FTC Decrypting Cryptocurrency Scams Workshop
June 25, 2018
Segment 2
Transcript

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]