunts have a big sway on an uninformed public.

PETER VAN VALKENBURGH: Centra had Floyd Mayweather as a spokesperson on Twitter, it seemed. And he had a picture of a table of money on his private plane and said, I'm going to get rich in the Centra ICO, which is now under investigation for unregistered securities issue. Centra, that is, not Floyd Mayweather. Although I don't know. Who knows? So be very wary of the scams and the word soup.

And if you don't feel like you can actually separate the wheat from the chaff as far as whether this is techno gibberish or actual real innovation, then you probably just shouldn't be participating. Maybe find a dear friend who you really do trust and is sophisticated with these things, if for some reason you feel compelled to get involved in the new technology. And then and then run it through them. Do your own research but be cautious even when you're doing your own research because word soup is word soup.

JASON ADLER: So we have just a couple of minutes remaining. And so I want to close with, what's on the horizon for cryptocurrency? And particularly I'm curious, are there developments that you see down the road that will pose new challenges or growing challenges for consumers?

RUMI MORALES: That's a lot to fill in in two minutes. I'll just give myself like a PSA. For anyone who's interested, I will be giving a talk this Wednesday here in Chicago. It will be live-streamed as well, at 12:00 at the Connectory. I'm going to be launching-- I'm going to be launching a new investment platform, but it's focused not just on blockchain but its interactions

with AI and IOT, other advanced technologies. And here we are, we've been talking about cryptocurrencies in isolation.

But the fact is there are a number of other advanced technologies that are being innovated upon at a fast if not faster rate. And you have to think about the interaction of crypto with that as well. So those are the thoughts that are in my head and I'll be talking more about that on Wednesday.

PETER VAN VALKENBURGH: One of the things that I always say as far as like how these things get adopted, right now it seems like no one is using them for payments, Rumi talked about a decentralized Facebook where you could get paid for your participation in a social network by the network, instead of all that money or that value going straight to Mark Zuckerberg. That's a good idea. And there are several projects that are trying to build that.

And most of them won't succeed but maybe one of them will. And that is maybe how these things really do eventually gain traction, someone will be using that without knowing they're using cryptocurrency, not really. It'll just be the best way to get the service, social networking, at the best price, frankly. Because we don't realize it but we pay a price every time we use Facebook. And if we were actually getting a positive price, or a negative price, actually, when you get paid to participate in a social network might be better.

But that kind of use, because people don't even know they're using it, means that there's all kinds of risks that are embedded in the system that you don't even know about. It's actually the exact same problem as Facebook at that point. You thought, this is just a great way to connect with your friends, but underneath there's a massive data mining operation that can swing American elections.

It's going to be the same with cryptocurrency. You thought you were just using a social network that was able to connect with your friends well, and oh hey, now I'm getting a little payment. But are you getting the right payment? Or is your data still being manipulated? Is it encrypted? It says it's encrypted. Is it robust? We're just building new layers on top of things. And that could make more efficiencies but it could also make it harder to disentangle fraud out of something that looks really slick and actually works until it doesn't.

JASON ADLER: OK, so with that, we'll end. You've all been great. And thank you for participating. We'll bring in the second panel now.

[APPLAUSE]

ELIZABETH KWOK: Hi, everybody. Thank you for staying around for panel two. We're just about to get started, I just wanted to send a quick reminder that if anybody does have questions, index cards are available outside. Or if you just raise your hand, somebody will come either collect a question or give you a index card if necessary. So my name is Elizabeth Kwok. I am an investigator in the division of Financial Practices of the Bureau of Consumer Protection.

This is Jason Moon and he is a staff attorney in the southwest regional office. To his left is Kyle Burgess, who is the executive director and editor in chief for Consumers Research. To her left is

Amy Kim, who is the global policy director and general counsel for the chamber of digital commerce. And to her left is Joe Rotunda, the director of the enforcement division at the Texas State securities board. And at the very end of the table is Dr. Marie Vasek who is an assistant professor in the computer science department at the University of New Mexico.

So obviously on the last panel, we've heard a lot about the wide array of ways that consumers can engage with cryptocurrencies. And I wanted to turn first to Kyle so that we could talk about the different pitfalls and types of scams that consumers are starting to encounter as they're engaging in this space.

KYLE BURGESS: Thank you. So I want to first start with saying that there is nothing inherent about this technology that makes it scammy. It's really-- we are seeing a lot of the same kinds of stand scams we've seen over time. So you know, my grandmother was actually one of the first people who ever had the internet in my world. And she also one of the first people I knew that got chain mail, and those kinds of scams. And so to go through the list, you'll hear a lot of these things are very similar to the kind of scams that you've seen from the early days of the internet.

So one example being an exit scam. The most recent one that I know of was by Confito, and it was for $375,000. And essentially Confito had offered a decentralized escrow project. And pretty much within overnight, there was a big legal problem for why Confito had to shut down and they walked away with $375,000 of investor money. They had a legitimate looking web site. They had a legitimate looking white paper. And they basically, you know, created a lot of hype and then were able to walk away. Bait and switch and impersonation is another really popular way for consumers to be scammed with initial coin offerings where a company will either pretend to be another reputable company, have like a similar URL address and maybe try to pretend to be that other company.

Or another thing is that they would have legitimate looking people on their web site, LinkedIn profiles, and actually be total frauds. One example of that was Benabit. They were offering a back loyalty program where if you invested, you would see great rewards from investing in this company. And they raised somewhere between-- well, I guess walked away with somewhere between $2.7 and $4 million. And the way that their scam came to light was someone noticed that the LinkedIn profiles of their founders were actually staff members at a UK boys' school who had nothing to do with the project.

You also see traditional Ponzi schemes where you're robbing from Peter to pay Paul, basically as new people come on the people who have been involved are getting the money at their returns from people who had already been-- or from the newer people. And as Andrew Smith talked about in the opening, you'll also see change or what I talked about with my grandmother, like pyramid schemes where everyone who is involved recruits more members. And as more members come in, there's a trickle up effect of that. And then there are ones that are not technological at all. They're just phishing scams where you'll get--

A most recent example is Betoken. Betoken was essentially offering to be a new version of Airbnb. And you would buy the token that would give you some ownership in that company-- not ownership, sorry. We'll get into the different types of ICOs in a minute. But they essentially

sent out an email pretending-- hackers, sorry, sent out an email pretending to be Betoken. And they added this sense of urgency of, you know, if you buy now, Microsoft is going to participate in this deal.

And by creating that sense of urgency in this fake email, people who are already kind of interested in ICO in this project, saw that sense of urgency and joined up. And they were able to get their login information and take about $833,000. And another kind of phishing scam is what's called an airdrop. And again, that is about a sense of urgency, where companies will offer either very low cost or free tokens to try to drive interest in the new projects.

And what they'll do is they'll require you to download something or they'll require you to get a native wallet, like a wallet that they've created. And by doing that, they'll be able to access your public and private keys, and also take whatever tokens you put in there. And so it seems like a great deal because you're getting something for low value or free, but actually they're getting a lot of information out of you and your money.

And then the last one I'll talk about is a pump and dump, where you'll see online forums or other groups of coordinated efforts to manipulate the value of a token. And so these groups move together, try to drive interest in the token. The volatility and the price increase. And then as soon as they all kind of hit a certain level, they all understand what it is, they will dump and they will walk away with the money. And those other consumers coming in will be caught up in that.

There's probably more but that's what I've got for you.

ELIZABETH KWOK: Yes, Kyle. Thank you. You've covered a lot of ground. I think one thing we would-- in seeing the wide array-- I wanted to ask Marie, based on your research, if you could just walk through kind of some of the hallmark commonalities of kind of red flags or pitfalls among these different scams that Kyle has already identified.

MARIE VASEK: Yeah, so a lot of my work concentrates on online Ponzi schemes. So a lot of these scams offer outrageous rates of return. They can kind of get away with it a bit in Bitcoin, because as we've seen over the years, sometimes the price of Bitcoin actually does skyrocket. And so a lot of these scammers go off of that and they offer returns that, you know, you can never actually get. And many of those also have some sort of affiliate marketing scheme.

So refer your friends, that sort of thing. Many of these will try to mask themselves as something else. So we see Ponzi schemes that are supposedly cloud mining scams. The thing to note with mining is that if you're guaranteed something, and it's ridiculously high, then it's probably a scam, even just the guarantee is usually a hallmark of a scam. Because in mining, the volatility of Bitcoin is so up and down, there's always new entrants to the mining market, you can't guarantee anything.

My work has also looked at online scam wallets. So these are services that pretend to be a wallet. They might hold your money, if you only have a small amount of money in it. But then once you put a larger amount in, they'll take all of your money and run. One of the big hallmarks of these is that they're currently primarily only offered on the dark web. So if somebody is advertising

themselves on the dark web to you, you should probably do some research on it offline. Don't just trust what you see.

Most of these services have large amounts of strongly negative reviews online, but yet you see them earning $10,000 to $20,000 every week. We've also looked into things like scam currency exchanges, which are, again, they pretend to be currency exchanges but just take your money. Scam mining operations, similar thing. Most of these have somewhat of a good reputation online for their legitimate services, and so it's really crucial that you look to that.

With many startups, it's hard to do that. So with mining operations, it's really hard to know which ones will succeed, which ones will fail, and which ones are just scams. And so for there, it's looking into the founders, looking into kind of the people around the projects. And a lot of times that will lead you to believe one is more legitimate than the other one. Though again, this is really hard. A lot of businesses fail that aren't even scams.

KYLE BURGESS: Some just pretty basic things to look at as well. I mean, we don't-- Consumers Research doesn't actually encourage people to go out and invest in them but we also know that they will. So we have a paper to help them in that process. But something to look at if you are considering investing would be the white paper itself. A lot of these white papers are copied. You can pay-- there's a guy on Fiver who you can give $140 to and he'll write your white paper for you. And you can you set up your fake web site and add this paper and have your founders and all of that for under $1,000. And the payoff for you as a scammer to do that is immense.

As Marie mentioned, if the team is anonymous, if you're looking at the website's page and the team-- there is no founders and you can't verify the legitimacy of that team with a third party, that's problematic. If there is no roadmap on the website for how the project is going to, like, is there a timeline? What's supposed to be achieved? As Peter mentioned before, if you can't understand what the token is supposed to even accomplish, that's a problem. Or if there is no compelling reason for a token to be involved.

If it's a project and it has nothing to do with cryptocurrency, yet has a token associated with it or a project that has nothing to do with blockchain, like a health records management service or a cloud data sharing service, or whatever it is, if there isn't some compelling reason to have a cryptocurrency token involved, that's a problem.

Some other general red flag is if it's like an Ethereum-based project, there's gas involved in running some of these projects. And if there are high fees for that gas, meaning that you have to use a little bit of Ethereum to run that project, that's something to look for as well. If they're asking for donations, or as I mentioned, downloading products or proprietary wallets, and I think they also mentioned last panel, celebrity endorsements. Like those are just some pretty obvious red flags.

MARIE VASEK: And another thing to look at when investing in a token is most legitimate tokens are listed on really high volume exchanges. So for instance, we talked earlier-- the other panel talked about how one of the large currency exchange in the US, Coin base, only offers six

different tokens. That's because they individually vet every single token that they list on their thing.

So what I usually recommend to people that want to invest in cryptocurrencies but don't want to do the legwork for them, is go to high reputation exchange.

JASON MOON: I'd like to jump here for just a minute, Marie. I had a follow up question about what you call in your research, the high yield investment program. Might also call it a Ponzi scheme. I'd like to talk about that a little bit. You've done some really interesting research where you've looked at, how long do these things last? What makes some last longer than others? And it appears to me from your research that you've probably analyzed thousands of online comments, which seems like a really tedious task to go through.

But let's talk about the kid who wants the Lamborghini and that kind of stuff. Who are the kind of people that are getting into these type of programs, based on what you reviewed in your research?

MARIE VASEK: OK, so there's a couple of questions I'm going to try to break it down as best as I can. So the first question was looking at what makes scams last longer. So there's about a new Ponzi scheme that uses cryptocurrency at least every day. And that's been fairly constant for the last few years. And one thing that makes them last longer is offering a lower rate of return.

So things that offer really high rates of return, crash really quickly. So if they're promising to double your money overnight, they're probably only going to last 12 to 24 hours. Whereas if they're offering maybe 5% a week, they can get all along maybe for a few months. Some Ponzi schemes last for years. The ones that last for years have to continually recruit members. One thing that makes some Ponzi schemes more effective than others is their marketing programs.

Others particularly market themselves in really needy communities. And so you can see Ponzi schemes that are really trying to attract themselves to new immigrants who might have a hard time accessing the normal financial system, hard time deciphering what's real, what's not. You also see Ponzi schemes that last really long that are into third world countries. So for example, there was a big Buzzfeed expose on how two of the most popular of the 50 websites in Nigeria were actually Bitcoin-based Ponzi schemes.

And a lot of people said that they invested in them because these Ponzi schemers were more reliable than their country's financial system. And this has since moved to other countries, like Ghana. So there's another-- so other things that make them last long, there's like a couple of groups online that just keep running one after another. So they'll run one successfully for a couple months, then they will get some really large person to invest a good amount of money into the scam, and then it will go away. It's usually the big hallmark is they're waiting their time until they get some sort of big fish and big pay out.

Now, who invests in Ponzi schemes? Normal people invest in them, to some degree. So they think they're smarter than somebody else. There's a really good amount of people online that knowingly invest in Ponzi schemes. There's all big forums where they talk about which one is

better than the other one. But the problem is that once they get enough of these Ponzi scheme investors, is that they can get onto normal consumers who don't know that it's a scheme, but think that, oh, these really smart people are investing in this. I should invest in that too.

So you see things like Bitconnect, which was used to be one of the most popular cryptocurrencies, which ended up being a Ponzi scheme. And you can talk to people that invested in it. And they thought that really smart people and a lot of people are investing in it, so it must be good. And therefore they should do it.

JASON MOON: Joe, I'd like to ask you a little bit about that also. But I'd like to talk about ICOs. Your office has done a lot of cases involving cease and desist letters, fraudulent ICOs, kind of the same line of questioning. Question one, who are the kind of people that fall for fraudulent ICOs? And question two, what makes an ICO take in more victims? Is it the white paper? Is it the marketing? What did have you seen in your investigation?

JOSEPH ROTUNDA: Great question. And just by way of background, my background is working for a state regulator and law enforcement agency. And I think there is a perception that regulators have a negative view of cryptocurrencies and these new technologies. And that's not true. We're content neutral. We are completely objective with what we're looking at. Our problem is not with the technology, it's with people. It's not the technology, it's the people.

And by people, what do I mean? I mean new markets, emerging markets, and trendy markets tend to attract bad actors. Why? Because they can capitalize on the buzz. They can capitalize on the newness of something. They can point to Bitcoin in December of 2017 and say, look, you could have been a millionaire. I'll take you there.

And that's really what our concern is now that we're seeing these ICOs that are kind of coming out. Last December, as the price of Bitcoin rose, our agency decided we were going to conduct a sweep. We decided we wanted to see what types of ICOs and what types of cryptocurrency investment offerings were being promoted in our state, because we really didn't know. We really had not taken a close look at it before.

And so we decided to do a sweep for 30 days. We were going to look at all the public solicitations that were targeting our residents. Why public solicitations? Because we wanted to see the ICOs and the investments that were trying to broadly recruit people. Not necessarily something on the dark web, but we wanted to see the promoters who are out there trying to attract new money from a large population of people. And we were shocked with what we found.

So 30 days, we opened 32 investigations. They lead to 10 law enforcement actions. We have a number of ongoing investigations right now. It was everywhere. And we didn't know that. And regulators didn't know that until we started all taking a look at this area. So how did we go about this? What did we look out with the ICOs? Well, we did a lot of undercover investigations, undercover investigation where we wouldn't necessarily announce that we work for a regulatory or law enforcement agency.

We pose as an investor trying to ask questions about a particular product. We may apply for a job as a salesperson at an ICO, try to join a marketing network, all these different things to try to gather some intelligence about what was out there. And it was kind of scary what we found. So going to see what we're talking about with the white papers and some of the ways that these white papers are used is concerning.

Found a number of white papers where I would read them, our staff would read them, our attorneys would go through them and they'd talk about a particular product or idea. And it sounded good. Broad, general, may sound good. But you take that white paper in addition to all the other marketing materials, and you realize you don't know who's behind the company. You don't know the name of the person or the people. You've no idea who they are.

And you don't know where that company is located because they're not telling you where they're located. This is an offering that exists only online, that people are turning their retirement money over to. It exists only online that they can't independently verify anything about. It's nothing more than a promise. And we saw a lot of that with the ICOs, with the white papers, where they were just promises.

I think it was mentioned earlier, some of the language on the white paper is oftentimes is-- I think Kyle mentioned it-- copied and pasted from or someone gets paid to actually produce. You see the same language over and over. It's like all these tokens are doing the exact same thing. It's like they have the same management team. It's like they have the same writers.

It's like they're running the same scheme.

JASON MOON: Joe, could you give us an example of some of the word soup that you've seen?

JOSEPH ROTUNDA: It's this word soup. It is literally just word soup. It is the kind of thing that an average person will read about something-- you know, let's take a look at like something would like the DNA timeline of where a company is hoping to be at a certain point in time. And they'll give a description about implementing a blockchain or so some type of DLS. And it's the exact same language as a completely different token. Maybe it's a utility token or something that has no bearing on the one that you're reading.

And we'd see that. And so you know, I'd sit there and I'd copy and paste that and I'd search the internet and just shoot messages to people, like did you know that your language is being used in this guy's white paper? You may want to get some royalties. And you know, sometimes you get a response. But a lot of times, you wouldn't, because I suspect this is something that's kind of going on.

But you know, that was really one of the biggest problems that I saw in this industry is that investors oftentimes didn't know who they were dealing with. There were unrealistic expectations of profits. The guaranteed returns, we've seen cryptocurrency mining programs that are promising 4.1% daily return. These things just don't exist. So you see some of these things with guaranteed returns, but you also don't know who you're dealing with.

So if something goes wrong, you have no way to seek redress against that person. You have no way to contact that company. They even have a telephone number, he's got an email address that may even bounce back at a later date. And so those were those were some of the big things that we saw.

JASON MOON: OK. Amy, I want to go to you for just a minute. And so we've got this problem we run into as regulators of the fraud versus failure problem, the problem of, let's say, it's an ill-conceived but good faith project to develop some type of blockchain application. This is a new industry. We're going to see examples of people that are really trying to develop a new product and they fail. So how do you as a-- how does your organization help us tell who are the good faith efforts versus the fraudsters? Is there anything you're working on in that respect?

AMY DAVINE KIM: Well, there is. And I'll just back up a little bit just to say that, just like other industries, this one is no different. There are bad actors, clearly. As a trade association, our member companies are interested and meaningfully contributing to a functioning marketplace and a functioning ecosystem that's focused on compliance. So you know, as you can see, some enforcement actions, I think, helps show that that is a functioning marketplace. I think when you have too many, I think this industry in particular because it's so new, is particularly sensitive to some of this reputational-- they can impact reputation.

So we're looking at that as a trade association very seriously, and thinking about how we can help to contribute to avoid some of these things so that consumers don't fall victim. And not just consumers, but others, you know others in the ecosystem who want this to look like a vibrant ecosystem with some pretty significant players investing a lot of money into blockchain solutions that are really going to transform so many things.

So we've done two things that I think are notable in this conversation. The first is years ago we co-founded the Blockchain Alliance, which is a public-private partnership with industry and law enforcement, including FTC, to help both sides share information and trends, or things like that, to help-- and there's webinars and training that have going on as part of that, so to help law enforcement understand the technology better, I think we do find a bit of unevenness within government, whether it's policy or enforcement or legislators.

So to help raise their awareness or understanding so that they know what they're looking at, they know what they're dealing with when they look at the things that we're talking about here, and how to better distinguish exactly the question that you just raised. You know, what are the businesses that are trying to be compliant but they've failed, versus the bad actors, that I think we've talked about here.

So that's been an ongoing effort. I was just on the phone with one of those agencies right before this panel, you know, trying to make sure that they're aware of the resources that we can offer, especially with the change in administration, a lot of change in government. So that's one.

And then the other that we've-- and in particular with respect to this-- is the Token Alliance. We established that late last year. And we have over 350 participants from industry on that group. And we're focusing on this ICO, what is being called ICOs, but really even broader than that,

distributions of digital tokens and how to help raise awareness. There's a lot of issues here, consumer protection is one.

But there's other issues there, too, whether it's security, commodities, and other aspects to that. And so our first task was really to bite off on an educational component and then a compliance component, a very specific compliance component. The educational component is there's a whole chapter dedicated to, here are the laws that apply to tokens, that can apply, depending on your functionality. And it's activities-based, typically. So SEC and CFTC of course come to mind. Consumer Protection is also in there. Tax, accounting, AML, and a host of others to make sure that some technologists-- make sure everyone's aware that you can't just think about the SEC or the CFTC.

You have to think about all these other things that can get triggered when you're operating in this environment. And we've done it not just for the US, but multiple countries. And we continue to add to that. And I hope even once we've published this document, we'll continue to add more countries to make it truly global. It's a ecosystem and you can't just-- you can't be myopic in how you're looking at the law.

The second part of it is a market analysis, you know, the economics. Why do we care? Like we're talking about this proliferation of activity in this space, so really just getting your hands around why this is important and why we need to be looking at this critically. And then the third is a set of guidelines. And I anticipate we'll keep adding to this because there's a lot to address. But the first bite that we took this was defining what people are calling utility tokens, tokens that have a consumptive purpose and truly want to be that, and do not want to be a security or a commodity.

And so we describe, if you're going down that road, you know, here are some of the things that you need to avoid so that you're not a security. If you're promising investment returns, if you're promising-- if you're building an expectation in the purchaser, you should be looking at yourself critically to see if you're a security. And then you'll have to go down a different compliance path. Things as far as the steps that you should take as you're thinking about launching a token that has a specific use, how to describe that specific use, to make sure that people understand it in plain English.

And then on some guidelines for how you're going to distribute that. And then also for the token-- what we're calling token trading platforms-- but exchanges that are trading in digital tokens, what steps they should go to to vet these tokens before they take them onto their platform to ensure that those platforms aren't not running afoul of the potential laws that could apply to them.

JASON MOON: Great, thank you. Joe, let's go back to you for just a second. In terms of your agency's enforcement and regulatory approach, is there a difference between the commodity, utility, security tokens in terms of how you view these offerings?

JOSEPH ROTUNDA: You know, the offerings that we address are the ones that appear to be fraudulent. That's the easy answer. However you want to label them, it's the ones that appear

fraudulent. But here is really what it comes down to. We're looking at companies who are trying to use digital assets to make a profit for others, right not necessarily the coins themselves, but the people behind the coins, the people that are using the coins, the people that are promoting ICOs.

Or we see a lot, a whole lot, of cryptocurrency mining programs. We see a lot of cryptocurrency trading programs. Forex was popular for a while. We had a lot of Forex cases and a lot of Forex investigations. Now it's cryptocurrency trading cases and cryptocurrency trading investigations. So instead of trading in foreign currency, people are trading in digital currencies. Those are the cases that we're really kind of keeping an eye on. And they have a high potential for fraud. And there's a reason for that.

And that is, we talked a little bit earlier about independent verification of different things. But you know, even in the case where somebody tries to show you something, tries to present something to you, you may not be able to independently verify. If a cryptocurrency mining program is showing clients or potential clients a picture of its mining farm, you don't know if that's its mining farm. A picture can be lifted from the internet and we find that we.

We just brought a case against a company that was using-- it had purchased stock footage and spliced the stock footage together to try to show a very professional quality video of the interior and exterior of its mining farms. It was stock footage that they purchased on the internet. But it appeared on the website and it was one of the big pitches for investors to come and make their investment because they could see this very sophisticated mining farm.

You know, we've had issues with celebrity endorsements or celebrities appearing in different offerings. Ruth Bader Ginsburg made her way in one of our offerings. You laugh. We do laugh. It's OK. It's therapeutic. But yeah, Ruth Bader Ginsburg was supposedly on the legal team of one of the-- and I think this is what happened, the company, and you know, not to make light of it, because it's humorous, but I think people lost money, so I can't-- but it was Ruth Bader Ginsburg.

So the company had a website that purported to show its team. You know, I talked earlier about how a lot of times we're going through these white papers and these marking materials, and we have no idea who is behind the company. This company, and it was called Lead Invest, threw that information right out at you. It had pictures, very professional pictures, kind of like these oval circles showing its people. And we thought, you know, I guess anybody can put anything on the internet, right?

Let's test this out. And so we took the first picture and we ran it through a search engine and it came back to being actually an attorney in San Antonio who just got her law license. And there was this law firm that was supposedly working with them. And we ran it through and it was like, no, this law firm is actually in Chicago. And we ran through a bunch of other things. We found some stock photos, right, the stock photograph of this person who was supposedly in charge of corporate tax and international law and securities law of something like that. That was interesting.

And then there was a picture of the code of compliance association for Lead Invest. And it was this picture of a group of people. And it's the kind of thing you could have looked over as you're

going through. But when you run it through the search engines, it came back to the George Washington School law 2005 edition of legal briefs. It was a photo taken at a gathering to honor the late Chief Justice Rehnquist with Ruth Bader Ginsburg standing among three former solicitor generals and two other people from Duke law.

And they took that picture and said this is our code of compliance association. And that's really what it was. So the headline in the paper when we brought the action was like, no, Ruth Bader Ginsburg is not selling you Bitcoin. She's not. But those are some of the things that I think we see there.

JASON MOON: So you're giving us some funny examples of some outrageous things that happened. Presumably, there's a few hard cases, right? There are companies that really do seem fairly legit. They pass the smell test in terms of the white paper.

JOSEPH ROTUNDA: Absolutely.

JASON MOON: But then they fail for whatever reason. So how do we approach that as regulators? Do we wait and see until the coin collapses and everybody loses their money? Or do we jump in ahead of time? What do we do about that?

JOSEPH ROTUNDA: I think regulators need to be proactive in any type of new market, especially in this new market with as quickly as it's grown. You know, we didn't have the public being pitched different types of investments like this on this scale a year ago. This is something that blew up late last year. And because of that, there are a lot of people who are at risk for some sort of fraudulent conduct, more so than I think-- I guess it's just an exponential amount.

So what we have to do is we really have to proactive. Regulators need to, number one, identify companies that are trying to do it right and work with them. The companies that are trying to do it right should get a telephone call from the regulator, not a cease and desist order. Not a lawsuit. We can usually work with them and either get them into compliance or if we can't, we can just do what we need to do. But we can at least try.

We need to identify the fraudulent schemes and we need to act quickly. We need to stop them. I think what we've learned is that the fraudulent schemes are very, very fragile. As Marie said, you know, these things-- some of the ones that are promising huge rates of return, they collapse upon themselves in 12-24 hours. Some of the ones that are offering 2-3% weekly, we need to be able to identify those. We need to do it proactively. We need to do it before we get complaints.

We need to be able to thoroughly investigate those cases and stop. If the ongoing conduct is fraudulent and people are going to get hurt, we need to stop it right away.

JASON MOON: Marie, maybe you can tell us a little bit. You've done some really interesting research. Well, let's talk about Ponzi schemes. This is my favorite subject. So let's go back to that. And you actually did a study of how long they typically last. Can you tell us what you found in terms of the timeframe? And then I want to move from there, really quickly, to your research on coins themselves. You did some interesting research on coin abandonment. You

know, a coin will skyrocket and then it will fall and it'll kind of maintain a certain level. Can you tell us what you found on that?

MARIE VASEK: Yeah, so the first one is about the length of Ponzi schemes. So about half of the Ponzi schemes we found died within a week of first being advertised. Some of these died because they got no traction. Some of them got too much traction and couldn't actually pay out when they said they would. And then about the other half last longer than that. These are usually the other half that so-called investors look for.

And we also note that within things that last shorter than a week, a lot of these people that invest in it are seeing this as some sort of like online gambling thing. So it's less of a Ponzi scheme investment thing and more of a, like, hey, let's see if everybody else is going to participate in this scheme and try to bring unity of our friends on the forum, and unity of everybody on Twitter, or whatever have you.

So then talking about the work on coins, so there's been this proliferation of coins. We looked at, like, on the order of 1,200 different coins that were offered in the past three, four years. And what we found is that some of them start at a good price because they had this big ICO beforehand. And then investors, a lot of times, will have to hold onto their money for a while. So the people who started the coin can get out first.

The investors, when they try to go out, there's all of this supply of coin. Nobody actually wants it because they can't actually use it for anything, and so it just falls right down. And so what we can see is that what happened is back in 2015, around there, there was a lot of coins that were introduced and then just abandoned. And we've seen in the last year a big resurgence of these coins. So they died. They went away after their big skyrocket. They were trading at less than $1 for years, and then now we've seen them starting to trade again.

A lot of this is because nobody has to rebuild infrastructure. So they were trading for like $1 and then pump and dump groups have happened upon them and say, oh, there's this thing. Why don't we try to like bootstrap off of it. We've seen what's happened is-- so there's been--

So what we try to do is we try to track the coins and look at all of the price peaks. And so what we've also seen is with the big move of Bitcoin in December of 2017, so Bitcoin skyrocketed during that time to a really high price, we saw some of the coins that didn't actually follow the price of Bitcoin and that's actually the first time we've really seen that, when Bitcoin has peaked at a price and then fallen fairly dramatically. And some other bit coins at that time didn't actually fall with Bitcoin.

They actually continued to skyrocket or they held constant. And so we started to see coins that have this value outside of Bitcoin, which I think is a pretty positive thing. We also saw a large quantity of coins, particularly low popularity coins that moved along with Bitcoin or moved slightly more dramatically than Bitcoin.

ELIZABETH KWOK: Great, thank you, Marie. So I think one, to take it back to some of the questions in the beginning that we discussed, we've spent a lot of time now talking about coins,

but as Kyle laid out for us in the beginning, there's obviously a lot of different ways that consumers are getting pulled into potential scams in the currency space. But one of the common things that we've heard from our panelists is this induced sense of urgency.

You know, you have to get in now. Prices are skyrocketing. You could have been a millionaire last December but let me lead you back there now. So Kyle, if you could just talk a little bit about maybe how consumers can identify these words and other ways they're getting pulled on a get in now way. And how they can maybe do research to see if it's real.

KYLE BURGESS: So I think I talked a lot about the kind of ways to identify it before in terms of like checking out the papers or verifying the founding team, noting other red flags like the requirement for gas or donations. If it's difficult to get in touch with anybody who actually works there. Even some of the bigger like wallets or exchanges, like Coin base, you can't actually get a human on the phone but that doesn't mean Coin base isn't a legitimate company. It's just their wait times for communication are very long because it's the most popular wallet in the US.

But in terms of things that consumers ought to be doing, there are companies out there that are trying to kind of solve this gap information asymmetry gap. There is a company called Coin Score and there's another one called ICO Guide. This is not an endorsement. I don't know enough about where they stand with how well their product-- or how well they've tested their products. But they're offering scores on different ICOs that are coming out. And they're basically aggregating a lot of data to, are their founders on the web page? Check yes.

Has the white paper been scanned and looked against other white papers for plagiarism? The Wall Street Journal actually recently did, I think it was in May, did a scan of over 1,400 white papers, or I guess cryptocurrency ICO companies. And 271 of those, which is almost 20%, had some suspicious language either on their white paper or on their website. They pretty much seemed like scams.

So 20% out there right now, it's just not likely that you're going to be in good shape if you don't go with something that you can't verify yourself.

ELIZABETH KWOK: Great, thank you. And Joe, you know, you talked a lot about what you found in your 30 days of research. And it seems rather daunting if all these stock images and you can buy video and splice it together and go to this level of even trying to attract a more accredited investor, for example. But what have you seen that is effective for consumers? Or what would you advise for a consumer trying to do their due diligence?

JOSEPH ROTUNDA: You know, I think first consumers need to realize that this, at this point in time, a really highly risky market. And they should not put any money into it that they can't lose. We talked to people who put their retirement savings into this market, their life savings. And they lose it. And they're devastated. So that's kind of the first thing.

Second thing is it never hurts to shoot an email to the regulator. You know, we're the regulator in Texas and we get emails quite a bit, you know, just saying, hey, what do you know about company x, y, or z? Our staff will check into that. We'll see if there's a reg d filing. We'll see if

there's any registrations. We'll see if we have any public information on that company and we'll be able to share it.

So that's something that is a tool that people should feel free to take advantage. The law enforcement and the regulatory agencies are there for a reason, and one of those reasons is to provide public information to consumers to help protect them. So there's those two different means.

Third is really conduct thorough due diligence. You know, as much due diligence as you can. The internet is a fantastic tool. You find all sorts of things on it. You know, that's how we're finding these fake pictures and these fake videos. You know, I hate to say it. I'd love to say we have some really secret law enforcement technique that we're able to use. You know, our law enforcement technique's called Google.

JASON MOON: Secret law enforcement technique, find the most technical language in the white paper, enter it in word for word, and see how many white papers pop up with the same language.

JOSEPH ROTUNDA: That's exactly right. You'll get a bunch. Google is going to go into overdrive. You can use the internet to find a whole lot of things like that. And you really, really can. And you know, I think another thing that is helpful, different secretaries of state maintain different levels of information. Sometimes you can get information about who's behind a company, where a company's located, if a company even is incorporated, if it's properly filed with the state it's doing business in.

And that goes for Companies House in the UK and overseas. There's ways to do that. But you know, I think it's been said before, it's a lot of the consumer protection issues are things that we talk about. You could take the word cryptocurrency out of it. If you're feeling too pressured to come in, if someone's telling you that you need to get in now to be the next Bitcoin millionaire and you feel high pressure, don't do it. If you don't understand what you're being told, if you don't understand what you're reading, don't do it.

If you can't explain it to someone else, don't do it. If it doesn't make sense to you, just don't do it. So it's these issues that I think really need to be kept in mind.

ELIZABETH KWOK: Great. And Amy, earlier you had mentioned the three things that the chamber has really started putting out there to help guide your members. And one of the things you were talking about was practices as well as kind of starting up the blockchain alliance. Are there any kind of tangible tidbits that consumers could look at when they're looking at a business's website or any hallmarks of, as you said, good actors?

AMY DAVINE KIM: Well, I mean, you know, what we're trying to do is to set out some guidelines for what businesses and technologists should be presenting to potential purchasers, whether it's a consumer or others. And so things like the white paper, make sure that it explains clearly and plainly. I think the lesson learned from what we're hearing here is clearly in plain English what the products or services that you're offering, how the token is supposed to work within that platform, and how those things will inter-relate.

It should also kind of disclose, you know, anything that's material to the functioning of the platform should be transparent and that should be laid out. And if there are risks of malfunction or other kind of disturbances on a platform, those should be talked about and how the company has decided to-- or how it's implemented technology to try to mitigate those risks.

So things like that, that should-- I mean, it sounds kind of obvious saying it, but any kind of professional business that would layout, here's how the platform is that we want consumers and others to use, and the types of detail that you'd want to see in there.

ELIZABETH KWOK: Great. Thank you. And Marie, you had mentioned even earlier this idea of there's a lot of resources out there online where you can see complaints about potential investment opportunities or business opportunities. Are there additional ways of searching, places that you found helpful when you looked at, you know, your over 1,200 ICOs and other Ponzi schemes?

MARIE VASEK: Yeah, so what we did is we-- so back when Satoshi Nakamoto created Bitcoin, he also created this forum to talk about it. It had a lot of different forms over the years. But currently, it's bitcointalk.org. It's a good place to look about all the different types of talk about all the sorts of scams. You can also go to reddit, though reddit in the cryptocurrency sphere is a bit hit or miss, just because of the politics of the moderators behind the different forums.

The best resource I've found is going to Bitcoin meet ups and talking to people about it, though that's not always useful is because I've found some of the people running these meet ups are also trying to sell you scams and trying to get specifically the consumers that don't really know anything because they're going to be more at risk. So that's a bit of a thing.

And similarly, looking at other seals and other sorts of those things on the websites, we found lots of very sophisticated things like this on Ponzi scheme websites, on fraudulent ICO websites. So we see Ponzi schemes that register companies in London which allow them to get like all of the security seals. And they get all of these like extended validation SSL certs. So there's a really strong incentive for scammers to get these surface level security seals and these surface level security stamps.

This is very similar to, oh, they have a group of people that work on it but all of them are stock photos and your favorite Supreme Court justices. So on one hand, yes, you should think about that. But on the other hand, they can be very misleading. And there's been a number of studies through the years, studies on these sorts of seals, that totally predated cryptocurrencies. And they found this similar finding that a seal is actually a stronger indicator of something fraudulent and something legitimate.

JASON MOON: I'm going to throw out this question to really any panelist who feels like they want to speak on it. When I was investigating the case I was working on, I was surprised just how-- these are not-- a lot of these are old scams, right? I mean, the basic chain letter where you pay money, you recruit two more people, they pay you. They recruit two more. And even the basic Ponzi scheme, you know, invest $500 and I will guarantee you a 100% return within 60 days.

How much is the novelty and buzz about Bitcoin, how much is it confusing and leading consumers into falling for things that they would never otherwise would have fallen for?

JOSEPH ROTUNDA: I think it plays a significant role, an absolutely significant role. And I think it's dangerous too. The average consumer, the average investor, the average person who's looking to somehow get into the cryptocurrency realm, by the time they're getting in, they really don't know too much about it. I didn't, I had no idea what I was getting into when I started taking a look at Bitcoin and other cryptocurrencies. But the thing that's dangerous about it is any promoter who's got a product can point to Bitcoin in December of 2017, November of 2017.

This isn't something that they throw out there as theoretical, like what we think we can make $20,000, you know, get a price of $20,000. They can show that it's been done before. And they're just kind of following in the footsteps. They're using a very similar technology. It's got a lot of the same buzzwords about it. It's using the same nomenclature. And it's something that investors can relate to.

They can understand-- they may not understand what a distributed ledger system is. But they can understand that Bitcoin rose in price to about $20,000-- 200, oh my god-- $20,000 in December of 2017.

KYLE BURGESS: We pulled down data from the Consumer Financial Protection Bureau complaints database. And we looked at virtual currency, digital currency, cryptocurrency. We looked at a lot of the different words to try to find the complaints that were specifically on not just ICOs but all manner of cryptocurrency. And there was a huge spike in December of complaints. It had been, like I'm looking at the graph right now, but kind of putzing along. There was a little bit of a spike last summer when ICOs first started to become popular.

And then in December the complaints skyrocketed, and by March they fell again. Because that buzz around the skyrocketing price of Bitcoin did get a lot more people involved and active. I will say, a lot of the complaints around that time weren't necessarily about scams so much as people being frustrated because they didn't hear back from Coin base for a couple of months. And I do really respect Coin base as a company, so I don't mean to rag on them.

But yeah, so it was things not related to necessarily being scammed. It was, like, couldn't access my funds or my account was closed without explanation. Or the bank thought that I was a scammer because I was interested in cryptocurrency.

JASON MOON: Marie, I don't remember what time period your research covered, but did the rise in the value of cryptocurrency extend the life of some Ponzi schemes out there?

MARIE VASEK: I don't have work on that, particularly. We do have some work on looking at the influence of the price of Bitcoin on the number of new coins. And so the thing to note is that while it does increase the number of scammy coins that increase, it also increases the number of legitimate coins because a lot of investment money to cryptocurrency startups are given in Bitcoin. And they're given in a different quarter.

And now all of a sudden, their Bitcoin is worth more and so they can start a coin more easily. So there's legitimate coins that have that same cycle as the fraud.

JASON MOON: Amy, have there been a sort of a trend or kind of a bubble of new startups that kind of come along to coincide with the massive value, increase in value of Bitcoin?

AMY DAVINE KIM: Yeah, I don't have statistically accurate studies on that, but our experience has been to see more of that, and more people who want to join the Chamber, too. So we've been careful there, as well, to make sure that-- there's no way we can-- it's hard to tell. So we can't ensure compliance of any memeber, but we do look for building a healthy ecosystem. So I don't have any statistical studies on it, but I have-- we just anecdotally have seen a rise in companies in this space.

But I do think, just to build on that point, I mean, we are focused on scams here and that's what this is all about. But there's a lot of really impressive, innovative, hardworking companies out there that are really trying-- both household names you may have heard as well startups that are really trying to make a difference with this technology. So I don't think it's-- some of these cases that we've described, I think, seem a little more straightforward and maybe more obvious.

And then some, maybe, you know, there's many out there that are real businesses that are trying to build something. Again, I think one of the dividing lines is are they asking you to invest or not? And the speed and some of the factors that we're talking about here, may be some flags for our average consumer to think about.

ELIZABETH KWOK: Great, thank you so much, Amy. And on that note, I think that concludes this panel. We're going to take a short break now until 3:05 and we'll reconvene for our final panel at that point.

[APPLAUSE]

DUANE POZZA: I'm happy to introduce our third panel, which is called Effective Approaches to Cryptocurrency Scams. We'll be talking more about some enforcement strategies, consumer education, and anything more that needs to be done in combating cryptocurrency scams. My name is Duane Pozza. I am an assistant director in the division of Financial Practices. Just one reminder, if there are-- if we have time at the end for audience questions, we will do those. So if you have questions in the middle of this panel, you can write them down on a note card and just hold them up. And we have someone who will be periodically scanning to see if anyone is holding up a notecard, grab it, and then we'll see if we have time for questions at the end.

So I'd like to just give a brief background of our distinguished panelists. Michael Frisch is at the CFTC. He's a senior trial attorney in the Division of Enforcement. He's based here in Chicago and works on cryptocurrency-related investigations and enforcement actions, including those involving market manipulation, fraud, and trade practice violations.

David Hirsch is at the SEC, where he is the cyber liaison and a senior counsel in the Fort Worth office. He's an enforcement attorney and also a member of the SEC's DLT working group, and

the dark web working group. Sarah Jane Hughes is the University Scholar and fellow in commercial law at Indiana University's Maurer School of Law. She's also a veteran of the Federal Trade Commission. Since 2014, Sarah Jane has served as the reporter for the uniformed law commission's work in this field.

Colleen Sullivan is the chief executive officer of CMT Digital Holdings. In her role as CEO, she oversees CMT Digital's trading investments and regulatory initiatives in the crypto assets and blockchain technology space. So I think a natural place to start this panel is to talk about enforcement actions, although that won't be the only thing we talk about. And I thought since we have some representatives from agencies that have done work in this area, we could start there. So I'll start with Mike, actually.

And this is a question for Mike and Dave. You can decide who gets to go first. Both of your agencies have obviously been active in the area of cryptocurrency fraud. And I'm wondering if you could just talk about what your agencies have said about their role in combating crypto frauds in this area and some of the work that's been done?

MICHAEL FRISCH: OK, I guess I'll start with the standard disclaimer. So I'm Mike Frisch. I'm speaking here not as a representative of the CFTC, so any opinions I give are my own. So we have to say that for all of our presentations. So on February 6, 2018, Giancarlo, who is the chairman of the CFTC, testified before the Senate Banking Committee. And there are some prepared remarks you can download off the internet if you want to see what he said there.

I think he gave a nice overview of how we view our role. So you know, unlike a security or a futures contract, there's no one regulator that's responsible for cryptocurrencies. So the CFTC, the position we've taken, is that Bitcoin is a commodity. Other cryptocurrencies are or can be a commodity. And our role is to investigate and, if appropriate, take enforcement action against firms in the space that are offering derivatives on cryptocurrency, futures contracts and options, and also companies that are involved in fraud and other kinds of market manipulation, both in connection with derivatives and also in the spot market.

So I guess what that means is we have a pretty-- we view that we have a pretty important role to go after this kind of bad conduct. But unlike our role with respect to futures exchanges, like the see me down the street, we don't have regulatory authority. And I think that's really important for people to remember when they're buying cryptocurrency on a Coin base or some other exchange. You know, we don't set rules for how money is, customer money is held.

We don't set rules for how trades are processed. We don't set rules for a host of other things that do exist in the regulated markets. So we have anti-fraud authority, that's pretty broad. But when it comes to the spot markets, our authority is basically just fraud and manipulation.

DAVID HIRSCH: And to echo what Michael had to say before I begin, the Securities Exchange Commission disclaims responsibility for any private publication or statement of any SEC employee, such as myself. The speech expresses my own views and does not necessarily reflect those of the commission, the commissioners, or agency staff.

MICHAEL FRISCH: His was better than mine. I will adopt that one as well.

DAVID HIRSCH: So the SEC has been fairly outspoken on the issue of cryptocurrencies, and also more accurately or more specifically, digital tokens. And the language we use, I think, is important. So cryptocurrency is to the extent it's just a one for one medium of exchange, something like Bitcoin. And we have not, I think, publicly taken an opinion one way or the other. But the extent is just an exchange of value. That is potentially a currency and therefore more likely, potentially, in the kind of wheel house of the CFTC.

And we, as an agency at the Securities and Exchange Commission, our first inquiry is jurisdictional. You know, is this a security or an investment contract such that we are the appropriate regulator to be involved and the appropriate person to be opining or to be assigning regulatory obligations to the players? Our chairman has been very outspoken on the topic of ICOs and ICO enforcement. And he's basically said while it is theoretically possible for an ICO to not be a security offering, as of a few months ago or as of, I guess, December, I think when he made the statement, he had never seen one like that.

So a lot of the ICOs bear the hallmarks of investment contracts. The analysis we run through is called Howie test. It's based off a 1940s Supreme Court case that basically said, if you are investing money with the expectation of profits, based on efforts of a third party, and that's not like an investment contract, it's a lot like a security, the SEC regulates those. And that creates obligations for the people who are promoting them. The promoters have to register with us. And that is very helpful for investors.

We are a disclosure-focused agency. And we can help protect investors by requiring people offering investments to disclose who they are, where they're based, what their prior experiences are like, setting limits and rules as the types of projections and statements they can make going forward. And so we, as an agency, have taken enforcement actions against people who have violated our rules, primarily for fraud, but also just for a registration violation.

There's a case called Munchy that came out in, I believe, November of last year, where it was basically an entity that was promoting its own internal digital token for the purpose of creating this new network of restaurants and consumers of restaurants, and reviewers. And they thought it'd be great to have this token that would work within their app that was available in the app store. And they had an ICO where they were going to sell these tokens out to the public. And we got involved and brought a settled cease and desist action against them were they acknowledged-- well, they neither admitted nor denied-- but we alleged that they had violated securities laws because their token was essentially a security and they hadn't registered with us.

So we are looking both to try and enforce registration obligations on the promoters, and also seeking to bring enforcement actions against scams and fraud.

DUANE POZZA: And what are some examples, just sort of briefly at a high level, of the kinds of frauds that the agencies have gone after in this space?

DAVID HIRSCH: So I was an investigator on a team that brought a action against a company that was called Arise Bank, which was an ICO that came out in December, was open through January, and we announced our action against them in early February. We saw it and awarded a temporary restraining order against them. They were a company that claimed to have raised upwards of $700 million. They said that their promoters were important members of the community. They said they had relationships with companies that would allow them to issue Visa cards, Visa branded cards, that would allow you to spend any of 700 different cryptocurrencies anywhere that would accept a Visa card.

And we were able to bring forth evidence suggesting those things were false. And they've since made filings in court suggesting they only raised about $3 million, so significantly shy of the $700 million they'd been telling people. So I think we are focused on bringing actions against companies that misrepresent either who they are, what they're doing, how far along in the process they are, or what the likelihood of returns are.

MICHAEL FRISCH: Sure, I'll speak to that. I want to echo a few things that David said. So the CFTC has been working really closely with the SEC on these matters. And I think that's important because we do have very different spheres of responsibility, whether a coin is being used like gold, or like a trading vehicle, or as an investment vehicle, as David explained. And you know, with the CFTC, it's the same thing. The first issue is always, do we have jurisdiction over this conduct.

So when the Ponzi schemes are caught and show up in court, I found that they-- as we've seen-- they often want to spend a lot more time talking about our lack of jurisdiction over their conduct, rather than what they were doing wasn't actually fraud. So we've had a couple of waves of cases. You know, in 2015, the first case came down. It's called Coin Flip, where the company was basically offering futures contracts and options-- I think it was options on Bitcoin. The commodities exchange act prohibits anybody offering futures or options without being registered with the CFTC.

So it was plainly illegal. The firm shut down and they weren't fined. I think, basically frankly, because it was the first case. I brought a case in 2016 against a trading platform called Bitfinex, where they were offering leverage margined trading to US customers. You can't do that under the Commodities Exchange Act unless you are registered with the CFTC, which they weren't. So that was the case that I worked on.

They stopped doing that and then pay the relatively small fine, $75,000. And we noted their cooperation in the settlement order. So those sorts of, I think, those cases fit into the whole derivatives on cryptocurrencies being offered in a legal way. There was no allegations of fraud in connection with those two cases. The next wave really ramped up when the price of Bitcoin took off in 2017. And we brought a number of cases, I think, eight or nine, don't quote me on the count, of firms making fraudulent promises.

You know, there's a case called Gelfman, where they were offering, you know, promising like pretty much the standard Ponzi pattern, promising huge returns, sending false trading statements when there was actually no trading going on to customers, and then claiming that there was a--

Mr. Gelfman created a fake, allegedly, hack where everyone's money mysteriously disappeared. But in reality, there was no hack and he had misappropriated the funds. So there's been a number of recent sort of Ponzi scheme-esque cases that we've seen a lot of those.

And we've been going after those under section 60 and rule 180.1 of the Commodity Exchange Act, which gives us jurisdiction to go after fraud and manipulation even when there's no derivative involved, which I can discuss if you want, but it might be a little too wonky for this group.

DUANE POZZA: We might come back to that.

MICHAEL FRISCH: OK.

DUANE POZZA: So clearly there's, for the agencies, different jurisdictional hooks. And there's different agencies involved in this area. And we also heard in the last panel from Joe about the states being very involved in the space as well. We heard in opening remarks that the FTC has brought cases in this area and under section five, [INAUDIBLE] practices law. Sort of a two part question that I'll direct to Colleen and Sarah Jane first, which is, are there gaps between what the agencies are doing? And alternatively, are there no gaps and there needs to be? Or what is the ideal level of coordination among the different folks and regulators who are concerned about this space?

COLLEEN SULLIVAN: Sure. So addressing the gap first-- and I feel like I should say that I am here with these regulators and former regulator. I'm speaking on my own behalf and not necessarily my partners at CMT Digital. But I will say when we started trading in the space, a significant gap in regulation, which Michael mentioned, is that there's the spot markets don't have a federal regulator sitting on top of them outside of FinCEN. And FinCEN would only cover certain aspects of what these crypto exchanges are doing.

So our view on trading in the market place was, we've traded for 21 years in regulated markets on regulated exchanges and regulated products. So we did a gap analysis, you know, what are we used to doing in these traditional markets versus what is it like on spot markets, the crypto spot markets? And we developed our own internal best practices and standards and decided that those were the ones that we would hold ourselves to.

So to provide a specific example, you know, unlike our traditional markets, you don't have a prime broker sitting in between the trading firm and the crypto exchanges. So your counterparty risk is to each and every crypto spot exchange that you trade on. So we developed, at this point, it's over 60 points in our questionnaire to evaluate counterparty risk, starting with basic things like, do you know who the management team is? Do you know where they're located? Have you spoken with them?

Really basic stuff. But then it gets into hacks. What's the cold wallet versus hot wallet storage policies and procedures? What's the banking relationship? Is this spot exchange regulated in a foreign jurisdiction? Have they had any enforcement actions? All of that. And then the exchange will either get a yes or no as to whether or not we're on board. And then we further go into how

much crypto and fiat are we comfortable leaving on those exchanges? And that's a dynamic risk assessment that goes on daily.

So that's how we've addressed that gap. What we're excited about, and Commissioner Quinn Pence has spoken about, is that Gemini is trying to put together the virtual commodity association, which is a self-regulatory organization for crypto exchanges that trade crypto assets that are deemed commodities. Generally, though, I think that's what we're seeing the industry start to do is self regulate where there's gaps. You know, I think Amy mentioned the Token Alliance with the Chamber of Commerce. There again, you see this push for standards and best practices. And that's really what the industry needs to do to protect itself.

SARAH JANE HUGHES: Last disclaimer of the day. I do not speak for the trustees of Indiana University or for the other faculty members of the Mauer School of Law at Indiana University in Bloomington, or for the Uniform Law commission. It's just me. And it will just have to do. And before I say anything else, I would like to have a show of hands, if that's OK, Duane? How many of you are lawyers?

OK, how many of you are investment advisors or people in financial services companies that are actively involved in this area? Actually, I was they would be a few more of you in this room. And I was hoping that there would be a few more of you in this room, because I think that's part of where some solutions, like industry self-regulation are going to have to come from, a multi-point approach to whether you as an enterprise-- your own enterprise-- whether you're going to partner with somebody, invest in somebody, acquire somebody, merge with somebody, that's a way in which you can help prevent fraud that affects enterprises and consumers at the same time, in my view.

And so how many of you thought you knew something about ICOs before you came into this room? Notice I used the word thought. OK. And then the next thing I want to know is how many of you learned something that you never imagined you would learn already today? That should be everybody, I suspect. But we haven't finished doing-- me too. We haven't finished doing our job yet, when we haven't done those kinds of things. The FTC-- and I worked there from 1974 to 1988-- does two things in addition to law enforcement. But it does two things really well. It does really great business education and really outstanding consumer education.

And I think in all of these arenas, more of both are needed. So I'd like to see more work, like your work. And yours is proprietary. But there are some touch points that could be public touch points for business education in this area so that businesses won't make some of these same mistakes because I fear that they are. And then I would like to just quickly talk about the fact that I think this is a multi-profession role, in terms of dealing with scam artists.

And the FTC has been involved in combating consumer fraud for at least 50 years. And when I joined them in 1974, there were several active cases. Some of those cases were about selling land that was 50 or more miles from the closest energy source, water supply, or it was under water, as investments. And it's-- Howie was an orange grove, if you didn't know that, in Florida. So the FTC and the SEC have been involved with cases like this for a long time.

The next kind of scam that came up involved business opportunities. And the one that stuck with me, which I think came from the Chicago regional office at that time, was someone who was offering franchises to grow mushrooms in your closet. Not like orange groves, but it's close. And then there were the free travel offers. And this was so long ago. And the first of those cases I brought here in the Northern District of Illinois with partners from the Chicago regional office and the US attorney's office here in Chicago. Were free travel offers but it was so long ago that they sent postcards to the intended victims.

And the victim called them because telephone war rooms hadn't really grown up because telephone calls were really expensive in the 1980s. Whereas if you got them to call you, it was free, unlike cell phones for a while. And then there were other things that went beyond that. But the telemarketing from Canada, telemarketing from other places, the stories are remarkably similar across a 50 year history. But there's one more-- there are two more big similarities.

One is, some of these people don't stay in business in the same name very long and almost all of these waves or iterations of scams involve some of the same people. So chasing these people across state borders, across international borders, figuring out how they were getting paid, talking to the credit card companies in the '80s because that's how they were getting paid in the '80s, looking at ACH transfers and other means by which people were receiving money that they took and ran with. And almost everybody has seen that movie The Rainmaker where the insurance company that wouldn't pay for the cancer treatments, eventually the guy ran to Switzerland after the judgment came out. That's what would happen.

So we started doing it-- I did-- I tell my students, including some who were just in the room, that one of my favorite things to do was first we froze their assets with an ex parte government order issued by a judge at crack of dawn. Then we'd find the US Marshal. Then we'd go get their bank account. And then you would serve them the papers saying that they'd just been sued so they couldn't touch the money at that point, so it was the only effective way to do some form of consumer restitution. That piece of this is new and it will be much harder to do that in this space, because it will be much more difficult to figure out where the money is going.

So that piece of the catch me if you can is the one that is the biggest challenge for those who are going to engage in enforcement in this area, in my personal opinion. But that means that we can't let it go that far. We have to try to head it off in a different direction with education, with more robust standards about who's going to invest, or buy, or partner with, and things of that kind, unless they're just pure frauds. I don't think we're going to fix the pure fraud problem. This is just the latest iteration of the pure fraud problem.

That went on longer than I meant, Duane.

DUANE POZZA: Well, just picking up on that--

DAVID HIRSCH: Yeah, if all right, I would just like to echo what you have said. The goal of fixing the pure fraud problem is a very difficult one. I admit it's daunting. But I think the FTC is doing a great thing by bringing people together here and virtually to become more educated about the potential for the pure fraud problem. At the SEC we have a robust program on

investor.gov that offers lots of guidelines and things to look at when you're thinking about investing, if you're thinking about investing in this space, questions you should be asking yourself and questions you should be asking the promoter.

I think that really the only way to address it is through education and through kind of benevolent skepticism when presented with an opportunity to really think carefully as to whether this is somebody you would trust to watch your dog. Is it somebody you really want to loan your money to, give your money to, invest your money with.

MICHAEL FRISCH: And if I had any advice for the general public related to like where to trade cryptocurrencies, as Colleen said, you know, there's a new push for self regulation and standards that frankly I applaud. But there's a wide variety, a wide variation between some of the stronger firms with US connections. I don't want to single anybody, but you know, Gemini and Coin Base, those are based in the US with strong connections to the US, that are regulated lightly because they take fiat money. So basically you can wire US dollars into those exchanges.

And so they're required to do some amount of know your customer, KYC, some amount of monitoring for money laundering and other things. And so there's some standards go along with those light requirements. But there are other exchanges that don't take wires of actual money, where they only accept cryptocurrencies to trade on. They're not based in the US. They have very light US connections.

So these firms only require an email account, an email address and a password. And you know, you could be wiring tens or hundreds of thousands of your hard earned dollars to some exchange overseas. You have no idea who is behind it, what policies, what consumer protections they have. There's very little, if any, recourse for you if the exchange is hacked or if the owners steal your money.

So to me, getting defrauded by some promoter starting a new coin is a risk, but as significant a risk, I think, is sending your money to some exchange that you know very little about. So that's, again, customers should be very careful about which exchange they choose to do business with.

COLLEEN SULLIVAN: And I'd to highlight something Michael and Sarah Jane both said there, because I think it's interesting. Sarah Jane mentioned how you could get a freeze on a bank account. And Michael's talking about some of the international exchanges where they're, what we call, crypto to crypto, so there's no bank account relationship. So I always think of one exchange in particular.

And I'm not aware of any fraud or anything bad going on there at all, I just use them as an example. They're the largest crypto exchange in the world right now, Binance. They launched in July of 2017. They've just grown rapidly. But they're crypto to crypto only. So to the extent there was some theme, you know, maybe not great going on there, there's not a bank that the regulators regulate that you can lean on to stop that activity if there's a gap in regulation with respect to the exchange itself. And there's no bank account to freeze if there's bad activity because it's just crypto to crypto.

And I think from a regulatory, arbitrage kind of way of thinking Binance is interesting too because the founders were originally based in Hong Kong. And the SFC had some issues about what they were listing. And finance, just then, relocated to Tokyo. FSA had similar issues in Tokyo and Binance moved to Malta. So there's not much tying exchanges physically to the jurisdictions they're located in. A lot of these exchanges are online training programs or whatever you want to call them, are in the cloud. They're in AWS. It's not like they have necessarily headquarters in a physical building where people are coming in every day.

So the regulators have an incredibly tough job, I think, in this new environment because it's all so small right now. So when you look at the total market cap of crypto assets, it's $252 billion, I think, as of this morning. It's fallen quite a bit since the highs. Gold is $8 trillion. Our global equities markets are $79 trillion. But you also have a huge retail population exposed to highly volatile assets. So how do you find that right balance of consumer protection and not stifle innovation? That's a lot to think about.

You guys have the hard job.

MICHAEL FRISCH: Yeah, I mean, just to add on, when AMF Global collapsed, that was a highly regulated, you know, US-based entity. And the CFTC is proud that there was no actual end user customer that lost any money. The system worked there. And whereas I know in 2017, or maybe it was late 2016, Bitfinex, another one of the companies that I brought a case against was hacked. I think they lost about, at that time, $72 million worth of Bitcoin.

And what they did is they basically decided to socialize the losses across the traders and gave everybody a 30% haircut. Now, is that OK? Who do you go to if you're a customer and you don't like that? I mean, there's no rules that the CFTC or any federal regulator I'm aware of has to-- or standards to enforce that. So again, not only when you think about are they going to steal my money, but things can go wrong. If you're trading on a regulated exchange here in the US you have so many more protections. You have protections from your money in bankruptcy. You have protections from-- there's a whole reparations process at the CFTC if you get defrauded by your broker.

So there's so many-- there's so much more for you there to trade on.

DAVID HIRSCH: I think I would echo that. And one of the things that is a focus for the SEC as an agency is trying to bring folks into the light and get them into a compliance regulatory framework. So we will be able, hopefully, to deal with them in a more traditional manner, that there is more traditional set of disclosures, but also protections and recourse in the event of bad things happening. So it would be a more traditional model of how they operate.

And I wanted to echo something Joe Rotunda said on the last panel, which is we as an agency don't view blockchain or distributed ledger technology as an ill or a problem. It's a people issue. And so, you know, the SEC has a three part mission. One is to protect investors. Two is to facilitate fair and efficient markets. And three is to facilitate capital formation. And so there can be some conflict there where new technology is maybe really effective at helping to facilitate capital formation and that's part of our mission statement. We need to encourage that.

We just can't allow that to happen fully at the expense of protecting investors or having markets that are fair and efficient. And some of the unregulated exchanges, if there's no one there monitoring, if there are no rules standardized that they're all playing by, I mean, how are you as a investor or consumer sure that there isn't market manipulation going on? There isn't spoofing. There isn't previewing of your orders and trading ahead of what it is you want to do. There's just a lot more uncertainty when you're dealing with folks who are not compliant or not within a larger framework of regulatory compliance.

DUANE POZZA: Sarah Jane.

SARAH JANE HUGHES: So there is a gap filler, in part, coming down the road pretty fast. And that is the work of the uniform law commission in this space. The uniform law commission has approved and will soon have a second piece. But the first piece is prudential regulation of people who issue virtual currencies in a centralized way, or who offered to transact them or take custody of them on behalf of others. One of the beauties of virtual currencies, if you want to do it that way, is it can be a peer to peer transaction.

But many people don't do peer to peer transactions. They use someone else to do that work for them like many of us still use banks to do that work for us. Or people perhaps with less means and people who might be more susceptible to some of these scams use money transmitters, MoneyGram, Western Union, all kinds of people like that, check cashers and others. So the uniform law commission's uniform law that was approved last year will do prudential regulation of the same model, basically, as money transmitter regulation that has been in place for several decades in many places.

It's lighter, in some respects, than money transmitter regulation. But it will have some additional protections, such as protection from the creditors of the provider. If you they're holding your money, they have to hold your money as a liability. And they will have to be able to protect it in some way that they can satisfy the regulator with. Money transmitter's net worth requirements and capital adequacy requirements tend to be on the heavy side. We tried to lighten it up to allow people who are innovators to be able to begin their businesses, do some testing in the wild, without having all of the responsibilities and without the significant upfront cost of getting a full license.

We have an intermediate space between a full exemption from this ex coverage for people who are not just trading house money or using house money to test below $5,000. From $5,000 to $35,000, this new act will require that you tell the state you're there and follow some of the consumer protection and disclosure requirements. So if you're going to handle other money-- now Peter Van Valkenburg, with whom we worked on this project, once said something that others have said today about if it quacks like a money transmitter, it ought to be regulated like a money transmitter.

But not necessarily using exactly the older money transmitter models because the definitions don't work. There is no interim registration or sandbox kind of space so you can do some testing in the wild. And like the bit license, model which many of the states did not care for, or they just are jealous of New York, I'm not sure which, that one they won't certainly want me to say, but

too bad, I already said it. The thing I think is though that process was used extraordinarily slow, there were only a handful of companies-- three, almost three years later, I think the announcement was June 24. But the license applications were due early August of 2015.

And we're talking about fewer than 15 companies that have received licenses.

COLLEEN SULLIVAN: Seven.

SARAH JANE HUGHES: Yeah.

COLLEEN SULLIVAN: And two trusts.

SARAH JANE HUGHES: Two trusts, right. I mean, it's a tiny number. And the two trusts, all of it seems to be going OK from what we can tell. But it is a very slow process. So if you file as a registrant under this law, you could continue to work until they told you weren't going to get a license from the state that was involved. The states, historically, have regulated non-depository providers of consumer financial services. And this is a way for them to continue in that role.

The states are often seen, sometimes accused, of being innovators or incubators in regulatory spaces that can be very valuable. Identify regulatory gaps that sometimes Congress has the wherewithal to address. Sometimes Congress doesn't. But I think it is really-- or they just don't have the appetite for it on the agenda that they have-- I think it's really important for a very strong web of collaboration with local, state, regulatory, and enforcement agencies, legislative bodies, and practitioners in financial advising, MNA, lawyers advising clients about partnerships.

And in Chicago, this huge FinTech industry that is coming here can be a very important player in a kind of important industry self-regulation that's worked pretty well in some other areas of the law and a market. And I'd like to think that that is a model that will be picked up. That will not solve all of these problems, but it will go very far as long as there continues to be robust enforcement a lot of education, aimed at different audiences.

DUANE POZZA: So we've talked a little bit around industry self-regulation. And in light of sort of the kind of hardcore frauds that we've been hearing about throughout the day, which is a challenge for anyone to deal with on the industry and the enforcement side, what is the sort of the practicalities of industry self-regulatory efforts in this space? And what role can industry play in either helping to identify frauds or helping law enforcement identify frauds? Or otherwise trying to get the fraud out of the space?

COLLEEN SULLIVAN: Yeah, so you know, I think why-- so in a new sort of asset class, in the new technology, I think where self-regulation is helpful with law enforcement is the initial participants in putting these standards and best practices forth are the ones actually in the space. So you take, again, for example, Gemini, they're operating a crypto spot exchange. And they've brought in NASDAQ to do market surveillance on the exchange. They've gone-- you know, so they see this gap. And they're implementing pieces from traditional exchanges that are regulated into their own marketplace.

And then their hope is to then take these standards of best practices and put them out there. But also as part of that effort, you've got trading firms like CMT that are collaborating with them. So then we can share what we're used to seeing in the marketplaces and what we're observing trading these marketplaces as an industry participant. So I think having that practical experience is part of the self-regulatory initiative in the early stages is important. With the hope then being that the regulators and these SROs are working together.

And I should clarify. The virtual community association that Gemini is working on is different than NFA and Finra. Those two SROs are mandated by Congress and receive funding from the government, and therefore they have more enforcement capability. The virtual community association will not be mandated by Congress any time soon, I would think. It's going to take a while to get there. But they will have their own sort of mechanisms within that structure to hopefully influence the behavior of the members that are part of that association.

Similar to the Token Alliance that Amy mentioned, the chamber has 160 different members. There are 300 plus participants in putting that together. Those are all industry participants. So it's just helpful, I think. I mean, I am in this industry 24/7 and I can barely keep up. So you have regulators who are doing nine million other things. I don't know how you even begin to stay on top of all of it. It's really challenging. And this technology, unlike-- to me, the internet was like a slow evolution compared to what we're seeing in the crypto, blockchain space. It's kind of incredible and exponential.

So I think that the industry helping participate in these early days, and I think the industry realizes it. Like the week, blockchain week, in New York, which was just six weeks ago, I went to four different self-regulatory meetings with people, four different groups, that are trying to put forth standards in different aspects of the industry. So I think the industry gets it. We have to start policing ourselves.

MICHAEL FRISCH: And I hope to see more referrals. I mean, the [INAUDIBLE] exchanges, like the CME and CBOT, many of the CFTC's enforcement actions start with a referral from an exchange. And the exchanges are in the best place to see whether wash trading, market manipulation, pump and dump schemes, or spoofing, or other bad practices are going on on their exchange. So I can't say that's not happening now. But I hope that it is something that will happen in the future.

COLLEEN SULLIVAN: Yeah. And that's a good thing to have in open dialogue with, like these groups that are putting together these best practices and standards coming in to meet with the FTC, the SEC, the CFTC, FinSEN and talking about how do we open that line of communication so we're sharing what we're seeing.

DUANE POZZA: And I'd actually like to broaden that conversation a bit, like what are the best ways to get complaints that enforcement can act on? I think there was even a suggestion in the previous panel that we should act before we even get a complaint based on how quickly these things are moving. Is that helpful to come from industry? Are consumer complaints very telling? Or are they sort of too late by the time we get them?

Like what are the ways that enforcement should or should gather information about this and figure out the biggest problems and go after them?

DAVID HIRSCH: So for us at the SEC, we have a very robust system where we take consumer industry expert, any complaints, it's called the tips, complaints, and referrals. So a lot of my investigations begin when someone comes in and gives me a TCR, tip, complaint, referral. And that would just be from anyone. So one of the reasons I like to be out in the public, like to be at these events speaking, is to request that anybody who is aware of things, doing research for yourself, if because of your position in the industry, if somebody gives you a hot tip that sounds too good to be true, please shoot me an email.

Please go to the SEC. Go to investor.gov. There's a link there where you can submit a complaint or a referral. But we get them from sister agencies, so Texas State securities board or other state regulators. We get them from criminal law enforcement agencies. We get them from the public. We get them from industry. But I think everybody who is interested in seeing a broader adoption of blockchain technology, or sees promise in this industry, agrees that it is going to be a quicker adoption and a smoother adoption with less fraud in the market.

And one of the ways to try and remove some of the fraud in the market is to notify regulators. Tell the cop on the beat there's a problem so that we can come in and try and clean it up.

SARAH JANE HUGHES: Were those that are moving really fast, that is a two day deal, that's never going to be a solution. But it just occurred to me throw out an idea that came to me some months ago and then I left it. And I thought about it again just listening to all of this, which is, I think that there could be some more focused community-delivered, not virtual-- not the virtual currency community, but communities and people who are counseling older individuals.

So in the state of Indiana and Massachusetts where we have homes, there are very robust counsels on aging that provide all kinds of services. I worry that vulnerable populations, people who don't speak English very well and are newly arrived, people who are at home a lot, vulnerable to the 15,000 telemarketing calls we all get every day but we're not there for, but they're there to answer the phone. They don't hear well. The English is sometimes accented [INAUDIBLE]. But I'm beginning to wonder if we shouldn't try to aim some education that people like that in churches who provide remarkable resource opportunities for certain kinds of people who might have some funds that they saved, they lost big savings in the deep recession.

And they're trying to get back to where they were financially. If we could think how to do something that would deliver at the local news level but way closer to the floor of the local news, I think we might suddenly provide people with that pause moment. Because Marie's-- her discussion of her research makes me think that what we have to do is make people not push the button to send the money, and that we have to find a more appropriate, fast response way, not to talk about specific companies, but to take something from your 60 point idea and figure out the facts that you guys have in the FPB or the BFCP has, whichever your politics are.

Because that's with the accents, I guess. The point here is we have to reach people before they push the button because for the most part, reaching them after they pushed the button on a fast moving fraud is no recovery.

MICHAEL FRISCH: And I agree with that. And to add one point is, look, I think banks, retail banks, have a role to play too. If you're an employee in a savings and loan in Omaha, and your client is a 70-year-old widower, and you see $13,000 wire to some cryptocurrency exchange in Bulgaria, then there should be a phone call, you know. Is this really what you're trying to do here?

And I think in this day and age, with the huge mega banks, and there's less of a one to one connection between bankers and their clients, I think some of that, that last line of defense has been weakened over time. Hopefully we can--

SARAH JANE HUGHES: So I thought we were supposed to learn that lesson from what happened to the government of Bangladesh. They had the $15 security system and I think the banks can do that but the outgoing wires are subject to a whole bunch of existing rules. And the question is, are the banks really doing this article 4A sales security procedure they're supposed to have and call the customer if it seems like an out of pattern deal, because the customer may say, yes. I authorized that transaction. Or the customer may say, as my late father and father-in-law both seemed to have had some of these problems, no, I don't remember that transaction.

And if I don't remember that transaction, I'm hoping the bank won't push the send button. But who knows?

DUANE POZZA: Sarah Jane raises the broader point of how do you reach consumers, especially when they're confronted with the sort of fear of missing out.

SARAH JANE HUGHES: Absolutely.

DUANE POZZA: What are the best ways to get them? I know the SEC did this stop and pause moment with the Howie coin, maybe you could talk about that, and other sort of strategies that we have to educate consumers who are still even trying to figure out, as we are today, the language around this and the terms.

DAVID HIRSCH: Sure. And another disclaimer, I had no involvement in this and really only found out it was happening when it went live on the web. But the SEC issued something that it called the Howie coin. And that calls back to the Howie test that I referred to when we started speaking today. And they said that the Howie coin-- they issued a white paper. And they said Howie coin is this great new investment opportunity. It could revolutionize the travel industry with the benefits of decentralization and blockchain.

Like they made their own word salad. They had pictures of people who don't actually work for the SEC or aren't associated with any offering in their offering. They had it very much like a scam white paper. And that if you click, I'm interested-- and it promised outlandish returns and did everything you would expect for a white paper that was ill-intended or malicious, and if you

click I'm interested to buy, it would automatically redirect you to investor.gov and would give you education about here are some of the things you should have been looking for in the white paper that should have clued you in that this is potentially a fraud or a scam.

And you should be skeptical go forward when you see things like this. I thought it was very clever, very creative, a good way to really put into practice the things that our chairman has been saying and that we as an agency have been saying for quite some time about the importance of investor education and investor awareness, and a healthy degree of skepticism when talking about investing your money.

SARAH JANE HUGHES: Because ultimately, turning the spigot of money on is the only way this is going to get solved. And that is clearly a collaborative venture that's going to go on for a long time. But I want you to do something for the audience just in case, and that is, we've talked about the Howie test. But we haven't told you what's in the Howie test. So, Howie test, please.

DAVID HIRSCH: Sure. The Howie test is, in analyzing whether something is an investment contract, and thus the equivalent of a security and the sort of thing that the SEC regulates, you got to ask yourself, is it an investment of money with the expectation of profits, in a common enterprise, based on the efforts of a third party? So Howie was an orange grove.

And basically, they said, you can invest here. You could buy part of the orange grove. And don't worry about it. We will-- you don't even have to live anywhere close to it. We will grow the trees. We will harvest the origins. We will take them to market. We will sell the oranges. You just sit back and let the money roll in. And the Supreme Court said that is effectively a security investment. That's an investment contract. It should be regulated like a security. If you're going to offer that, you need to register with the securities and exchange commission unless you qualify for an exemption.

And the same rule has been applied to pay phones. Some of the younger people in the audience, I can tell you what pay phones are later. It's been applied to lots of different things. It's a very flexible analysis that says, because people we're working up against, in some cases, are also clever. They're trying to find ways to engineer how they describe what they're offering around the plain language of the regulations. And the courts have said, that's not good enough.

It's not the words you use. It's the substance of what it is you are doing. And so Howie is a very flexible test. And it's been applied in the same way to orange groves, to pay phones, and now to digital tokens. If you're offering something with the idea that the investor, the purchaser, is going to profit as a result of something you're going to one day build, or that you're in the process of building, or that you're going to make more successful and that's going to generate more money for the investor, you may well be offering an investment contract. And that is likely going to be regulated by us unless you can establish why you qualify for an exemption.

DUANE POZZA: So we have two minutes left. And my last question, it's a speed round, then. We often, as enforcement agencies regulators are always balancing enforcement with protecting consumers with innovation in a very innovative space. And we're always mindful of that. This is an area where we've heard of a lot of consumer harm and a lot of fraud. At the same time, it is a

rapidly growing innovative space. Do you have concerns about a balance between enforcement and pro-consumer innervation here?

And what is the best way for-- and I'm looking at Colleen to answer this question first, for enforcement to go about protecting consumers while keeping open pro-consumer innovation?

COLLEEN SULLIVAN: So I don't think I can really speak to the enforcement side. But what I will share is three weeks ago I was part of the blockchain impact summit at the United Nations. And I was part of that financial inclusion working group. And in my group, we had former refugees, very interesting group. And one of the things that I brought up was digital identity and the potential around that.

So you know, if a refugee is in a place where there's an unstable government, well, starving in a place where there's an unstable government to the extent that they have some type of the device that can hook up to the internet, where they can have a digital identity, a digital wallet. They have assets in the fiat of that country. They can convert those assets into some type of crypto asset, held on their digital wallet, and they have an identity, there's value in knowing that if you have to leave some place-- these are things I think sometimes we take for granted here.

But if you have to leave that place and go somewhere else, no one can take that from you. You can also start over and people will know maybe you were a doctor in the place that you left. And now you can start your profession where you've gone. So I tend to think about that in terms of doing our best to not stifle innovation. There's also regulatory arbitrage that we need to worry about. But consumer protection is so critical. And the stories that were shared in the prior are, frankly, heartbreaking.

So I don't have the answers. I just know that striking that balance is a really, really tricky thing in this space.

SARAH JANE HUGHES: So I'm going to say something completely different. But I absolutely agree with Colleen first. And the thing I think that we need is better data. And if you went, and I did, the Consumer Financial Protection Bureau has a great complaint database that you can look at. But in this particular arena, it lumps remittance payments, wire transfers, and virtual currency problems into one category.

And the most recent search I did preparing for this panel showed-- this was last week-- approximately 6,800 complaints. But when you read them, many of them, the person being-- the entity, rather, being complained about was a bank. So that is harder when you get down to the more granular level and you look at what the complaint actually is about, it may or may not have anything to do with virtual currency, to the degree that agencies can keep better-- keep and then publish better data.

They can enable many of the people in this room and groups that are working to have a better idea of where these problems are actually arising, which will allow a lighter hand for the people who are registering and trying hard to comply with the law and provide a better flashlight being flashed on the persons who are not doing this in a way that is above board.

DUANE POZZA: Great. We're out of time. So thanks to our panel.

[APPLAUSE]

And now for closing remarks is Todd Kossow, the head of our Chicago office.

TODD KOSSOW: Thanks, Duane. And thanks to our last panel. So as Duane said, I'm Todd Kossow. And I'm the director of the Federal Trade Commission's Midwest region office here in Chicago. Well, it's certainly been an interesting afternoon. I want to thank all of you for joining us today, both in the room and on the webcast. And thank you, again, to all of our exceptional panelists and all three panels. We certainly covered a lot of ground this afternoon in a short period of time.

So we were very pleased to be able to start the workshop today with remarks from the FTC's new director of the Bureau of Consumer Protection, Andrew Smith. We're really glad that Andrew was able to come out from Washington to join us for this event. And as Andrew said earlier, we're here today to advance the conversation about understanding and effectively combating cryptocurrency scams. And I think our three panels today helped us do just that.

In the interest of getting you all on your way, I wanted to highlight just a few takeaways from today's workshop. As we heard from our first panel, the cryptocurrency landscape is rapidly changing. We're seeing an ever increasing number of cryptocurrencies, and an expansion in the way consumers can use, buy, and otherwise engage with these cryptocurrencies. Our first set of panelists talked about the technology's potential, but also about the perils consumers face from the often misleading and confusing information that they need to digest in this marketplace.

Our second set of panelists told us about the various frauds that we're seeing in the cryptocurrency marketplace. From cryptojacking to deceptive investment opportunities to sham ICOs, there's no shortage of ploys that consumers need to be aware of and look out for. In many ways, these are the same old scams that simply are taking advantage of new technology, with some added challenges thrown in. These scams can sometimes be difficult to detect and our panelists talked about how consumers can better spot them and protect themselves.

Our third panel helped us take stock of where we are and where we can go from here in terms of preventing cryptocurrency scams. Our friends from the CFTC and the SEC spoke about the complementary roles their agencies play alongside the FTC, state authorities and others in monitoring the cryptocurrency space. And we did learn about the Howie test this afternoon.

Coordination is important, and we're all committed to working together to advance an effective law enforcement approach. And in addition to robust enforcement strategies, as Sarah mentioned, consumer and business education in this area is essential. Providing practical advice to consumers attempting to navigate the cryptocurrency marketplace can help minimize the spread of scams.

So as Andrew said earlier, the FTC will remain an active enforcer of consumer protection laws as new technologies emerge or existing ones develop. And we'll pair that with timely consumer

education. Of course, for us to stay on top of how developments in technology are affecting consumers, it's critical for us to hear from them directly. If you or someone you know experiences a cryptocurrency scam, please file a complaint with the FTC at ftc.gov [INAUDIBLE].

Finally and importantly for all the lawyers in the room, particularly those who need to report their CLE in just a couple of days, I'll remind those of you who are seeking Illinois CLE to pick up your attendance certificate from the registration table. And also please grab an evaluation and fill it out and submit if for us there. For those listening via the webcast, you can contact us at midwestregion@ftc.gov, midwestregion@ftc.gov to receive your CLE certificate of attendance.

Again, I'd like to thank the terrific staff at the FTC who put together today's workshop. And a big thank you to DePaul University for hosting. Thank you all for coming.

[APPLAUSE]