Conference Title: NFAS001 | Digital Assets and Customer Protection: Answering Common Questions

Date: October 4, 2022

Joel Giamalva: Hello, everyone, and welcome to today's webinar hosted by NFA and the CFTC. It's just past the top of the hour, so I think we're going to get things started. My name is Joel Giamalva and I'm a Communications Associate at NFA, the self-regulatory organization for the US derivatives industry. I'm joined by Dan Rutherford, the Associate Director of the Office of Customer Education and Outreach at the CFTC, and Jorge Herrada, Director of the Office of Technology Innovation at the CFTC.

Before we dive into the main content of today's presentation, I know Dan has some housekeeping he'd like to address, so I'll hand over the reins to Dan.

Dan Rutherford: Thanks, Joel, and thanks to the NFA for having us today. We're really looking forward to the presentation and getting to answer some of these common questions for you. But before we get started, I have to read our common disclaimer and this disclaimer will apply to both Jorge and I. So let's dig in.

This presentation is provided for the general information and educational purposes only and does not provide legal or investment advice, guidance or interpretation to any individual or entity. The views presented herein are the speaker's own and do not necessarily reflect the views of the Commodity Futures Trading Commission or the commissioners. References to any products, services, or resources or the use of any entity, organization, trade, firm, or corporation name do not constitute or imply endorsement, recommendation, or favoring by the CFTC or the United States government. The CFTC does not guarantee the accuracy or completeness of any information contained in third-party resources or websites referenced herein.

Joel Giamalva: Thanks, Dan. As you may know, this week is World Investor Week. World Investor Week is a week-long global campaign promoted by IOSCO to raise awareness about the importance of

investor education and protection and highlight the various initiatives of regulators in these two critical areas. Ultimately, the week is designed to educate you, the investing public, on how to safely participate in these markets. Both NFA and the CFTC are members of IOSCO, and we both make investor education and protection a top priority.

Today is an opportunity for Dan, Jorge, and I to provide everyone with some crucial investor protection information about digital assets and customer protection. Throughout the presentation, Dan, Jorge, and I will be covering a variety of topics to help you understand more about digital assets. Dan will answer questions about the different types of fraud trends in the digital asset space, before Jorge answers questions about stablecoins, NFTs, and other topics. I'll explain the risks associated with investing in this marketplace and describe how investors can protect themselves from fraud.

Following our prepared remarks, we've allocated some time to answer any questions you might have. To ask a question, locate the box labeled Ask a Question on the left side of your webinar screen. Please type the question you would like to ask into the box and click the send button. Dan, Jorge, and I will get to these questions at the end of today's presentation.

We'll start with introductions from Dan and Jorge. Starting with Jorge, can you briefly describe your offices, and what you do as part of your position at the CFTC?

Jorge Herrada: Thank you, Joel. Thank you for the opportunity to present as part of World Investor Week. So I was recently appointed by Chair Behnam as the head of a new office, the Office of Technology Innovation. It's the successor to LabCFTC. In a few seconds, I'll tell you a little bit more about what that does. But just a personal note, I just recently returned from a one-year secondment at the Federal Reserve Board of Governors, where I contributed to the research on CBDCs. And then upon returning, I was promoted to Director of the Office of Technology Innovation.

And I would say that really, I try to summarize what the OTI does in a simple acronym ICE, I-C-E. That's the I stands for innovation. We're really focused on finding firms out there that are doing innovative work, whether it is work for maybe it's tracing crypto transactions or interesting data sets and bringing those tools in-house to help CFTC to innovate. Also on the C for the ICE is consulting and collaboration. We consult with commissioners and other divisions within the CFTC and collaborate with things like IOSCO and [inaudible] and other organizations outside of the CFTC.

And finally, the E for education. And that's really a big part of what we do. And that's why we're happy to be part of this today is to try to educate folks within CFTC about innovation, particularly around in the crypto sphere, and also to share that education with other government agencies and further outside of the government with the industry and market participants. So I'll hand that over to Dan.

Dan Rutherford: Thanks, Jorge. The Office of Customer Education and Outreach is sort of the customer education arm of the CFTC, if you will. So if Jorge is working with informing other government agencies and market participants, our role is specifically targeting most commonly individual retail traders, although we're happy to work with and engage with larger customers as well. And we're dedicated to helping customers protect themselves from fraud or violations of the Commodity Exchange Act. And that language really comes from sort of the founding language that created the Customer Protection Fund and the Dodd-Frank Act.

And so what we do is we develop evidence-based educational materials and initiatives, and we do public speaking events and conduct other forms of outreach, not only to talk to customers one-on-one but also other educators and organizations that can help extend and amplify our messages. We also work with other federal agencies through organizations like the Financial Literacy Education Commission and IOSCO. And basically, you can check out a lot of what we do by visiting the Learn and Protect section at cftc.gov. And if you want to reach out to us, the best way is to reach us by email at education@cftc.gov. Joel.

Joel Giamalva: Thanks to both of you for being here today. Dan, this year's World Investor Week key topics are investor resiliency, sustainable finance, frauds and scams, and digital assets. Dan, what would you like investors to know about some or all of these topics?

Dan Rutherford: Well, let's start a little bit with what World Investor Week is about. World Investor Week was started by the Committee on Retail Investors (Committee 8) of IOSCO, which is the International Organization of Securities Commissions. And it was started as a way to create awareness around investor education and customer protection issues. And so every year, they put out key topics for various members of IOSCO to talk about. And this year's key topics are, as you said, how to be a resilient investor, sustainable finance, and ESG investing, avoiding frauds and scams, and considering digital assets.

And when you think about sort of what all of that means or what sort of the educational aspects of all that really is about is just doing your homework. You could really just boil it down to that. We've started a new saying in our office. Make a plan, learn the markets, know the risks. And if investors just follow those steps, then they'll be better able to manage risk and avoid trouble. And when we talk about resilience, that basically equates to risk management. And managing risk requires some planning.

So when we talk about risk, the fundamental questions are how much risk can you afford? So it's determining your risk capital, how much money you can afford to trade and invest with, and not investing more than you can afford to lose. And this is especially important when you're trading on margin. Not only does leverage amplify your risk, but you could potentially lose more than your initial margin amounts. So you want to not only determine your overall risk capital amount but also consider your entry and exit points and how much loss you're willing and able to accept on each trade and investment you make.

Also when we talk about risk management do you have too many eggs in one basket? Are you thinking about longer-term savings needs as well as your hedging and speculating? And as events like Hurricane Ian remind us, there are also events that occur around us that could have significant impacts on our finances. And so ask yourself, are you adequately insured? Do you have an emergency fund? Those types of things so that situations don't throw you off track.

Having a plan also helps you weigh the pros and cons and make decisions rationally. In sort of a cooler state of mind, when you can sit down and think about what works, what won't work for you, and really, pour some thought into it. And it helps you avoid certain biases while you're trading or high pressure, emotionally charged tactics that fraudsters will sometimes use. So having a plan really is a good first step.

Being resilient also means doing your research and making sure you understand the risks. So there are weather risks, inflation risks, geopolitical risks. There are a lot of different factors that could impact markets. And you need to be familiar not only with what you're buying but also what could make that underlying asset increase or decrease in value.

And the same goes for ESG investments and digital assets. For ESG products, which are primarily securities, you want to ask yourself, are they really that sustainable? Are they really living up to that ESG label, or are they sort of greenwashing their product? And there you have to take a close look at the disclosure documents and at the same time, make sure that any ESG investment actually meets your overall savings and trading objectives.

When it comes to digital assets, do you know the risks associated with them, especially fraud risks? Remember, over-the-counter cash market trading platforms, where you can buy or sell digital assets for dollars are not supervised by regulators like other exchanges, banks or brokers. And that in and of itself increases a lot of risk. Your funds may be co-mingled with other traders. There may be undisclosed conflicts of interest. There's the threat of hacks and theft.

And if you're dealing with a website that is operating offshore and that is not registered as a money service business with FinCEN or your state regulator, it could just disappear one day with all your money or refuse to let you make withdrawals. And we see a lot of that. I'll cover some of the common frauds that we see here in a minute. So just, remember, make a plan, learn the markets, know the risks. Next question.

Joel Giamalva: Thanks, Dan. Talking about those current fraud trends, what are you seeing now?

Dan Rutherford: Well, overall fraud complaints are up and most of that increase is driven by complaints around digital asset fraud. It's important to note here that while the CFTC's regulatory oversight authority over commodity cash markets is extremely limited, the CFTC has asserted general anti-fraud manipulation enforcement authority over Bitcoin and other virtual currency commodities since 2014. And as a result of customer tips and complaints, the Commission has also brought a number of fraud and manipulation related enforcement actions against participants and companies in the digital asset markets.

OCEO also closely monitors that complaint data so we can identify fraud trends and anti-fraud or anti-fraud customer education priorities for us. And that said, what we've seen is that frauds and theft continue to be a major concern. Presently, the CFTC doesn't publicly release complaint statistics, but I can say generally that the total number of complaints we've received over the past five years or so have more than doubled. And the majority of those complaints by product type in 2022 were about digital assets.

And just to give you some sort of reference, some data from some other government agencies. In 2021, the Internet Crime Complaint Center, which is operated by the FBI, received more than 34,000 complaints and total money lost that was reported as lost increased by nearly 600% year-over-year from about 246 million in 2020 to 1.6 billion in 2021. The Federal Trade Commission has

logged more than 46,000 complaints between January 1st, 2021 and March 2022. And there are people claiming losses. Those loss numbers have exceeded more than $1 billion.

So keep in mind that some of these reports can overlap. People may report to more than one agency and fraud is commonly underreported overall. So the hard numbers themselves may severely undercount what's actually going on out there, but it gives you a good indication of the scale and scope that we're seeing in terms of sort of this general doubling of complaints. One private sector estimate out there is that about $14 billion worth of crypto asset-based crime. There was about $14 billion in crime globally in 2021. And that's up from just over almost $8 billion in 2020. So again, we're seeing more than doubling in terms of the amounts involved.

In terms of general trends, we don't see the big hacks like the Mt. Gox's occurring as much as we used to. Those are decreasing, but individual scams and thefts from individuals are way up. And scams by crime category, if you look at some of the industry information, tends to be the biggest area. So the fraudsters and the criminals are really targeting individuals out there. Next question.

Joel Giamalva: Okay. Dan, talking more about digital asset frauds. Can you describe what kind of digital asset related frauds you're seeing?

Dan Rutherford: Well, the complaints we see at the CFTC haven't really changed that much from last year. We still are seeing a tremendous amount of romance related scams and generally, just overall, most of the fraud that we see originates on social media. I don't want to name names, but the major platforms that are out there. Dating apps have seen a significant increase.

And we're also seeing a lot of so-called "wrong numbers" where people will just randomly send you a text message or send you a message via one of these apps, and they develop into a conversation that develops into a relationship, that develops into someone inviting you to trade on some platform

you've probably never heard of. And so romance scams continue to be a big thing, and not only here, but globally.

Fee frauds, if you're familiar with fee frauds, these tend to occur when again, you meet someone on social media, they convince you to come trade on this platform. The pitch might be give us $1,000, and in 30 days, we'll give you back $10,000. And so the people that fall for these schemes will hand over their money. They might be shown balance sheets, account balances that climb and climb and climb beyond their wildest expectations. So after 30 days when they want to get their money back, suddenly they're told they have to pay a tax or they have to pay a fee, or they have to pay a commission, or they have to upgrade to a higher-level status or something along those lines. There's always one fee. And then when they pay that fee, they have to pay another fee. Until ultimately, they just give up.

Another sort of common scam along that thread is just refusing to pay withdrawals. People will get – they might be teased into these platforms. They might invest a few hundred dollars and the customer service people might show them how to withdraw a low amount or a low dollar amount of a few dollars or $20 or what have you. And they think it's legitimate at that point. And so they pour more money into the plan. And then when they try to get their money back, they just – it's crickets or the site disappears altogether.

Fraudulent wallet apps. We've seen those quite a bit. A lot of times these come through phishing attacks. So you really have to be careful of phishing. And that's not only with fraudulent apps, but also with customer service messages, trouble with your account all those sorts of messages that you would expect to see in sort of a phishing type message. So you really have to be careful with returning emails and clicking on links or QR codes that are embedded in emails.

In terms of thefts, we see a lot of that occurring in the DeFi space, common rug pulls. But it's also because the technology is so new and novel. There are some known and many unknown

vulnerabilities that people are still taking advantage of. And so you have to be very careful with the – if you go that route, you have to be very cautious about has the software been security checked or has it been validated, and all of that? And maybe Jorge can maybe spend a little time when he's talking about that. But that's where we see a lot of common thefts and hacks are in the DeFi space.

Joel Giamalva: Okay. Thanks, Dan. Jorge, turning to you, and Dan just mentioned DeFi. If someone is considering investing in a DeFi project, what do they need to consider?

Jorge Herrada: Thank you, Joel. And again, I appreciate all of Dan's words and wisdom. And look, if I was going to put it in a word, I would use the word caution. When you're dealing with DeFi or decentralized finance, there are lots of risks. And Dan kind of covered some of that. I would also put a little plug-in for this that there is – at cftc.gov if you just Google digital assets, there's cftc.gov/digitalassets. You'll see a bunch of great consumer advisories that Dan and his team have put together.

Again, I like the fact that Dan talked about risk capital, understanding how much capital you have to invest. And I would simply say that if you can't afford to lose your investment, do not invest. I mean, there's recent experiences such as Celsius and Terra Luna should give investors pause and DeFi platforms do get hacked.

I mean, some that come to mind are like the Ronin hack of March of 2022, which is $615 million. Poly Network hack, August of 2021, $620 million. The Wormhole Attack, February 2022, $326 million. And the list goes on. And then, of course, there's this series of things called rug pulls where someone will hype a particular project and then once people have invested in, say, that DeFi project, then all of a sudden the project goes quiet and you can't get your funds back.

In May of 2022, according to the Rekt, R-E-K-T, Rekt database of cyber-attacks, DeFi protocols have lost 4.75 billion in total due to scams, hacks, and exploits. And of that 4.75 billion, only about

a billion has been returned, which maybe is better than you might think. But nonetheless, 4.75 billion is a rather large number and their database has reported a total of 2,782 attacks.

Another thing I would say, and again, there's some significant questions as to what is legal and what is not. And I can't really comment on some ongoing cases, but a simple Google search will show some cases that CFTC is bringing and some cases the FCC is bringing in the DeFi space. But it is, I mean, the question is, how do I invest in DeFi? And the answer is with caution, and certainly, with some question about whether you're getting involved with something that might be illegal and puts you at some risk.

And the other thing I would sort of add here is that I'm always struck by the fact that there's a lot of DeFi projects with really earnest people who are taking security and hacks seriously. And again, another word of caution about that. And yet you find these things being hacked. We just talked about the total hacks of 4.75 billion. And if the insiders who are really motivated to keep their project safe can't understand their vulnerabilities, I again, would suggest exercising caution. Because when you're looking at DeFi projects, if the insiders can't specifically understand all the risks associated with their platforms, it's hard for an outsider to understand all of it.

So for some more information, you may want to check out the US Department of Treasury's new publication came out in September of 2022, entitled Crypto Assets Implications for Consumers, Investors, and Business. And there's a section on risks and exposures for consumers, investors, and businesses. So that's certainly worth looking at.

And I would just sort of end by saying this. Most new projects fail and others could be out and out fraud. So take time to research and understand the projects, the technology, the use case demand, competing projects, governance. Who's behind the effort, the developers track record, how your money will be used, and when or if you can get it back? Dan mentioned sometimes it is difficult or impossible to get it back. Was the code audited by a reliable third party? Was security tested?

Closely review their white papers and other documents. If they don't make sense or don't exist, walk away.

So to summarize, I would say if you choose to invest in DeFi, do it with caution. Take to heart what Dan talked about with risk capital. In other words, understanding how much money you're willing to lose because you may lose all of it, and definitely do your research. So thank you for that question.

Joel Giamalva: Thank you, Jorge. And you just mentioned Terra. And recently, the Terra stablecoin collapsed. Can you describe stablecoins and walk us through what happened and what are the lessons we can take away from this?

Jorge Herrada: Yeah, great question. And yeah, Terra Luna is a great object lesson of what we were just talking about in the previous slide. But let's start by stepping back for a second and talk about the four major types of stablecoins. There are fiat-backed, asset-backed, crypto-backed generally over-collateralized, and algorithmic stablecoins.

So the fiat-backed ones are ones where they're, say, representing US dollars and US dollars or cash-like instruments are stored to back those stablecoins. Asset-backed are more things like gold or other commodities like that that when you have a stablecoin that indicates that it's for one ounce of gold, ideally that stablecoin would be asset-backed 100% with the underlying asset.

Crypto-backed, that's tokens like something like DAI, which are generally over-collateralized. So, for example, if you want to say $100 worth of DAI stablecoin, you might deposit $150 worth of Ether. And so as ether fluctuates up and down, the fact that it's over-collateralized will allow you to sort of to back that stablecoin. And then ultimately, Terra Luna was an algorithmic stablecoin and it was supported by its sister coin, Luna.

So let's dig deeper a little bit. I should mention, though, before I go too far, that I was looking at the numbers recently and we saw that 92% of the stablecoins are fiat-backed, and then the asset-backed stablecoins make up about 6% of the market. So algorithmic stablecoins only represent a small part of the market. I think it was in one point some or 2% of the market. But if you have all your eggs in that basket, say the Terra Luna, that could be catastrophic. And in fact, with the Terra Luna, a lot of people, because of the interest that it provided, some people had put significant funds in there.

So on May 7th, Terra had a market value of about 18 billion. By May 9th, it had dropped considerably. And I think the view is now it's about as close to zero as you can get. So Terra was – that was in May 9th of 2022. It was launched in February of 2020. And again, unlike stablecoins that we just talked about that are backed by fiat, Terra Luna was backed by its sister token, Luna. Sorry, Terra is the stablecoin. Luna was the sister token. And it relied on this sort of algorithm to buy or sell Terra or Luna, users would purchase one and burn the other.

For example, in the good old days, in the good old days when Luna had some value, let's say, Luna was selling for $25, to mint the Terra users would buy the Luna, and then they would burn an equivalent amount of Luna to get the Terra. So for example, if you wanted 100 Terra, which is a stablecoin with Luna, let's say at $25, you would have to burn four Luna tokens to get your Terra. On the other hand, if you wanted to get Luna from the Terra, you would take the Terra and burn that to get the Luna.

But the idea behind that was that the arbitrageurs would keep market forces, would keep them stable. So if the value of Terra is below $1, then users and arbitrageurs could burn Terra to get one dollar's worth of Luna. And when the value of the Terra is above $1, then you can go ahead and burn $1 worth of Luna to get the Terra. Anyway.

So it's basically, the two were meant to be used together and Luna would fluctuate in value. Terra was not supposed to fluctuate in value, and Luna was some sort of shock absorber. And so there was an anchor protocol that was launched in June of 2020. In essence, it was offering about a 20% return on Terra. And wow, imagine being able to receive 20% interest on your money when interest rates were near zero. I certainly know that in my bank account, I was getting less than 0%. I'm sorry, like 0.2%. So less than 1%. And if you could reliably get 20% interest, I can understand why people were attracted to this and it worked great until it didn't.

But what happened was once there was some sort of question and people started questioning the value of Terra. Terra and Luna fell into a death spiral. And as Terra's price dropped in confidence, the entire project dropped as well. So Luna ended up being minted. More and more Luna was created because, again, Luna value could – like let's say Luna falls to $0.10, then to make a dollar, you'd have to burn ten Luna to make one Terra. So Luna value rapidly depreciated as the arbitrageur scooped up Terra, burnt it, and minted Luna, then dumped the Luna on the market. The supply of Luna went from 340 million to 176 billion by May 12th.

So what were the lessons learned? I know that was a mouthful, but be very cautious with algorithmic stablecoins. If we've learned anything, the algorithmic stablecoins are not nearly as stable as something like a fiat-backed stablecoin. If something sounds too good to be true, this is something that Dan likes to say. If something sounds too good to be true, it probably is too good to be true. 18% to 20% interest during a time of low interest should give you pause.

And many people seeking returns lost a great deal of money investing in Terra Luna. There's certainly lots of cases where people took mortgages out on their house, or borrowed significant amounts of money to invest in Terra and Luna using it through say, the anchor protocol, and were really counting on that. And in the end, instead of getting a 20% return on investment, they ended up losing everything they had.

So yeah, thank you again for that question. Hopefully, I didn't bore too many people with that long-winded answer. So back to you, Joel.

Joel Giamalva: Thanks, Jorge. So another interesting trend from the last few years are NFTs. Has this trend come and gone and how can one protect themselves when purchasing NFTs? And are there any use cases other than colorful JPEGs?

Jorge Herrada: Yeah, these are great questions, Joel. Well, on the question of whether they've come or gone, of course, we don't know. But what we can say is that the market interest in NFTs has declined, according to DappRadar. They said the third quarter of 2022 saw – again, third quarter of 2022 saw 3.4 billion in sales. That was down from 8.4 billion the previous quarter and down from 12.5 billion at the market's peak in the first quarter of the year.

So clearly, we're seeing a drop. And of course, you've heard many cases where individuals have bought NFTs for X number of millions of dollars, and they found that they can't sell them for very much once they go out there. So it is a challenge to protect yourself when buying NFTs. And here's some recent stories. And I pulled some of these stories from a website that I know we're not to plug anything, but anyways, I would say there's an interesting website called web3isgoinggreat. com and it does chronicle a lot of the different scams and rug pulls out there. So it's certainly worth looking at because it's one place where you can see a lot of this activity in one location.

So just looking back in just this month alone, September 25th there's a guy named Jason Falovitch who had four of his NFTs stolen that were valued at about $150,000, but he spent $377,000. And he tweeted shortly after that, he says, boy, he's been hacked by over $1 million hacking ETH and NFTs. So September 18th, the scammer would earn 13 ETH, about $17,500 from a fake mutant ape scheme. Mutant ape is one of the most popular NFTs out there.

The owner of a legitimate mutant ape was approached with an offer to trade their ape for another mutant ape. And with a sweetener of 0.5 ETH and the trader agreed, moved forward with performing the trade on Sudoswap, one of the platforms that allows for NFT-to-NFT trades. But unfortunately, didn't check the mutant ape that he was buying was actually not the genuine article. So they ended up losing out on a somewhat valuable ape.

So let's see here. So there again, there's a long, long list. You might think to yourself, well, gee, what about using a reputable source like OpenSea? And again, that's one of the better-known ones out there. But there are some issues there. Like there's a stale listing issue that even in August of 2022, they've solved a lot of their issues. But again, there were some cases where somebody had purchased a NFT and it was out there, and due to this issue with stale listings. It ended up getting sold from underneath them at some very low price.

So there are other little scams to be aware of. One of them is wallet drainers. That's where when you connect your wallet to the NFTs, it is possible to have the funds pulled out if you have auto-approved turned on. And there's, of course, rug pulls, OTC scams, and so on. So if you can't resist buying an NFT, do your homework. There are some really great articles out there on how to safely invest in NFTs, so you may want to check that out.

And one last thing, positive use cases. I've seen some pretty interesting things on NFTs for carbon credits. So I think that's pretty fascinating where you can get, say, a carbon credit that references a specific acre of, say, forest in the Amazon or something that Vitalik Buterin talks a lot about Soulbound tokens. With a Soulbound token, it's something that is specific to a given individual. And so an example of that would be an academic credential and possibly ticketing for concerts. So those are some ideas here of some NFTs that do have some potential value.

Joel Giamalva: Okay, Jorge. Recently, the Ethereum network upgraded from proof of work to proof of stake. Can you briefly explain proof of stake and its benefits and risks?

Jorge Herrada: Sure. So as many people listening probably are aware, Ethereum went through a major upgrade where they went from proof of work to proof of stake. And some have likened it to switching from an internal combustion engine to an electric motor while driving down the road at 100mph. It was pretty impressive. I stayed up till late into the evening to watch the launch party with about 41,000 other people, where we watched it go live. But the idea of proof of stake is for people that are validators, that you basically you take a certain amount of ETH. In this case, I'm talking about specifically Ethereum. But obviously, there are other proof of stake networks out there.

And so you deposit a certain amount of ETH. And by doing so, you're basically saying that I am available to validate blocks on the network. And if I act maliciously, in other words, if I vote on blocks that aren't legitimate, then the network can take some of my funds away. So basically, you're proving you're acting honestly because you're taking the risk that if you act dishonestly, people will notice that and they'll take your funds away.

And also with proof of stake, if you fail to vote when you're supposed to, there's also a slashing condition where some of your stake will be taken away. And then that's because two-thirds of the validators have to vote that a block is legit for that block to be added to the blockchain. And so they don't want people standing on the sidelines not voting and blocks then not being added.

So what are the major benefits? Well, one of the biggest benefits is sustainability. I mean, it reduced the energy consumption by a factor of 1000. So before this change, they said that Ethereum was using the amount of electricity that you might utilize for the entire country of Switzerland. So all of a sudden, that was all pretty much turned off. I mean, some of the mining rigs moved to some other Ethereum variants, but for the most part, the vast majority of that mining went away because it was no longer economically viable.

The merge really preps Ethereum for reduced transaction fees and increased throughput. So in other words, they did have to make this one change to be prepared to do the other changes such as sharding. And the proponents of this change also say that it's less vulnerable to 51% attacks, and a bonus was that the ETH supply is now stabilizing instead of increasing. In the past, it would go up by 4.5%.

So quickly running through the risks. It is high stakes. Making a major change like this has potential implications. Things could go wrong. Something that they did not consider could still happen. And there's a lot of things like DeFi that are built on top. So there could be issues if a problem comes out. There are some in the Ethereum community that worry that Ethereum could become more centralized via staking pools. And so those are the two major risks that are associated with it. So back to you, Joel.

Joel Giamalva: Thanks, Jorge. Last question for both of you. Has the CFTC released any new materials, or do you have any programs coming up that today's listeners may want to know about?

Dan Rutherford: Thanks, Jorge. I'll start off and then let Jorge jump in. So tomorrow actually starting at noon Eastern, we're going to be presenting a couple of our own panel discussions. My panel will take a look at trends in high-risk trading and discuss how financial educators can use risk education to help investors, especially new investors spot frauds and avoid problems. Jorge, do you want to talk about your panel?

Jorge Herrada: Sure. So we have a panel tomorrow. It's actually going to be worth diving into. I'll highlight that one of our special guests in the panel is actually going to be somebody from the IRS. So if you've ever wondered about tax treatment associated with crypto, that's certainly worth diving into. We, of course, have somebody from the SEC and we have others. So we have that coming up. And we're also looking forward in the future of trying to put together an event, a conference, and

so keep your eyes out for that. But again, that is something that we're considering and it's coming up. So again, back to you, Joel.

Dan Rutherford: I just have a few more things. So Joel, we have AARP Tele town hall on Thursday for folks in Massachusetts. So if you're in AARP and live in Massachusetts, you might want to tune in to that. And then we also released three new flyers in honor or in recognition of World Investor Week. The first is called Curious About Crypto? Watch Out For Red Flags. And then we have a second one called 14 Digital Asset Risks to Remember, where we briefly outline a number of the risks, some of which we talked about today. And then 10 Digital Asset Terms You Should Know. So again, some basic just key terms to help people familiarize and understand some of the content. And you can see some of our latest advisories and articles again in the Learn and Protect section of cftc.gov.

So I guess now it's my turn to ask Joel some questions. Joel, what are some of the risks associated with virtual currency?

Joel Giamalva: Yeah. Thanks, Dan. Great question. To start with, cryptocurrency is a form of currency that only exists digitally and usually has no central issuing or regulating authority. Instead, cryptocurrency uses a decentralized system to record transactions and manage the issuance of new units. This makes it nearly impossible to counterfeit or double-spend cryptocurrency. Cryptocurrency can be used to buy regular goods and services, although many people invest in cryptocurrencies as they would in other instruments like stocks or futures.

The lack of centralized authority regulating cryptocurrency is one risk to be aware of. While, for example, the American dollar is issued and controlled by the Federal Reserve, cryptocurrency has no such backing. Cryptocurrency is not issued by a central bank or government authority, which means its value, is largely dependent on supply and demand for it, and it is immune to government controls or inflation.

Investors may perceive this lack of regulation as a benefit, but it carries several significant risks, which investors should know before getting involved with cryptocurrency. And price volatility is one of those risks with cryptocurrency. The value of crypto can fluctuate rapidly, gaining or losing massive value in short time. This can be financially devastating for investors. The massive gains of some cryptocurrencies can be alluring, but investors should be aware of the volatility of their potential investments beforehand. Investors should be very cautious and monitor any investments they make.

And one more risk is the very limited oversight on the cryptocurrency market currently. With the rise of cryptocurrency occurring in just a short time, many countries are still deciding how to enforce regulations on this new marketplace. Without the authority to enforce oversight at this time, fraud and scams have grown tenfold, with criminals taking advantage of investors entering the marketplace. And I'll push it back to you, Dan.

Dan Rutherford: Great. What are some common signs of fraud? And can you describe how to protect against different fraud techniques?

Joel Giamalva: Yeah. Thanks, Dan. So when receiving an email or any form of communication, investors should always look out for telltale signs of phishing, common scam used to steal sensitive information. Before clicking any links or giving any information, investors should verify the sender and the email address before responding or clicking any links. Investors should be very suspicious of any attachments from senders they do not recognize. These attachments can download viruses, which steal sensitive information and damage computer hardware.

Investors can also be tipped off to suspicious activity by the contents of the communication itself. Generic greetings from unknown senders and poor grammar can be signs of phishing from foreign countries. Investors should always take precautions when dealing with correspondence, and it's

not wrong to have a healthy dose of skepticism, especially when their data and personal information are at stake.

And here are just a few important things to always keep in mind when it comes to protecting yourself. First, always ask for written materials. Legitimate firms looking to conduct a legitimate business will never have a problem providing written information. Second, beware of get-rich-quick schemes. If it sounds too good to be true, it probably is like Dan said before. Be particularly vigilant if you have recently retired or came into money and are looking for safe investments. It's also crucial that you always stay alert when you're online.

Today, you can receive investment pitches and other communications through social media posts and texts. It's not just via the cold call or flyer in the mail. It's best to avoid these communications or to have a solid plan for refusing these offers, especially when it comes to cold calls and other unsolicited communications. You do not have to be polite. Simply hanging up the phone, deleting a text or email, or blocking a social media account are solid steps towards protecting yourself.

As a final tip, be wary of fake websites, which have been created to appear identical to official business websites or use similar names to deceive investors into sharing sensitive information and financial resources. Before giving any information, verify websites are owned and operated by the firms.

NFA also has an arbitration program that is available to investors who need assistance solving disputes. The program is designed for disputes between customers and NFA members, their employees, and associates. Customers should consider filing a claim if they believe they've lost money because of unfair or improper treatment by an NFA member. Also, if you have any questions on investor education and protection, you can always reach out to NFA's Information Center at the contact information seen on the screen. Back to you, Dan.

Dan Rutherford: Thanks, Joel. Where can more investor resources be found?

Joel Giamalva: Yeah. On the NFA side, NFA has an investor-specific web page that has our latest investor newsletters, information on best practices for investors who are just getting started with investing, FAQs, more information on arbitration services, and an archive of investor education materials and resources, and webinars just like this one. You can also subscribe to the CFTC's Investor Alerts and NFA's Investor Newsletter to stay up to date on the latest information, including warnings about fraud and news about upcoming webinars and other educational events for investors.

And before we turn to your questions, Dan will speak one more time to pass along more information about investor education, resources, and materials.

Dan Rutherford: Yeah. So I don't need to go over these. I think most of these we've already talked about. I think we'll leave them up on the screen for a few minutes. And if you want to grab a screengrab, it'd probably be the easiest thing to do to remember the links. Again, these are some of the new flyers that we recently published, along with the report that Jorge mentioned from Treasury, the digital assets resources that he mentioned earlier on, and also a copy of the President's Working Group on stablecoins.

Both of the reports from Treasury, also provide a lot of good information about sort of what the current state of the markets are, the environment is in this digital asset space and offers a lot of information in terms of terminology and other things. So if this is a space that you're interested in, then those are both pretty valuable reads.

Joel Giamalva: Great. Yeah. We'll leave that on screen for anyone watching and we'll move into the Q&A section. So we've got a question here. Both of you can jump in if you feel like you can answer it. The question is, I've purchased cryptocurrencies through an exchange. I often get phishing emails

that mimic the exchange. I've tried to let the exchange know with the expectation that they do something about this, but they don't seem interested. Shouldn't they be?

Dan Rutherford: Oh, well, I could take a crack. I mean, certainly, they should be, and a lot of times the way that some platforms, and again, I'm sort of thinking about all of the similar experiences that I've had with my bank, with PayPal, with my investment accounts, etc., you name it. And you have a brand where you have an account, and you'll likely get – you might be phished over it. A lot of times, the companies will respond by putting out their own anti-fraud alerts or information about these sorts of phishing schemes. They're hard to combat because you don't really know who's behind them.

But yeah, I mean, that might be something you can think about if the exchange isn't taking their security or customer protection seriously. You might want to explore and look around and see what others do and make your own judgments.

Joel Giamalva: Okay. Great. Next question here. Should the crypto holdings of those in the C-suite of a crypto exchange or lending platform be treated like SEC disclosure rules, where they need to report holdings and disclose purchases or sales of their crypto within certain time periods?

Dan Rutherford: That sounds more like a policy question that I don't feel qualified to sort of explore. Jorge, any thoughts?

Jorge Herrada: Yeah, that's a good question because it is – you're right. It is much more of a policy question. And yeah, it would be difficult to comment on it. But I think that one thing that the CFTC has certainly said is that we have a regulatory regime. And to the extent that these products fit within that regulatory regime, I think the message that I see often is if it's the same activity, it's the same rules. So I think the questioner is probably onto something. But again, when it comes to policy, it's something that's best to leave more senior people to comment on. But thank you for that question.

Joel Giamalva: Great. It seems like we have one more question here. If anyone else would like to submit questions, do so now, and we'll be sure to answer it before the end of our presentation. But I'll ask the question now. It goes, how are crypto prices on exchanges created, and how do I know I'm getting a good execution?

Jorge Herrada: Yeah. This is Jorge. That's a great question. Because, well, how are prices created on exchanges? There really are – the way I see it, there's kind of two major types of exchanges. There's sort of the centralized order book exchanges that are out there. You're sort of your Coinbase's and Gemini's and Kraken's and others where prices are a meeting of supply and demand. And obviously, if a price on one particular exchange is out of whack with another exchange, then people will tend to move their crypto back and forth between different exchanges to take advantage of sort of arbitrage opportunities when prices are sort of out of whack.

I would say, obviously, you're best-off sticking with sort of firms or exchanges that do take regulation seriously. But there's also in the DeFi space, there's these decentralized exchanges sometimes referred to as DEXs. And many of them use these non-order book approaches, which are automated market maker or AMM ones. And that is using more of a formula to set the prices there.

So the answer to the question is sort of a little complicated. The answer is the prices are going to vary between these decentralized exchanges and different crypto exchanges. But for the most part, the hope is that with arbitrage with people looking for discrepancies in prices, then these different traders that are looking for those discrepancies. Those price discrepancies will tend to disappear, as there is fluidity in the market between these different exchanges, whether decentralized or centralized exchanges.

Joel Giamalva: Great. Thanks, Jorge. And we got another question here. It asks, how can we listen to tomorrow's panel about IRS's tax treatment for crypto?

Dan Rutherford: I can take that one. That's a good one. So the easiest way would be to go to the cftc.gov website and hover over the News and Events tab. You'll see a drop-down that comes up. One of the selection options will be events. Click on events and then you'll look for the October 5th date in the table and there will be a registration link involved with or included with the event description. So you can click on that, click through to that, and you should be able to find it.

Also, you can probably find a registration link on our social media channels. So we're on Twitter, Facebook, and LinkedIn. So if you search for CFTC on those platforms, you should be able to find links to registration or links to register for tomorrow's event. Thanks.

Jorge Herrada: And I would add one more thing to it. And I appreciate the mechanics on that. I'll give you a little teaser on that. One of the questions that might come up and that you might think about is, and again, the whole focus of the panel tomorrow is not on just the IRS. IRS is just one of the people participating in the panel. I myself will be participating in the panel. But there is a question that you might be thinking about, which is what was the taxable implication of the merge?

When the merge occurred, there was a second token that was sort of spun up out in a way, an airdrop, which was the ETH Powell token that occurred at the time of the fork. So then the question is, what is the tax implications of the merge? And hopefully, we will get an answer to that question. So I would say, tune in for that exciting answer directly from the IRS tomorrow. So we'll leave it at that.

Joel Giamalva: Okay. Well, thanks to both of you. And seeing that we're almost at the top of the hour and that there are no more questions, that's going to do it for today's webinar. And before we sign off today, I want to remind everybody that you'll be able to access the transcript and a recording of today's webinar on NFA's website in the coming weeks, and you can reference that at any time if

you want to go over what we've covered today. So from me, thank you again for joining and I hope you learned something new in joining the webinar. Thank you and have a great day.